Cryptographie Paris 13

(version 2008/2009)

Daniel Barsky

15 septembre 2008

Résumé

Le but de ce cours est une introduction à la cryptographie moderne utilisée dans la transmission et le stockage sécurisé de données. L'accent mis sur les principes et les outils mathématiques utilisés (arithmétique, algèbre, algorithmique, complexité, probabilité, théorie de l'information,..), ainsi que sur les protocoles.

Les problèmes informatiques, les produits et les normes sont décrits dans des cours plus appliqués (réseaux, sécurité réseaux,...)

Table des Matières

Chapitre 1

Introduction et terminologie.

L'objectif fondamental de la cryptographie est de permettre à deux personnes appelées traditionnellement, ***Alice*** et ***Bob*** de communiquer à travers un canal peu sûr de telle sorte qu'un opposant passif ***Éve*** ne puisse pas comprendre ce qui est échangé et que les données échangées ne puissent pas être modifiées ou manipulées par un opposant actif ***Martin***.

Après un rapide historique de la cryptographie on examinera les principaux systèmes cryptographiques modernes utilisés pour la transmission et le stockage sécurisé de données.
On ne s'intéresse qu'aux systèmes crypographiques destinés à transmettre des flux importants et variés d'informations (paiement sécurisé par internet, données bancaires, cartes de crédit, protection des conversations entre téléphones mobile, WiFi,...) entre de nombreux interlocuteurs qui nécessitent des systèmes cryptographiques structurés et rapides.
On ne décrira pas de systèmes cryptographiques reposant sur la dissimulation de l'information secrète au sein d'un document, d'une image (***stéganographie***,...). Par contre on s'intéressera à la stéganographie quand elle est utilisée pout le marquage de document ***watermarking*** ou ***tatouage***. Le tatouage permet de protéger les possesseurs de copyright sur des documents numériques en cachant une signature dans l'information de sorte que même une partie modifiée du document conserve la signature et de découvrir l'origine de fuites en marquant de façon cachée et unique chaque copie d'un document confidentiel.

Un système cryptographique ne se conçoit pas indépendamment des attaques dont il peut être l'objet. On indiquera donc pour chaque système cryptographique quelques attaques et sa résistance à ces attaques.
L'accent sera mis sur les principes et les outils mathématiques utilisés (arithmétique, algèbre, algorithmique, complexité, probabilité, théorie de l'infor-

mation,..). Quelques protocoles seront décrits.

On évoquera rapidement les systèmes d'infrastructure pour les Systèmes à Clef Publique (Public Key Infrastructures ou PKI) et les systèmes de Management des Clefs Secrètes (Symmetric Keys Management). On évoquera aussi quelques grands types de menaces et d'attaques sur les systèmes cryptographiques.

Les problèmes de mise en oeuvre informatique, les produits et les normes sont décrits dans des cours plus appliqués (réseaux, sécurité réseaux,...).

On emploiera indifféremment les mots cryptographie, chiffrement et codage.

Les mots en gras figurent dans l'index à la fin du volume avec un renvoi à leur définition.

Ce cours s'est beaucoup inspiré des cours de François Arnaux, [2], Jean-Louis Pons, [21], et Guy Robin, [24], des livres de Douglas Stinson, [31], Neal Koblitz, [18], John Daemen et Vincent Rijmen, [8], Serge Vaudenay, [32], Lawrence Washington, [33], Benne de Weger, [34] et Gilles Zémor [37], des deux tomes de l'ouvrage collectif édité par Touradj Ebrahimi, Franck Leprévost, Bertrand Warusfel, [11], [12] et d'articles de WIKIPEDIA ainsi que de l'ouvrage de Simon Singh, [29], pour la partie historique.

1.1 Qu'est ce que la cryptographie.

La cryptographie ou science du secret est un art très ancien, c'est

l'art de remplacer un secret encombrant par un secret miniature

Le secret encombrant est le contenu du message il est remplacé par un petit secret qui est la clef de déchiffrement dont la taille est en en gégéral de quelques centaines à quelques milliers de bits à comparer aux mégabits d'un message.

La ***cryptographie*** est l'art de rendre inintelligible, de crypter, de coder, un message pour ceux qui ne sont pas habilités à en prendre connaissance. Le chiffre, le code est le procédé, l'algorithme, la fonction, qui permet de crypter un message.

La ***cryptanalyse*** est l'art pour une personne non habilitée, de décrypter, de décoder, de déchiffrer, un message. C'est donc l'ensemble des procédés d'attaque d'un système cryptographique.

La ***cryptologie*** est l'ensemble formé de la cryptographie et de la cryptanalyse.

La cryptologie fait partie d'un ensemble de théories et de techniques liées à la transmission de l'information (théorie des ondes électro-magnétiques, théorie du signal, théorie des codes correcteur d'erreurs, théorie de l'information, théorie de la complexité,...).

Un expéditeur ***Alice*** veut envoyer un message à un destinataire ***Bob*** en évitant les oreilles indiscrète d'***Ève***, et les attaques malveillantes de ***Martin***.

Pour cela Alice se met d'accord avec Bob sur le cryptosystème qu'ils vont utiliser. Ce choix n'a pas besoin d'être secret en vertu du principe de Kerckhoffs, cf. section 1.2.

L'information qu'Alice souhaite transmettre à Bob est le ***texte clair***. Le processus de transformation d'un message, M, pour qu'il devienne incompréhensible à Ève est appelé le ***chiffrement*** ou la ***codage***. On génère ainsi un ***message chiffré***, C, obtenu grâce à une ***fonction de chiffrement***, E, par $C = E(M)$.

Le processus de reconstruction du message clair à partir du message chiffré est appelé le ***déchiffrement*** ou ***décodage*** et utilise une ***fonction de déchiffrement***, D. On demande que pour tout message clair M

$$D(C) = D(E(M) = M$$

Autrement dit on demande que tout message codé provienne d'un et d'un seul message clair (D est une fonction injective des messages codés vers les messages clairs et E est une fonction surjective des messages clairs sur les messages codés).

Un ***algorithme cryptographique*** est l'ensemble des fonctions (mathématiques ou non) utilisées pour le chiffrement et le déchiffrement. En pratique les fonctions E et D sont paramétrées par des ***clés***, K_e la ***clé de chiffrement*** et K_d la ***clef de déchiffrement***, qui peuvent prendre l'une des valeurs d'un ensemble appelé ***espace des clefs***. On a donc la relation suivante

$$\begin{cases} E_{K_e}(M) = C \\ D_{K_d}(C) = M \end{cases}$$

Le type de relation qui unit les clés K_e et K_d permet de définir deux grandes catégories de systèmes cryptographiques

- Les systèmes à ***clef secrètes*** ou ***symétriques***: (DES, AES, IDEA, Blowfish,...)
- Les systèmes à ***clefs publiques*** ou ***asymétriques***: (RSA, El-Gamal, un cryptosystème elliptique,...)

En outre les fonctions de codage E et de décodage D peuvent fonctionner de deux façons

- ***en continu***: chaque nouveau bit est manipulé directement
- ***par bloc***: chaque message est d'abord partionné en blocs de longueur fixe. Les fonctions de chiffrement et déchiffrement agissent alors sur chaque bloc.

Chacun de ces systèmes dépend d'un ou deux paramètres de taille assez réduite (128 à 2048 bits) appelés la clef de chiffrement et la clé de déchiffrement. Les clefs de chiffrement et de déchiffrement n'ont aucune raison d'être identiques. Seule la clef de déchiffrement doit impérativement être secrète.

1.2 Principes de Kerckhoffs.

En 1883 dans un article paru dans le Journal des sciences militaires, [17], Auguste Kerckhoffs (1835-1903) posa les principes de la cryptographie moderne. Ces principes et en particulier le second stipulent entre autre que la sécurité d'un cryptosystème ne doit pas reposer sur le secret de l'algorithme de codage mais qu'elle doit uniquement reposer sur la clef secrète du cryptosystème qui est un paramètre facile à changer, de taille réduite (actuellement de 64 à 2048 bits suivant le type de code et la sécurité demandée) et donc assez facile à transmettre secrètement.

Ce principe a été très exactement respecté pour le choix du dernier standard de chiffrement, l'algorithme symétrique AES, par le NIST. Ce dernier a été choisi à la suite d'un appel d'offre international et tous les détails de conception sont publics. Ce principe n'est que la transposition des remarques de bon sens suivantes:

- Un cryptosystème sera d'autant plus résistant et sûr qu'il aura été conçu, choisi et implémenté avec la plus grande transparence et soumis ainsi à l'analyse de l'ensemble de la communauté cryptographique.

- Si un algorithme est supposé être secret, il se trouvera toujours quelqu'un soit pour vendre l'algorithme, soit pour le percer à jour, soit pour en découvrir une faiblesse ignorée de ses concepteurs. À ce moment là c'est tout le cryptosystème qui est à changer et pas seulement la clé.

Les systèmes conçus dans le secret révèlent souvent rapidement des défauts de sécurité qui n'avaient pas été envisagés par les concepteurs.

1.3 Qualités d'un cryptosystème.

Les qualités demandées à un système cryptographique sont résumées par les mots clefs suivants:

- ***Confidentialité***: seules les personnes habilitées ont accès au contenu du message.
- ***Intégrité des données***: le message ne peut pas être falsifié sans qu'on s'en aperçoive.
- ***Authentification***:
  - l'émetteur est sûr de l'identité du destinataire c'est à dire que seul le destinataire pourra prendre connaissance du message car il est le seul à disposer de la clef de déchiffrement.
  - , le receveur est sûr de l'identité de l'émetteur grâce à une ***signature***
- ***Non-répudiation*** qui se décompose en trois:
  - ***non-répudiation d'origine*** l'émetteur ne peut nier avoir écrit le message et il peut prouver qu'il ne l'a pas fait si c'est effectivement le cas.
  - ***non-répudiation de réception*** le receveur ne peut nier avoir reçu le message et il peut prouver qu'il ne l'a pas reu si c'est effectivement le cas.
  - ***non-répudiation de transmission*** l'émetteur du message ne peut nier avoir envoyé le message et il peut prouver qu'il ne l'a pas fait si c'est effectivement le cas.

On peut regarder ces quatre qualités du point de vue de l'émetteur. Alice veut être certaine

- qu'une personne non-autorisée (Ève) ne peut pas prendre connaissance des messages qu'elle envoie, ***confidentialité***.
- que ses messages ne seront pas falsifiés par un attaquant malveillant (Martin), ***intégrité***.
- que le destinataire (Bob) a bien pris connaissance de ses messages et ne pourra pas nier l'avoir reçu, ***non-répudiation***.

de plus elle veut être certaine que son message ne sera pas brouillé par les imperfections du canal de transmission (cette exigence ne relève pas du cryptage mais de la correction d'erreur).

Bob veut être certain

- que personne d'autre que lui (et Alice bien sûr) n'a accès au contenu du message, ***confidentialité***.
- que le message reçu vient bien d'Alice ***authentification***, par exemple qu'un attaquant malveillant (Oscar) ne puisse pas se faire passer pour Alice, ***mascarade*** ou ***usurpation d'identité***
- que le message n'a pas été falsifié par un attaquant malveillant (Martin), ***intégrité des données***
- que l'expéditeur (Alice) ne pourra pas nier avoir envoyé le message, ***non-répudiation***

1.4 Attaques sur un chiffrement.

La ***cryptanalyse*** est l'ensembles des procédés d'attaque d'un cryptosystème. Elle est indispensable pour l'étude de la sécurité des procédés de chiffrement utilisés en cryptographie. Son but ultime est de trouver un algorithme de déchiffrement des messages. Le plus souvent on essaye de reconstituer la clef secrète de déchiffrement.

On suppose, en vertu des principes de Kerckhoffs, pour toutes les évaluations de sécurité d'un cryptosystème que l'attaquant connait le système cryptographique utilisé, la seule partie secrète du cryptosystème est la clef.

Par exemple dans un cryptosystème basé sur des régistres à décalage on suppose que l'attaquant connait la forme des récurrences linéaires ainsi que la fonction de combinaison mais pas les conditions intiales des récurrences qui constituent la clef du code.

On doit distinguer entre les ***types d'attaques*** d'un adversaires et les ***buts des attaques*** d'un adversaire.
Les principaux types d'attaques:

- ***attaque à texte chiffré connu***: l'opposant ne connait que le message chiffré y.
- ***attaque à texte clair connu***: l'opposant dispose d'un texte clair x et du message chiffré correspondant y
- ***attaque à texte clair choisi***: l'opposant a accès à une machine chiffrante. Il peut choisir un texte clair et obtenir le texte chiffré correspondant y, mais il ne connait pas la clef de chiffrement.
- ***attaque à texte chiffré choisi***: l'opposant a accès à une machine déchiffrante. Il peut choisir un texte chiffré, y et obtenir le texte clair correspondant x, mais il ne connait pas la clef de déchiffrement.

En plus de ces attaques basées sur une étude de messages codés, il y a aussi des ***attaques physiques***. Le principe de ces attaques est d'essayer de reconstituer la clef secrète par exemple en espionnant la transmission entre le clavier de l'ordinateur et l'unité centrale ou en mesurant la consommation électrique du microprocesseur qui effectue le décodage du message ou encore en mesurant son échauffement. Ensuite on essaye de remonter de ces données physiques aux clefs de codage et décodage.

Une méthode pour résister à ce type d'attaque sont les protocoles de preuve sans transfert de connaissance (zero-knowledge proof) dont on donne une idée à la section 11.5.
Le but de l'attaque d'un adversaire peut être soit de ***découvrir la clef du chiffrement*** et de pouvoir ainsi décrypter tous les messages de l'émetteur ou plus modestement de ***décryter un message particulier*** sans nécessairement disposer de la clef du code.

Garantir la confidentialité des communications entre Alice et Bob suppose donc qu'Ève ne peut pas

- trouver M à partir de $E(M)$ (le crypto-système doit être résistant aux attaques sur le message codé)
- trouver la méthode de déchiffrement D à partir d'une famille de couples, $\{(M_i, E(M_i)\}$, (message clair, message codé correspondant).

- accéder à des données contenues dans le micro-processeur qui code et décode et plus généralement ne puisse pas espionner les ordinateurs d'Alice et de Bob

1.5 Différentes notions de sécurité d'un cryptosystème.

- La ***sécurité inconditionnelle*** qui ne préjuge pas de la puissance de calcul du cryptanalyste qui peut être illimitée.
- La ***sécurité calculatoire*** qui repose sur l'impossibilité de faire en un temps raisonnable, compte tenu de la puissance de calcul disponible, les calculs nécessaires pour décrypter un message. Cette notion dépend de l'état de la technique à un instant donné.
- La ***sécurité prouvée*** qui réduit la sécurité du cryptosystème à un problème bien connu réputé difficile, par exemple on pourrait prouver un théorème disant qu'un système cryptographique est sûr si un entier donné n ne peut pas être factorisé.
- La ***confidentialité parfaite*** qualité des codes pour lesquels un couple (message clair, message chiffré) ne donne aucune information sur la clef.

Toutes ces notions de sûreté reposent sur la ***théorie de l'information*** de Claude Shannon, cf. le chapitre 13.1.

Il a pu donner un sens précis basé sur les probabilités à la notion de sécurité inconditionnelle si l'on précise le type d'attaques permises. Il a aussi donné un sens précis à la notion de confidentialité parfaite.

La notion de sécurité calculatoire repose sur la ***théorie de la complexité***, cf chapitre 13.2. Dans la pratique il faut préciser le type d'attaque. C'est la sécurité calculatoire que l'on utilise dans la plupart des évaluations de sécurité des systèmes cryptographiques. Elle repose sur la remarque suivante: même avec des ordinateurs faisant 10^9 opérations élémentaires par seconde un calcul qui nécessite 2^{100} opérations élémentaires est hors de portée actuellement car pour l'effectuer il faut environ $4 \cdot 10^{13}$ années!

La sécurité prouvée consiste à ramener la sécurité d'un cryptosystème à un problème que l'on sait ou que l'on espère être calculatoirement difficile comme par exemple la factorisation des entiers en facteurs premiers. Ceci permet de classifier les différents cryptosystèmes suivant leur sécurité et de procéder à une veille technologique rationnelle.

Chapitre 2

Historique.

Il y a historiquement deux grandes familles de codes classiques avec des hybrides

- Les codes à répertoire
- Les codes à clefs secrètes qui se subdivisent en deux familles
  - les codes de transposition ou de permutation qui sont des codes par blocs.
  - les codes de substitution qui peuvent être des codes par blocs ou par flots

On trouve des utilisations attestées par des documents historiques comme par exemple

- Scytale à Sparte vers -450, (principe des codes de permutation).
- Code de Jules César vers -50, (principe des codes de substitution).

2.1 Codes à répertoire.

Ils consistent en un dictionnaire qui permet de remplacer certains mots par des mots différents. Ils sont très anciens et ont été utilisés intensivement jusqu'au début du 20-ième siècle. Ils ont fait l'objet d'une critique sévère de A. Kerchkoffs dans son article fondateur.
On peut par exemple créer le dictionnaire suivant:

rendez-vous ↔ **175**	demain ↔ **oiseaux**
midi ↔ **à vendre**	Villetaneuse ↔ **au marché**

La phrase en clair:

RENDEZ VOUS DEMAIN MIDI VILLETANEUSE

devient avec ce code

175 OISEAUX À VENDRE AU MARCHÉ

Il faut donc disposer de dictionnaires qui prévoient toutes les possibilités. Donc, sauf si on se restreint à transmettre des informations très limitées, la taille du dictionnaire s'accroit démesurément. Au 19e siècle on avait ainsi pour des usages commerciaux ou militaires des dictionnaires de plusieurs milliers de mots de codes. Tout changement du code nécessitait l'envoi de documents volumineux avec un risque d'interception non négligeable.

Ces codes manquent de souplesse ils ne permettent pas de coder des mots nouveaux sans un accord préalable entre l'expéditeur et le destinataire. Pour cela il faut qu'ils échangent des documents ce qui accroît le risque d'interception du code. Ils ne sont pas adaptés à des usages intensifs entre de nombreux correspondants. Ils ne sont pratiquement plus utilisés pour les usages publics. Par contre ils peuvent rendre des services appréciables pour un usage unique.

2.2 Codes de permutation ou de transposition.

On partage le texte en blocs, on garde le même alphabet mais on change la place des lettres à l'intérieur d'un bloc (on les permute).

Un exemple historique dont le principe est encore utilisé est la ***méthode de la grille*** (principe de la ***scytale*** utilisée par les spartiates vers -450 AJC).

On veut envoyer le message suivant:

RENDEZ VOUS DEMAIN MIDI VILLETANEUSE

L'expéditeur et le destinataire du message se mettent d'accord sur une grille de largeur fixée à l'avance (ici une grille de 6 cases de large).

L'expéditeur écrit le message dans la grille en remplaçant les espaces entre les mots par le symbole □. Il obtient:

R	**E**	**N**	**D**	**E**	**Z**
□	**V**	**O**	**U**	**S**	□
D	**E**	**M**	**A**	**I**	**N**
□	**M**	**I**	**D**	**I**	□
V	**I**	**L**	**L**	**E**	**T**
A	**N**	**E**	**U**	**S**	**E**

Il lit le texte en colonne et obtient ainsi le message crypté:

R□D□VAEVEMINNOMILEDUADLUESIIESZ□N□TEC

Pour pouvoir modifier le code rapidement sans toucher à son principe et pouvoir ainsi augmenter la sécurité les deux interlocuteurs peuvent décider l'ajout d'une clef.

Le but est de pouvoir changer facilement le cryptage d'un message tout en gardant le même algorithme de codage. Pour cela on rajoute une ***clé secrète*** constituée par l'ordre de lecture des colonnes.

***Exemple* 2.2.1.** On choisit la clé: **CAPTER**
On numérote les colonnes en fonction du rang des lettres du mot CAPTER dans l'alphabet c'est à dire

$$\mathbf{2, 1, 4, 6, 3, 5}$$

et on lit les colonnes dans l'ordre indiqué.

EVEMINR□D□DADUADLUZ□N□TENOMILEESIIES

On a 6! codes différents.

Pour décoder le message précédent on range en colonne sur la grille en suivant l'ordre des colonnes donné par le mot de code

	E				
	V				
	E				
	M				
	I				
	N				

$\Longrightarrow$

R	E		D		
□	V		U		
D	E		A		
□	M		D		
V	I		L		
A	N		U		

$\Longrightarrow$

R	E	N	D	E	Z
□	V	O	U	S	□
D	E	M	A	I	N
□	M	I	D	I	□
V	I	L	L	E	T
A	N	E	U	S	E

On a affaire à un code à clef secrète ou code symétrique car la clef de décodage est la même que la clef de codage ou s'en déduit facilement.

Pour éviter d'allonger démesurement la hauteur de la grille et pour éviter d'avoir à coder la totalité du message avant de commencer la transmission, on travaille sur des blocs de taille $m = k \times \ell$ où k est la largeur de la grille et ℓ sa hauteur. On a alors un système de codage par blocs, symétrique ou à clef secrète.

Pour des raisons de sécurité il ne faut pas que ℓ et k soient trop petits. Il faut aussi compléter les blocs incomplets d'une manière qui ne diminue par la sécurité du code.

2.2.1 Cryptanalyse des codes de substitution.

Si l'on ne dispose que d'un texte chiffré, on peut essayer d'attaquer ces codes par ***force brute*** c'est à dire en essayant de manière exhaustive toutes les permutations de colonnes possible. Rappelons qu'un calcul comportant plus de 10^{80} opérations élémentaires est impraticable actuellement en un temps raisonnable. Si la grille comporte n colonnes on aura $n!$ permutations de colonnes possibles.

D'après la formule de Stirling $n! \sim \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$, donc dès que le nombre de colonne dépasse 50 on a plus de 10^{85} permutations et on est assuré qu'une attaque par force brute est impraticable. Mais ce n'est pas la seule attaque possible.

Il y a par exemple des attaques à texte clair choisi. On prend un message constitué d'un seul 1 et complété par des zéros et de regarde le résultat en faisant varier la place du 1. On en tire rapidement des informations non-triviales sur la permutation.

2.3 Codes de substitution.

Dans les codes de substitution par flots ou par blocs l'ordre des lettres est conservé mais on les remplace par des symboles d'un nouvel alphabet suivant un algorithme précis.

Exemple* 2.3.1. *Code de César:

Pour coder on remplace chaque lettre par son rang dans l'alphabet.

A=1, B=2, C=3,....,M=13, N=14,...,S=20,...,X=24, Y=25, Z=26

D'après Suetone, dans son ouvrage "Vie des douze Césars", Jules César pendant la guerre des Gaules avait utilisé le code de substitution par flot suivant

lettre codée=lettre claire+3 modulo 26

Le message en clair

RENDEZ VOUS DEMAIN MIDI VILLETANEUSE

devient

UHQGHC YRXV GHPDLQ PLGL YLOOHWDQHXVH

On peut considérer toute la famille des codes

lettre codée=lettre claire+n modulo 26

où $\boldsymbol{n}$ est un entier entre 0 et 25 appelé la clef du code.

Avec la clef $n = 7$ le texte codé du message précédent devient:

YLUKLG CVBZ KLTHPU TPKP CPSSLAHULBZLBZL

Le ***décodage*** se fait en utlisant la relation

lettre claire=lettre codée -n mod 26

On a affaire à un ***code en continu ou par flots*** symétrique ou à clef secrète.

2.3.1 Cryptanalyse des codes de César.

Le code de César ne résiste pas à une attaque à texte chiffré connu. On considère un message codé avec une substitution monoalphabétique:

JTVMNKKTVLDEVVTLWTWITKTXUTLWJERUTVTWTHDXATLIUNEWV.
JTVIEVWELOWENLVVNOEDJJTVLTPTXYTLWTWUT
SNLITTVQXTVXUJXWEJEWTONKKXLT.

Décodage par ***analyse de fréquence***, ctte méthode a été mise au point au moyen ge par des lettrés arabes.

Analyse de fréquence

Lettre	% français	% texte	Lettre	% français	% texte
A	9,4	1	N	7,2	5
B	1,0	0	O	5.1	2,5
C	2,6	0	P	2,9	1
D	3,4	2,5	Q	1,1	1
E	15,9	8	R	6,5	1
F	1	0	S	7,9	1
G	1	0	T	7,3	20
H	0,8	1	U	6,2	4,5
I	8,4	3,8	V	2,1	12
J	0,9	5,1	W	0	9,9
K	0	4,7	X	0,3	6
L	5,3	9	Y	0,2	1
M	3,2	1	Z	0,3	0

On peut donc faire l'hypothèse que T=E puis que V=S (à cause des lettres doublées) puis que les voyelles A, I, O, U correspondent à D,E, N, X et finalement on obtient la correspondance

A	B	C	D	E	F	G	H	I	J	K	L	M
D	R	O	I	T	S	H	M	E	F	G	J	K
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
L	N	P	Q	U	V	W	X	Y	Z	A	B	C

Exercices. 1

2.3.1. Le message suivant a été codé avec un code de César, décodez-le.

YN PHEVBFVGR RFG HA IVYNVA QRSNHG

2.3.2. On choisit un alphabet à $M \geq 2$ lettres, on associe à chaque lettre de l'alphabet un entier entre 0 et $M-1$. Un ***code affine*** sur cet alphabet est un code dont la fonction de codage est

$$E : \mathbb{Z}/M\mathbb{Z} \longrightarrow \mathbb{Z}/M\mathbb{Z}$$
$$x \longmapsto ax + b$$

avec a (mod $M\mathbb{Z}$) et premier à M, b (mod $M\mathbb{Z}$). On suppose qu'on utilise l'alphabet latin avec 26 lettres. On considère le code affine avec $M = 26$, $a = 7$, $b = 5$. Codez avec ce code le texte:

IL SEMBLERAIT BIEN QUE CE TEXTE AIT UNE SIGNIFICATION.
LE TOUR EST DONC JOUE

2.3.3. Le message suivant a été codé avec le code affine associé à l'alphabet latin, $M = 26$:

NMDGXP IDIIDHX AKVAVPA ZQX NKTAUAQDGTPX SZ
NMRCCKXLXQU SX ERHXQXKX IDPXX PZK GD KXAXURURVQ
SX GD NGX.

Décodez-le.

2.4 Le code de Vigénère.

La faiblesse des codes de César et des systèmes analogues est que la fréquence des lettres est conservée ce qui permet une cryptanalyse aisée par analyse de fréquences.

Pour améliorer la sécurité on peut faire un code de César par blocs dans lequel on change de substitution pour chaque lettre d'un bloc. On obtient ainsi le ***code de Vigénère***, mis au point par Leon Batista Alberti au 15-ième siècle et développé par Blaise de Vigénère:

- On se fixe une longueur de bloc m.
- On découpe le message en blocs de m-lettres.
- On chiffre par blocs de m lettres. On décide par exemple que la première lettre d'un bloc de m est codée avec un code de César de clef n_1, la deuxième avec un code de César de clef n_2 et la m-ième par un code de César de clef n_m.

Très sûrs pendant plusieurs siècles, ces codes ont été cryptanalysés officiellement par Charles Babbage et Friedrich Wilhelm Kasiski au 19-ième siècle.

Le code de César est un ***code monoalphabétique***. Le code de Vigénère est un code ***polyalphabétique*** ou ***par blocs***.

***Exemple* 2.4.1.** $m = 5$, $n_1 = 3$, $n_2 = 14$, $n_3 = 7$, $n_4 = 22$, $n_5 = 19$, le message en clair est:

$M=\Big\{$Ce système de codage n'est pas sûr, mais plus que le code de César si la clé est longue$\Big\}$.

on partage en blocs de taille 5 en partant de la gauche

CESYS TEMED ECODA GENES TPASS URMAI SPLUS QUELE
CODED ECESA RSILA CLEES TLONG UE**XXX**

Les XXX ont été ajoutés pour compléter le dernier bloc. La manière de compléter le dernier bloc peut être une faiblesse du code. Dans chaque bloc on code la première lettre avec le code de César de clef $n_1 = 5$,..., la cinquième lettre du bloc avec le code de César de clef $n_5 = 19$. Le message codé devient:

$e(M)=$ FSZUL WST**AW** HQVZT JSU**AL** WDHOL XFTWB VDSQL
TILHX FCK**AW** HQLOT UGPHT FZL**AL** WZVJZ XSETQ

2.4.1 Cryptanalyse des codes de Vigenère.

La cryptanalyse du cryptosystème de Vigénère peut se faire à texte chiffré connu si le message est assez long, cf. le chapitre 1.4. On remarque que des répétitions de lettres assez longues (en général on cherche des triplets ou ***trigrammes***) doivent correspondre dans le texte clair à des répétitions de lettres aussi. Ceci permet de majorer la taille de la clé. On se ramène alors à la cryptanalyse d'un chiffrement de César. Cette cryptanalyse a été mise au point au 19e siècle.

Ici compte tenu de la faible longueur du texte on ne trouve que les doublets ou ***digrammes* AW** et **AL** éloignés de 40 lettres et 45 lettres dont le PGCD est 5 ce qui suggère une clef de longueur 5.

Une fois que l'on a déterminé la longueur de la clef, le décodage est le même que celui de 5 codes de César.

Exercices. 1

2.4.1. **Indice de coïncidences** Étant donné une suite $x = x_1x_2 \dots x_n$ de caractères x_i d'un alphabet Z on définit le nombre n_c d'indices i tels que $x_i = c$ et l'***indice de coïncidences***, I qui est la probabilit pour que deux caractres de la suite x soient identiques

$$I = \Pr_{K,J}[x_K = x_L \mid I < J]$$

où K et L des variables aléatoires indépendantes sur $\{1, \dots, n\}$ équidistribuées.

1. Montrer que $I = \sum_{c \in Z} \frac{n_c(n_c - 1)}{n(n-1)}$.
2. Montrer que l'indice de coincidence est invariant quand on substitue l'alphabet Z' à l'alphabet Z.
3. Montrer que l'on peut utiliser l'indice de coïncidences pour faire une cryptanalyse du code de Vigenère si l'on connait une borne supérieure de la taille des blocs.

2.4.2. On associe à chaque lettre de l'alphabet latin son ordre compris entre 0 et 25. Le message suivant a été codé avec un code de Vigénère associé à l'alphabet latin:

CS AZZMEQM, CO XRWF, CS DZRM GFMJECV. X'IMOQJ JC LB NLFMK CC LBM WCCZBM KFIMSZJSZ CS URQIUOU. CS ZLPIE ECZ RMWWTV, SB KCCJ QMJ FCSOVJ GCI ZI ICCKS, MK QMLL YL'CV ECCJ OKTFWTVM JIZ CO XFWBIWVV, IV ACCI CC C'OCKFM, JINWWB U'OBKSVUFM.

Décodez-le.

2.5 Chiffrement de Hill.

Ce cryptosystème généralise celui de Vigénère. Il a été publié par L. S. Hill en 1929.

- On choisit un alphabet de n lettres (on prendra dans nos exemples $n = 26$) et une taille m pour les blocs, par exemple $m = 2$. Alors $\mathcal{P} = \mathcal{E} = (\mathbb{Z}/26\mathbb{Z})^2$, (en général $\mathbb{Z}/n\mathbb{Z}$).
- La clef de codage est une matrice inversible $K \in \mathrm{GL}_m(\mathbb{Z}/n\mathbb{Z})$, si $n = 26$ et $m = 2$

$$K = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/26\mathbb{Z})$$

Si $(x_1, x_2) \in \left(\mathbb{Z}/26\mathbb{Z}\right)^2$ est le message clair alors le message codé sera:

$$(y_1, y_2) = e_K((x_1, x_2)) = (x_1, x_2)\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (ax_1 + cx_2, bx_1 + dx_2)$$

La clé de déchiffrage est la matrice inverse de K dans $\mathrm{GL}_m(\mathbb{Z}/n\mathbb{Z})$.

Par exemple avec $m = 2$ et $K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$ alors $K^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$.

Comme pour le code de César on peut considérer des codes de Hill affines constitués d'une matrice de $\mathrm{GL}_m(\mathbb{Z}/n\mathbb{Z})$ et d'un vecteur V de $(\mathbb{Z}/n\mathbb{Z})^m$. L'algorithme de codage est donné par

$$M \longmapsto KM + V$$

où M est un bloc de taille m du message clair identifié à un vecteur de $(\mathbb{Z}/n\mathbb{Z})^m$.

2.5.1 Cryptanalyse des codes de Hill.

Le cryptosystème de Hill succombe facilement aux attaques à texte clair choisi.

Exercices. 1

2.5.1. 1. En utilisant la correspondance

$$\text{Alphabet} \longrightarrow \mathbb{Z}/26\mathbb{Z} = \{0, 1, \ldots, 25\}$$

Numériser le texte ci-dessous (du moins une partie)

Des chercheurs tentent de visualiser des raisonnements mathematiques dans les emotions comme la honte ou la compassion.

2. Chiffrer le message précédent avec une méthode par décalage de clef 7.

3. Chiffrer le message avec une mthode par substitution en utilisant la clef $k : Z\mathbb{Z}/26\mathbb{Z} \to Z\mathbb{Z}/26\mathbb{Z}$ définie par

$$k(\lambda) = \begin{cases} 8\lambda + 1 & \text{si } \lambda \neq 7 \text{ et } 25 \\ 0 & \text{si } \lambda = 7 \\ 8 & \text{si } \lambda = 25 \end{cases}$$

Donner la fonction réciproque de k.

4. Chiffrer le message avec une méthode de Vigenère de clef $k = (2; 19)$.

2.5.2. (Cryptanalyse par analyse de fréquence). On considère le message chiffré avec une méthode de substitution.

eohokrilppofoyvkesfivsglomihisvsyoelkvije
ooyhiswzyqowgliyvsvowqoxicioppovqowohhohoeikroowmih
eikvsasvorlfisyoqomlsweoqojlvqoeohosyqlwvhsoeeoeovi
lnqoxickihjzysgloowvisywsmiwwoqoqolnkoyvglivhoasyxvm
mfoyfseeowomvkoyvksygliyvoivhzswkoyvwzsniyvommfiltzlh
qrlsoveoqohysohhimmzhvqlxhzlmoqonmohvwsyvohxzlaohyofo
yviewlheoazelvszyqlkesfivmhoazbisvoyqolnfseeolyglokov
ilnmzlhhisvivvosyqhoksygkoyvglihiyvoiyolpkoyvmmfqsksi

1. Donner le tableau des fréquence des lettres, et des fréquences des bigrammes les plus fréquents.

2. En déduire la clef de chiffrement et le message clair correspondant.

2.5.3. Montrer que le chiffrement de Hill ne résiste pas à une attaque à texte clair choisi.

2.6 Commentaires historiques.

Les méthodes historiques pour authentifier un message se retrouvent dans les cryptosystèmes modernes

On utilisait des messagers qui devaient échanger des signes de reconnaissance convenus (phrase de reconnaissance, lettres d'introduction, etc..) avec le

destinataire pour authentifier le messager, l'expéditeur ou le destinataire, afin déviter les faux messages.

Pour éviter la falsification du message on le mettait dans une enveloppe scellée revétue de cachets, le message lui-même était signé, l'écriture permettait elle aussi l'authentification du message, etc...

Le destinataire pouvait parfois accuser réception en guise de protocole de non répudiation.

La cryptanalyse a été pratiquée depuis la plus haute antiquité. Le code de César a été cryptanalysé par les lettrés arabes du 9-ième siècle; Al Kindi a décrit la méthode de l'analyse statistique.

Tous les rois avaient leurs cryptographes-cryptanalystes (les Rossignol pour Louis XIV) et leur cabinet noir.

Les rapports entre cryptographie et cryptanalyse sont analogues aux rapports entre blindage et artillerie. Le code de César a tenu 9 siècle, celui de Vigenère a tenu 4 siècles, le standard DES a tenu 20 ans. le standard RSA est en passe d'être supplanté par les codes elliptiques.

Chapitre 3

Quelques méthodes de codage.

Dans la partie historique nous avons donné des exemples de chiffrement par blocs (code de Hill) et de chiffrement par flots (code de César). Les systèmes de ***chiffrement par blocs*** agissent sur les données avec une transformation fixe des grands blocs de données en clair; les systèmes de ***chiffrement par flots*** (ou ***chiffrement par flux***) agissent avec une transformation variant avec le temps sur des données en clair individuelles.

Le chiffrement par blocs est le plus répandu et jouit d'une meilleure réputation que le chiffrement par flots plus facile à analyser mathématiquement.

Le schéma général du chiffrement par blocs symétrique ou à clef secrète est le suivant:

1. coder l'information source en binaire. On obtient ainsi une chaîne de caractères composée de 0 et de 1.

2. découper cette chaîne en blocs de longueur donnée (par exemple 64 bits ou 128 bits ou 256 bits).

3. chiffrer un bloc en faisant un ***OU exclusif*** (ou ***XOR***) bit à bit avec une clé secrète, k, qui est une suite de 0 et de 1 de même longueur, (un XOR est donc l'addition sans retenu en base deux).

4. déplacer et permuter certains bits du bloc.

5. recommencer un certain nombre de fois l'étape précédente, on appelle cela une ***ronde***.

6. passer au bloc suivant et retourner à l'étape 3 jusqu'à ce que tous les blocs soient chiffrés.

Le OU exclusif ou XOR entre deux blocs en binaire, m et n, est noté $m \oplus n$, par exemple

$$m = 1001111010001111, \quad n = 1011111000010111$$
$$m \oplus n = 0010000010011000$$

Le schéma général de chiffrement par blocs asymétrique ou à clef publique est le suivant:

1. coder l'information source en binaire. On obtient ainsi une chaîne de caractères composée de 0 et de 1.
2. découper cette chaîne en blocs de longueur donnée (par exemple 1024 bits à 2048 bits pour RSA et El Gamal, 256 bits pour les codes elliptiques).
3. chiffrer un bloc en utilisant la fonction de chiffrement (exponentiation modulaire pour RSA).
4. passer au bloc suivant et retourner à l'étape 3 jusqu'à ce que tous les blocs soient chiffrés.

Le problème pratique qui se pose ensuite est le protocole d'envoi des blocs successivement obtenus. Il faut que ce protocole ne diminue pas la sureté du cryptosystème.

3.1 Les modes de chiffrement.

Que ce soit pour DES ou des cryptosystèmes symétriques plus récents comme IDEA ou AES ou pour des cryptosystèmes asymétriques comme RSA ou El-Gamal les clés sont de longueur fixée. Les messages eux peuvent avoir une longueur arbitraire. Pour adapter la taille du message à celle de la clef on décompose le message par blocs de taille fixe correspondant aux tailles des clés que l'on chiffre ensuite un à un et que l'on envoie successivement. Pour cela quatre modes de chiffrement par blocs sont possibles: ECB, CBC, CFB et OFB.

3.1.1 Le mode ECB, Electronic Code Book.

Le mode ***ECB***, ***Electronic Code Book***, est le mode le plus simple. Le message, M, est découpé en blocs , $(m_i)_{i\geq 1}$, et chaque bloc est crypté séparément par

$$c_i = E(m_i)$$

ou $E = E_k$ dépend de la clé secrète k et c_i est le bloc crypté correspondant. On procède donc suivant le schéma suivant:

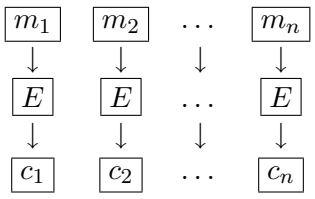


Figure 3.1: Diagramme du mode ECB

On transmet $c_1||c_2||\ldots||c_n$.

Sécurité du mode ECB

Un bloc de message m_i sera toujours codé de la même manière, ce qui nuit à la sécurité du codage. D'autre part un attaquant malveillant peut permuter deux blocs ou remplacer un bloc par un autre sans que le destinataire s'en aperoive.

La procédure ECB n'est jamais utilisée en pratique.

3.1.2 Le mode CBC, Cipher Block Chaining.

Le mode ***CBC***, ***Cipher Block Chaining***, a été introduit pour qu'un bloc ne soit pas codé de la même manière s'il apparît dans deux messages différents ou s'il apparaît deux fois dans un message.

Le message, M, est découpé en blocs , $(m_i)_{i\geq 1}$, et chaque bloc est crypté de la manière suivante. On commence par choisir un bloc initial c_0. Chaque bloc clair m_i est d'abord modifié en faisant un XOR de ce bloc avec le bloc crypté précédent, c_{i-1} puis on crypte le résultat obtenu par XORisation avec la clef

$$\begin{aligned} c_1 &= E_k(m_1 \oplus c_0) \\ c_2 &= E_k(m_2 \oplus c_1) \\ &\vdots \\ c_i &= E_k(m_i \oplus c_{i-1}) \\ &\vdots \end{aligned}$$

suivant le schéma donné à la figure 3.2 page 32.
On transmet le message $c_0||c_1||\ldots||c_n$.

Le bloc initial c_0 peut être choisi de l'une des manières suivantes:

1. On génère c_0 aléatoirement et on le transmet en clair avec le message
2. On génère c_0 aléatoirement et on le transmet de manière confidentielle
3. On utilise un $c0$ fixe qui fait partie des constantes du cryptosystème
4. On utilise un $c0$ fixe qui fait partie de la clé sécrète du cryptosystème

On recommande en général d'utiliser l'une des deux première solutions. Les deux dernières font que si le premier bloc est identique dans deux messages différent il sera codé de la même manière ce qui nuit à la sécurité du code.

Le déchiffrement nécessite de connaître la fonction inverse de la fonction de codage $D_k = E_k^{-1}$ pour décrypter

$$m_i = c_{i-1} \oplus D_k(c_i)$$

Sécurité du mode CBC

Ce système de transmission par blocs a une bonne sécurité et n'affaiblit pas le crytosystème, mais il nécessite de connaître la fonction inverse D_k de E_k.

3.1.3 Le mode CFB, Cipher FeedBack.

Le mode ***CFB***, ***Cipher FeedBack***, a été introduit pour ne pas avoir à calculer la fonction inverse, D_k, de la fonction de chiffrage E_k.

Le principe est le même que clui du mode CBC. Le message, M, est découpé en blocs , $(m_i)_{i\geq 1}$, et chaque bloc est crypté de la manière suivante. On commence par choisir un bloc initial m_0, choisi suivant les mêmes principes que le blocs e_0 en mode CBC.

Chaque bloc clair m_i est XORé avec le crypté du bloc de sortie précédent, c_{i-1}, suivant le schéma:

$$\begin{aligned} c_0 &= E_k(m_0) \\ c_1 &= m_1 \oplus E_k(c_0) \\ c_2 &= m_2 \oplus E_k(c_1) \\ &\vdots \end{aligned}$$

$$c_i = m_i \oplus E_k(c_{i-1})$$
$$\vdots$$

on fait donc un XOR du bloc d'indice i le crypté du bloc d'indice $i-1$, suivant le schéma donné à la figure 3.3 page 32.
On transmet le message $c_0||c_1||\dots||c_n$.

Sécurité du mode CFB

Ce mode est moins sûr que le CBC et est utilisé par exemple pour les cryptages réseaux. L'intérêt est que le déchiffrement ne nécessite pas de calculer D_k, en effet:

$$m_i = c_i \oplus E_k(c_{i-1})$$

(se souvenir que l'on calcule modulo 2 sans retenu, bit à bit) d'où un gain de temps.

3.1.4 Le mode OFB, Output FeedBack.

Le mode ***OFB***, ***Output FeedBack***, est une variante de CFB qui permet d'avoir un cryptage et un décryptage totalement symétrique:

$$z_i = E_k(z_{i-1}); \quad c_i = m_i \oplus z_i$$

en suivant le schéma donné à la figure 3.4 page 33
On transmet le message $c_0 c_1 \dots c_n$.

Ce mode est utilisé par exemple pour les cryptages satellites et se déchiffre par

$$z_i = E_k(z_{i-1}); \quad m_i = c_i \oplus z_i$$

Sécurité du mode OFB

Sa sureté est équivalente à celle du mode CFB.

3.1.5 Le mode CTR, Counter-mode encryption.

Le mode ***CTR***, ***Counter-mode encryption***. Ce mode de cryptage est lui aussi totalement symétrique, mais en outre facilement parallélisable. Il utilise pour chiffrement un compteur de valeur initiale T

$$c_i = m_i \oplus E_k(T+i)$$

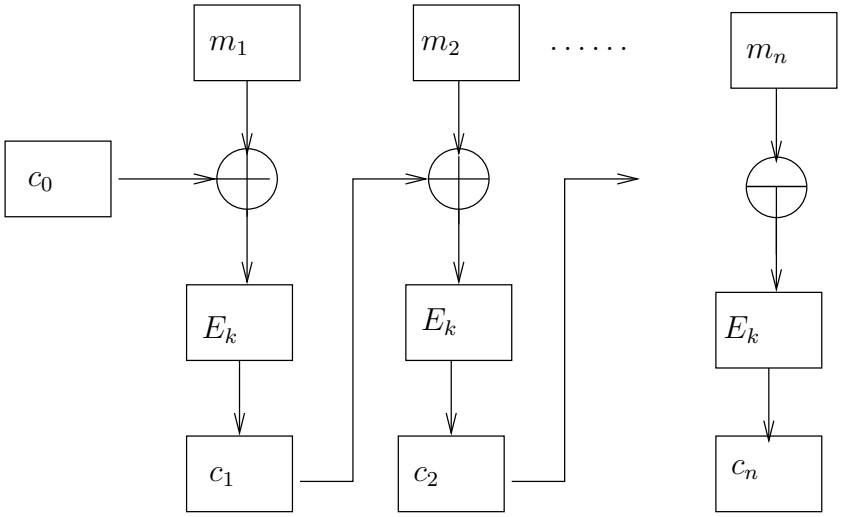


Figure 3.2: Diagramme du CBC

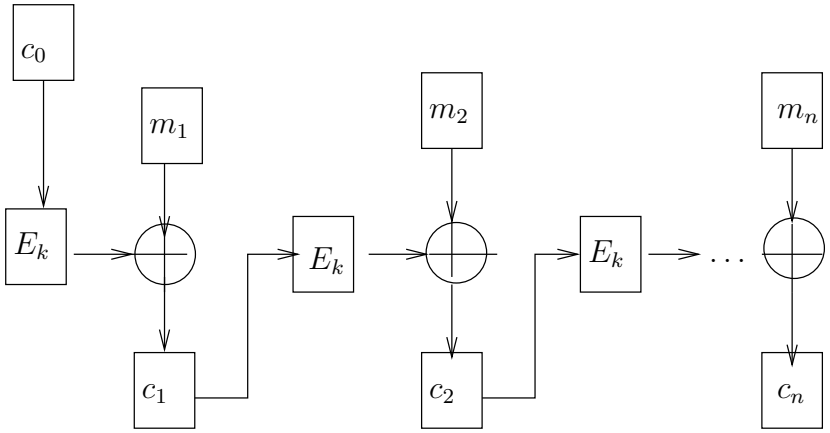


Figure 3.3: Diagramme du mode CFB

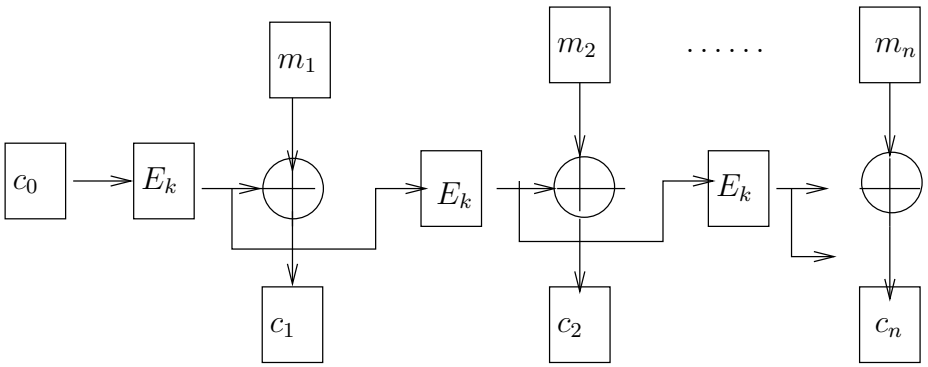


Figure 3.4: Diagramme du mode OFB

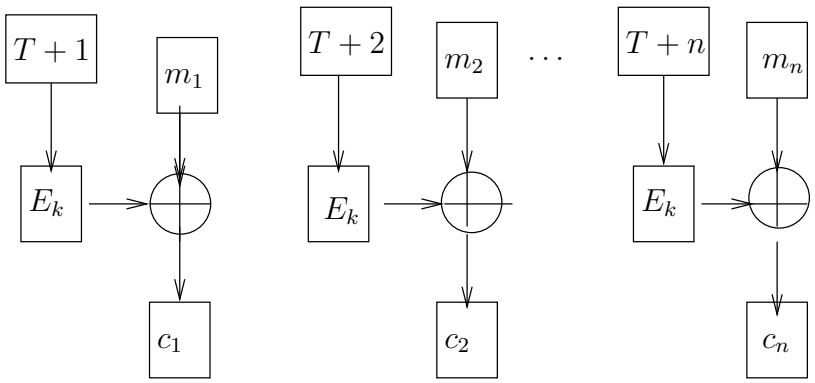


Figure 3.5: Diagramme du mode CTR

en suivant le schéma donné à la figure 3.5 page 33
Le déchiffrage est identique

$$m_i = c_i \oplus E_k(T + i)$$

L'intérêt d'un tel mode est principalement que les différents calculs de cryptage et décryptage sont indépendants, comme pour le mode ECB, mais qu'un même bloc n'est a priori jamais codé de la même façon.

Sécurité du mode CTR

Sa sureté est équivalente à celle du mode CFB.

Chapitre 4

Les codes modernes.

Tout d'abord nous donnons une description un peu formelle d'un cryptosystème. Nous décrirons au chapitre 6, 7, 8, 9, des cryptosystèmes réels.

Définition 4.0.1. *Un cryptosystème est un dictionnaire entre les messages en clair et les messages chiffrés.*

Afin de travailler efficacement sur les codes et définir de manière quantitative leur sécurité on est amené à les modéliser et donc à définir de manière axiomatique un cryptosystème:

Définition 4.0.2. *Formellement un cryptosystème est un quintuplet*

$$(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$$

où

- $\mathcal{P}$ *est un ensemble fini de blocs :* **les mots en clair**
- $\mathcal{C}$ *est un ensemble fini de blocs:* **les mots codés**
- $\mathcal{K}$ *est un ensemble : l'***espace des clefs**
- *Pour tout* $K \in \mathcal{K}$ *on a une* **règle de chiffrement** $e_K \in \mathcal{E}$ *et une* **règle de déchiffrement** *correspondante* $d_K \in \mathcal{D}$. *Chaque* $e_K : \mathcal{P} \to \mathcal{C}$ *et* $d_K : \mathcal{C} \to \mathcal{P}$ *sont des fonctions telles que* $d_K(e_K(x))) = x$ *pour tout* $x \in \mathcal{P}$

Pour chaque $K \in \mathcal{K}$ *(la clef du code) la transformation* e_K *est appelée le* **procédé de chiffrement**, *ou l'***algorithme de codage**, *entre les textes en clair* $\mathcal{P}$ *et les textes codés* $\mathcal{C}$.

La fonction inverse d_K *de* e_K *est appelée la* **fonction de décodage**.

On exige que tout message codé puisse être décodé.

Un code moderne est donc constitué

- D'un algorithme de chiffrement $f = f_{K_C}$, supposé connu de tous, dépendant d'un paramètre K_C, la clé de chiffrement. L'algorithme est fixé et public, seule la clé change, (on applique le principe de Kerckhoffs).

- De la valeur de la clé de chiffrement, K_C qui est secrète ou non suivant que l'on a affaire à un code à clef secrète ou à un code à clef publique.

- D'un algorithme de déchiffrement $g = g_{K_D} = f^{-1}$ (supposé connu de tous) dépendant d'une clé de déchiffrement, K_D, différente ou non de K_C.

- De la valeur de la clé de déchiffrement, K_D, qui est toujours secrète.

4.1 Objectifs des codes actuels.

Rappelons les qualités attendues d'un cryptosystème. Tout d'abord les qualités fonctionnelles:

1. ***Confidentialité des données***: Les messages ne peuvent être déchiffrés que par le destinataire.

2. ***Intégrité des données***: Ils ne peuvent être modifiés par un tiers non autorisé.

3. ***Authentification***: L'identité des différents participants peut être vérifiée.

4. ***Non-répudiation***: L'expéditeur ne peut nier avoir émis le message et le destinaire ne peut nier l'avoir reçu.

Ensuite les qualités pratiques

1. Il doit résister aux attaques connues et si possible avoir une sécurité prouvée.

2. Il doit permettre de coder et décoder rapidement (en temps réel pour certaines applications).

Il n'existe pas de codes qui réunissent toutes ces qualités simultanément. Il faut donc un compromis adapté à chaque situation.

4.2 Les familles de codes modernes.

Les principales familles de codes modernes sont

- Les codes par flot (registres à décalage)
- les codes par blocs $\begin{cases} \text{les codes symétriques (ou à clé secrète).} \\ \text{les codes asymétriques (ou à clé publique)} \end{cases}$

Les codes à clef publique sont basés sur la notion de fonction à sens unique définie au chapitre 4.4.

4.3 Codes symétriques.

Les principes des codes symétriques commerciaux modernes du type DES (Data Encrytion Standard), cf. chapitre 8, ont été mis au point dans les années 1970 par IBM avec l'aide de la NSA (National Security Agency), ce sont des hybrides de codes de substitutions et de codes de transpositions basés sur un schéma de Feistel.

Ils restent très sûrs avec des clés assez courtes de 128 bits à 256 bits. Leur sûreté est non prouvée. Leur cryptanalyse a fait des progrès (cryptanalyse linéaire et différentielle), ce qui permet de mieux cerner leur sûreté.

Les codes à clé secrète sont les plus employés actuellement car ils sont éprouvés, résistants, rapides et assez facile à mettre en oeuvre. Actuellement leur sécurité est garantie (mais non prouvée) avec des clés assez courtes de 128 à 256 bits pour le standard actuel AES.

Mais il faut échanger la clé secrète avec le destinataire d'où un risque. Ils nécessitent un grand nombre de clés. Il faut

$$\frac{n(n-1)}{2}$$

clés pour que n interlocuteurs puissent échanger des informations d'où un problème de fabrication et d'échange de clefs fiables.

Ils ont du mal à réaliser sans ***tiers de confiance*** le partage des clefs, la signature, l'authentification, et la non répudiation des messages transmis. Ils s'adjoignent parfois un code asymétrique pour cela comme dans le cryptosystème ***PGP***.

La génération actuelle de codes symétriques est le cryptosystème AES, décrit au chapitre 8, développé dans les années 2000 à la suite d'un appel d'offre

international par John Daemon et Vincent Rijmen, [8]. Il utilise dans sa conception nettement plus de mathématiques que son prédécesseur le DES, ce qui permet une meilleure appréhension de sa sécurité.

4.4 Codes asymétriques.

Les principes des codes asymétriques ont été mis au point par Diffie et Hellman en 1976. Ils ont dégagé la notion de ***fonction à sens unique***. Ce sont des fonctions qui sont faciles à calculer c'est à dire ***calculable en temps polynomial*** en fonction de la taille des données mais tel que l'image réciproque (les antécédents) d'un élément soit très difficile à calculer explicitement au moins calculatoirement, c'est à dire que le temps de calcul soit prohibitif, voir la sous-section 13.2.3 et suivants. Autrement dit on demande que la fonction inverse ne soit pas calculable en temps polynomial en fonction de la taille des données.

Le premier exemple de fonction à sens unique du à Diffie, Hellmann et Merkle était basée sur le problème du ***sac à dos***, cf. section 9.2 page 99, dont il avait été démontré qu'il appartenait à la classe des ***problèmes de type NP*** (NP pour Non Polynomial), autrement dit il existe des instances (des réalisations) de ce problème qui sont dans la classe NP (c'est un théorème). ***Attention cela ne veut pas dire que toutes les instances de ce problème sont de type*** NP.

Un problème de la classe NP est un problème dont la solution exige un calcul en ***temps non polynomial*** en fonction de la taille des données, sous réserve de la validité de la conjecture $\boldsymbol{P \neq NP}$, cf. la sous-section 13.2.2. On peut donc espérer qu'il permette de fabriquer un cryptosystème offrant une sécurité calculatoire élevée.

Malheureusement les instances connues du problème du sac à dos ne sont pas de type NP. En particulier les réalisations pratiques de Diffie, Hellmann et Merkle utilisaient des sacs à dos qui n'étaient pas dans la classe NP. Leur cryptosystème a succombé à l'attaque des cryptanalystes (en particulier Shamir).

Dans la solution suivante, 1978, le ***cryptosystème RSA*** (***Rivest-Shamir et Adleman***) décrit au chapitre 9, la fonction à sens unique sous-jacente est la multiplication des entiers qui appartient à la classe $\boldsymbol{P}$ (P pour Polynomial) des ***problèmes polynomiaux en temps***. Sa fonction réciproque la ***factorisation des entiers*** est actuellement dans la classe NP des problèmes non polynomiaux en temps, c'est un **fait d'expérience pas un théorème**.

D'autres solutions sont apparues peu après:

- le ***sytème El Gamal***, cf. chapitre 9, qui repose sur l'exponention dans $\mathbb{Z}/p\mathbb{Z}$ avec p premier et sur l'application inverse qui est le logarithme discret,
- les ***codes basés sur les courbes elliptiques***. Ils reposent sur la structure de groupe des points des courbes elliptiques sur un corps fini cf. chapitre 9.

Les cryptosystèmes asymétriques reposent sur des structures mathématiques élaborées. Leur sûreté est bonne mais non prouvée. Leur cryptanalyse dépend beaucoup des progrès des mathématiques correspondantes.

Sauf pour les codes elliptiques, ils nécessitent des clés longues (1024 à 2048 bits) pour avoir une sûreté équivalentes à celle d'un cryptosystème à clef secrète de 128 à 256 bits. Ils sont 1000 à 1500 fois plus lents. Mais ils permettent de réaliser facilement les fonctionnalités suivantes

- partage des clefs,
- authentification
- intégrité
- non répudiation

et bien d'autres encore grâce au fait que la clef est en fait constituée de deux clefs, la clef de codage et la clef de décodage, et que cette dernière est attachée à une personne et la caractérise.

Ils ne nécessitent que n paires de clés (une clé secrète et une clé publique) pour n interlocuteurs.

On les utilise souvent pour la transmission des clés secrètes des codes symétriques.

4.5 Les échanges de clefs.

Un problème important rencontré dans l'utilisation d'un cryptosystème est l'***échange des clefs*** entre des interlocuteurs. C'est un des moments où la sécurité du cryptosystème est la plus vulnérable. Il faut trouver un protocole sûr pour l'échange des clefs.

Rappelons que dans un cryptosystème à clef secrète lorsque deux interlocuteurs veulent converser il leur faut échanger une clef. Il faut donc autant de clefs qu'il y a de paires non ordonnées d'interlocuteurs c'est à dire pour n interlocuteurs $\binom{n}{2} = \frac{n(n-1)}{2}$. Le nombre de clefs à échanger entre n interlocuteurs est donné par le tableau 4.1 page 40.

nombre d'interlocuteurs	nombre de clés secrètes	nombre de clés publiques
2	1	2
3	3	3
4	6	4
5	10	5
⋮	⋮	⋮
10	45	10
⋮	⋮	⋮
100	4950	100
⋮	⋮	⋮
1000	499 500	1 000
⋮	⋮	⋮
1 000 000	499 999 500 000	1 000 000

Figure 4.1: Nombre de clefs à échanger

Par contre dans un système à clef publique il faut autant de paires de clefs qu'il y a d'interlocuteurs. Chaque interlocuteur dispose en effet d'une clef publique qui figure dans un annuaire et que n'importe qui peut utiliser pour crypter les messages qui lui sont adressés et d'une clef privée, strictement personnelle, pour décrypter les messages qu'il reçoit.

4.5.1 Protocole d'échange de clefs.

Diffie, Hellmann et Merkle ont résolu vers 1974 le problème de partage d'une clé secrète sans envoi physique de la clef.

Leur protocole utilise de l'arithmétique modulaire, cf. la sous-section 13.3.4. Ils travaillent dans les entiers modulo un nombre premier p. Leur alogorithme est le suivant:

1. Alice et Bob choisissent d'un commun accord sur une ligne non protégée un grand nombre premier p. et α un générateur de $\mathbb{Z}/p\mathbb{Z}$

2. Alice choisit a et calcule $\alpha^a = \alpha_a \pmod{p}$
3. Bob choisit b et calcule $\alpha^b = \alpha_b \pmod{p}$
4. Alice et Bob échangent α_a et α_b sur un canal non nécessairement protégé
5. Alice calcule $\alpha_b^a \pmod{p}$ et Bob calcule $\alpha_a^b \pmod{p}$

On a

$$\alpha_b^a \equiv \alpha^{ab} \equiv \alpha_a^b \pmod{p}$$

c'est la ***clef commune d'Alice et Bob***.

Sureté du protocole d'échange de clefs.

Pourquoi ce protocole est-il sûr? Si Ève intercepte la communication entre Alice et Bob, elle peut lire les nombres α_a et α_b.

Pour calculer la clef commune d'Alice et de Bob, il faut qu'Eve puisse calculer α^{ab} à partir de α^a et α^b en connaissant α. La seule méthode connue actuellement est de trouver a et b à partir de α^a et α^b, c'est à dire qu'elle puisse calculer le ***logarithme discret*** dans $\mathbb{F}_p$.

Pour l'instant il n'existe pas d'algorithme rapide, c'est à dire polynomial en temps en fonction de la taille des données, pour calculer le logarithme discret dans $\mathbb{F}_p$. Les meilleurs algorithmes connus sont ***sous-exponentiels***, cf. la sous-section 13.4. Pour un premier p de l'ordre de 10^{500} il faut des mois, voire des années, pour calculer un logarithme discret.

Par contre cet échange de clef peut-être soumis à d'autres types d'attaques.

Chapitre 5

Applications de la cryptographie.

Jusqu'au 20-ième siècle la cryptographie (légale) était essentiellement réservée aux militaires et aux diplomates et accessoirement aux industriels et banquiers.

Le développement des moyens de communications électromagnétiques facile à intercepter, des stockages de données confidentielles dans des sites assez faciles à pénétrer et sur des supports (bandes ou disques, magnétiques optiques) faciles à dupliquer ont généré une demande de cryptosystèmes sûrs, faciles d'emploi et rapides pour des usages civils et commerciaux.

Les codes symétriques ou à clefs secrètes, type DES (Data Encryption Standard), IDEA (International Digital Encryption Algorithm), AES (Advanced Encryption Standard) ont été créés pour couvrir ces besoins. L'application première de la cryptographie reste encore la transmission sécurisée de données sensibles amis d'autres applications commencent à se développer.

Le commerce en ligne (e-commerce: paiement par carte bancaire...), les transactions bancaires et boursière (e-banking:la consultation des données bancaires, ordres de bourse, virements de compte à compte,...), l'administration en ligne (e-administration: déclaration d'impôts, paiement de la TVA pour les entreprise,...), la télévision payante (chaîne payante, pay per view,...), la protection des télécommunication (internet, WIFI, Bluetooth, GSM, téléphonie mobile,...), l'identification automatique (avions, camions suivi par GPS,...), le tatouage ou watermarking des données numériques ainsi que la gestion des droits numériques (digital right management), etc. ont entraîné une explosion de l'utilisation de la cryptographie mais aussi une extension de son champ d'applications.

Cette extension a été facilitée par la mise au point des procédés de transferts de clefs de Diffie et Hellman et des codes asymétriques ou à clefs publiques

de type RSA ou El Gamal.

Les codes à clef publique permettent de résoudre avec des protocoles légers les questions de transfert de clefs, d'identification, d'authentification, de signature entre correspondants.

Aujourd'hui les plus gros utilisateurs de cryptosystèmes sont les institutions financières (banques, bourses,...), les télécommunications (téléphonie mobile, WIFI, Internet, télévision payante,...), les sites d'achats en ligne, ...

Il est probable que le tatouage ou watermarking des données numériques ainsi que la ***gestion des droits numériques*** (***digital right management*** ou ***DRM***) vont entraîner une demande accrue de cryptographie.
Le mariage de la cryptographie et de la théorie de la complexité aboutit à des extensions spectaculaires du champ de la cryptographie classique. Ces nouvelles applications sont développées au chapitre 11 page 133.

5.1 Quel cryptosystème choisir.

Chacun des cryptosystèmes existant codes par flots, codes par blocs à clé secrète, codes à clés publiques ont leurs avantages et leurs inconvénients. Ils ont chacuns des applications privilégiées et sont souvent utilisés en association, cf. PGP.

Les codes par flots basés sur les registres à décalage sont utilisés dans les télécommunications (télévision à péage, téléphones portables,...), à cause de leur rapidité. Ils permettent de faire du codage et du décodage à la volée en temps réel. Par contre leur faible résistance aux attaques et l'augmentation de la puissance de calcul font qu'ils seront probablement supplantés à terme par des systèmes plus sûrs.

Les codes par blocs symétriques ou à clé secrète sont les plus employés car ils réalisent un excellent compromis entre rapidité et sécurité. Ils ne nécessitent que des clefs assez courtes pour un bon niveau de sécurité (128/256 bits). Par contre ils nécessitent d'échanger de nombreuses clés secrètes ce qui constitue un risque pour leur sécurité. On peut les associer à un cryptosystème à clef publique pour échanger les clefs qui doivent être changées très régulièrement pour garder une bonne sécurité et ausi pour réaliser les signatures et authentifications.

Les cryptosystèmes asymétriques ou à clefs publiques sont plus lents. Ils nécessitent des clés longues (1024 à 2048 bits actuellement) sauf les codes elliptiques (128 à 256 bits actuellement). Ils ne nécessitent pas d'échange

de clés secrètes et permettent de réaliser facilement des fonctionalités très utiles (signature, authentification, non répudiation,...).

5.2 Quelques utilisations de la cryptographie.

La nécessité de pouvoir identifier de manière sûre:

- le titulaire d'un compte en banque qui veut retirer de l'argent, ou qui paye par carte bancaire,
- un avion au moment de la procédure d'atterrissage, un véhicule suivi par GPS,
- sur un champ de bataille ses propres troupes et celles de l'ennemi,...

a entraîné le développement des ***protocoles d'identification*** largement basés sur les principes des codes asymétriques.

La recherche d'une sécurité accrue pour les sites sécurisés de paiemant en ligne profite du développement des

- Les protocoles de preuves sans apport de connaissance.
- La signature aveugle.

basés sur la théorie de la ***preuve sans apport de connaissance*** (***zero-knowledge proof***).

La nécessité de conserver l'anonymat dans certaines situations (secret médical par exemple, secret de la vie privée, etc..) peut être assuré grâce au

- Le ***transfert inconscient***.

Il y a encore bien d'autres applications.

5.3 Quelles mathématiques pour la cryptographie.

Actuellement tous les cryptosystèmes utilisent des mathématiques. Elles sont utilisées aussi pour définir et tester la sécurité des cryptosystèmes. Parmi les disciplines mathématiques utilisées pour la cryptographie on a:

- Logique: théorie de la complexité.
- Probabilités pour la théorie de l'information.

- Analyse harmonique pour la théorie du signal
- Combinatoire (théorie de graphes): construction de cryptosystèmes asymétriques, preuves sans apport d'information, partage de secret à seuil.
- Algèbre: théorie des corps finis, des polynômes sur un corps fini,... pour les codes symétriques.
- Théorie des nombres (arithmétique modulaire, théorie algébrique des nombres) : construction de cryptosystèmes asymétriques (RSA, El-Gamal), générateurs de nombres aléatoires.
- Géométrie algébrique sur un corps fini: construction de cryptosystèmes basés sur les courbes elliptiques sur un corps finis, cryptosystèmes basés sur les codes correcteurs d'erreurs.
- Algorithmique (algèbre, théorie des nombres et géométrie effective): mesure de la complexité algorithmique, réalisation pratique d'algorithmes performants, évaluation de la sécurité des cryptosystèmes.

La réalisation pratique des cryptosystèmes repose sur une implantation informatique, leur **degré de sécurité**, leurs performances en dépendent grandement.

5.4 Lutte contre le brouillage.

Le canal de transmission d'un message est souvent brouillé de manière naturelle (parasites dus aux activités humaines ou aux phénomènes naturels dans les transmissions électromagnétiques, hertziennes ou filaires).

Le stockage des données se dégrade naturellement avec le temps (action des particules très énergiques, poussières, rayures sur les CD et DVD, etc.).

Pour lutter contre tous ces brouillages on dispose de la théorie des codes correcteurs d'erreurs. Elle est basée

- sur la théorie des espaces vectoriels sur un corps fini.
- sur la théorie des polynômes sur un corps fini.
- plus généralement sur la géométrie algébrique sur un corps fini.

***Exemples* 5.4.1.** Exemples de codes correcteurs d'erreurs

L'exemple le plus simple de code correcteur d'erreurs est la répétition du message un certain nombre de fois en espérant que les parasites (supposés aléatoires) n'affecteront pas toujours la même partie du message. Mais cette méthode est lourde pour des messages longs et ralentit fortement la transmission des données.

Autre exemple de code correcteur d'erreurs: on suppose que le message est une suite de 0 et de 1 (des bits). On les groupe par paquets de 7 et on ajoute dans chaque paquet de 7 bits un huitième bit (0 ou 1) de telle sorte que la somme de ces 8 chiffres soit paire (code de Hamming). Ce code repère au plus une erreur dans chaque groupe de 8 bits.

Chapitre 6

Codes à confidentialité parfaite.

La théorie de l'information due à Claude Shannon, cf. chapitre 13.1, permet de définir un ***code à confidentialité parfaite***. Grossièrement il s'agit de codes tels que la connaissance du texte crypté ne permette d'avoir aucune information sur le texte en clair.

De tels codes existent, ce sont les ***codes de Vernam*** ou ***codes à masques jetables***, (1917). Ils reposent sur la fabrication de clefs *au hasard* aussi longues que le texte à coder et qui ne servent qu'une fois.

La mise en oeuvre de ces codes est lourde et délicate. La fabrication de clefs 'au hasard' est un problème très difficile et mal résolu. Le stockage et la transmission de ces clés posent un problème de sécurité.

Ils sont rarement utilisés.

Le principe de ces codes est le suivant. On tranforme le texte en une suite de chiffres en base b (souvent $b = 2$). On fabrique ensuite une suite aléatoire de chiffres de même longueur et l'on ajoute (on XORe) les deux suites ainsi obtenues sans retenue, c'est à dire que l'on fait le calcul chiffre à chiffre modulo b.

***Exemple* 6.0.2.** On transforme les lettres de l'alphabet en nombres de 1 à 26 donc ici $b = 26$

$$\text{lettre codée} \equiv \text{lettre claire} + \text{lettre de la clé} \mod 26$$

On code le message ***chiens*** qui comporte 6 lettres avec la clef ***KZUTEG***

$$(\text{message=CHIENS}) + (\text{clef=KZUTEG}) = \text{NHDYSZ}$$

On constate que si l'on avait envoyé le message ***cerise*** avec la clé ***KCNPZC*** on aurait obtenu

(message=CERISE) + (clé=KCNPZC) =NHDYSZ

Il est donc impossible de remonter au texte clair si on change de clé aléatoirement à chaque fois.

Cet exemple montre que la confidentialité est parfaite. Ces codes sont très sûrs. Mais leur mise en oeuvre est très délicate et ils sont très lents.

Chapitre 7

Registres à décalage.

On veut des codes par flots qui imitent les codes de Vernam mais qui soient très rapides et très faciles à mettre en oeuvre afin de pouvoir coder et décoder à la volée en temps réel (Télévision, radio, DVD, cinéma, téléphones portables et mobiles,...).

Une famille de tels codes est basée sur les ***registres à décalage à rétroaction linéaire***, on abrégera souvent leur nom en registre à décalage, ou ***suites récurrentes linéaires sur un corps fini*** ou encore dans la terminologie anglo-saxone ***linear shift feedback register***) en abrégé ***LSFR***.

On fabrique avec les registres à décalage des ***suites pseudo-aléatoires*** pour générer la clef du code. Ces codes sont beaucoup moins sûrs que les codes de Vernam mais ne nécessitent pas la fabrication et la transmission d'une clef aléatoire de la longueur du message à transmettre. Ils sont aussi très utilisés pour le codage par flots.

La méthode de codage est la XORisation du texte en clair par la suite construite à l'aide du LSFR.

7.0.1 Régistres à décalage ou suites récurrentes linéaires sur un corps fini.

On considère le corps fini à 2 éléments $\mathbb{F}_2 \simeq \mathbb{Z}/2\mathbb{Z}$, cf. chapitre 13.6.1
On fixe un entier m, la longueur de la récurrence, et des éléments

$$k_1, \ldots, k_m \in \mathbb{Z}/2\mathbb{Z}, \quad \text{les conditions initiales}$$
$$c_0, \ldots, c_{m-1} \in \mathbb{Z}/2\mathbb{Z} \quad \text{les coefficients de la récurrence}$$

On construit une suite d'éléments $(z_i)_{i\in\mathbb{N}}$ de $\mathbb{Z}/2\mathbb{Z}$:

$$z_1 = k_1, \ldots, \ z_m = k_m, \quad z_{m+1} = c_0 z_1 + \cdots + c_{m-1} z_m$$

$$z_{m+i} = c_0 z_i + \cdots + c_{m-1} z_{m-1+i} = \sum_{j=0}^{m-1} c_j z_{j+i}$$

On montre facilement que la suite ainsi construite est périodique (i.e. il existe $T \in \mathbb{N}$ tel que $z_{i+T} = z_i$ pour i assez grand); mais si on choisit bien les c_j la période est grande devant m.

***Exemple* 7.0.3.** Exemple: m=4, $(k_1, k_2, k_3, k_4) = (1, 0, 0, 0)$ et

$$z_{i+4} = (z_i + z_{i+1}) \mod 2$$

On vérifie que la période est 15.
En effet les 15 premiers éléments de la suite dont

$$100010011010111$$

Ensuite on a $z_{16} = 1$, $z_{17} = 0$, $z_{18} = 0$, $z_{19} = 0$ et donc la suite se répètera à l'identique.

Définition 7.0.1. *L'ensemble constitué par les conditions initiales et les coefficients de la récurrence est appelé un* **régistre à décalage à rétroaction linéaire** *ou* **LSFR**.

L'application de $\left(\mathbb{F}_2\right)^m$ dans lui même qui au vecteur $\begin{pmatrix} u_{m+i-1} \\ u_{m+i-2} \\ \vdots \\ u_{i+1} \\ u_i \end{pmatrix}$ associe le vecteur $\begin{pmatrix} u_{m+i} \\ u_{m+i-1} \\ \vdots \\ u_{i+2} \\ u_{i+1} \end{pmatrix}$ est clairement $\mathbb{F}_2$-liméaire.

Proposition 7.0.2. *Soit $(u_n)_{n\in\mathbb{N}}$ une suite récurrente linéaire de relation de récurrence*

$$z_{m+i} = c_0 z_i + \cdots + c_{m-1} z_{m-1+i} = \sum_{j=0}^{m-1} c_j z_{j+i}$$

La matrice, T, associée à l'application linéaire

$$\mathbb{F}_2^m \longrightarrow \mathbb{F}_2^m$$

$$\begin{pmatrix} u_{m+i-1} \\ u_{m+i-2} \\ \vdots \\ u_{i+1} \\ u_i \end{pmatrix} \longmapsto \begin{pmatrix} u_{m+i} \\ u_{m+i-1} \\ \vdots \\ u_{i+2} \\ u_{i+1} \end{pmatrix}$$

est

$$T = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & & \\ \vdots & & \ddots & \ddots & \\ 0 & 0 & \dots & 0 & 1 \\ c_0 & c_1 & \dots & c_{m-2} & c_{m-1} \end{pmatrix}$$

Cette matrice est appelée la **matrice de transition** *du LSFR*

Démonstration*:* facile □

À une suite récurrente linéaire donné par la relation de récurrence $z_{m+i} = \sum_{j=0}^{m-1} c_j z_{j+i}$ on associe un polynôme, $C(X) = X^m - \sum_{k=1}^{m-1} m c_k X^k$, appelée le ***polynôme caractéristique*** de la récurrence. Les $c_k \neq 0$ avec $1 \leq k \leq m$ sont appelé ***branchements*** pour une raison qui apparaît sur le schéma 7.1 page 52. On peut réaliser sous forme d'un circuit électronique une suite récurrente linéaire de longueur m sur le corps $\mathbb{F}_2$.

On dispose de m mémoires, $(z_i)_{0 \leq i \leq m-1}$, appelées ***bascules*** pouvant chacune contenir un symbole binaire 0 ou 1. Ces cases sont contrôlées par une horloge. À chaque pas d'horloge le contenu de la mémoire z_{i-1} est remplacée par celle de la mémoire z_i pour $1 \leq i \leq m-1$ le contenu de la mémoire z_0 est envoyé à l'extérieur pour être utilisé et le contenu de la mémoire z_{m-1} est remplacé par la combinaison

$$c_0 z_0 + c_1 z_1 + \cdots + c_i z_i + \cdots + c_{m-1} z_{m-1}$$

conformément au schéma de la figure 7.1
Autrement dit dans le fonctionnement d'un LSFR, à chaque pas d'horloge on sort le bit de plus petit poids; tous les bits sont décalés vers la gauche et le bit de plus grand poids est mis à jour par la formule de récurrence.
Il y a une deuxième manière de réaliser un LSFR qui correspond au schéma 7.2 page 52:

On considère les données suivantes:

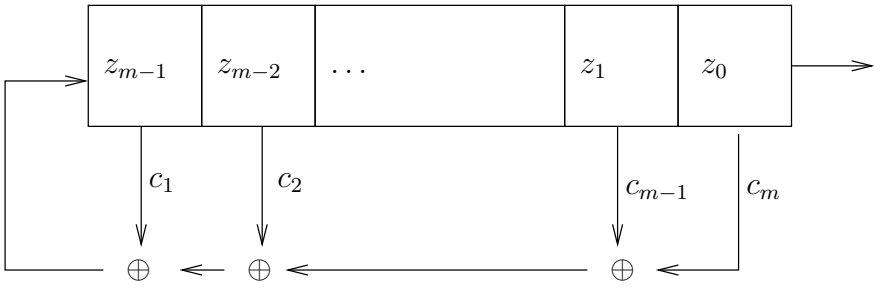


Figure 7.1: Diagramme d'un LSFR (présentation de Fibonacci)

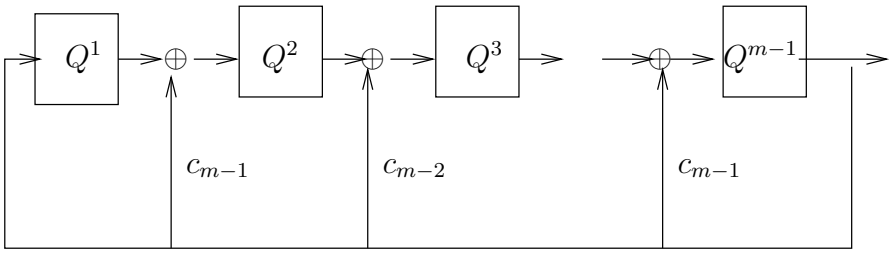


Figure 7.2: Diagramme d'un LSFR (présentation de Galois)

1. un entier m
2. $m-1$ éléments de $\mathbb{F}_2$ $Q_1^{(0)}$, $Q_1^{(0)}$,..., $Q_i^{(0)}$,..., $Q_m^{(0)}$, les conditions initiales
3. m nombres de $\mathbb{F}_2$, a_0, a_1,.., a_i,..., a_{m-1}, a_m avec $a_0 \neq 0$ et $a_m \neq 0$.

À partir de ces données initiales on construit pour $1 \leq i \leq m$ une suite d'éléments de $\mathbb{F}_2$, $k \mapsto Q_i^{(k)}$, de la manière suivante:

$$Q_i^{(k)} = Q_{i-1}^{(k-1)} + a_{i-1} Q_m^{(k-1)} \text{ pour } i \geq 2$$
$$Q_1^{(k)} = Q_m^{(k)}$$

La suite $k \mapsto Q_m^{(k)}$ est un LSFR, appelé LSFR de Galois.

***Exemple* 7.0.4.** $C(X) = X^4 + X^3 + 1$, $z_n = z_{n-3} + z_{n_4}$. La suite de condition initiale $(0, 1, 1, 0)$ se complète en

$$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$$

et ensuite elle est périodique.

7.0.2 Cryptage avec un LSFR.

Pour crypter à l'aide d'un LFSR on commence par transformer le message, M, en une suite binaire (par exemple à l'aide des codes ASCII des symboles), c'est à dire en une suite, $(m_i)_{i\in\mathbb{N}}$, d'éléments de $\mathbb{F}_2$ puis on XORise la suite obtenue avec la suite récurrente linéaire fournie par le LFSR, $(x_i)_{i\in\mathbb{N}}$ pour obtenir le message codé, $(c_i)_{i\in\mathbb{N}}$ sous forme d'une suite d'éléments de $\mathbb{F}_2$:

$$\begin{array}{cccccc} m_0 & m_1 & m_2 & \dots & m_i & \dots \\ \oplus & \oplus & \oplus & \dots & \oplus & \dots \\ x_0 & x_1 & x_2 & \dots & x_i & \dots \\ \hline c_0 & c_1 & c_2 & \dots & c_i & \dots \end{array}$$

Le décodage est symétrique c'est à dire que l'on XORise le message chiffré (supposé être une suite binaire) avec récurrente linéaire fournie par le LFSR. L'exemple suivant on donne un exemple académique de cryptage et décryptage à l'aide d'un LSFR

***Exemple* 7.0.5.** On considère le LSFR sur $\mathbb{F}_2$, défini par la relation de récurrence

$$u_{n+4} = u_{n+1} + u_n$$

et les conditions initiales $(k_0, k_1, k_2, k_3) \in \mathbb{F}_2^4$.

Montrer que pour tout choix de conditions initiales la période de la suite récurrente linéaire $(u_n)_{n\in\mathbb{N}}$ est majorée par 15, (étudier la période de la suite $n \to \alpha^n$ où α est n'importe quelle racine du polynôme $X^4 - X - 1$.

On code par XORisation à l'aide du LFSR précédent avec les conditions initiales $(k_0, k_1, k_2, k_3) = (1, 0, 0, 0)$. Chaque lettre de l'alphabet est codée par le quintuplet $(a_0, a_1, a_2, a_3, a_4)$ tel que $a_0 + 2a_1 + 4a_2 + 8a_3 + 16a_4)$ soit le rang de la lettre dans l'alphabet ordinaire compté entre 1 et 26, le quintuplet $(0, 0, 0, 0, 0)$ correspond à l'espace entre deux mots (exemples: A la première lettre de l'alphabet est codée $(1, 0, 0, 0, 0)$, M la treizième de l'alphabet lettre est codée $(1, 0, 1, 1, 0)$).

Le début de la suite $n \to u_n$ est

$$u_0 = 1,\ u_1 = 0,\ u_2 = 0,\ u_3 = 0,\ u_4 = U_0 + u_1 = 1,\ u_5 = u_1 + u_2 = 0,$$
$$u_6 = u_2 + u_3 = 0,\ u_7 = u_3 + u_4 = 1,\ u_8 = u_4 + u_5 = 1,\ u_9 = u_5 + u_6 = 0, ...$$

Donc si on veut coder MA on le tranforme par le codage précédent en $(0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$ on XORise cette suite fini avec la suite $(u_0, \dots, u_9)$ et il vient

$$0, 1, 1, 1, 0, 1, 0, 0, 0, 0$$

$$\begin{aligned}&\oplus 1,0,0,0,1,0,0,1,1,0\\ =&1,1,1,1,1,1,0,1,1,0\end{aligned}$$

7.1 Utilisation pratique des LFSR en cryptographie.

Les LFSR sont facile à casser (algorithme de Massey-Berlekamp), d'où plusieurs types d'améliorations consistant à utiliser plusieurs LFSR que l'on combine par une ***fonction booléenne*** c'est à dire une fonction d'un ensemble fini dans un ensemble fini. Cette fonction est appelée ***fonction de combinaison*** ou ***fonction de filtrage***. On lui demande de satisfaire certains critères cryptographiques.

Remarquons que le cardinal de l'ensemble, $\mathcal{B}_n$, des fonctions boolénnes de $\mathbb{F}_{2^n}$ dans $\mathbb{F}_2$ est 2^{2^n} et qu'il croit donc extrèmement vite

n	4	5	6	7	8
$\mathcal{B}_n$	2^{16}	2^{32}	2^{64}	2^{128}	2^{256}

Le choix de bonnes fonctions cryptographiques nécessite donc des études mathématiques.

Les améliorations les plus utilisées sont:

- ***Non Linear Combining Generator*** en abrégé ***NLCG***: combinaison booléenne en sortie de plusieurs LFSR.
- ***Non Linear Filter Generator*** en abrégé ***NLFG***: filtrage des registres d'un même LFSR par une fonction booléenne.
- ***Clock Control Generator*** en abrégé ***CCG***: contrôle d'horloge

La fonction booléenne utilisée est appelée ***fonction de combinaison*** ou ***fonction de filtrage***. On lui demande de satisfaire certains critères cryptographiques.

Un NLCG utilise n LFSR dont les sorties sont les entrées d'une fonction booléenne, f, à n variables: $\mathbb{F}_2^n \longrightarrow \mathbb{F}_2$, son diagramme est donné à la figure 7.9 page 61
Un NLFG de longueur m utilise un LFSR (de longueur m) dont les bits sont les entrées d'une fonction booléenne, f, à m variables: $\mathbb{F}_2^m \longrightarrow \mathbb{F}_2$, son diagramme est donné à la figure 7.3 page 55
Nous allons donner trois exemples de fonctions booléennes.

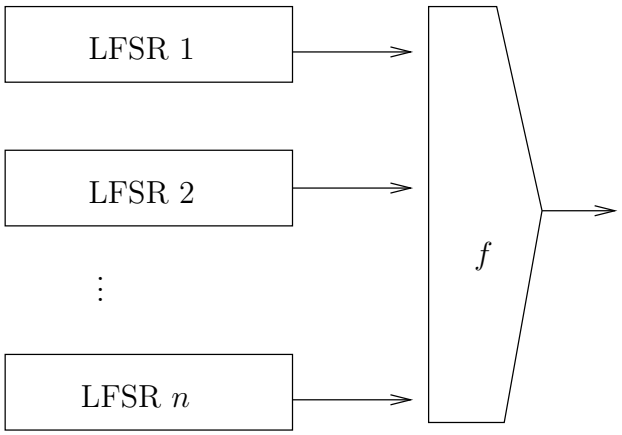


Figure 7.3: Diagramme d'un NLCG

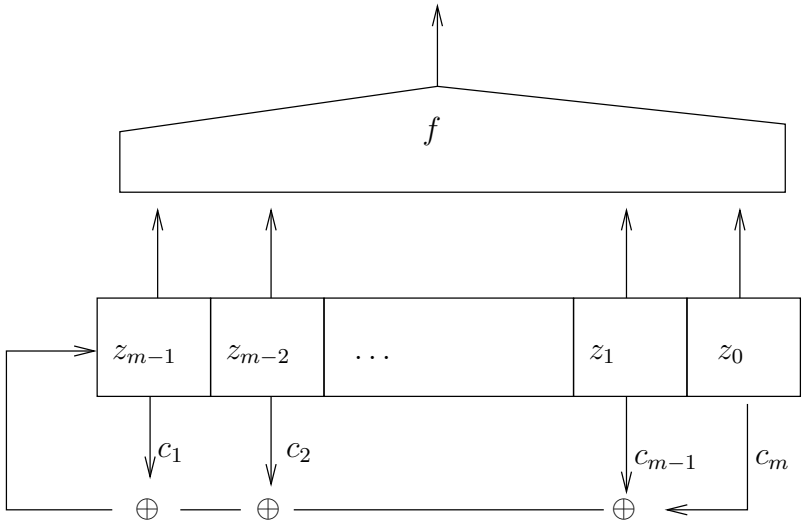


Figure 7.4: Diagramme d'un NLFG

7.1.1 Le système $A5/1$.

Le système $A5/1$ est utilisé pour protéger les liaisons GSM. Il repose sur emploi de trois LFSR, voir la figure 7.7, dont les polynômes a associées sont:

- $C_1(X) = X^{19} + X^{18} + X^{17} + X^{14} + 1$
- $C_2(X) = X^{22} + X^{21} + 1$
- $C_1(X) = X^{23} + X^{22} + X^{21} + X^8 + 1$.

Remarquer que $19+22+23 = 64$, c'est donc le nombre de conditions initiales nécessaires pour pouvoir décrire complètement les trois LFSR.

La synchronisation de ces LFSR est fixée par les bits de déclenchement, s_1, s_2, s_3 situés en position 9, 11, 11 en partant de 0. Le registre est mis à jour si son bit de déclenchement est en accord avec la majorité des trois bits de déclanchement. La fonction de majorité s'écrit

$$\mathrm{Maj}(s_1, s_2, s_3) = (s_1 \wedge s_2) \vee (s_1 \wedge s_3) \vee (s_2 \wedge s_3)$$

où les tables des opérations $\wedge$ ou ***opération "et"*** (multiplication bit à bit modulo 2 sans retenu) et $\vee$ ou ***opération "ou exclusif"*** (addition bit à bit modulo 2 sans retenue) sont donnés par les figures 7.5 et 7.6:

s_1 \ s_2	0	1
0	0	0
1	0	1

Figure 7.5: table de $\wedge$

s_1 \ s_2	0	1
0	0	1
1	1	0

Figure 7.6: table de $\vee$

Donc au moins deux registres sont mis à jour à chaque unité de temps.

La mise à jour des registres est faite de la manière suivante: on calcule b_i par les formules suivantes

$$b_1 = R_1[13] \oplus R_1[16] \oplus R_1[17] \oplus R_1[18]$$
$$b_2 = R_2[20] \oplus R_2[21]$$

$$b_3 = R_3[7] \oplus R_1[20] \oplus R_1[21] \oplus R_1[22]$$

Ensuite si le régistre i est mis à jour on supprime $R_i[m_i]$ ($m_1 = 18$, $m_2 = 21$, $m_3 = 22$) on déplace le contenu de tous les régistres vers la gauche et on insère b_i dans le régistre $R_i[0]$.
Le bit de sortie, b, est

$$b = R_1[18] \oplus R_2[21] \oplus R_3[22]$$

Il peut arriver que le registre i ne soit jamais actualisé.

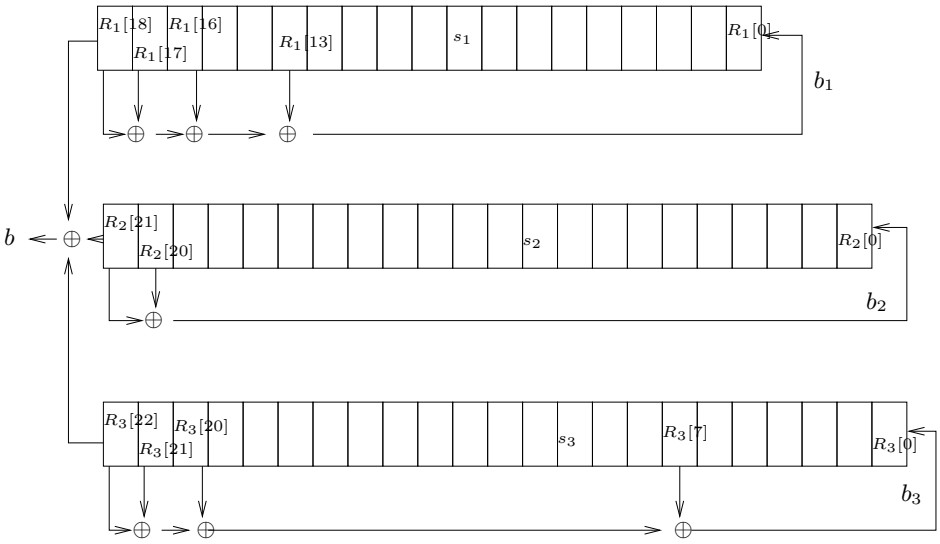


Figure 7.7: Le cryptosystème A5/1

7.1.2 Le système bluetooth/E0.

Le système bluetooth/E0 est un système de sécurisation des communications radio entre une unité centrale et des périphériques (clavier, souris, imprimante,...) reposant sur un système de chiffrage en continu (par flots), $E0$.

Il utilise quatre LFSR donnés par les polyômes

- $C_1(X) = X^{25} + X^{20} + X^{12} + X^8 + 1$

- $C_2(X) = X^{31} + X^{24} + X^{16} + X^{12} + 1$
- $C_3(X) = X^{33} + X^{28} + X^{24} + X^4 + 1$
- $C_4(X) = X^{39} + X^{36} + X^{28} + X^4 + 1$

dont les sorties sont notées x_0, x_1, x_2, x_3. Le flux de sortie du cryptosystème est donné par la boucle suivante:

$$
\begin{aligned}
&y_t = \sum_{i=1}^{4} x_t^i \in \{0,1,2,3,4\} \\
&z_t = (\oplus_{i=1}^{4} x_t^i) \oplus c_t^0 \in \{0,1\} \\
&s_{t+1} = (s_{t+1}^1, s_{t+1}^0) = \left[\frac{y_t + z_t}{2}\right] \in \{0,1,2,3\} \\
&c_{t+1} = (c_{t+1}^1, c_{t+1}^0) = s_{t+1} \oplus T_1(ct) \oplus T_2(c_{t-1} \in \{0,1,2,3\} \quad \text{Sortie : } z_t
\end{aligned}
$$

avec $T_1(x_1, x_0) = (x_1)$, $T_2 = (x_0, x_0 + x_1)$ et où (c_{t+1}^1, c_{t+1}^0) désigne les deux bits d'un nombre compris entre 0 et 3 écrit en base 2 (ici $\oplus$ désigne le "ou exclusif" ou addition sans retenue modulo 2 bit à bit).

***Remarque* 7.1.1.** Les x_i appartiennent á $\{0,1\}$ considéré tantôt comme des éléments de $\mathbb{F}_2$,tantôt comme des éléments de $\mathbb{Z}$, même remarque pour z_t, alors que les y_t, s_t et c_t sont considérés comme des éléments de $\mathbb{Z}$.

Exercices.

7.1.1. Montrer que le LFSR de Galois est effectivement un LFSR.

7.1.2. On considère le LSFR sur $\mathbb{F}_2$, défini par la relation de récurrence

$$u_{n+4} = u_{n+1} + u_n$$

et les conditions initiales $(k_0, k_1, k_2, k_3) \in \left(\mathbb{F}_2\right)^4$.

1. Montrer que pour tout choix de conditions initiales la période de la suite récurrente linéaire $(u_n)_{n\in\mathbb{N}}$ est majorée par 15.
2. On code par XORisation à l'aide du LFSR précédent avec les conditions initiales $(k_0, k_1, k_2, k_3) = (1,0,0,0)$. Chaque lettre de l'alphabet est codée par le quintuplet $(a_0, a_1, a_2, a_3, a_4)$ tel que $a_0 + 2a_1 + 4a_2 + 8a_3 + 16a_4$) soit le rang de la lettre dans l'alphabet ordinaire compté entre 1 et 26, le quintuplet $(0,0,0,0,0)$ correspond à l'espace entre deux mots (exemples: A la première lettre de l'alphabet est codée $(1,0,0,0,0)$, M la treizième de l'alphabet lettre est codée $(1,0,1,1,0)$).

(a) Crypter avec ce LSFR le message suivants *Les sanglots longs des violons de l'automne bercent mon coeur d'une langueur monotone*

(b) Décoder le message page 60.

7.1.3. Vérifier que la fonction de majorité du système A5/Ien est effectivement une.

7.1.4. Donner les suites récurrentes linéaires associées aux trois LFSR du système A5/1.

7.1.5. Étude du système A5/1.
L'ensemble des LSFR R_1, R_2, R_3 comprend 64 régistres. dont les remplissage initial constitue la clef du cryptosystème A5/1.

1. Montrer qu'il existe des états initiaux de R_1 tels que quels que soit les états initiaux de R_2 et R_3, R_1 ne change pas au cours du temps.

2. Confirmer ou Infirmer la phrase suivante: Il existe des clefs différentes de A5/1 qui génèrent une suite constante de zéros ($b = 0$ toujours).

3. Donner une bonne borne inférieure du nombre de clefs de A5/1 qui génére une suite constante de zéros.

1	1	0	0	0	1	0	0	1	0	1	1	0	0	1
1	0	1	0	1	1	0	0	1	0	1	1	1	0	0
1	0	0	0	1	0	0	0	1	0	0	0	0	1	1
0	0	1	1	1	1	0	1	1	0	0	0	1	0	1
1	1	1	1	1	0	0	1	1	0	0	0	0	0	1
0	0	0	1	1	0	0	0	1	0	0	0	1	0	1

Figure 7.8: décodage à l'aide d'un LSFR première partie

1	0	0	0	1	0	1	0	1	1	0	0	1	0	1
1	0	1	1	1	0	0	0	0	0	0	0	0	1	1
1	0	1	0	0	1	0	1	1	0	1	1	0	0	1
0	0	1	0	1	1	0	0	1	1	0	1	1	1	0
0	0	1	0	1	0	0	1	1	0	1	0	1	1	1

Figure 7.9: décodage à l'aide d'un LSFR suite

Chapitre 8

Codes à clefs secrètes.

Devant l'explosion des besoins de cryptages pour des données non-classifiées (c'est à dire non militaires et non diplomatiques) le ***National Bureau of Standards*** des Etats-Unis a lancé un appel d'offre avec un cahier des charges en 1973.

Cet appel d'offre a donné naissance au cryptosystème ***DES*** (***Data Encrytion Standard***). Il a été publié en 1975 et adopté par le NBS en 1977 comme standard de cryptage pour les applications non classifiées. Il reprend les principes et une partie du système de cryptage d'IBM denommé LUCIFER.

Il est à la base d'autres cryptosystèmes plus récents comme IDEA, FEAL, CAST, RC5, BLOW-FISH.

Il est remplacé aujourd'hui par ***AES*** (***Advanced Encrytion Standard***) de J. Daeme et V. Rijmen, basé sur le même principe avec une clé plus longue (128 à 256 bits), plus structuré et avec des fonctionnalités plus étendues. AES a été retenu en 2000 après un appel d'offre international.

Nous allons tout d'abord décrire un modèle assez général de système cryptographique à clef publique, les réseaux de substitution-permutation, qui modélise assez nien et DES et AES ainsi que deux méthodes d'attaque contre ce modèle, la cryptanalyse linéaire et la cryptanalyse différentielle. Ces deux attaques font partie des attaques classiques contre ce type de système et elles ont démontré leur efficacité contre des systèmes proposés concurremment à DES et AES.

8.1 Réseaux de substitution-permutation.

Nous allons décrire un schéma de chiffrement assez général les ***réseaux de substitution-permutation*** qui couvrent des systèmes classiques de chiffrement à clef secrète ainsi que deux méthodes d'attaques contre eux la ***cryptanalyse linéaire*** et la ***cryptanalyse différentielle***.

Un réseaux de substitution-permutation est un type particulier d'algorithme de chiffrement itéré qui modélise bien les deux exemples de chiffrement itérés que nous décrirons le DES et l'AES. C'est un algorithme de chiffrement itérés par blocs.Il répète N_e fois un algorithme de chiffrement, g, appelé fonction d'étage. On introduit une clef secrète K à partir de laquelle on construit N_e+1 sous-clefs, K^1, K^2,..., K^{N_e+1}, appelées ***clefs d'étages***. L'algorithme qui permet de construire les K^i à partir de K est appelé l'***algorithme de diversification*** des clefs

On se donne deux entiers ℓ et m. Un texte clair et un texte chiffré seront des vecteurs de $\mathbb{F}_2^{\ell m}$ donc des vecteurs de longuer $\ell.m$ constitués de 0 et et 1. On se donne aussi une permutation

$$\pi_S : \{0,1\}^\ell \longrightarrow \{0,1\}^\ell$$

et une permutation

$$\pi_P : \{1,2,\ldots,\ell m\} \longrightarrow \{1,2,\ldots,\ell m\}$$

Une chaîne binaire $x = (x_1, x_2, \ldots, x_{\ell m}) \in \{0,1\}^{\ell m}$ peut être considérée comme la concaténation de m sous chaînes de longueur ℓ

$$x = x_{(1)}||x_{(2)}||\ldots||x_{(m)}$$

et pour $1 \leq i \leq m$ on a

$$x_{(i)} = (x_{(i-1)\ell+1}, \ldots, x_{i\ell}).$$

On notera $w^e = (w_i^{e-1})_{1\leq i\leq \ell m}$ la chaine d'entrée à l'étage e qui est en fait la chaîne de sortie de l'étage $e-1$. L'algorithme consiste dans les étapes suivantes

1. XORiser w^{e-1} avec la clef de l'étage e, K^e; on note le résultat

$$u^e = \begin{cases} (u_1^e, u_2^e, \ldots, u_{\ell m}^e) \\ u_{(1)}^e||u_{(2)}^e||\ldots||u_{(m)}^e \end{cases} \qquad \text{avec } u_{(i)}^e = (u_{(i-1)\ell+1}^e, \ldots, u_{i\ell}^e)$$

2. Appliquer la permutation π_S à chacune des***S*-boîtes**, ou chaînes, $u^e_{(i)}$, on note le résultat

$$v^e = \begin{cases} (v^e_1, v^e_2, \dots, v^e_{\ell m}) \\ v^e_{(1)} || v^e_{(2)} || \dots || v^e_{(m)} \end{cases} \qquad \text{avec } v^e_{(i)} = (v^e_{(i-1)\ell+1}, \dots, v^e_{i\ell})$$

3. Appliquer la permutation π_P au indices de v^e, On note w^e le résultat, c'est à dire que

$$w^e = v^e_{\pi_P(1)}, v^e_{\pi_P(2)}, \dots, v^e_{\pi_P(\ell m)}$$

4. À la sortie de l'étage N_e, XORiser v^{N_e} avec K^{N_e+1}, c'est le message codé y, donc $y = v^{N_e} \oplus K^{N_e+1}$.

***Exemple* 8.1.1.** . Cet exemple est tiré de [31] On suppose $\ell = m = N_e = 4$. On code l'héxadécimal sur des quadruplets de 0 où de 1 de la manière suivante

$$0 \mapsto (0,0,0,0), \quad 1 \mapsto (0,0,0,1), \dots, \quad 9 \mapsto (1,0,0,1),$$
$$A \mapsto (1,0,1,0), \quad F \mapsto (1,1,1,1)$$

On défint π_S de la manière suivante (l'entrée et la sortie sont en héxadécimal)

z	0	1	2	3	4	5	6	7	8	9	A	b	C	D	E	F
$\pi_S(z)$	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

À chaque étage $1 \leq i \leq 4$ on 4 S-boîtes notée S^i_j avec $1 \leq j \leq 4$ sur lesquelles agit la permutation π_S.

La permutation π_P définie de la manière suivante (l'entrée et la sortie sont des nombres ordinaires)

z	1	2	3	4	5	6	7	8	9
$\pi_S(z)$	1	5	9	13	2	6	10	14	3

z	10	11	12	13	14	15	16
$\pi_S(z)$	7	11	15	4	8	12	16

agit donc sur le mot formé des sorties des 4 S-boîtes.

L'algorithme de diversification de la clef ets le suivant. On part d'une clef $K = (k_1, \dots, k_{32}) \in \{0,1\}^{32}$ sur 32 bits et on définit K^e comme les 16 bits consécutifs de K commençant par k_{4e-3}.

On suppose maintenant que la clef est

$$K = \quad 0011 \quad 1010 \quad 1001 \quad 0100 \quad 1101 \quad 0110 \quad 0011 \quad 1111$$

Les sous-clefs sont alors

$$\begin{array}{rcccc} K^1 = & 0011 & 1010 & 1001 & 0100 \\ K^2 = & 1010 & 1001 & 0100 & 1101 \\ K^3 = & 1001 & 0100 & 1101 & 0110 \\ K^4 = & 1101 & 0110 & 0011 & 1111 \end{array}$$

Si on part du texte clair

$$x \quad = 0010 \quad 0110 \quad 1011 \quad 0111$$

Le chiffrement s'effectue alors de la manière suivante : le texte en clair est $x = w^0 = 0010 \quad 0110 \quad 1011 \quad 0111$

$$\begin{array}{rcccc} w^0 & = 0010 & 0110 & 1011 & 0111 \\ K^1 = & 0011 & 1010 & 1001 & 0100 \\ u^1 = & 0001 & 1100 & 0010 & 0011 \\ v^1 = & 0100 & 0101 & 1101 & 0001 \\ w^1 = & 0010 & 1110 & 0000 & 0111 \\ K^2 = & 1010 & 1001 & 0100 & 1101 \\ u^2 = & 1000 & 0111 & 0010 & 1010 \\ w^2 = & 0100 & 0001 & 0010 & 1000 \\ K^3 = & 1001 & 0100 & 1101 & 0110 \\ u^3 = & 1101 & 0101 & 0110 & 1110 \\ v^3 = & 1001 & 1111 & 1011 & 0000 \\ w^3 = & 1110 & 0100 & 0110 & 1110 \\ K^4 = & 0100 & 1101 & 0110 & 0011 \\ u^4 = & 1010 & 1001 & 0000 & 1101 \\ v^4 = & 0110 & 1010 & 1110 & 1001 \\ K^5 = & 1101 & 0110 & 0011 & 1111 \\ y = & 1011 & 1100 & 1101 & 0110 \end{array}$$

y est le texte chiffré. Tout ceci est résumé dans le diagramme 8.1 page 66

8.2 Cryptanalyse linéaire.

La cryptanalyse linéaire peut être appliquée contre tout algorithme de chiffrement itéré comme les réseaux de substitution-permutation (l'exposé ci-après est tiré de l'excellent tutorial de Howard M. Heys disponible sur internet). Il s'agit d'un attaque à texte clair connu. On dispose donc d'un grand nombre des paires de textes clairs et du texte correspondant chiffré.

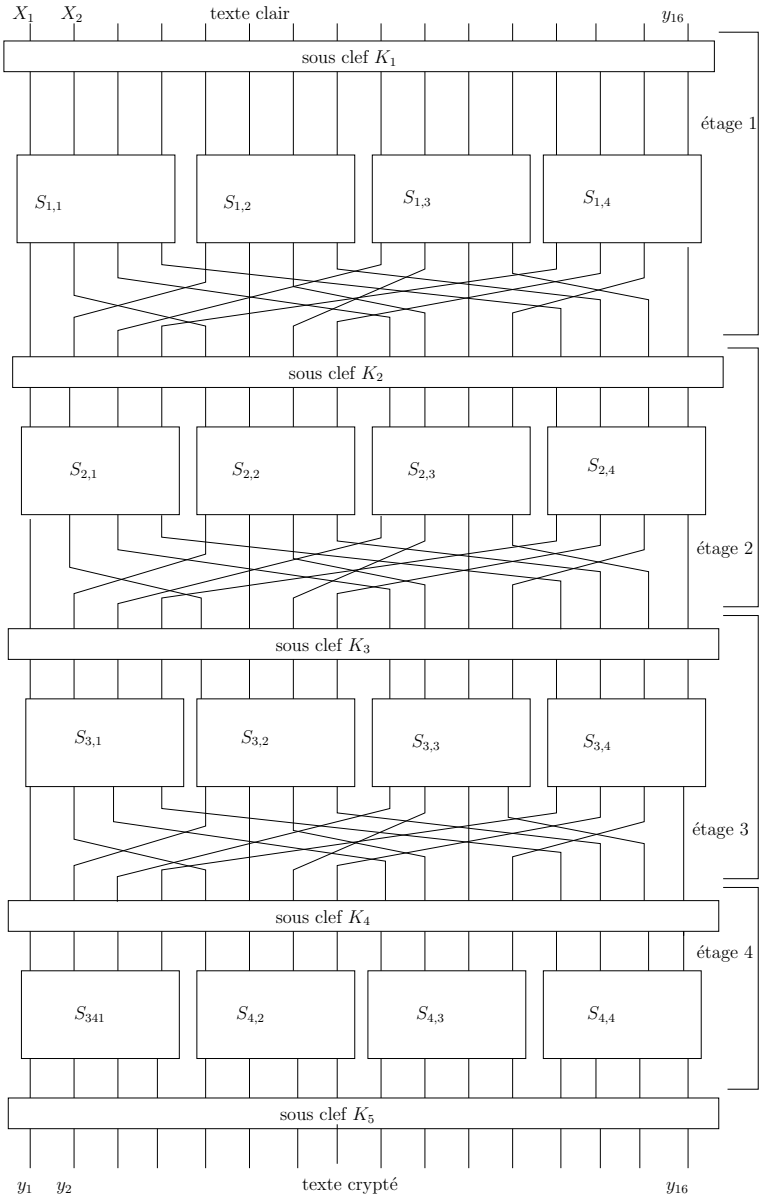


Figure 8.1: Réseau de substitution permutation

Nous montrerons seulement comment déterminer des parties de la clef du dernier étage, la clef K^5 dans notre exemple, il faut ensuite tirer partie de

cette information.

On suppose qu'il existe une $\mathbb{F}_2$-combinaison linéaire des bits d'entrée et de sortie qui ait lieu avec une probabilité nettement supérieure ou nettement inférieure à $\frac{1}{2}$. Autrement dit qu'il existe $i_1, i_2, \ldots, i_u$ et $j_1, j_2, \ldots, j_v$ tels que si $x = (X_1, X_2, \ldots X_N$ sont les bits d'entrée (du message en clair) considérés comme des variables aléatoires définies sur $\{0,1\}$ et $Y_1, Y_2, \ldots, Y_m$ sont les bits de la sortie (du message chiffré) considérés comme des variables aléatoires définies sur $\{0,1\}$ on ait

$$\mathbf{Pr}\left\{X_{i_1} \oplus X_{i_2} \oplus \cdots \oplus X_{i_n} \oplus Y_{j_1} \oplus Y_{j_2} \oplus \cdots \oplus Y_{j_m} = 0\right\} >> \frac{1}{2}$$

Le principe est alors d'approximer une partie de l'algorithme de chiffrement par cette combinaison linéaire sur $\mathbb{F}_2$.

Le succès de cette méthode repose sur le lemme suivant qui nécessite des hypothèses rarement vérifiée en pratique mais qui heuristiquement justifie la méthode.

Lemme 8.2.1 (Lemme d'emplilement)**.** *Soit des variables aléatoires indépendantes $\mathbf{X}_1, \ldots, \mathbf{X}_r$ définies sur l'ensemble $\{0,1\}$ et on suppose que pour $1 \leq i \leq r$ il existe des nombres réels $0 \leq p_i \leq 1$ tels que*

$$\mathbf{Pr}\left\{\mathbf{X}_i = 0\right\} = p_i$$

On définit le biais ϵ_i de la variable aléatoire $\mathbf{X}_i$ par

$$\epsilon_i = p_i - \frac{1}{2}, \quad -\frac{1}{2} \leq \epsilon_i \leq \frac{1}{2}$$

alors le biais, $\epsilon_{i_1,i_2,\ldots,i_n}$ de la variable aléatoire $\mathbf{X}_{i_1} \oplus \mathbf{X}_{i_2} \oplus \cdots \oplus \mathbf{X}_{i_n}$ est

$$\epsilon_{i_1,i_2,\ldots,i_n} = 2^{n-1} \prod_{j=1}^{n} \epsilon_{i_j}$$

Démonstration*:* Voir [31]. □

***Exemple* 8.2.1.** On continue l'exemple 8.1.1 On considère la S-boîte de l'exemple et on considère chacune des entrées $x_i \in \{0,1\}$, $1 \leq i \leq 4$, de la S-boîte comme une variable aléatoire que l'on note $\mathbf{X}_i$ et de même on considère la sortie $y_j \in \{0,1\}$, $1 \leq j \leq 4$, de la S-boîte comme une variable aléatoire que l'on note $\mathbf{Y}_j$. Le tableau 8.2 page 68 enumère les valeurs possibles des 8 variables aléatoires $\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3, \mathbf{X}_4, \mathbf{Y}_1, , \mathbf{Y}_2, \mathbf{Y}_3, \mathbf{Y}_4$:

$\mathbf{X}_1$	$\mathbf{X}_2$	$\mathbf{X}_3$	$\mathbf{X}_4$	$\mathbf{Y}_1$	$\mathbf{Y}_2$	$\mathbf{Y}_3$	$\mathbf{Y}_4$
0	0	0	0	1	1	1	0
0	0	0	1	0	1	0	0
0	0	1	0	1	1	0	1
0	0	1	1	0	0	0	1
0	1	0	0	0	0	1	0
0	1	0	1	1	1	1	1
0	1	1	0	1	0	1	1
0	1	1	1	1	0	0	0
1	0	0	0	0	0	1	1
1	0	0	1	1	0	1	0
1	0	1	0	0	1	1	0
1	0	1	1	1	1	0	0
1	1	0	0	0	1	0	1
1	1	0	1	1	0	0	1
1	1	1	0	0	0	0	0
1	1	1	1	0	1	1	1

Figure 8.2: valeurs possibles des 8 variables aléatoires $\mathbf{X}_i, \mathbf{Y}_i$

Les entrées des quatres premières colonnes sont ligne par ligne simplement les valeurs d'entrées rangées par ordre lexicographique. Les entrées des 4 dernières colonnes sont les valeurs correspondantes de π_S.

On considère la variable aléatoire $\mathbf{X}_1 \oplus \mathbf{X}_4 \oplus \mathbf{Y}_2$. La probabilité qu'elle prenne la valeur 0 s'obtient par exemple en comptant le nombre de ligne du tableau précédent pour les quelles

$$\mathbf{X}_1 \oplus \mathbf{X}_4 \oplus \mathbf{Y}_2 = 0$$

et en divisant par le nombre de lignes, soit $16 = 2^4$. On voit facilement que

$$\mathbf{Pr}\left\{\mathbf{X}_1 \oplus \mathbf{X}_4 \oplus \mathbf{Y}_2 = 0\right\} = \mathbf{Pr}\left\{\mathbf{X}_1 \oplus \mathbf{X}_4 \oplus \mathbf{Y}_2 = 1\right\} = \frac{1}{2} \tag{8.1}$$

Le biais de la variable aléatoire $\mathbf{X}_1 \oplus \mathbf{X}_4 \oplus \mathbf{Y}_2 = 0$ est donc 0.

Par contre il est facile de voir que le biais de la variable aléatoire $\mathbf{X}_3 \oplus \mathbf{X}_4 \oplus \mathbf{Y}_1 \oplus \mathbf{Y}_2$ vaut $-\frac{3}{8}$. Il n'est pas difficiel de calculer les biais des $2^8 = 256$ variables aléatoires de cette forme.

On utilise pour représenter tous ces biais la notion suivante. Chaque variable aléatoire est écrite sous la forme

$$\Big(\bigoplus_{i=1}^{4} a_i \mathbf{X}_i\Big) \oplus \Big(\bigoplus_{i=1}^{4} b_i \mathbf{Y}_i\Big), \quad a_i, b_i \in \{0,1\}$$

Pour rendre la notation plus compacte on traite chacun des vecteurs binaires (i.e. composés d'élements de $\mathbb{F}_2$) (a_1, a_2, a_3, a_4) et (b_1, b_2, b_3, b_4) comme des nombres hexadécimaux (appelés ***somme d'entrée*** et ***somme de sortie***). De cette façon chacune des 256 variables aléatoires est nommé par une paire unique de nombres hexadéimaux (a, b).

Par exemple la variable aléatoire $\mathbf{X}_1 \oplus \mathbf{X}_4 \oplus \mathbf{Y}_2$ a pour somme d'entrée $(1, 0, 0, 1)$ qui vaut 9 en hexadécimal et pour somme de sortie $(0, 1, 0, 0)$ qui vaut 4 en hexadécimal.

Pour une variable aléatoire possédant la somme d'entrée $a = (a_1, a_2, a_3, a_4)$ et $b = (b_1, b_2, b_3, b_4)$ pour somme de sortie on note $N_L(a, b)$ le nombre de 8-uplets binaires $(x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4)$ tels que

$$(y_1, y_2, y_3, y_4) = \pi_S(x_1, x_2, x_3, x_4)$$

et

$$\Big(\bigoplus_{i=1}^{4} a_i x_i\Big) \oplus \Big(\bigoplus_{i=1}^{4} b_i y_i\Big) = 0$$

Le biais,$\epsilon(a, b)$, de la variable aléatoire ayant a et b comme somme d'entrée et de sortie est donné par

$$\epsilon(a, b) = \frac{N_L(a, b) - 8}{16}$$

La table qui contient toutes les valeurs de N_L est appelée la ***table d'approximation linéaire***. On donne à la page 70 la table d'approximation linéaire 8.3 pour le réseau de substitution-permutation étudié

Pour faire une cryptanalyse linéaire d'un réseau de substitution-permutation il faut un ensemble d'approximations linéaires des S-boîtes qui pourront être utilisé pour obtenir une approximation linéaire d'un réseau de substitution-permutation moins le dernier étage. On montre comment marche le procédé sur l'exemple 8.1.1.

***Exemple* 8.2.2.** Considérons le réseau de substitutions-permutations décrit dans l'exemple 8.1.1 64. On veut en trouver une approximation linéaire

a \ b	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
1	8	8	6	6	8	8	6	14	10	10	8	8	10	10	8	8
2	8	8	6	6	8	8	6	6	8	8	10	10	8	8	2	10
3	8	8	8	8	8	8	8	8	10	2	6	6	10	10	6	6
4	8	10	8	6	6	4	6	8	8	6	8	10	10	4	10	8
5	8	6	6	8	6	8	12	10	6	8	4	10	8	6	6	8
6	8	10	6	12	10	8	8	10	8	6	10	12	6	8	8	6
7	8	6	8	10	10	4	10	8	6	8	10	8	12	10	8	10
8	8	8	8	8	8	8	8	8	6	10	10	6	10	6	6	2
9	8	8	6	6	8	8	6	6	4	8	6	10	8	12	6	10
A	8	12	6	10	4	8	10	6	10	10	8	8	10	10	8	8
B	8	12	8	4	12	8	12	8	8	8	8	8	8	8	8	8
C	8	6	12	6	6	8	10	8	10	8	10	12	8	10	8	6
D	8	10	10	8	6	12	8	10	4	6	10	8	10	8	8	10
E	8	10	10	8	6	4	8	10	6	8	8	6	4	10	8	8
F	8	6	4	6	6	8	10	8	8	6	12	6	6	8	10	8

Figure 8.3: table d'approximation linéaire

partielle de la forme

$$x_{i_1} \oplus x_{i_2} \oplus \cdots \oplus x_{i_u} \oplus y_{j_1} \oplus y_{j_2} \oplus \cdots \oplus y_{j_v} = 0 \tag{8.2}$$

En fait on se contentera d'une qppromation linéaire probabiliste, c'est à à dire qu'on demande que les variables aléatoires correspondantes vérifient cette relations avec un biais impotant c'est à dire que l'on demande

$$\mathbf{Pr}\left\{\mathbf{X}_{i_1} \oplus \mathbf{X}_{i_2} \oplus \cdots \oplus \mathbf{X}_{i_u} \oplus \mathbf{Y}_{j_1} \oplus \mathbf{Y}_{j_2} \oplus \cdots \oplus \mathbf{Y}_{j_v} = 0\right\} >> \frac{1}{2} \text{ ou } << \frac{1}{2} \tag{8.3}$$

Par exemple dans la S-boîte de notre exemple la relation

$$\mathbf{X}_1 \oplus \mathbf{X}_2 \oplus \mathbf{Y}_1 \oplus \mathbf{Y}_3 \oplus \mathbf{Y}_4 = 0$$

a lieu avec un biais égal à $\frac{1}{4}$, comme on le montre facilement en étudiant la table d'approximation linéaire, ref. 8.3.

À partir des approximations linéaires locales des S-boîtes on peut obtenir une approximation linéaire globale du type de la relation 8.2. On utilise les approximations linéaires suivantes des S-boîtes $S_{i,j}$:

$$S_{1,2} : \mathbf{X}_1 \oplus \mathbf{X}_3 \oplus \mathbf{X}_4 = \mathbf{Y}_2 \text{ avec biais } + \frac{1}{4}$$
$$S_{2,2} : \mathbf{X}_2 = \mathbf{Y}_2 \oplus \mathbf{Y}_4 \text{ avec biais } - \frac{1}{4}$$
$$S_{3,2} : \mathbf{X}_2 = \mathbf{Y}_2 \oplus \mathbf{Y}_4 \text{ avec biais } - \frac{1}{4}$$
$$S_{3,4} : \mathbf{X}_2 = \mathbf{Y}_2 \oplus \mathbf{Y}_4 \text{ avec biais } - \frac{1}{4}$$

On note $\mathbf{U}_i$, respectivement $\mathbf{V}_i$, les variables aléatoires correspondant aux 16 bits d'entrée de l'étage i, respectivement aux 16 bits de sorties de l'étage i. La variable aléatoire correspondant au j-ème bit d'entrée de l'étage i, respectivement au j-ème bit d'e sortie de l'étage i sera notée $\mathbf{U}_{i,j}$, respectivement $\mathbf{V}_{i,j}$. Autrement dit $\mathbf{U}_i = (\mathbf{U}_{i,j})_{1 \leq j \leq 16}$ et $\mathbf{V}_i = (\mathbf{V}_{i,j})_{1 \leq j \leq 16}$. On note ausse $\mathbf{X}$ le texte clair et $\mathbf{Y}$ le texte crypté.

On ne cherche une approximation linéaire que pour les 3 premiers étages on obtiendra ainsi quelques bits de la clef K_5.

On a $\mathbf{U}_1 = \mathbf{X} \oplus K_1$. On utile l'approximation linéaire de $S_{1,2}$ pour le premier étage et il vient avec un biais de $\frac{1}{4}$

$$\mathbf{V}_{1,6} = \mathbf{U}_{1,5} \oplus \mathbf{U}_{1,7} \oplus \mathbf{U}_{1,8}$$

(8.4)

Pour l'approximation linéaire du 2-ième étage il vient avec un biais de $-\frac{1}{4}$

$$\mathbf{V}_{2,6} \oplus \mathbf{V}_{2,8} = \mathbf{U}_{2,6}$$

Comme $\mathbf{U}_{2,6} = \mathbf{V}_{1,6} \oplus K_{2,6}$ on a alors une approximation linéaire de la forme avec biais $-\frac{1}{4}$

$$\mathbf{V}_{2,6} \oplus \mathbf{V}_{2,8} = \mathbf{V}_{1,6} \oplus K_{2,6}$$

En combinant avec 8.4 on obtient la relation

(8.5) $\mathbf{V}_{2,6} \oplus \mathbf{V}_{2,8} \oplus mathbf X_5 \oplus \mathbf{X}_7 \oplus \mathbf{X}_8 \oplus K_{1,5} \oplus K_{1,7} oplus K_{1,8} \oplus K_{2,6} = 0$

dont le biais est $-\frac{1}{8}$.

Au 3-ième étage on l'approximation avec biais de $-\frac{1}{4}$

$$\mathbf{V}_{3,6} \oplus \mathbf{V}_{3,8} = \mathbf{U}_{3,6}$$

et aussi avec biais de $-\frac{1}{4}$

$$\mathbf{V}_{3,14} \oplus \mathbf{V}_{3,16} = \mathbf{U}_{3,14}$$

et comme $\mathbf{U}_{3,6} = \mathbf{V}_{2,6} \oplus K_{3,6}$ et $\mathbf{U}_{3,14} = \mathbf{V}_{2,8} \oplus K_{3,14}$ on a

$$\mathbf{V}_{3,6} \oplus \mathbf{V}_{3,8} \oplus \mathbf{V}_{3,14} \oplus \mathbf{V}_{3,16} \oplus \mathbf{V}_{2,6} \oplus K_{3,6} \oplus \mathbf{V}_{2,8} \oplus K_{3,14} = 0 \tag{8.6}$$

avec biais $+\frac{1}{8}$.

En combinant (8.5) et (8.6) il vient

$$\mathbf{V}_{3,6} \oplus \mathbf{V}_{3,8} \oplus \mathbf{V}_{3,14} \oplus \mathbf{V}_{3,16} \oplus \mathbf{X}_5 \oplus \mathbf{X}_7 \oplus \mathbf{X}_8 \oplus \\ \oplus K_{1,5} \oplus K_{1,7} \oplus K_{3,6} \oplus K_{3,14} = 0$$

Remarquons que

$$\begin{aligned} \mathbf{U}_{4,6} &= \mathbf{V}_{3,6} \oplus K_{4,6} \\ \mathbf{U}_{4,8} &= \mathbf{V}_{3,14} \oplus K_{4,8} \\ \mathbf{U}_{4,14} &= \mathbf{V}_{3,8} \oplus K_{4,14} \\ \mathbf{U}_{4,16} &= \mathbf{V}_{3,16} \oplus K_{4,16} \end{aligned}$$

il suffit de regarder le diagramme 8.1 page 66.

Il vient alors avec biais $-\frac{1}{32}$

$$\mathbf{U}_{4,6} \oplus \mathbf{U}_{4,8} \oplus \mathbf{U}_{4,14} \oplus \mathbf{U}_{4,16} \oplus \mathbf{X}_5 \oplus \mathbf{X}_7 \oplus \mathbf{X}_8 \oplus \Sigma_K = 0$$

avec

$$\Sigma_K = K_{1,5} \oplus K_{1,7} \oplus K_{3,6} \oplus K_{3,14} \oplus K_{4,6} \oplus K_{4,8} \oplus K_{4,14} \oplus K_{4,16}$$

Donc Σ_K est fixé et vaut 0 ou 1 puisque que l'on suppose que l'on fait une cryptanalyse avec des messages cryptés avec la même clef. Par conséquent

$$\mathbf{U}_{4,6} \oplus \mathbf{U}_{4,8} \oplus \mathbf{U}_{4,14} \oplus \mathbf{U}_{4,16} \oplus \mathbf{X}_5 \oplus \mathbf{X}_7 \oplus \mathbf{X}_8 = 0$$

avec probabilité $\frac{15}{32}$ ou $1 - \frac{15}{32} = \frac{17}{32}$ suivant que $\Sigma_K = 0$ ou 1.

Donc finalement on a une approximation linéaire partielle des 3 premiers étages avec un biais de $\pm\frac{1}{32}$. Tout ceci est résumé dans le diagramme 8.4 page 73.

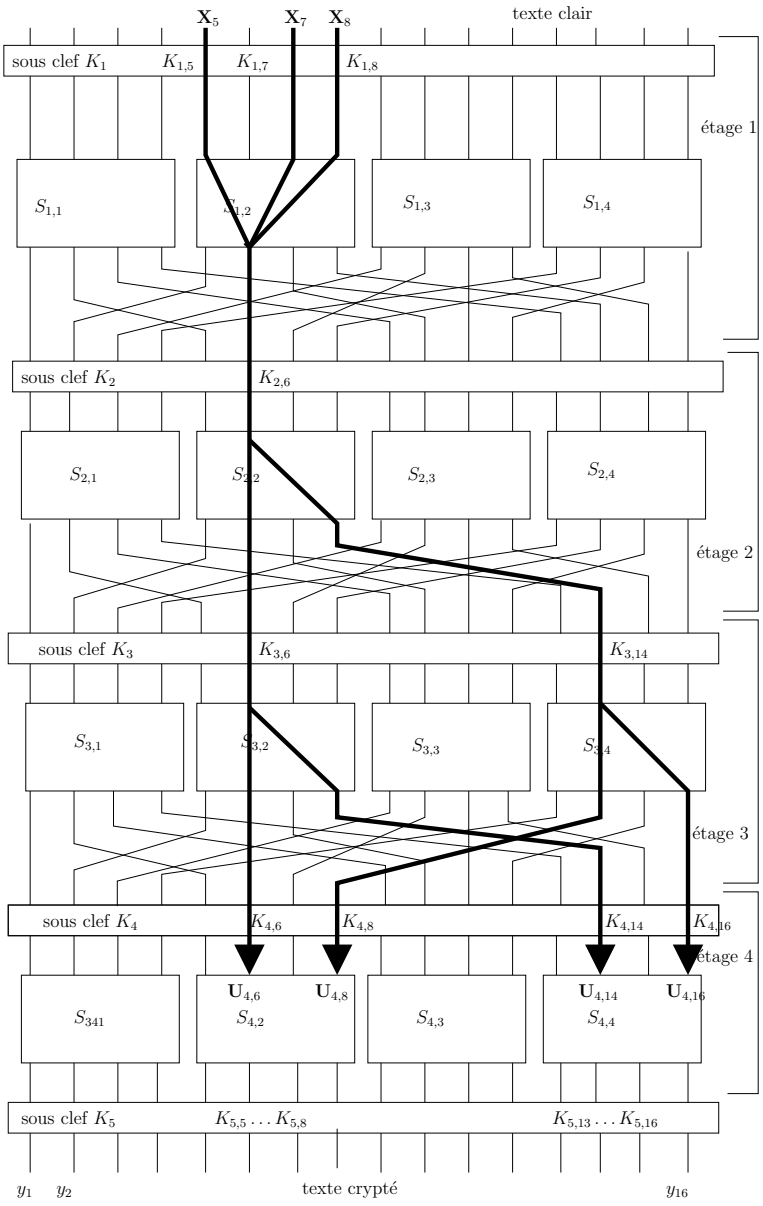


Figure 8.4: Approximation linéaire

Nous montrons comment cette information peut-être utilisée pour calculer quelques bits de la clef. On suppose que l'on a T paires de texte clair et de

texte chiffré. On va montrer comment cette attaque permet de récupérer 8 bits de la clef K_5, à savoir les bits

$$K_{5,5},\ K_{5,6},\ K_{5,7},\ K_{5,8},\ K_{5,13},\ K_{5,14},\ K_{5,15},\ K_{5,16}$$

Il y a $256 = 2^8$ possibilités différentes pour ces 8 bits.

On note $\mathscr{T}$ l'ensemble des T paires de texte clair et de texte chiffré. Pour chaque couple $(x, y) \in \mathscr{T}$ et pour chaque sous-clef K_5 candidate il est possibleen XORisant y avec la clef K_5 et en appliquant π_P^{-1} et π_S^{-1} de calculer les quantités $u_{4,6}, u_{4,8}, u_{4,14}, u_{4,16}$ et ensuite de calculer les valeurs

$$x_5 \oplus x_7 \oplus x_8 \oplus u_{4,6} \oplus u_{4,8} \oplus u_{4,14} \oplus u_{4,16}$$

prises par la variables aléatoire correspondante

$$\mathbf{T} := \mathbf{U}_{4,6} \oplus \mathbf{U}_{4,8} \oplus \mathbf{U}_{4,14} \oplus \mathbf{U}_{4,16} \oplus \mathbf{X}_5 \oplus \mathbf{X}_7 \oplus \mathbf{X}_8$$

Pour chacune des 256 sous-clefs on a un compteur que l'on incrémente toute les fois que la variable aléatoire $\mathbf{T}$ prend la valeur zéro pour un couple $(x, y) \in \mathscr{T}$. On s'attend, et c'est ce qui se produit en pratique, que pour la plupart des sous-clefs la valeur du compteur soit à peu près $\frac{T}{2}$ et que pour la sous-clef correcte la valeur du compteur soit proche de $\frac{T}{2} \pm \frac{T}{32}$. On identifie ainsi 8 bits de la sous-clef K_5.

Un calcul de complexité montre que si une approximation linéaire a un biais de ϵ il faudra un nombre de paires de texte clair et de texte chiffrée de l'ordre de $c\epsilon^{-2}$ où la constante c est petite.

8.3 Cryptanalyse différentielle.

La cryptanalyse différentielle utilise la comparaison du XOR de deux entrée avec le XOR des deux sorties correspondantes.

On considère $x' = (x'_1\ x'_2 \dots\ x'_n)$ et $x'' = (x''_1\ x''_2 \dots\ x''_n)$ deux entrées et $y' = (y'_1\ y'_2 \dots\ y'_n)$ et $y'' = (y''_1\ y''_2 \dots\ y''_n)$ les sorties correspondantes. On note

$$\Delta x = x' \oplus x'' = (x'_1 \oplus x''_1 \dots\ x'_n \oplus x''_n)$$
$$\Delta y = y' \oplus y'' = (y'_1 \oplus y''_1 \dots\ y'_n \oplus y''_n)$$

On traite les couples d'entrée et de sortie comme des variables aléatoires que l'on note $\mathbf{X}, \mathbf{Y}, \Delta\mathbf{X}, \Delta\mathbf{Y}$. Si le système cryptographique était parfait la

probabilité pour qu'un Δy provienne d'un Δx devrait être de $\frac{1}{2^n}$ où n est le nombre de bits de $\mathbf{X}$. La cryptanalyse différentielle exploite le fait qu'il peut arriver qu'un Δy particulier arrive avec une très grande probabilité , $p_D >> \frac{1}{2^n}$, d'un Δx particulier. Le coupe $(\Delta x, \Delta y)$ est appelée une différentielle.

Il s'agit d'une attaque à texte clair choisi. On suppose que le cryptanalyste dispose d'un grand nombre de quadruplets (x',x",y',y") où la valeur de Δx est fixée et que tous les textes sont chiffrés avec la même clef inconnue K. Pour chacun des quadruplets on commence par déchiffrer y' et y'' en utilisant toutes les sous clefs candidates pour le dernier étage.

On commence par regarder les caractéristiques différentielles des S-boîtes. On remarque que dans ce cas $\Delta y = \pi_S(x') \oplus \pi_S(x'')$. On reprend l'exemple 8.1.1 et on examine les caractéristiques différentielles de ses S-boîtes

***Exemple* 8.3.1.** On considère la S-boîtes de l'exemple 8.1.1. On fixe un $\Delta x = (1011)$. On peut réaliser ce Δx à l'aide des couples (x', x'') suivants

$$\Delta^{-1}(1011) = \{(0000,\ 1011),\ (000,\ 1010), \ldots,\ (1111,\ 0100)\}$$

Pour chaque couple (x', x'') de $\Delta^{-1}(1011)$ on calcule le $\Delta y = \pi_S(x') \oplus \pi_S(x'')$ correspondant, il vient :

(8.7)

x'	x''	$y' = \pi_S(x')$	$y'' = \pi_S(x'')$	$\Delta y = y' \oplus y''$
0000	1011	1110	1100	0010
0001	1010	0100	0110	0010
0010	1001	1101	1010	0111
0011	1000	0001	0011	0010
0100	1111	0010	0111	0101
0101	1110	1111	0000	1111
0110	1101	1011	1001	0010
0111	1100	1000	0101	1101
1000	0011	0011	0001	0010
1001	0010	1010	1101	0111
1010	0001	0110	0100	0010
1011	0000	1100	1110	0010
1100	0111	0101	1000	1101
1101	0110	1001	1011	0010
1110	0101	0000	1111	1111
1111	0100	0111	0010	0101

La dernière colonne du tableau donne la distribution de Δy

0000	0001	0010	0011	0100	0101	0110	0111
0	0	8	0	0	2	0	2

1000	1001	1010	1011	1100	1101	1110	1111
0	0	0	0	0	2	0	2

Comme on le voit la distribution est très irrégulière. Comme on la fait précédemment on peut dresser la table des Δy en fonction des Δx, c'est à dire la table des

$$N_D(\Delta x, \Delta y) = \text{Card}\left\{(x', x'') \in \Delta(x) : \pi_S(x') \oplus \pi_S(x'') = \Delta(y)\right\}$$

ce qui est fait à la figure 8.5 page 76

Δx \ Δy	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
1	0	0	0	2	0	0	0	2	0	2	4	0	4	2	0	0
2	0	0	0	2	0	6	2	2	0	2	0	0	0	0	2	0
3	0	0	2	0	2	0	0	0	0	4	2	0	2	0	0	4
4	0	0	0	2	0	0	6	0	0	2	0	4	2	0	0	0
5	0	4	0	0	0	2	2	0	0	0	4	0	2	0	0	2
6	0	0	0	4	0	4	0	0	0	0	0	0	2	2	2	2
7	0	0	2	2	2	0	2	0	0	2	2	0	0	0	0	4
8	0	0	0	0	0	0	2	2	0	0	0	4	0	4	2	2
9	0	2	0	0	2	0	0	4	2	0	2	2	2	0	0	0
A	2	2	2	0	0	0	0	0	6	0	0	2	0	0	4	0
B	0	0	8	0	0	2	0	2	0	0	0	0	0	2	0	2
C	0	2	0	0	2	2	2	0	0	0	0	2	0	6	0	0
D	0	4	0	0	0	0	0	4	2	0	2	0	2	0	2	0
E	0	0	2	4	2	0	0	0	6	0	0	0	0	0	2	0
F	0	2	0	0	6	0	0	0	0	4	0	2	0	0	2	0

Figure 8.5: table de distribution des différences d'une S-boîte: valeurs de $N_D(\Delta x, \Delta y)$

On constate que la somme des lignes vaut toujours 16.

On constate que la distribution des différences d'une S-boîte n'est pas affectée si on XORe l'entrée ou la sortie avec une clef K, en effet

$$x' \oplus x'' = (x' \oplus K) \oplus (x'' \oplus K), \quad y' \oplus y'' = (y' \oplus K) \oplus (y'' \oplus K),$$

car $K \oplus K = 0$ puisque nous sommes en caractéristique 2.

On défint le ***rapport de propagation***, $R_p(\Delta x, \Delta y)$, pour un couple différentiel $(\Delta x, \Delta y)$ de la manière suivante:

$$R_p(\Delta x, \Delta y) = \frac{N_D(\Delta x, \Delta y)}{2^m}, \quad m \text{ nombre de bits d'entrée}$$

en fait $R_p(\Delta x, \Delta y)$ est une probabibilité conditionnelle

$$R_p(\Delta x, \Delta y) = \mathbf{Pr}\left\{x' \oplus x'' = \Delta x \mid y' \oplus y'' = \Delta ybig\right\}$$

On utilise alors les S-boîtes

$$\begin{aligned}
S_{1,2} &: \Delta x = B \longrightarrow \Delta y = 2 \text{ avec probabilité } \frac{8}{16} \\
S_{2,3} &: \Delta x = 4 \longrightarrow \Delta y = 6 \text{ avec probabilité } \frac{6}{16} \\
S_{3,2} &: \Delta x = 2 \longrightarrow \Delta y = 5 \text{ avec probabilité } \frac{6}{16} \\
S_{3,3} &: \Delta x = 2 \longrightarrow \Delta y = 5 \text{ avec probabilité } \frac{6}{16}
\end{aligned}$$

Toutes les autres S-boîtes auront des différences d'entrée et de sortie égale à zéro, voir la figure 8.6 page 78.

Comme le différentiel d'entrée est $\Delta X = (000,\ 1011,\ 0000,\ 0000)$ le différentiel de sortie sera (avec les notations déjà utilisée pour la cryptanalyse linéaire) d'après le tableau (8.7)

$$\Delta V_1 = (0000,\ 0010,\ 0000,\ 0000)$$

Puis d'après les différences demandées pour la S-boîte $S_{2,3}$ on aura (car 4 en hexadécimal vaut 0100 en binaire)

$$\Delta U_2 = (0000,\ 0000,\ 0100,\ 0000)$$

Maintenant on lit dans le tableau (8.7) que

$$\Delta V_2 = (0000,\ 0000,\ 0110,\ 0000)$$

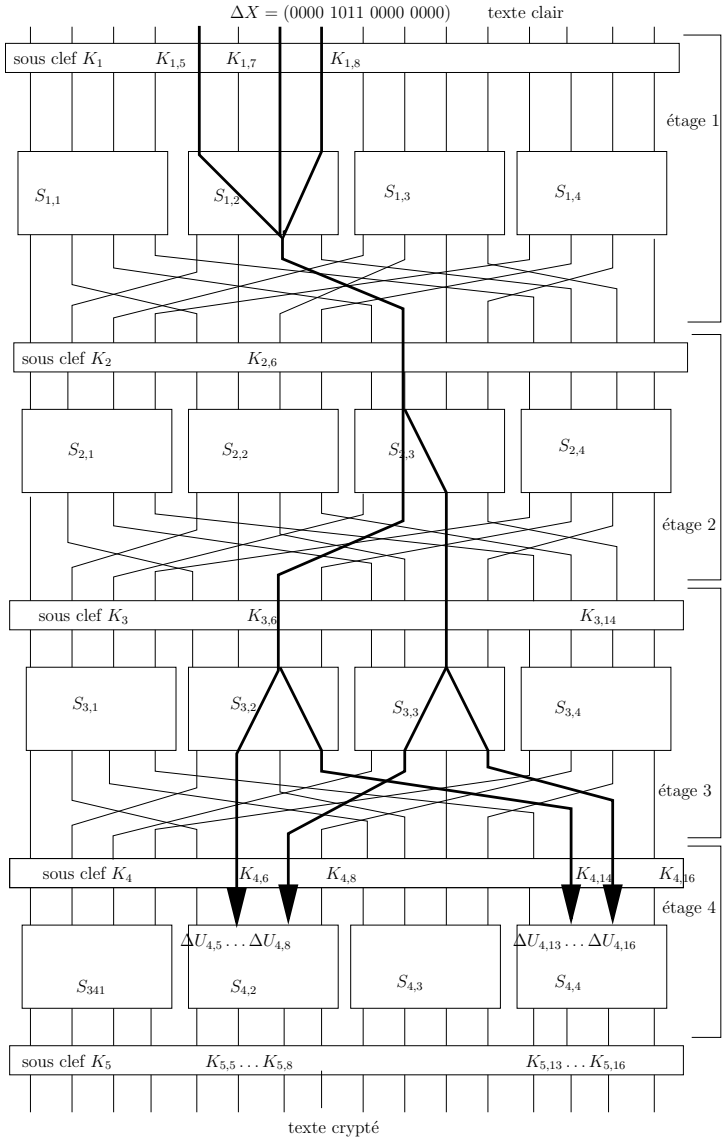


Figure 8.6: Chemin differentiel

Puis en suivant le chemin indiqué dans la figure 8.6 page 78, on voit que

$$\Delta U_3 = (0000,\ 0010,\ 0010,\ 0000)$$

et toujours d'après le tableau (8.7) on aura

$$\Delta V_3 = (0000,\ 0101,\ 0101,\ 0000)$$

et enfin en regardant la figure 8.6 page 78

$$\Delta U_4 = (0000,\ 0110,\ 0000,\ 0110)$$

Ce ΔU_4 a une probabilité de

$$\frac{8}{16} \times \frac{6}{16} \times \left(\frac{6}{16}\right)^2 = \frac{27}{1024}$$

Pendant la crypanalyse on va disposer de beaucoup de texte avec un différentiel d'entrée de la forme $\Delta X = (000,\ 1011,\ 0000,\ 0000)$. Avec une grande probabilité, $\frac{27}{1024}$ les différents différentiels intermédiaires auront lieu, ce seront les ***bonnes paires*** les autres seront les ***mauvaises paires***. Nous sommes maintenant en mesure d'extraire des bits de la clef K_5.

Rappelons tout d'abord la remarque importante: les différentielles $(\Delta U_i, \Delta V_i)$ ne sont pas affectés par la clef K_i

.

Pour chaque paire de texte chiffré on essaye les 256 valeurs des bits

$$K_{5,5}, K_{5,6}, K_{5,7}, K_{5,8}, K_{5,13}, K_{5,14}, K_{5,14}, K_{5,16}$$

de la clef K_5. On déterminent ensuite les valeurs de

$$\Delta U_{4,5} \ldots U_{4,8} \text{ et } \Delta U_{4,13} \ldots U_{4,16}$$

qui ne dépendent pas de la valeur de la clef K_4. On détermine aussi les valeurs de $\Delta U_{4,5} \ldots U_{4,8}$ et $\Delta U_{4,13} \ldots U_{4,16}$ à partir le paire de texte clair correspondante qui ne dépend pas des clefs intermédiares K_1, K_2 et K_3. On crée un compteur pour chacune des 256 sous-clefs possible et on l'incrémante toutes les fois que les deux résultats coïncident. OIn s'attend à ce que la bonne clef donne une probabilité proche de $\frac{27}{1024}$ de réussites.du test.

Comme les différences pour les S-boîtes $S_{4,1}$ et $S_{4,3}$ doivent être zéros on peut filtrer et ne pas tester pour les paires de messages qui ne respectent pas cette condition.

L'attaque marche dans cet exemple avec 5000 paires de textes clairs et cryptés correspondants. La détermination du nombre de paires repose toujours sur des hypothèses de variables aléatoires indépendantes qui ne sont jamais vérifiées. Néanmoins il semble qu'un nombre de pair de messages de l'ordre de $\frac{c}{p_D}$ donne un bon ordre de grandeur.

8.4 Description de DES.

C'est un ***système cryptographique produit***, basé sur un schéma de Feistel, cf. sous-section 8.4.1. Il compose des opérations de cryptage, autrement dit il effectue un produit d'opérations de cryptage. Il répéte 16 fois un algorithme appelé la ***fonction d'étage*** qui dépend d'un paramètre la ***clef d'étage***. La répétition de cet algorithme mélange les bits du message en clair en respectant les principes de C. Shannon: ***confusion et diffusion***.

- La confusion gomme les relations entre le texte clair et le texte chiffré pour éviter les attaques par analyse statistique. Autrement dit un changement d'un seul bit dans le texte clair doit affecter un grand nombre de bits (idéalement tous) du texte chiffré.
- La diffusion disperse la redondance du texte clair dans le texte chiffré, par exemple deux lettres doublées ne doivent pas rester côte à côte après cryptage.

8.4.1 Schéma de Feistel.

Un bon algorithmes à clé secrète doit transformer le message clair en un message crypté qui ressemble autant que possible à une suite aléatoire, pour limiter au minimum les risques d'une attaque par analyse statistique du texte chiffré, de ses redondances, etc...

Le problème est que, si l'on sait depuis longtemps construire des fonctions qui ont l'air aléatoire, on ne savait pas avant les travaux de Feistel construire des bijections aléatoires. La solution apportée par Feistel est très élégante : on suppose par exemple qu'on a une fonction f *presque aléatoire* qui prend comme argument un mot de n bits, et renvoie un mot de n bits (qui donne l'impression d'avoir été choisi au hasard). L'algorithme de chiffrement va procéder en chiffrant des blocs de $2n$ bits, qu'on partage en 2, partie gauche G, partie droite D. L'image du bloc (G, D) par le schéma de Feistel est le bloc (L, R), avec $L = D$, et $R = G \oplus f(D)$ où $\oplus$ est l'opération XOR.. Cette transformation est cette fois bijective, car si on a un tel couple (L, R), on retrouve (G, D) par $D = L$ et $G = R \oplus f(L)$.
Bien sûr, la partie droite n'a pas été transformée (juste envoyée à gauche). C'est pourquoi on répète le schéma de Feistel un certain nombre de fois (on parle de tour - le DES en comporte 16).

La plupart des algorithmes à clé secrète de la fin du XXè s. était des schémas de Feistel. L'avénement de l'AES, qui n'en est plus un, marque la fin de la

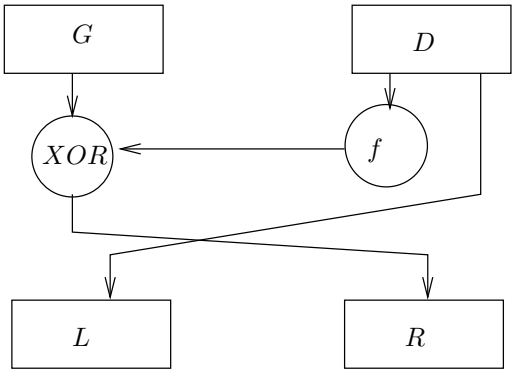


Figure 8.7: Schéma de Feistel

prédominance de tels algorithmes.

8.4.2 Quelques apects techniques de DES.

DES utilise une clé K de 56 bits utiles, en fait une clé de 64 bits dont les bits 8, 16, 24, 32, 40, 48, 56 ne sont pas utilisés pour la clé mais participent à un code correcteur qui permet de vérifier que la clé n'a pas été altérée.

DES est un cryptosystème par blocs qui travaille sur des blocs de 64 bits.

La clé de DES est trop courte pour les puissances de calcul actuelles. La taille de la clé secrète 56 bits le rend aujourd'hui vulnérable aux attaques par force brute. En 1997 la clé a été cassée en 3 semaines par une fédération de machines sur internet. Elle a été cassée en 56 heures en 1998.

En 1999 la clé a été cassée en moins d'une journée, 22 heures, grâce à un ordinateur dédié couplé avec un réseau de plusieurs millers d'ordinateurs.

Afin de prolonger la durée de vie de DES en attendant AES on a introduit le triple DES. Il consiste à appliquer successivement au message DES muni de la clef K, à le décoder avec DES muni de la clef K' et de le recoder avec DES muni de la clef K. Au total tout se passe comme si on avait codé le message avec une clé nettement plus longue.

C'est un système de chiffrement itéré à 16 étages

1. La clé K donne naissance à 16 sous-clés, les clefs d'étage, de 48 bits K_1, K_2,...,K_{16}

2. Etant donné un bloc de texte clair de 64 bits, X, on construit, grâce à la fonction d'étage g_0, un nouveau texte, X_0, par permutation de l'ordre des bits grâce à la ***permutation initiale*** IP.

$$g_0(X) = X_0 = IP(X)$$

3. on sépare les 32 bits de gauche, L_0, et les 32 bits de droites, R_0, de X_0, donc $X_0 = L_0R_0$

4. On effectue 16 itérations (ou tours ou étages). On calcule la valeur de la fonction d'étage $g(X_{i-1}, K^i) = L_iR_i$, $1 \leq i \leq 16$ suivant la règle

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

où $\oplus$ est la somme bit à bit sans retenue ou 'ou exclusif' ou 'XOR' dans $\mathbb{Z}/2\mathbb{Z}$ de L_{i-1} et $f(R_{i-1}, K_i)$ et où f une fonction non linéaire qui participe à la diffusion et qui est décrite par les ***S-boîtes***

5. Pour finir on applique la permutation inverse de la permutation initiale, IP^{-1}, à $R_{16}L_{16}$

Pour une description plus précise voir [31] ou [11].
le schéma 8.8 page 83 résume ce qui précède.

8.5 Description d'AES.

Le principe de l'AES est très proche du DES. C'est aussi un système cryptographique produit constitué d'une suite d'opérations de permutation et de substitution. Contrairement à AES ce n'est pas un schéma de Feistel.

AES travaille sur des blocs de 128 bits avec des clefs de longueur 128, 192 ou 256 bits. À l'origine AES pouvait travailler sur des blocs de longueur $N_b \times 32$ bits où N_b variait de 4 à 8, finalement la taille de blocs d'AES a été fixée à 128 bits et donc N_b a été fixé à 4.
Le passage à une clé de 128 bits minimum rend impossible dans le futur prévisible les recherches exhaustives de clefs. Si on suppose que l'on a un algorithme capable de comparer en une seconde 2^{56} clefs (i.e de casser DES en une seconde) il lui faudra 149 mille milliards d'années pour casser AES.

Exercices. 1

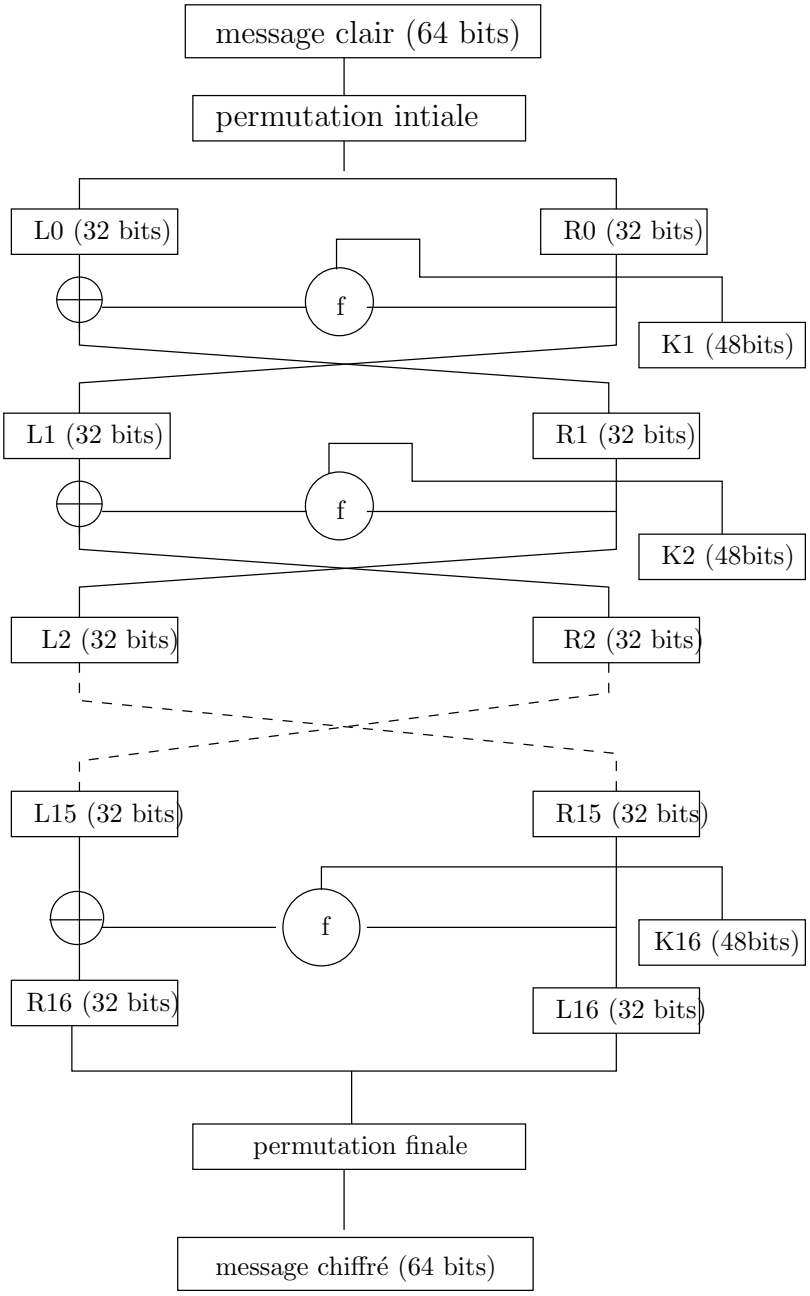


Figure 8.8: Architecture du DES

8.5.1. Justifier cette affirmation.

AES résiste à toutes les attaques connues (**attention ce n'est qu'un fait d'expérience pas une preuve**).

Le diagramme 8.9 page 85 décrit un tour d'AES le diagramme 8.10 page 86 décrit le codage en AES et le diagramme 8.11 page 87 décrit le décodage en AES.

8.5.2 Quelques apects techniques d'AES.

Pour toute la partie mathématique on pourra consulter dans les compléments mathématiques la section sur les extensions de corps et les anneaux de polynômes sur un corps fini, section 13.6 page 182.

AES est un ***système de chiffrement itéré*** constitué d'un algorithme de chiffrement sur des blocs de 128 bits, la ***fonction d'étage***, répété N_e fois, avec N_e allant de 10 à 14, et d'une clef secrète de 128, 192 ou 256 bits et pour chaque étage d'une clef d'étage de longueur fixe, 128 bits.

Un ***algorithme de diversification de clef***, **ExpandKey**$[i]$, permet de créer une clef pour chacun des étages, i, à partir de la clef secrète K.

On notera N_e le nombre d'étages. La fonction d'étage, g, est l'ensemble des opérations que l'on fait subir au texte qui arrive à l'étage i. Elle est la même pour tous les étages sauf le dernier.

La fonction g consiste en l'application successive de 4 opérations **SubBytes**, **ShiftRows**, **MixColumns**, **AddRoundKey**. Pour le dernier étage on applique seulement les opérations **SubBytes**, **ShiftRows** et **AddRoundKey**.

À partir de la clef secrète, K, on génére des sous clefs d'étage par l'algorithme de diversification de la clef, **ExpandKey**$[i]$. On obtient les clefs d'étage: K^1,...,K^{N_e}.

On note x un bloc de 128 bits du texte initial (texte en clair), w^i le texte utilisé en entrée à l'étage i (c'est donc un bloc de 128 bits) et y sera le bloc correspondant crypté final.

Tous les textes sont supposés transformés en une suite de zéros et de uns. Si K et L sont deux telles suites on note

$$K \oplus L$$

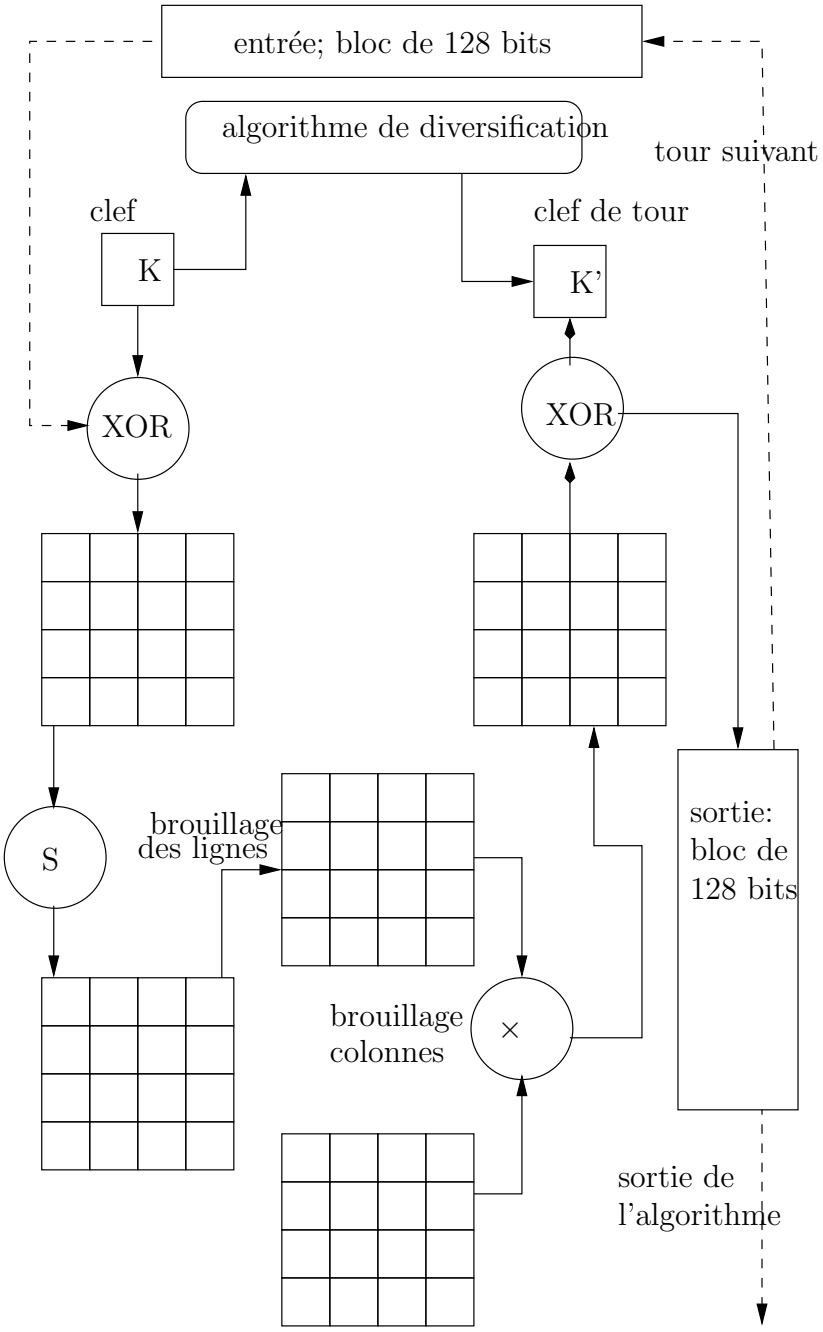


Figure 8.9: Diagramme d'un tour d'AES

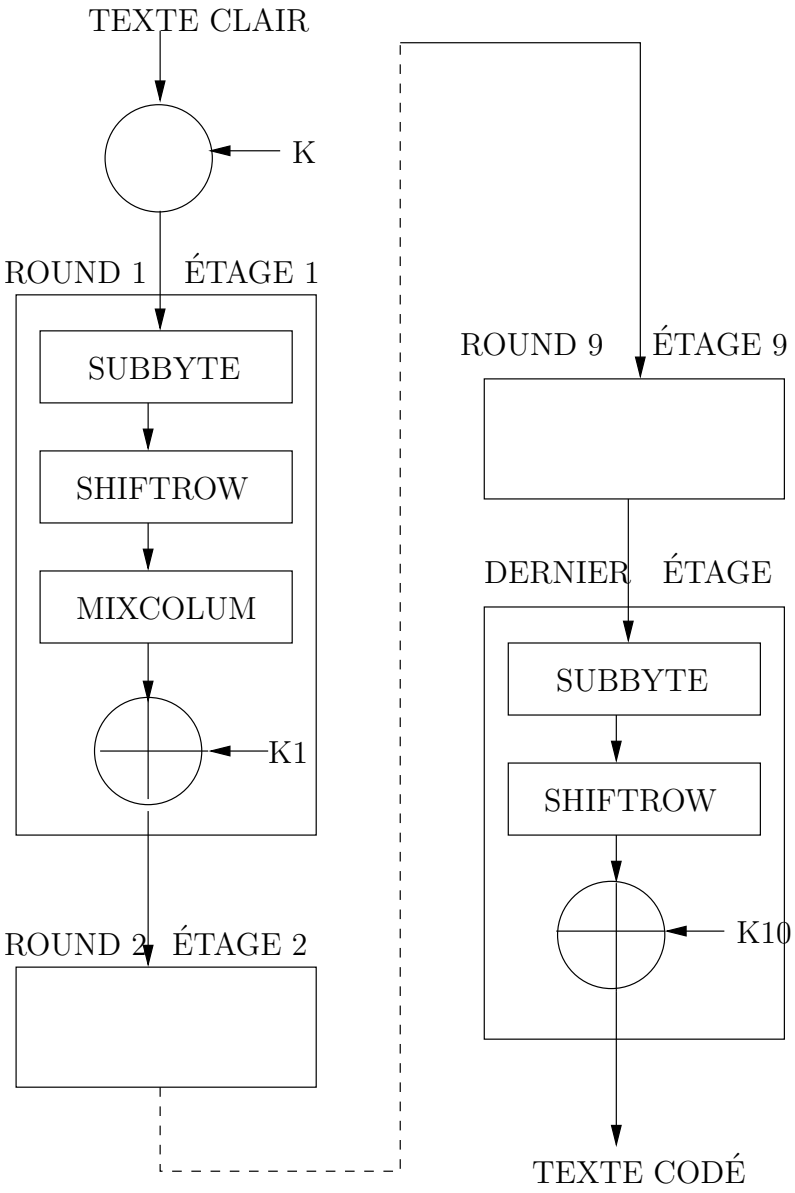


Figure 8.10: Diagramme du codage en AES

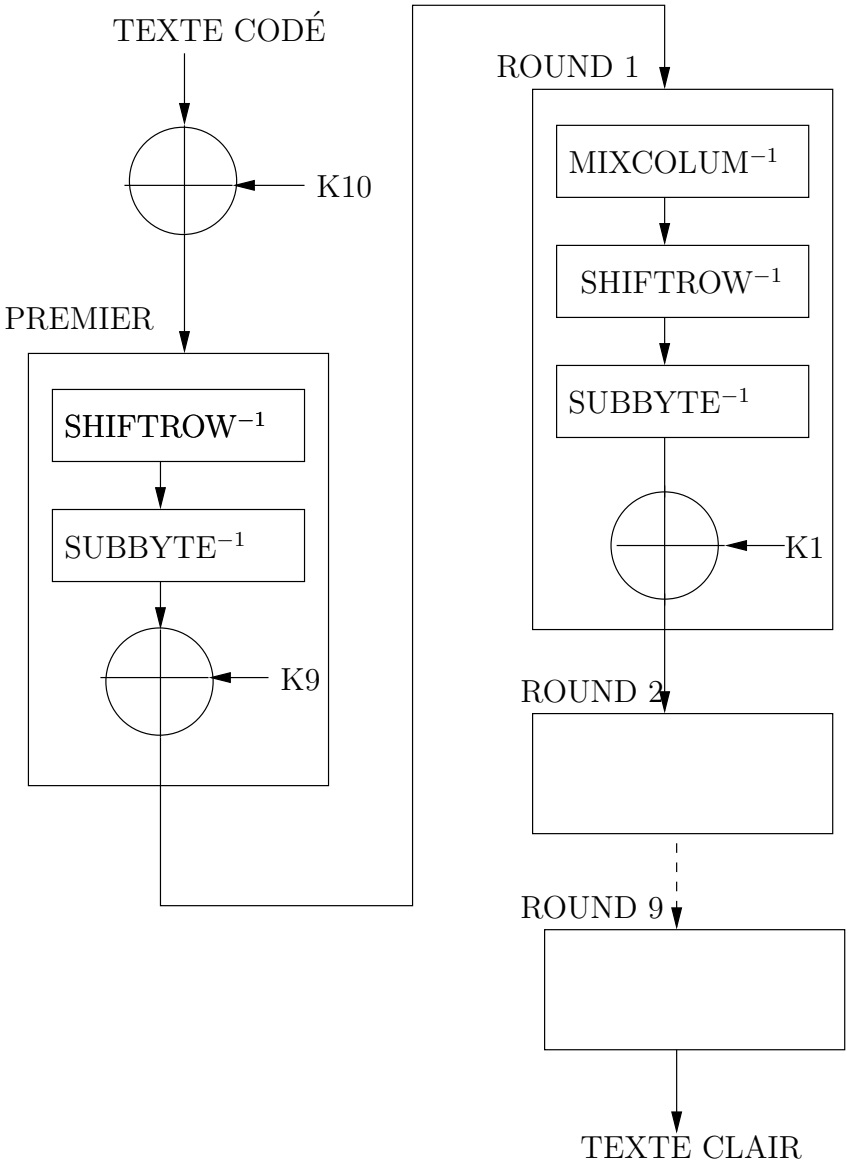


Figure 8.11: Diagramme du décodage en AES

l'opération XOR entre le suite K et la suite L.

Avec ces notations la description schématique d'AES est la suivante. On notera **State** l'écriture du flux d'entrée-sortie sur lequel opère chaque algorithme. Donc on prend le bloc de 128 bits sur lequel opère AES que l'on considère comme une suite 16 octets que l'on range en une matrice 4×4.

Un octet étant confondu avec un élément de $\mathbb{F}_{256}$ de la manière suivante: $\mathbb{F}_{256}$ est identifié aux polynômes de $\mathbb{F}_2[x]$ de degré ≤ 7 par l'isomorphisme

$$\mathbb{F}_{256} \simeq \mathbb{F}_2[x]/(x^8 + x^4 + x^3 + x + 1)\mathbb{F}_2[x]$$

Donc **State** est une matrice de $M_{4\times 4}(\mathbb{F}_{256})$ construite suivant le schéma 8.12 page 88.

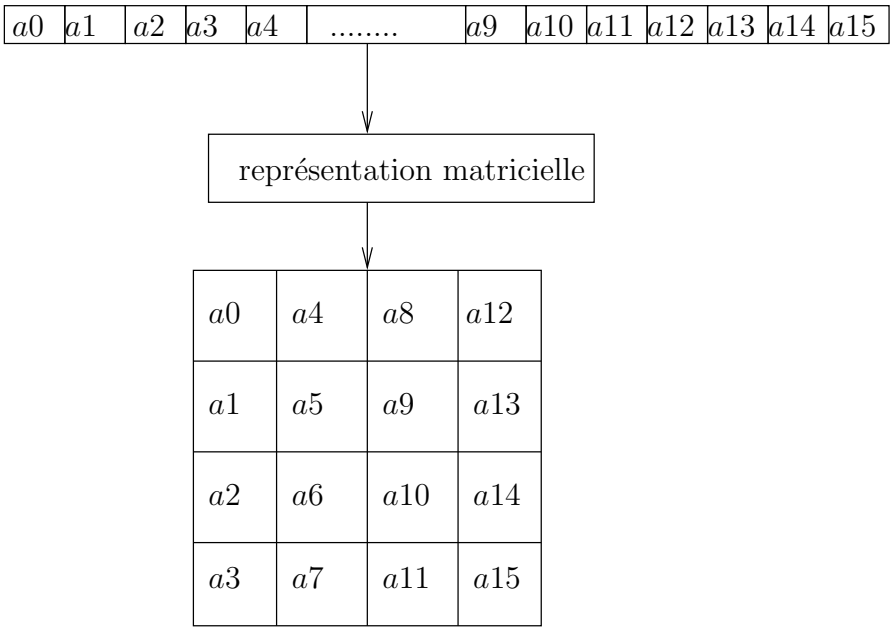


Figure 8.12: La matrice **State**

L'algorithme se déroule de la manière suivante:

1. On initialise w^0 à x et et on effectue l'opération **AddRoundKey**

$$W^0 \oplus K$$

2. Pour chacun des $1 < i \leq N_e - 1$ étages suivants on effectue sur w^i les opérations suivantes
   (a) l'opération de substitution **SubBytes**
   (b) sur le résultat de **SubBytes** une permutation notée **ShiftRows** (permutation circulaire sur les éléments des lignes de la matrice des octets $s_{i,j}$)
   (c) sur le résultat de **ShiftRows** une opération notée **MixColumns** (application linéaire sur l'espace des matrices sur $\mathbb{F}_{2^8}$)
   (d) Sur le résultat de **MixColumns** l'opération **AddRoundKey**$[i]$ avec la sous-clé de l'étage i
3. Pour le dernier étage N_e on supprime l'opération **MiXColumns**

On va décrire maintenant chacune des opérations utilisées.

L'opération ExpandKey

L'opération **ExpandKey** dépend de la taille de clé choisie, $N_k \times 32$, qui peut être égale à 128, 160, 192, 224 ou 256 bits. On supposera dans la suite que la longueur de la clef est de 192 bits, donc $N_k = 6$.

Extension de la clef secrète K. On écrit la clef K sous forme d'une matrice de N_k colonnes de 4 bytes chacune (donc 4 lignes, l'élément d'une ligne étant un mot de 8 bits), dénotées k_0,...,k_5

k_0	k_1	k_2	k_3	k_4	k_5

Ensuite cette matrice est étendue en une matrice de taille $4(N_e + 1)$ où N_e est le nombre d'étages par l'algorithme suivant

- Si i n'est pas un multiple de N_k (la longueur de la clef) alors la colonne d'indice i, k_i, est la XORisation de la colonne d'indice $i - N_k$, k_{i-N_k}, et de la colonne d'indice $i-1$, k_{i-1}. C'est donc l'addition bit à bit sans retenue de la colonne k_{i-N_k} et de la colonne k_{i-1}, $k_i = k_{i-N_k} \oplus k_{i-1}$.
- Si i est un multiple de N_k on applique à chacun des bytes de la colonne k_{i-1} la permutation π_S décrite au paragraphe suivant suivie d'une rotation dans les bytes de la nouvelle colonne k_{i-1}, notée **Rotword**, et de

l'addition d'une constante d'étage définie en héxadécimal par [**Fieldto Binary**(x^{j-1}) 000000] pour l'étage j (autrement dit on ajoute **Fieldto Binary**(x^{j-1}) au premier byte de la clef d'étage après application de **Rotword**, c'est à dire à a_1 avec les notations ci-dessous). On XOR le résultat obtenu avec la colonne k_{i-N_k}.

On obtient ainsi

k_0	k_1	k_2	k_3	k_4	k_5	k_6	k_7	$dots$	$k_{i\cdot 4}$	...	$k_{(i+1)4-1}$	...
clé d'étage 0				clé d'étage 1				...	clé d'étage i			...

La rotation **Rotword** est définie comme suit

$$\textbf{Rotword}: \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix} \longmapsto \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_0 \end{pmatrix}$$

Exercices. 1

8.5.2. Vérifier que les constantes d'étages définies ci-dessus on pour valeur (en hexadécimal)

étage 1 01000000 étage 2 02000000 étage 3 04000000
étage 4 08000000 étage 5 10000000 étage 6 20000000
étage 7 40000000 étage 8 80000000 étage 9 1B000000
étage 10 36000000

L'opération **ExpandKey** montre bien la réalisation des concepts de diffusion et de confusion de Shannon. Prenons la clef de 128 bits

$$K = 00000000000000000000000000000000$$

en hexadécimal et voyons ce que sont les clefs dérivées pour chacun des dix étages, on trouve:

$$
\begin{array}{lcl}
\textbf{RoundKey}[00] & = & 00000000000000000000000000000000 \\
\textbf{RoundKey}[01] & = & 62636363626363636263636362636363 \\
\textbf{RoundKey}[02] & = & 9B9898C9F9FBFBAA9B9898C9F9FBFBAA \\
\textbf{RoundKey}[03] & = & 90973450696CCFFAF2F457330B0FAC99 \\
\textbf{RoundKey}[04] & = & EE06DA7B87A1581759ED42B27E91EE2B \\
\textbf{RoundKey}[05] & = & 7F2E2B88F8443E098DDA7CBBF34B9290 \\
\textbf{RoundKey}[06] & = & EC614B851425758C99FF09376AB49BA7 \\
\textbf{RoundKey}[07] & = & 21751873550620BACAF6B3CC61BF09B \\
\textbf{RoundKey}[08] & = & 0EF903333BA9613897060A04511DFA9F \\
\textbf{RoundKey}[09] & = & B1D4D8E28A7DB9DA1D7BB3DE4C664941 \\
\textbf{RoundKey}[10] & = & B4EF5BCB3E92E21123E951CF6F8F188E
\end{array}
$$

8.5.3. Vérifier que la diversification de la clef (en hexadécimal)

$$K = 00000000000000000000000000000000$$

est bien celle donnée par le tableau précédent.

8.5.4. Construire la diversification complète de la clé (en hexadécimal)

$$2B7E151628AED2A6ABF7158809CF4F3C$$

L'opération SubBytes

L'opération **SubBytes** est la seule opération non linéaire. On suppose que le message w^i est un nombre de 128 bits=16 octets, $(s_{i,j})_{0\leq i,j\leq 3}$, écrit en base 2. On le réécrit sous la forme d'une matrice S_i, où les $s_{i,j}$ sont des octets.

$$S_i = \begin{matrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{matrix}$$

L'opération **SubBytes** consiste en une permutations π_S sur $\{0,1\}^8$, agissant indépendamment sur chacun des octets $s_{i,j}$ de l'étage i.

Pour décrire π_S on travaille dans un surcorps du corps à 2 éléments, $\mathbb{F}_2$, le corps fini à 256 éléments, $\mathbb{F}_{2^8}$, que l'on identifie avec les polynômes de degré ≤ 8, munis de l'addition et de la multiplication modulo le polynôme irréductible de $\mathbb{F}[x]$, $x^8+x^4+x^3+x+1$, cf. paragraphe 13.6.2, page 186, de rappel sur les anneaux de polynômes,

$$\mathbb{F}_{2^8} \simeq \mathbb{F}_2[x]/(x^8+x^4+x^3+x+1)\mathbb{F}_2[x]$$

L'application **BinarytoField** associe à l'octet $a_7a_6\dots a_1a_0$ l'élément

$$\textbf{BinarytoField}(a_7a_6\dots a_1a_0)=\sum_{i=0}^{7}a_ix^i$$

du corps $\mathbb{F}_{2^8}$. L'application inverse est **FieldtoBinary**. On a dans le corps $\mathbb{F}_{2^8}$ l'opération **FieldInv** qui à un élément $z\neq 0$ du corps associe z^{-1} et à $z=0$ associe 0.

***Exemple* 8.5.1.** Calcul dans $\mathbb{F}_{2^8}$. Calculons **FieldInv**(00000011) on a:

- **FieldtoBinary**(00000011)=$x+1$
- **FieldInv**$(x+1)$=$x^7+x^6+x^5+x^4+x^2+x$

car on a l'identité de Bézout

$$(x+1)(x^7+x^6+x^5+x^4+x^2+x)+(x^8+x^4+x^3+x+1)=1$$

obtenue par l'algorithme d'Euclide ou directement,

donc dans $\mathbb{F}_{2^8}\simeq\mathbb{F}[x]/(x^8+x^4+x^3+x+1)$

$$(x+1)^{-1}=(x^7+x^6+x^5+x^4+x^2+x)$$

et donc

- **BinarytoField**$(x^7+x^6+x^5+x^4+x^2+x)$=(11110110)

Revenons à la description de l'opération **SubBytes** c'est à dire à la description de la permutation π_S pour le mot de 8 bits $(a_7a_6\dots a_1a_0)$ consiste en

- application de **BinarytoField** à $(a_7a_6\dots a_1a_0)=(b_7b_6\dots b_1b_0)$ qui donne $a\in\mathbb{F}_{2^8}$
- application **FieldInv** à a qui donne a^{-1} si $a\neq 0$ ou 0 si $a=0$
- ajout de l'élément $c=(c_7c_6\dots c_1c_0)=$ **BinarytoField**(01100011) à a^{-1} pour obtenir $b=(b_7b_6\dots b_1b_0)$
- application de **FieldtoBinary** à b

c est une constante d'AES.

Exercices. 1

8.5.5. Calculer **SubBytes**(00000011).

L'opération ShiftRows

C'est la permutation cyclique dans les lignes de la matrice S_i décrite par le diagramme ci-dessous

$$\begin{array}{|c|c|c|c|} \hline a & b & c & d \\ \hline e & f & g & h \\ \hline i & j & k & l \\ \hline m & n & o & p \\ \hline \end{array} \longrightarrow \begin{array}{|c|c|c|c|} \hline a & b & c & d \\ \hline f & g & h & e \\ \hline k & l & i & j \\ \hline p & m & n & o \\ \hline \end{array}$$

L'opération MixColumns

C'est une transformation linéaire dans les colonnes de la matrice **State**; la colonne j est transformée de la manière suivante (les calculs sont faits dans $\mathbb{F}_{2^8}$)

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

Polynomialement cette opération s'interprète de la manière suivante Chacune des colonnes de la matrice **State** est considérée comme un polynôme de degré 3 à coefficients dans $\mathbb{F}_{256}$.

L'opération **MixColumns** consiste alors à effectuer pour chaque colonne une multiplication du polynôme correspondant à la colonne par un polynôme fixe $c(x) = 03x^3 + x^2 + x + 02$ suivie d'une réduction modulo le polynôme x^4+1 de façon à obtenir un polyôme de degré inférieur ou égal à 3 de $\mathbb{F}_{256}[X]$ qui est interprété comme une colonne d'une matrice de $M_4(\mathbb{F}_{256})$.

L'opération AddRoundKey

AddRoundKey$[i]$ est l'addition de la clef obtenue à l'étage i par l'algorithme de diversification des clés, **ExpandKey**$[i]$, au texte obtenu à l'issue de l'étape **MixColumns**.

On écrit la clef **ExpandKey**$[i]$, de 128 bits, sous la forme d'une matrice de 4×4 bytes et on l'ajoute au résultat de l'étape précédente par un XOR

$$\begin{array}{|c|c|c|c|} \hline a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ \hline a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ \hline a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ \hline a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \\ \hline \end{array} \bigoplus \begin{array}{|c|c|c|c|} \hline k_{0,0} & k_{0,1} & k_{0,2} & k_{0,3} \\ \hline k_{1,0} & k_{1,1} & k_{1,2} & k_{1,3} \\ \hline k_{2,0} & k_{2,1} & k_{2,2} & k_{2,3} \\ \hline k_{3,0} & k_{3,1} & k_{3,2} & k_{3,3} \\ \hline \end{array} = \begin{array}{|c|c|c|c|} \hline b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} \\ \hline b_{1,0} & b_{1,1} & b_{1,2} & b_{1,3} \\ \hline b_{2,0} & b_{2,1} & b_{2,2} & b_{2,3} \\ \hline b_{3,0} & b_{3,1} & b_{3,2} & b_{3,3} \\ \hline \end{array}$$

8.6 Infrastructure des systèmes à clef secrète.

Les ***infrastructures pour les systèmes à clef secrète*** consistent en toutes les dispositions techniques et l'organisation nécessaires pour gérer un système cryptographique à clef secrète.

Autant il est facile pour un ordinateur de retenir une clé secrète de 128 bits, autant c'est difficile pour une personne. On utilise alors le système des mots de passe. Mais pour ne pas affaiblir la sécurité du cryptosystème le mot de passe doit obéir à certaines règles

- Avoir une entropie, cf. le paragraphe 13.1.3 page 153, au moins égale à 128 bits. De manière approximative ceci signifie que le mot de passe doit être aussi difficile à deviner qu'une suite aléatoire de 128 zéros et uns. Pour avoir une entropie de 128 bits il suffit de choisir 22 caractères au hasard dans un alphabet de 64 lettres (minuscules, majuscules, chiffres, point et espace).
- Il doit résister aux attaques-dictionnaires.
- Un mot de passe ne doit pas être réutilisé

On peut prendre les mesures suivantes pour améliorer la sécurité d'un système de mots de passe

- On utilise le mot de passe pour calculer une clé de session qui change à chaque fois.
- On rajoute des ingrédients pour éviter les attaques dictionnaires (sel).
- On itère la fonction de hachage, par exemple 1000 fois. Pour l'utilisateur le temps de calcul est à peine affecté. Pour l'attaquant qui procède par attaque-dictionnaire, c'est prohibitif.

On utilise aussi un ***système de gestion des clefs*** (***Symmetric Keys Management***) qui

1. émet les clefs
2. les authentifie
3. les archive
4. les garde en dépôt

Un des systèmes les plus utilisés est ***Kerberos***, cf. [34].

8.6.1 Exemple: protocole d'accès HTTP

On décrit de manière succincte le système de controle d'accès par mot de passe utilisé dans le protocole HTTP (norme RFC 2617). Ici le client est un navigateur (browser) qui désire avoir accès à un document protégé appelé ***Uniform Resource Identifier*** (***URI*** en abrégé) d'un site Web. Il y a deux protocoles d'accès, nous ne décrivons que le protocole de base (basic protocol en anglais).
Dans le protocole de base le serveur garde en mémoire des triplets (realm-value, userid, password) où realm-value est une partie du serveur HTTP, userid est un identifiant de l'utilisateur et où password est un mot de passe attribué à l'utilisateur.

Lorsque un utilisateur envoie une requête pour accéder à un URI, le serveur envoie la demande suivante

`WWW-Authenticate: basic realm=‘‘⟨realm-value⟩’’`

L'utilisateur doit répondre alors

`Authentification basic: basic ⟨basic-credential⟩`

où ***basic-credential*** est la chaîne de caractère

`⟨userid⟩:⟨ password⟩`

Si le triplet (realm-value, userid, password) est correct le serveur répond à la reque d'URI. Sinon il envoie le message d'erreur

`HTTP/1.0 401 Unauthorized`

et recommence le processus de demande.

8.7 Attaques par force brute contre les codes symétriques

On peut se demander quelle est la sécurité d'un cryptosystème symétrique (DES, AES ou LFSR) face à une ***attaque par force brute*** (en anglais ***brute force attack***. on décrit trois types d'attaques par force brute

1. Les attaques par recherche exhaustive
2. Les attaques dictionnaires
3. Les attaques répertoires

8.7.1 Attaques par recherche exhaustive.

Cette attaque consiste à essayer systématiquement toutes les clefs possibles jusquèà ce que l'on tombe sur la bonne clef. On peut simplifier le modèle de cette attaque en supposant que l'on a un oracle (un dispositif) qui répond par oui ou par non à la question:

cette clef est-elle correcte?

On peut définir la complexité par le nombre d'appels à l'oracle qui seront nécessaire pour obtenir la bonne clef. On aura une notion de ***complexité dans le pire des cas*** (worst case complexity en anglais), une notion de ***complexité en moyenne*** (average complexity en anglais), etc...

Dans le cas d'un espace de clefs contenant N clefs qui sont générées uniformément on peut montrer que la meilleure attaque a une complexité dans le pire des cas de N appels à l'oracle et une complexité en moyenne de $\sim \frac{N}{2}$ appels à l'oracle.

En effet La meilleure attaque consiste à ordonner sans réptition les clefs de l'espace des clefs suivant un ordre aléatoire et à interroger l'oracle. Si on se place dans le pire des cas la bonne clef est la dernière et il a donc fallu interroger l'oracle N fois.

Si la bonne clef est la i-ième dans la liste il a fallu interroger l'oracle i fois. Commme la liste a été faite au hasard la probabilité que la bonne clef soit la i-ième est $\frac{1}{N}$. Par conséquent la complexité en moyenne, c'est à dire le nombre d'appels qu'il a fallu faire à l'oracle en moyenne, est

$$\sum_{i=1}^{N} \frac{i}{N} = \frac{N+1}{2}$$

8.7.2 Attaques dictionnaires.

Cette attaque est une attaque à texte clair choisi qui cherche à retrouver la clef secrète..

On choisit un (ou plusieurs) texte clair x et on calcule les message codés, $E_{K_i}(x)$, correspondant pour M clefs K_i choisies au hasard dans l'espace des clefs si leur distribution est équirépartie et plus généralement choisies en accord avec leur loi de distribution. On range le s couples $(E_{K_i}(x), K_i)$ dans un dictionnaire. Les $E_{K_i}(x)$ jouent le rôle d'index de rangement, de mot à définir, et les K_i sont les définitions correspondantes

***Remarque* 8.7.1.** Il se peut qu'il y ait des clefs K_i et K_j telles que $E_{K_i}(x) = E_{K_i}(x)$.

Si maintenant on reçoit un message $E_K(x)$ on compare le résultat avec le dictionnaire ce qui donne donne une indication sur la clef K.

8.7.3 Attaques répertoires.

Cette attaque cherche à retrouver le message clair correspondant au message codé sans se soucier de la clef secrète. C'est une attaques à texte chiffré connu.

On choisit un (ou plusieurs) texte clair x et on calcule pour M clefs K_i de l'espace des clefs et on calcule les couples $(E_{K_i}(x), x)$. On range le tout dans un répertoire. Les $E_{K_i}(x)$ jouent le rôle d'index de rangement dans le répertoire et x la rubrique correspondant.

Si on reçoit un message codé y on le compare avec les entrées du répertoire c'est à dire les $E_{K_i}(x)$ et si on a pour un i particulier $E_{K_i}(x) = y$ alors x peut-être un candidat pour le texte clair correspondant

Chapitre 9

Codes à clefs publiques.

Diffie et Hellman ont dégagé vers 1976 la notion de ***code à clef publique ou code asymétrique*** fondé sur la notion de fonction à sens unique.

Les codes asymétriques les plus utilisés:

- **RSA** basé sur la difficulté calculatoire de la factorisation des grands entiers.

- **El Gamal** basé sur la difficulté calculatoire de calculer le logarithme discret dans un corps fini.

- **Menezes-Vanstonne** basés sur le logarithme associé au groupe des points d'une courbe elliptique sur un corps fini. C'est une modification d'autres cryptosystèmes, comme El Gamal. Sa sureté peut être mieux analysée. La longueur de sa clé est bien inférieure à celle des systèmes RSA et El Gamal pour une sureté équivalente. Ils offrent des fonctionnalités supplémentaires comme la possibilité de monter un cryptosystème basée sur l'identité.

Il existe d'autres codes asymétriques peu utilisés en pratique comme

- **McEliece** basé sur la théorie algébrique des codes correcteurs d'er -reurs. Il repose sur la difficulté calculatoire du décodage d'un code linéaire (problème NP complet). Considéré comme sûr il nécessite des clefs extrèmement longues 10^{19} bits.

- **Chor-Rivest** basé une instance du problème du **sac-à-dos**.

9.1 Principe des codes à clef publique.

9.1.1 Fonctions à sens unique.

On cherche une fonction f entre des ensembles $\mathcal{P}$ et $\mathcal{E}$ telle que

- le calcul de $f(x)$ pour $x \in \mathcal{P}$ se fait en temps polynomial en fonction de la taille des données, cf la sous-section 13.2.3.
- le calcul de $f^{(-1)}(y)$ pour $y \in \mathcal{E}$ ne se fait pas en temps polynomial en fonction de la taille des données. Le plus souvent la fonction f possède une ***porte dérobée*** (trapdoor) qui permet de calculer facilement $f^{-1}(y)$ lorsqu'on a une information supplémentaire comme la clef secrète.

Autrement dit on cherche des fonction $f : \mathcal{P} \rightarrow \mathcal{E}$ appartenant à la classe des problèmes P (calculables en temps polynomial en fonction de la taille des données) et telle que la fonction réciproque (ou l'image réciproque si ne suppose pas f bijective) $f^{(-1)}$ appartienne à la classe des problèmes NP, (non calculables en temps polynomial en fonction de la taille des données, mais vérifiables en temps polynomial).

La mise au point de telles fonctions a révolutionné la cryptographie et élargi son champ d'application.

9.2 Le cryptosystème Merkle-Hellman.

Ce cryptosystème qui fut historiquement un des premiers proposés (il a été publié en 1978) repose sur le problème du ***sac-à-dos***. Génériquement il a une sécurité prouvée, car le problème du sac-à-dos est gfénériquement dans la classe NP. Malheureusement comme l'a montré Shamir sa sécurité ne repose pas sur un problème de sac-à-dos générique mais sur une instance particulière de ce problème qui elle peut ne pas être dans la classe NP.

9.2.1 Le problème du sac-à-dos.

Le problème du sac-à-dos s'énonce de la manière suivante

- Soit a un ensemble d'entiers $\{a_1, a_2, \ldots, a_n; s\}$.
- Existe-t-il un sous-ensemble de $\{a_1, a_2, \ldots, a_n\}$ dont la somme soit s

Intuitivement on peut considérer que les a_i représentent la taille de paquets que l'on veut mettre dans un sac-à-dos de taille s, ou encore qu'ils représentent des billets et des pièces monnaies destinées à payer un objet dont le prix est s.

L'interêt de ce problème du sac-á-dos pour la cryptographie tient au théorème suivant

Théorème 9.2.1 (Karp 1972)**.** *Le problème du calcul de la solution, supposée exister, du sac-à-dos est un problème génériquement NP-complet*

Pour la définition de NP-complet voir la sous-section 13.2.2.

De manière un peu approximative ce théorème signifie que génériquement trouver une solution, que l'on sait exister, au problème du sac-à-dos est difficile c'est à dire que la calcul de la solution nécessite un temps exponentiel en fonction de la taille des données. Le mot générique signifie qu'il existe au moins un ensemble a ayant une solution tel que le calcul de la solution ne se fasse pas en temps polynomial en fonction de la taille des données.

Le problème est de cacher une clef secrète, une porte dérobée, ou trapdoor qui permette au destinataire du message de le décoder.

On choisit un entier M on dira que $a = \{a_1, a_2, \ldots, a_n; s\}$ est un problème de sac-à-dos modulo M s'il existe

$$\{a_{k_1}, \ldots, a_{k_m}\} \subset \{a_1, a_2, \ldots, a_n\}$$

tel que

$$a_{k_1} + \cdots + a_{k_m} \equiv s \mod M$$

9.2.2 Description du cryptosystème Merkle-Hellman.

L'idée principale de Merkle et Hellman consiste à choisir un sac-à-dos particulier dont la solution est triviale et à cacher cette forme particulière du sac-à-dos par une transformation secrète connue du seul destinataire du message.

La forme retenue par Merkle et Hellman est le ***sac-à-dos super-croissant*** (***super-increasing knapsack***).

Une suite d'entier $\{b_1, b_2, \ldots, b_n, b_{n+1}\}$ est dite super-croissante si l'on a

$$b_i > \sum_{j=1}^{i-1} b_j; \quad \text{pour } 1 \leq i \leq n+1$$

On remarque que si la suite $\{b_1, b_2, \ldots, b_n, b_{n+1}\}$ est super-croissante et si $M = b_{n+1}$ alors tout problème de sac à $\{b_1, b_2, \ldots, b_n; s\}$ modulo M est équivalent au problème de sac-à-dos $\{b_1, b_2, \ldots, b_n; s\}$ sur les entiers naturels. Ce dernier est un problème facile. On remarque que b_n est dans le sous-ensemblme de la solution si et seulement si $b_n \leq s$ et on peut alors ramener le problème initial au problème de sac-à-dos $\{b_1, b_2, \ldots, b_{n-1}; s'\}$ avec $s' = \begin{cases} s - b_n \\ \text{ou} \\ s \end{cases}$.

La transformation secrète destinée à cacher le fait que l'on a un sac-à-dos super-croissant est simplement la multiplication par un nombre secret M. Le crypto-système de Merkle et Hellman est donc le suivant

1. Paramètre public n.
2. fabrication de la clef: choisir un suite super croissante
$$\{b_1, b_2, \ldots, b_n, b_{n+1} = M\}$$
choisir un nombre $W \in \mathbb{Z}/M\mathbb{Z}$ et une permutation π de $\{1, \ldots, n\}$. Calculer $a_i = Wb_{\pi(i)} \pmod M$ pour $1 \leq i \leq n$.
3. Clef Publique: $K_p = (a_1, a_2, \ldots, a_n)$
4. Clé sécrète: $K_s = (b_1, b_2, \ldots, b_n, M, W, \pi)$
5. Message: une suite de zéros et de uns de longuer n, $m = m_1 m_2 \cdots_n$.
6. Codage: $c = \sum_{i=1}^{n} m_i a_i$
7. Décodage: calculer $CW^{-1} \pmod M$, résoudre le problème de sac-à-dos super-croissant $x_1 b_1 + \cdots + x_n b_n = cW^{-1} \pmod M$ et alors $m_i = x_{\pi(i)}$.

Le crypto-système Merkle-Hellman revient à trouver un vecteur dans un réseau. Un ***réseau*** (***lattice***) est l'ensembles des combinaisons à coefficients entiers relatifs de vecteurs de $\mathbb{R}^n$. Trouver un petit vecteur au sens de la norme euclidienne est aussi un problème difficile. mais il y a des cas où ce problème devient facile. Plus précisément l'***algorithme LLL*** peut être utilisé. En particulier il peut être utilisé pour casser des crypto-systèmes comme celui de Merkle-Hellman.

9.3 Le système RSA.

Le système RSA est nommé d'après le nom de ses inventeurs: Rivest, Shamir, Adleman.

Il est basé sur la fonction à sens unique ***produit de deux entiers***

$$\begin{aligned} f: \quad & \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \\ & (n, m) \longmapsto f(n, m) = n \times m \end{aligned}$$

sa fonction réciproque étant la décomposition d'un nombre entier en un produit de deux facteurs non-triviaux (c'est à dire différents de 1 et du nombre lui même) et donc finalement sur la décon en facteurs premiers d'un entier, cf. la section arithmétique dans les compléments de mathématiques, section 13.3 page 161.

Le calcul du produit de deux nombres entiers est une opération "facile", "rapide", "calculatoirement facile" (c'est à dire faisable en temps polynomial en fonction de la taille des données) alors que la décomposition en facteurs premiers n'est pas "facile", est "lente", "calculatoirement difficile" (c'est à dire qu'elle n'est pas faisable en temps polynomial en fonction de la taille des données). En effet on montre, cf. la sous-section 13.2.3, que si les nombres entiers n et m s'écrivent avec moins $k \leq \max\{[ln_2 n], [\ln_2 m]\}$ chiffres en base 2 alors le temps nécessaire pour calculer le produit $m \times n$ est proportionnel à k^2.

9.3.1 Description du cryptosystème RSA.

On a un ensemble $(A_i)_{i \in I}$ de correspondants (personnes physiques ou ordinateurs). Le principe du cryptosystème RSA est le suivant (pour toutes les définitions arithmétiques voir le paragraphe 13.3)

- Chacun des correspondants A_i choisit deux nombres premiers p_i et q_i distincts. On note $n_i = p_i q_i$, le ***module du cryptosystème*** de A_i et $\varphi(n_i) = (p_i - 1)(q_i - 1)$, l'indicatrice d'Euler de n_i.
- A_i choisit ensuite un nombre e_i l'***exposant de la clé publique*** premier avec $\varphi(n_i)$ (ce que l'on note $e_i \wedge \varphi(n_i) = 1$). D'après le petit théorème de Fermat, théorème 13.3.18 page 172, on peut imposer $1 \leq e_i \leq \varphi(n_i) - 1$, ce que l'on fait toujours en pratique.
- Puis A_i calcule l'inverse d_i de e_i modulo $\varphi(n_i)$, d_i est appelé l'***exposant de la clé secrète***. C'est à dire, d'après la définition de l'inverse

modulo n_i, qu'on cherche $d_i \in \mathbb{N}$ tel qu'il existe $k_i \in \mathbb{N}$ avec

$$d_i \times e_i = 1 + k_i\varphi(n_i) \text{ et } 1 \leq d_i \leq \varphi(n_i) - 1$$

Le calcul se fait par l'algorithme d'Euclide étendu, cf. la sous-sous-section 13.3.3.

- Chacun des correspondants A_j publie dans un annuaire public les nombres n_j et e_j qui forment sa ***clé publique de chiffrement*** et garde secret p_j, q_j et d_j qui forment sa ***clé secrète de déchiffrement***.

En pratique on choisit les nombres premiers p_i et q_i de taille comparable de telle sorte que leur produit $n_i = p_iq_i$ soit un nombre d'au moins 300 chiffres en base 10 et plutôt 500 pour une protection longue.

Remarque* 9.3.1.** Bien distinguer entre e ***ne divise pas n et e est ***premier avec*** n, (e, n sont des entiers positifs).

e ne divise pas n signifie qu'il n'existe pas d'entier f tel que $n = ef$.
e est premier avec n signifie qu'il n'existe aucun diviseur commun entre e et n, c'est qu'il n'existe aucun entier d tel que d divise e et d divise n.

***Exemple* 9.3.1.** 9 ne divise pas 15 mais 9 n'est pas premier à 15 car 3 divise à la fois 9 et 15.

9.3.2 Protocole d'envoi d'un message en RSA.

Alice veut envoyer un message $\mathcal{M}$ à Bob. La clef publique d'Alice (resp Bob) est (n_a, e_a), (resp. (n_b, e_b)), sa clef secrète est (p_a, q_a, d_a) (resp. $(p_b, q_b, d_)b)$. Elle suit le protocole suivant

1. Alice commence par transformer le message en une suite de chiffres, par exemple en remplaçant les lettres et les différents symboles utilisés par des chiffres (de 0 à 255 dans le cas du code ASCII).

2. Alice regarde dans l'annuaire public la clé de chiffrement n_b, e_b de Bob. Elle découpe le message $\mathcal{M}$ en blocs M de taille approximativement n_b.

3. Elle calcule
$$f_b(M) = M' \equiv M^{e_b} \mod n_b$$
et envoie $M' = f_b(M)$ à Bob.

4. Pour récupérer le texte en clair Bob calcule

$$f_b^{-1}(M') = (M')^{d_b} = f_b(M)^{d_b} \equiv M^{e_b d_b} = M^{1+k_b\varphi(n_b)} \mod n_b$$

D'après le théorème d'Euler (cf. théorème 13.3.23 page 175) on a

$$M^{\varphi(n_b)} \equiv 1 \mod n_b$$

et par conséquent

$$f_b^{-1}(M') \equiv M \mod n_b$$

Si la taille de M est adaptée à celle de n_b, il n'y a pas d'ambiguitét Bob récupère donc bien le message d'Alice.

Exercices. 1

9.3.1. Bob choisit comme nombre premier $p = 17$ et $q = 19$, comme exposant $e = 5$. donner sa clef publique.

9.3.2. Bob choisit comme nombre premier $p = 17$ et $q = 19$ et comme exposant $e = 5$. Donner sa clé secrète de déchiffrement d.

9.3.3. Bob choisit comme nombre premier $p = 17$ et $q = 19$ et comme exposant $e = 5$. Alice et lui décident d'un protocole RSA dans lequel les messages sont des nombres en base 10 que l'on code par bloc de 2 chiffres en base 10. Alice veut envoyer le message 462739.

1. Écrire le message codé qu'elle envoie à Bob.
2. Décoder le message qu'a reçu Bob et vérifier que c'est bien celui qu'a envoyé Alice.

9.3.4 Protocole de signature RSA.

Le cryptosystème RSA permet aussi facilement de réaliser l'authentification de l'expéditeur (en admettant que sa clef privée n'est utilisée que par lui).

1. Alice commence par découper le message $\mathcal{M}$ en blocs M de taille bien choisie par rapport à n_a et n_b. Elle crypte chaque bloc du message avec sa clé secrète, d_a, elle obtient à partir du texte en clair M un premier texte crypté, M''

$$M'' = f_a^{-1}(M) \equiv M^{d_a} \mod p_a q_a$$

2. Avec la clé publique de Bob, elle crypte M'' et obtient un deuxième texte crypté, M'

$$M' = f_b(M'') = f_b(f_a^{-1}(M))$$

qui constitue sa signature du message M.

3. Elle crypte alors le message M avec la clé publique de Bob en suivant le protocole précédent et obtient le texte crypté du message $f_b(M)$

$$f_b(M) = M^{e_b} \mod n_b$$

4. Elle envoie à Bob le couple

$$(f_b(M), M')$$

qui constitue le message chiffré et signé d'Alice à Bob.

Pour décoder et vérifier la signature qui authentifie l'expéditeur du message, d'Alice, Bob effectue les opérations suivantes

1. Il calcule d'une part

$$\begin{aligned} f_b^{-1}(M') &\equiv M'' \mod n_b \\ &\equiv f_a\Big(f_b^{-1}\Big((f_b\big(f_a^{-1}(M) \pmod{n_b}\big)\Big)\Big) \mod n_a \\ &\equiv M \mod n_a \end{aligned}$$

(Si le choix de la taille des blocs M est bien choisie par rapport à n_a et n_b, il n'y a pas d'ambiguité au décodage)

2. Il calcule d'autre part, en décodant comme au paragraphe 9.3.2,

$$f_b^{-1} f_b(M) \equiv M \mod n_b$$

3. Il compare les deux résulats obtenus. S'il constate que $M = M$, c'est à dire que les deux résultats sont les mêmes, il est sûr alors que le message vient d'Alice car seule Alice connait

$$f_a^{-1} \Longleftrightarrow d_a$$

c'est à dire sa clé secrète. De plus il est sûr que le message n'a pas été altéré.

Sécurité de la signature RSA

Le protocole de signature RSA décrit ci-dessus souffre de quelques failles de sécurité dues aux propriétés de RSA.

Soit $K_p = (n, e)$ et $K_s = (n, d)$ des clefs publiques et privées utilisées pour une signature. La signature du message m est simplement la paire $\sigma = m \pmod n$.

On peut donc choisir un σ au hasard et construire un message en clair $m = \sigma^e \pmod n$. La paire (m, σ) est un message signé parfaitement valable simplement on n'a pas le contrôle du message crypté m.

Si on a deux messages signés (m_1, σ_1) et (m_2, σ_2) on crée un autre message sigé parfaitement valide qui est $\big((m_1 m_2 \pmod n), (\sigma_1 \sigma_2 \pmod n)\big)$.

On peut remédier à ces failles de sécurité en utilisant des fonctions de hachage.::

Exercices. 1

9.3.4. Bob choisit comme nombre premier $p_b = 17$ et $q_b = 19$ et comme exposant $e_b 5$. Alice choisit comme nombres premier $p_a = 11$ $q_a = 21$ et comme exposant $e_a = 7$. Calculer les exposants secrets d'Aice et Bob. Alive et Bob utilisent un protocole RSA en base 10 par bloc de 2 chiffres. Alice envoie et signe le message suivant 462739. Donner le message reçu par Bob.

9.3.5. Bob et Charles utilisent un cryptosystème RSA avec le même module $n = pq$ mais avec des exposants différents, l'exposant b pour Bob et c pour Charles que l'on suppose premier entre eux. Alice leur envoie le même message clair x qu'elle crypte avec leur clef publique. Elle envoie donc $y_b \equiv x^b \pmod n$ à Bob et $y_c \equiv x^c \pmod n$ à Charles.

Éve intercepte les deux messages cryptés y_b et y_c. Montrer qu'Éve peut retrouver le message clair x sans connaître les clefs secrètes de Bob et Charles (indication: trouver des entiers e et f tels que $x \equiv y_b^e \big(y_c^f\big)^{-1}$).

Calculer x avec $n = 18721$, $b = 43$, $c = 7717$, $y_b = 12677$, $y_c = 14702$.

9.3.6. Montrer que le cryptosystème RSA ne résiste pas aux attaques à texte chiffré choisi. En particulier étant donné un texte chiffré y, montrer comment choisir un deuxième texte chiffré $\tilde{y} \neq y$ tel que la connaissance du texte clair $\tilde{x}$ correspondant permette de calculer le texte clair x correspondant ày (indication: utiliser le fait que si e_K est la fonction de chiffrement on a

$$e_K(x)e_K(\tilde{x}) \mod n = e_K(x\tilde{x} \mod n)$$

9.3.7. On suppose que Bob, Bernard et Bertrand utilisent un cryptosystème RSA avec des modules différents n_1,n_2, n_3 et le même exposant $b = 3$. On suppose que les n_i sont deux à deux premiers entre eux.

Alice chiffre un message x avec les clefs publiques de Bob, Bernard et Bertrand et le leur envoie. Montrer qu'Éve qui intercepte les trois messages peut récupérer x sans factoriser aucun des n_i.

9.3.6 Exemple académique de codes RSA.

Alice publie sa clé publique $(n_A, e_A) = (65, 5)$, sa clef secrète est d_A.

Bob publie sa clé publique $(n_B, e_B) = (77, 7)$, sa clef secrète est d_B.

Pour trouver les clefs secrètes on décompose en un produit de facteurs premiers n_A et n_B

$$n_A = 13 \cdot 5 \text{ et } n_B = 7 \cdot 11$$

On calcule ensuite les indicatrices d'Euler correspondantes

$$\varphi(n_A) = 12 \times 4 = 48 \text{ et } \varphi(n_B) = 6 \times 10 = 60$$

En utilisant l'algorithme de PGCD décrit au paragraphe 13.3.3 page 166 (ou directement) on calcule d_A

$$5 \times 29 = 145 = 1 + 3 \times 48 \Longrightarrow d_A = 29$$

respectivement d_B

$$7 \times 43 = 301 = 5 \times 60 + 1 \Longrightarrow d_B = 43$$

Alice veut transmettre le message 3 à Bob. Elle calcule donc

$$3^7 \equiv 31 \mod 77 = 7 \times 11$$

et elle envoit 31 à Bob. Bob décode en calculant

$$31^{43} \equiv 31^{1+2+8+32} \equiv 31 \cdot 37 \cdot 58 \cdot 37 \cdot 31 \equiv 3 \mod 77$$

(remarquer la manière de calculer une puissance).

Si Alice veut signer le message elle n'envoie pas seulement 31, mais elle calcule d'abord

$$f_a^{-1}(3) = (3^{29} \mod 65) = 48$$

puis elle calcule

$$f_b\big(f_a^{-1}(3)\big) = f_b(3^{29} \mod 65) = (48^7 \mod 77) = 27$$

puis elle envoie à Bob le couple

$$(31, 27)$$

constitué de la signature et du message.

Pour décoder Bob calcule

$$f_a\big(f_b^{-1}(27)\big) = f_a(27^{43} \mod 77) = (48^5 \mod 65) = 3 \mod 65$$

et

$$31^{43} \equiv 3 \mod 77$$

et il constate que les deux résultats coincident. L'expéditeur du message est bien Alice.

***Remarque* 9.3.2.** Pour signer le message Alice aurait pu aussi bien mener les calculs dans l'ordre inverse, c'est à dire calculer d'abord avec la clé publique de Bob

$$\widetilde{M}'' = f_b^{e_b}(M) \mod n_b$$

puis crypter avec sa clé secrète d_a le résultat $\widetilde{M}''$ et obtenir un deuxième texte crypté, $\widetilde{M}'$

$$\widetilde{M}' = f_a^{-1}(\widetilde{M}'') = f_a^{-1}(f_b((M)) \equiv (\widetilde{M}'')^{d_a} \mod n_a$$

qui constitue sa signature du message M.

Elle crypte alors le message M avec la clé publique de Bob en suivant le protocole précédent et obtient le texte crypté du message $f_b(M)$

$$f_b(M) = M^{e_b} \mod n_b$$

Elle envoie à Bob le couple

$$(f_b(M), \widetilde{M}')$$

Bob décode en calculant d'une part

$$f_a(\widetilde{M}') \equiv \widetilde{M}'' \mod n_a$$

$$f_b^{-1}(f_a((\widetilde{M}')) = f_b^{-1}(f_a(f_a^{-1}(f_b(M)))) \equiv M \mod n_b$$

Les deux protocoles ont leurs avantages et inconvénients. On préfère en général le premier protocole car il suit de plus près la manière traditionnelle de signer une lettre: on signe d'abord avant de la mettre dans l'enveloppe. Le second protocole consiste à mettre la lettre dans l'enveloppe et à signer l'enveloppe.

9.3.7 Exemple de code RSA.

On choisit un alphabet à 40 lettres

$$\begin{array}{cccccc} \text{A= 0}, & \text{B= 1}, & \text{C= 2}, & \text{D= 3}, & \text{E= 4}, & \text{F= 5}, \quad \ldots, \\ \ldots, & \text{X= 23}, & \text{Y= 24}, & \text{Z= 25}, & \square\text{=26}, & .\text{= 27}, \quad ?\text{= 28}, \\ \text{euros= 29}, & \text{0= 30}, & \text{1= 31}, & \ldots, & \text{8= 38}, & \text{9= 39}, \end{array}$$

On choisit comme clé publique le couple

$$n = 2047, \quad e = 179$$

on a

$$40^2 \leq 2047 \leq 40^3$$

on choisit donc de découper les messages en clair en blocs de deux lettres et les messages chiffrés en blocs de trois lettres.

On écrit chaque bloc de deux symboles clairs X_1X_2 sous la forme $40x_1 + x_2$ où x_i est le nombre entre 1 et 39 correspondant à X_i.

On écrit chaque bloc de trois symboles codés $Y_1Y_2Y_3$ sous la forme $40^2y_1 + 40y_2 + y_3$ où y_i est le nombre entre 0 et 39 correspondant à Y_i.

Le message clair est

ENVOYEZ euros2500.

Pour le coder on considère les blocs

$$\begin{array}{rr} \text{EN} = 4 \times 40 + 13 = 173, & \text{VO} = 21 \times 40 + 14 = 854, \\ \text{YE} = 24 \times 40 + 4 = 964, & \text{Z}\square = 1026, \\ \text{euros2} = 1192, & \text{50} = 1430, \\ \text{0.} = 1110 & \end{array}$$

Codage du message

$$\begin{array}{rl} \text{EN} \mapsto (173)^{179} & \mod 2047 = 854 = 0 \times 40^2 + 21 \times 40 + 14 = \text{AVO} \\ \text{VO} \mapsto (854)^{179} & \mod 2047 = 1315 = 0 \times 40^2 + 32 \times 40 + 35 = \text{A25} \\ \text{YE} \mapsto (964)^{179} & \mod 2047 = 452 = 0 \times 40^2 + 11 \times 40 + 12 = \text{ALM} \\ \text{Z}\square \mapsto (1026)^{179} & \mod 2047 = 1295 = 0 \times 40^2 + 32 \times 40 + 15 = \text{A2P} \\ \text{euros2} \mapsto (1192)^{179} & \mod 2047 = 511 = 0 \times 40^2 + 12 \times 40 + 31 = \text{AM1} \end{array}$$

$$50 \mapsto (1430)^{179} \mod 2047 = 1996 = 1 \times 40^2 + 9 \times 40 + 36 = \text{BJ6}$$
$$0. \mapsto (1110)^{179} \mod 2047 = 1642 = 1 \times 40^2 + 1 \times 40 + 2 = \text{BBC}$$

Le message codé est donc

AVOA25ALMA2PAM1BJ6BBC

Pour décoder on factorise

$$2047 = 23 \times 89 \Longrightarrow \varphi(2047) = 22 \times 88 = 1936$$

et on déduit par l'algorithme d'Euclide que

$$d = 411.$$

***Remarque* 9.3.3.** En fait les paramètres de ce code sont mal choisis car 22 divise 88 et donc on peut prendre pour d n'importe quel inverse de 179 modulo 88 comme par exemple 59. On constate que $411 = 59 + 4 \times 88$

9.3.8 Sécurité du système RSA.

La sécurité de RSA repose sur les faits suivants:

- on ne sait pas décoder sans connaître l'exposant de la clé secrète d
- trouver d équivaut à factoriser $n = pq$
- on ne connait pas d'algorithme polynomial en temps en fonction de la taille des données (c'est à dire de la longueur des nombres n et e) pour calculer d c'est à dire pour factoriser n, les meilleurs sont en

  $$O\left(e^{C\sqrt{\ln_2 n \ln_2 \ln_2 n}}\right) \text{ opérations.}$$

  on dit que l'algorithme est ***sous-exponentiel***

Ce sont des faits d'expérience pas des théorèmes.

Depuis sa création le système RSA a résisté à toutes les attaques de manière satisfaisante si l'on choisit bien p, q et e, mais il faut constamment augmenter la taille de pq. On est partie de 512 bits, et même 389 bits pour les cartes à puces, à 2048 bits. Cette augmentation de taille est nécessitée par l'augmentation de la puissance des ordinateurs et par les progrès mathématiques des algorithmes de factorisations des entiers.

Pour construire et utiliser un code RSA on a besoin de savoir faire rapidement (c'est à dire en temps polynomial au plus) les opérations suivantes:

- construire des grands nombres premiers
- calculer des PGCD
- faire de l'arithmétique modulaire (addition, multiplication, exponentiation)

Pour évaluer et tester la sécurité du code RSA, il faut en particulier

- évaluer la rapidité des algorithmes de factorisations de grands nombres entiers
- Démontrer que la clef secrète de déchiffrement d ne peut pas être obtenue sans factoriser $n = pq$ et plus généralement qu'elle ne peut pas être calculée en temps polynomial en fonction de n.
- montrer que l'on ne peut pas décoder un message sans la clef secrète

9.3.9 Attaques du système RSAA.

Bien,que le système RSA soit considéré comme sûr il y a de nombreuses manières de mal l'utiliser et d'ouvrir des failles de sécurité.

Attaques sur les petits exposants I

On envoie le même message x à plusieurs destinataires qui ont pour clef publique (e, n_1), (e, n_2),...,(e, n_k) avec le même exposant e. On envoie donc $y_i = x^e \pmod{n_i}$ pour $1 \leq i \leq k$.

Si on suppose que le nombre de destinataires, k, est supérieur à l'exposant e il devient facile à un opposant qui intercepte l'ensemble des messages codés $(y_i)_{1\leq i\leq k}$ de les décrypter.

Supposons pour simplifier que les $(n_i)_{1\leq i\leq k}$ soient deux à deux premiers entre eux. Soit $n = \prod_{1\leq i\leq k} n_i$. Le théorème des restes chinois (théorème 13.3.19 page 173, montre qu'il existe y avec $y < n$ tel que

$$y \equiv y_i \mod n_i, \quad 1 \leq i \leq k$$

Nous avons donc

$$y \equiv x^e \mod n_i, \quad 1 \leq i \leq k$$

et par conséquent puisque les $(n_i)_{1\leq i\leq k}$ sont deux à deux premiers entre eux on a

$$y \equiv x^e \mod n$$

Comme l'entier naturel x^e est plus petit que n car x est plus petit que chacun des n_i et que n est le produit de plus de e entiers n_i (ici l'hypotse que l'exposant est petit, i.e. inférieur à k) est cruciale. Comme $y < n$ on en déduit que l'on a en fait

$$y = x^e$$

Comme e est public il ne reste plus qu'extraire la racine e-ième de y pour récupérer x.

Attaques sur les petits exposants II

Si l'xposant public e est petit il existe un algorithme polynomial en fonction de la taille des données qui permet de trouver la racine d'une équation polynomiale modulo n de degré e si au moins l'une des racines est de taille inférieure à $n^{\frac{1}{e}}$.

On peut utiliser cet algorithme pour décrypter efficacement un message crypté en RSA avec un exposant public $e = 3$ si l'on connait les deux tiers des bits en clair du message. De même si $e = 3$ et si l'on dispose de deux messages dont les textes en clair ne diffèrent que sur une fenêtre connue de longueur $\frac{1}{9}$ de celle du texte clair on peut décrypter les deux messages.

On a des résultats analogues si l'exposant secret d est petit $< \sqrt[4]{n}$.

9.4 Le cryptosystème El Gamal.

Le cryptosystème El Gamal est basée sur la fonction à sens unique ***logarithme discret***. On considère un groupe cyclique fini, G, de cardinal n engendré par un générateur, g. Donc

$$G = \left\{ g^i \;\middle|\; 0 \leq i \leq n-1 \right\}$$

On suppose que le calcul de g^i est "facile", "rapide" "calculatoirement facile" (c'est à dire faisable en temps polynomial en fonction de la taille des données) mais que le calcul de i connaissant g^i n'est "pas facile", est "lent", "calculatoirement difficile" (c'est à dire: n'est pas faisable en temps polynomial en fonction de la taille des données). Si $a = g^i$, i est appelé le ***logarithme discret*** de a.

Autrement dit G est isomorphe au sous groupe additif de $\mathbb{Z}/n\mathbb{Z}$ et la sécurité du cryptosystème El-Gamal repose sur la difficulté à calculer explicitement cet isomorphisme en un temps raisonnable.

On utilise les deux réalisations suivantes de G. On considère un nombre premier p et on choisit

$$G = \left(\mathbb{Z}/p\mathbb{Z}\right)^* \simeq \mathbb{F}_p^*$$

c'est à dire que le G est le groupe des éléments inversible pour la multiplication de $\mathbb{Z}/p\mathbb{Z}$ les entiers modulo p, pour la définition voir dans les compléments mathématiques, le paragraphe sur les congruences 13.3.4 page 169.

D'après un théorème de Gauss, théorème 13.3.17 page 172, le groupe multiplicatif de $\mathbb{Z}/p\mathbb{Z}$ est cyclique et le calcul de $g^i \mod p$ est rapide alors qu'on ne connait pas d'algorithme en temps polynomial pour calculer i connaissant $a = g^i$ pour de bons choix de p. Plus généralement on peut considérer le groupe multiplicatif des éléments inversibles d'un corps fini à $q = p^s$ éléments, $\mathbb{F}_q$.

Une autre réalisation est de prendre comme groupe G le groupe des points d'une courbe elliptique sur un corps fini, $E(\mathbb{F}_q)$ qui donne lieu aux cryptosystèmes elliptiques, cf le paragraphe 9.5 page 118. Ils se développent actuellement car ils possèdent des avantages en terme de taille de clé et de sécurité prouvée.

9.4.1 Description du cryptosystème El Gamal.

On considère le cryptosystème suivant: Soit p un nombre premier tel que le problème du logarithme discret dans $\mathbb{Z}/p\mathbb{Z}$ soit difficile.

Soit g une racine primitive modulo p, cf. le théorème 13.3.17 page 172, c'est à dire que g est un générateur du groupe cyclique $(\mathbb{Z}/p\mathbb{Z})^*$.

Soit $\mathcal{P} = \left(\mathbb{Z}/p\mathbb{Z}\right)^*$, les messages en clair, et soit $\mathcal{C} = \left(\mathbb{Z}/p\mathbb{Z}\right)^* \times \left(\mathbb{Z}/p\mathbb{Z}\right)^*$ les messages cryptés et enfin soit l'espace des clefs

$$\mathcal{K}_b = \left\{(p, g, \alpha, \beta); \beta \equiv g^\alpha \mod p\right\} \quad \text{où} \quad \begin{cases} (p, g, \beta) & \text{est la clef publique} \\ \alpha & \text{est la clef secrète} \end{cases}$$

Alice veut transmettre un message, $\mathcal{M}$, à Bob

1. Bob choisit un grand nombre premier p_b, un générateur g_b du groupe cyclique multiplicatif $\left(\mathbb{Z}/p_b\mathbb{Z}\right)$ et un entier α_b inférieurs à $p_b - 1$

2. Bob calcule $\beta_b = g_b^{\alpha_b}$; alors le triplet (β_b, g_b, p_b) constitue sa clef publique, α_b est sa clef secrète.

3. Alice découpe le message $\mathcal{M}$ en blocs M de taille inférieure à p_b, elle choisit un entier k_a (inférieur à $p_b - 1$) pour chacun des blocs M et calcule
$$y_1 \equiv g_b^{k_a} \pmod{p_b} \text{ et } y_2 = \beta_b^{k_a} M$$

La paire $e_{K_b}(M, k_a) = (y_1, y_2)$ est le message codé qu'Alice envoie à Bob.

Pour décoder

1. Bob calcule
$$M \equiv y_2 (y_1^{\alpha_b})^{-1} \mod p_b$$

Comme $y_1^{\alpha_b} = g_b^{k_a \alpha_b} \pmod{p}$ on a:

$$d_K(y_1, y_2) = y_2 (y_1^{\alpha_b})^{-1} \equiv \beta_b^{k_a} M (g_b^{k_a \alpha_b})^{-1} \equiv$$
$$\equiv g_b^{\alpha_b k_a} M g_b^{-\alpha_b k_a} \equiv M \mod p$$

et comme M est inférieur à p_b il n'y a pas d'ambiguité dans le décodage.

Pour une bonne sécurité, Alice doit changer souvent k_a.

9.4.2 Signature El Gamal.

On reprend les notations précédentes. Soit M un bloc d'un message $\mathcal{M}$ qu'Alice veut transmettre en le signant à Bob.

1. Alice choisit elle-aussi un grand nombre premier p_a tel que le problème du logarithme discret dans $\left(\mathbb{Z}/p_a\mathbb{Z}\right)^*$ soit difficile.

2. Elle choisit aussi un générateur g_a de $\left(\mathbb{Z}/p_a\mathbb{Z}\right)^*$ et un entier $0 \leq \alpha_a \leq p_a - 2$ et elle calcule $\beta_a = g_a^{\alpha_a}$.

Elle dispose ainsi elle aussi d'une clef publique (p_a, g_a, β_a) et d'une clef privée (secrète) α_a. Pour signer le message M, Alice réalise les opérations suivantes

1. elle choisit $k'_a \in (\mathbb{Z}/p\mathbb{Z})^*$ secret et premier à $p_a - 1$.

2. elle calcule

$$\gamma_a \equiv g_a^{k'_a} \mod p_a$$
$$\delta_a \equiv (M - \alpha_a \gamma_a) {k'_a}^{-1} \mod (p_a - 1)$$

3. la signature du bloc M est alors $\text{sign}_{K_a}(M, k'_a)$ avec

$$\text{sign}_{K_a}(M, k'_a) = (\gamma_a, \delta_a)$$

4. Puis elle envoie le couple

$$\big(e_{K_b}(M, k_a), \text{sign}_{K_a}(M, k'_a)\big)$$

c'est à dire le quadruplet $\big((y_1, y_2), (\gamma_a, \delta_a)\big)$.

On constate que

$$\beta_a^{\gamma_a}\gamma_a^{\delta_a} \equiv g_a^M$$

***Remarque* 9.4.1.** La condition k'_a premier à $p_a - 1$ est nécessaire car Alice utilise pour calculer δ_a la quantité $k'^{-1}_a \pmod{p_a - 1}$.

Cette procédure réalise bien une signature du bloc M. Pour vérifier la signature et décoder Bob suit le protocole suivant:

1. Bob reçoit le couple constitué par le message crypté par Alice de la signature de ce message c'est à dire le quadruplet $\big((y_1, y_2), (\gamma_a, \delta_a)\big)$.

2. Il décode le message à l'aide de sa clé secrète et récupère M.

3. Il calcule

$$\beta_a^{\gamma_a}\gamma_a^{\delta_a} \mod p_a$$

et il vérifie que

$$\beta_a^{\gamma_a}\gamma_a^{\delta_a} \equiv g_a^M$$

S'il en est ainsi il est sûr que l'expéditeur du message est bien Alice.

On constate que cette procédure réalise bien une signature du message M car pour fabriquer le couple (γ_a, δ_a) Alice a utlisé sa clef secrète et si l'on remplace dans la formule donnant δ_a la clé secrète α_a par un autre nombre compris entre 0 et $p_a - 1$ on n'aura plus l'égalité

$$\beta_a^{\gamma_a}\gamma_a^{\delta_a} \equiv g_a^M \mod p_a$$

9.4.3 Sécurité du système EL Gamal.

La sécurité du cryptosystème EL Gamal repose sur les faits suivants:

- on ne sait pas décoder sans connaître la clé secrète α
- trouver α équivaut à trouver le logarithme discret de $\beta = g^\alpha$ dans $(\mathbb{Z}/p\mathbb{Z})^*$
- on ne connait pas d'algorithme polynomial en temps en fonction de la taille des données (c'est à dire de la longueur du nombre p) pour calculer α. Les meilleurs sont en

$$O\Big(e^{C\sqrt{\ln_2(p)\ln_2\ln_2(p)}}\Big) \text{ opérations.}$$

Ce sont des faits d'expérience pas des théorèmes.

9.4.4 Exemple académique de code El Gamal.

Alice et Bob veulent correspondre en employant le système El-Gamal. Alice choisit comme paramètres

$$p_a = 263,\ g_a = 5,\ \alpha_a = 47$$

Bob choisit comme paramètres

$$p_b = 257,\ g_b = 5,\ \alpha_b = 67$$

On vérifie facilement que p_a et p_b sont des nombres premiers, que g_a et g_b sont respectivement des générateurs des groupes cycliques $\mathbb{Z}/p_a\mathbb{Z}$ et $\mathbb{Z}/p_b\mathbb{Z}$. Il suffit pour cela de vérifier (par exemple à l'aide d'une table ou d'un système de calcul faisant de l'arithmétique modulaire) que

$$\begin{cases} g_a^e \not\equiv 1 \mod p_a & \forall\, 1 < e < p_a - 1 \text{ divisant } p_a - 1 \\ g_b^e \not\equiv 1 \mod p_b & \forall\, 1 < e < p_b - 1 \text{ divisant } p_b - 1 \end{cases}$$

En effet d'après le corollaire 13.3.24 le plus petit entier non nul e tel que $g_a^e \equiv 1 \pmod{p_a}$ est un diviseur de $p_a - 1$. Ici $p_a - 1 = 262 = 2 \times 131$, donc il suffit de vérifier que $g_a^{131} \not\equiv 1 \pmod{263}$ et $p_b - 1 = 256 = 2^8$, donc il suffit de vérifier que $g_b^{128} \not\equiv 1 \pmod{257}$.

Alice calcule $\beta_a = p_a^{\alpha_a} \pmod{p_a} = 40$ et sa clef publique est

$$K_a = (p_a = 263, g_a = 5, \beta_a = 40)$$

sa clé secrète est $\alpha_a = 47$.

Bob calcule $\beta_b = p_b^{\alpha_b} \pmod{p_b} = 201$ et sa clef publique est

$$K_b = (p_b = 257, g_b = 5, \beta_b = 201)$$

sa clé secrète est $\alpha_b = 67$.

On suppose qu'Alice et Bob s'envoient des nombres de deux chiffres en base 10. Alice envoie à Bob le message M qu'elle code en $(y_1, y_2) = (76, 251)$ à l'aide la clé publique de Bob et d'un k_a qu'elle garde secret.
Bob décode le message en effectuant l'opération

$$\begin{aligned} y_2(y_1^{\alpha_b})^{-1} \pmod{257} &= 251 \times 76^{-67} \pmod{257} \\ &= 251 \times 76^{256-67} \pmod{257} \\ &= 251 \times 76^{189} \pmod{257} = 251 \times 155 \pmod{257} \\ &= (-6) \times 155 \pmod{257} = 98 \end{aligned}$$

.Le message en clair d'Alice est $M = 98$.

On peut retrouver le paramètre k_a à l'aide d'une table des puissances de g_b (mod 257). On sait que

$$y_1 = g_b^{k_a} \pmod{257} = 76, \quad y_2 = \beta_b^{k_a} M \pmod{257} = 251$$

On trouve à l'aide d'une table ou d'un logiciel de calcul d'arithmétique modulaire $k_a = 139$.

Si Alice veut envoyer le message $M = 87$ à Bob avec les mêmes paramètres, y compris k_a, elle effectue le calcul

$$\begin{aligned} z_1 &= y_1 = g_b^{k_a} \pmod{257} = 76 \\ z_2 &= \beta_b^{k_a} \times 87 \pmod{257} = 201^{139} \times 87 \pmod{257} = 173 \end{aligned}$$

Pour un bon choix de p le système El-Gamal resiste bien aux attaques. Comme le système RSA il est assez lent et nécessite des clefs longues 1024 à 2048 bits actuellement). Il se transpose sans difficulté à n'importe quel groupe cyclique où le problème du logarithme discret est difficile, en particulier pour le groupe des points d'une courbe elliptique sur un corps fini. Avec ce groupe malgré les difficultés algorithmique on a de bons codes avec des clefs courtes (128 à 256 bits actuellement) dont la sécurité peut être au moins partiellement prouvée.

9.5 Le cryptosystème elliptique Menezes-Vanstone.

Ce système basé sur le groupe des points d'une courbe elliptique, cf. la section 13.7 page 196, définie sur un corps fini $\mathbb{F}_q$ est une variante du cryptosystème El Gamal.

Soit E une courbe elliptique définie sur le corps fini $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$ ($p > 3$ premier) telle que E contienne un sous-groupe cyclique H, engendré par un point $\mathscr{B}$ de E, dans lequel le problème du logarithme discret soit difficile. Soit

$$\begin{aligned} P &= \mathbb{F}_p^* \times \mathbb{F}_p^*, \text{ les textes en clair} \\ C &= E \times \mathbb{F}_p^* \times \mathbb{F}_p^*, \text{ les textes chiffrés} \end{aligned}$$

Posons, $|H|$ la cardinal de H, et posons

$$K = \big\{(E, \alpha, a, \beta) : \beta = a \cdot \alpha\big\}$$

l'espace des clefs où $\alpha \in E$. Les valeurs α et β sont publiques et $a \in \mathbb{Z}/|H|\mathbb{Z}$ est secret et choisi au hasard.

Pour $K = (E, \alpha, a, \beta)$, et pour un nombre aléatoire secret $k \in \mathbb{Z}/|H|\mathbb{Z}$, et pour $x = (x_1, x_2) \in P = \mathbb{F}_p^* \times \mathbb{F}_p^*$, on chiffre le message x à l'aide de la clef K et du nombre aléatoire k en posant

$$\mathscr{E}_K(x, k) = (y_0, y_1, y_2),$$

où

$$\begin{aligned} y_0 &= k \cdot \alpha, & (c_1, c_2) &= k \cdot \beta, \\ y_1 &= c_1 x_1 \pmod p, & y_2 &= c_2 x_2 \pmod p \end{aligned}$$

Pour déchiffrer un message chiffré

$$y = (y_0, y_1, y_2)$$

on effectue les opérations

$$\mathscr{D}_K(y) = \big(y_1 c_1^{-1} \pmod p, \quad y_2 c_2^{-1} \pmod p\big),$$

où $a \cdot y_0 = (c_1, c_2)$.

9.6 Infrastructure des systèmes à clef publique.

Les ***infrastructures des systèmes à clef publique*** ou ***PKI*** (***Public Key Infrastructure***) consistent en toutes les dispositions techniques et organisationnelles nécessaires pour gérer un système cryptographique à clef publique.

On a un ensemble d'interlocuteurs en réseau qui se sont mis d'accord sur un cryptosystème à clef publique (par exemple RSA), sur une fonction de hachage (cf. le chapitre 10 page 126) et sur un protocole de signature. On suppose que chacun d'entre eux dispose d'une paire (K_e, K_d) (clé publique, clé sécrète), (clé de chiffrement, clé de déchiffrement) et que chacun d'entre eux est capable de chiffrer, déchiffrer et signer.

Du fait que les clés publiques ne sont pas confidentielles, il n'est pas nécessaire de les crypter pour les transmettre. Mais il est très important et même vital pour la sécurité des transmissions de s'assurer de l'authenticité des clés ainsi transmises.

En effet si Alice désire transmettre sa clef publique à Bob, n'importe quel opposant, Martin par exemple, peut intercepter le message la contenant. Martin peut ensuite envoyer un message à Bob en se faisant passer pour Alice et contenant sa propre clé publique et donnant comme adresse de retour sa propre adresse. Ainsi il est capable de lire les messages cryptés que Bob envoie à Alice avec la soit-disant clé publique d'Alice que Bob croit posséder. Une fois qu'il les a décryptés et lu il peut les envoyer à Alice dont il possède la clé publique en les modifiant s'il l'estime nécessaire.

Il faut donc d'une certaine manière faire un lien entre chacun des participants au réseau et sa clé publique. Pour cela on utilise les ***certificats***.

Un certificat consiste en une clef publique et une identité digitale (par exemple une suite de symboles contenant le nom du propriétaire de la clef, de la même manière qu'on met une étiquette sur une clé ordinaire), le tout étant cacheté à l'aide de la signature digitale d'une personne ou d'une organisation en laquelle on a confiance et appelée un ***Tiers de Confiance*** (***Trusted Third Party*** ou ***TTP***) ou encore ***Certification Authority*** ou ***CA***.

Pratiquement on peut par exemple concaténer, mettre bout à bout, la clef publique, le nom de son possesseur et signer le message obtenu à l'aide de la clef privée du Tiers de Confiance (il faut que personne ne puisse usurper l'identité du Tiers de Confiance).

Il existe plusieurs modèles de réseau avec Tiers de Confiance, avec deux modèles extrèmes, le modèle hiérarchique qui repose sur des ***TTP*** distincts des utilisateurs et le modèle distribué où chaque utilisateur est son propre ***CA***.
Un système très employé de système hiérarchique de Tiers de Confiance est le ***modèle X.509***, [34].

Un autre système en voie de développement est le ***chiffrement basée sur l'identité***, ***ID-PKC***, ***Identity Based Public Key Cryptography*** dont l'idée est due à I. Shamir et dont la première réalisation pratique est due à Boneh et Franklin, il est décrit au paragraphe 9.6.1 page 122. Leur solution est basée sur l'accouplement de Weil sur les courbes elliptiques, cf. section 13.7.5 page 204.

Il y a aussi des systèmes non hiérarchiques de PKI fondé sur des chaînes de certificats et une distribution de clefs décentralisées.

Les fonctions principales d'un PKI sont

- Émission de paires de clefs (clé publique, clé privée)
- Attribution d'***identifiants uniques*** aux participants au réseau
- Conservation des clefs
    1. Dépot de clefs, utile quand il s'agit de garantir la continuité d'un service en cas de changement de titulaire
    2. Archivage des clefs, utile pour pouvoir relire de vieux messages
    3. Sauvegarde des clefs, utile en cas de perte de clef
    4. Récuperation de clef perdues

  ces fonctions ne sont pas très distinctes
- Émission et publication des certificats
- Révocation des certificats, maintien et émission des listes de certificats révoqués, ***CRL***.
- fixer leur durée de validité
- Archiver les certificats expirés (important pour les problèmes de non-répudiation)
- Donner une datation sécurisée

Un certain nombre de règles doivent être respectées

a) [**Axiome 1**]: *les clés secrètes doivent l'être et le rester.* En pratique personne, en dehors des propriétaires légitimes, ne doit y avoir accès; la sécurité n'étant pas basée sur l'ignorance des cryptosystèmes mais sur celle des clés, il est plus facile de changer une clef compromise qu'un algorithme.

b) [**Axiome 2**]: *les clés secrètes doivent exister seulement*

   1. en clair, à l'intérieur d'un module résistant (***TRSM***, ***Tamper Resistant Security Module***)
   2. chiffrées ou au moins en morceaux à l'extérieur.

c) [**Axiome 3**]: *limiter le déploiement des clefs*: les clés doivent se trouver en un nombre minimal d'endroits pour limiter les expositions et les risques.

d) [**Axiome 4**]: *séparer les clefs*: les clés doivent être crées et utilisées pour un seul objectif, le raffinement dépendant de la politique de sécurité.

e) [**Axiome 5**]: *synchroniser les clés*: il faut vérifier que toute clé a été employée sans risque pour la sécurité des autres clés.

f) [**Axiome 6**]: *journal des événements*: tous les événements de gestion de toutes les clefs sont transcrits dans un journal, lui même géré de manière sûre.

***Exemple* 9.6.1 (Certificat PGP).** Le certificat PGP, utilisé en PKI distribuée, contient les informations suivantes

- numéro de version PGP utilisée
- la clef publique du porteur du certificat ainsi que l'algorithme employé (RSA, DH ou DSA)
- la signature digitale du propriétaire du certificat
- les informations sur l'identité du porteur du certificat
- la période de validité du certificat
- l'algorithme symétrique préféré du propriétaire du certificat qui sera utilisé pour chiffrer l'information

***Exemple* 9.6.2 (Certificat X.509).** Le certificat X.509, utilisé en PKI hiérarchique, contient les informations suivantes

- *Version*: numéro de version X.509 utilisée
- *Serial number*: numéro de série du certificat (propre à chaque CA)
- *Signature Algo ID*:identifiant du type de signature utilisée
- *Issuer Name*: *Distinguished Name* (DN) du CA qui émet le certificat.
- *Validity period*: la période de validité du certificat
- *Subject Name*: *Distinguished Name* du détenteur de la clef publique.
- *Subject public key info*: informations sur la clef publique de ce certificat.
- *Issuer unique ID*: identifiant unique de l'émetteur de ce certificat.
- *Subject unique ID*: identifiant unique du détenteur de la clef publique.
- *Extensions*: Extensions génériques optionnelles.
- *Signature*: signature numérique du CA sur les champs précédents.

9.6.1 Cryptographie basée sur l'identité.

Dans ce schéma la clef publique d'un utilisateur, Alice, est indéniablement lié à son identité (user ID), ce peut-être une concaténation de son adresse, son numéro de sécurité, sociale, son numéro de téléphone...

Ensuite un algorithme public permet de calculer la clef publique d'Alice, donc plus besoin de consulter des annuaires et pas de risque d'usurpation d'identité à ce stade.

Un tiers de confiance appelé ***KGC***, ***Key Generator Center*** possède un secret, la ***clé maître*** ou ***Master Key***, qui lui permet de calculer la clé privée d'Alice après vérification de son identité.

La sûreté du système repose sur la difficulté de calculer la clé maître à partir de couples (clé privée, clé publique).

Le point faible du système est que tout repose sur la confiance envers le KGC qui peut contrefaire toute signature et dispose de toutes les clefs privées. Pour emédier à cette faiblesse on peut envisager d'avoir plusieur KGC dont

chacun ne fabrique qu'un morceau de la clé privée qui est finalement assemblée par l'utilisateur, Alice, qui sera donc la seule à la connaître.

Un schéma de cryptographie basée sur l'identité (ou ***Identity Based Encryption*** en anglais, en abrégé ***IBE*** proposé par Boneh et Franklin [6] est le suivant:

> Le KGC dispose de deux groupes $(G_1, +)$ et $(G2, *)$ cycliques d'ordre n et d'un couplage symétrique e, c'est à dire d'une application
>
> $$e: \ G_1 \times G_1 \longrightarrow G_2$$
>
> telle que si on note 0 l'élément neutre de G_1 et 1 celui de G_2 on ait
>
> 1. $e(S_1+S_21, T) = e(S_1, T)*e(S_2, T)$, pour tous $S_1, S_2, T \in G_1$
> 2. $e(S, T_1 + T_2) = e(S, T_1) * e(S, T_2)$, pour tous $S, T_1, T_2 \in G_1$
> 3. $e(S, T) = 1$, pour tout $S \in G_1$, resp pour tout $T \in G_1$ implique $T = 0$, resp. $S = 0$.
> 4. $e(S, T)$ soit calculable rapidement.
>
> Il dispose d'un générateur P de G_1.
>
> IL choisit aléatoirement $s \in \left(\mathbb{Z}/qZfield\right)^*$, la clef maître, et calcule $P_{\text{pub}} = sP = \underbrace{P + P + \cdots + P}_{s \text{ fois}}$.
>
> Il choisit deux fonctions de hachage cryptographiques
>
> $$H_1: \ \{0,1\}^* \longrightarrow G_1^*$$
> $$H_2: \ G_2 \longrightarrow \{0,1\}^n$$
>
> où $\{0,1\}^*$ désigne les suites finies composées d'éléments de $\{0,1\}$, autrement dit une suite arbitraire finie de 0 et de 1 et G_1^* désigne les suites finies composées d'éléments de G_1, autrement dit une suite arbitraire finie de $S \in G_1$ et où n est un entier fixé.

On note $\mathscr{M} = \{0,1\}^n$ l'espace des messages clairs et $\mathscr{C} = G_1^* \times \{0,1\}^n$ l'espace des messages chiffrés
La clef secrète de l'utilisateur est faite de la manière suivante.

> Pour une chaîne de caractère ID représentant la clef publique d'Alice

1. le KGC calcule $Q_{ID} = H_1(ID) \in G_1^*$
2. il génère la clef secrète d'Alice: $d_{ID} = sQ_{ID}$

Pour chiffrer un message $M \in \mathscr{M}$ avec la clef publique ID d'Alice, Bob calcule

1. $Q_{ID} = H_1(ID)$
2. Il choisit aléatoirement $r \in \big(\mathbb{Z}/qZfield\big)^*$
3. $C = \big(rP, M \oplus H_2\big(g_{ID}^r\big) \in G_1^* \times \{0,1\}^n$ où $\oplus$ est l'opération XOR habituelle sur les suites de 0 et de 1 et où $g_{ID} = e(Q_{ID}, P_{\text{pub}} \in G_2^*$.

Pour déchiffrer le message chiffré $C = U, V) \in G_1^* \times \{0,1\}^n$ Alice effectue les opérations suivantes

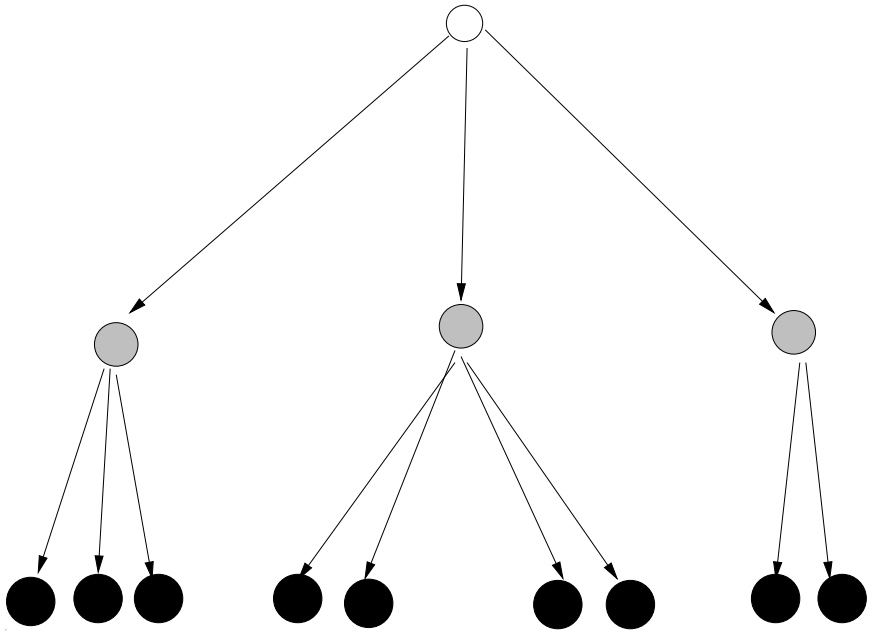
1. Elle calcule $M = V \oplus H_2\big(e(d_{ID}, U)\big)$

On a bien

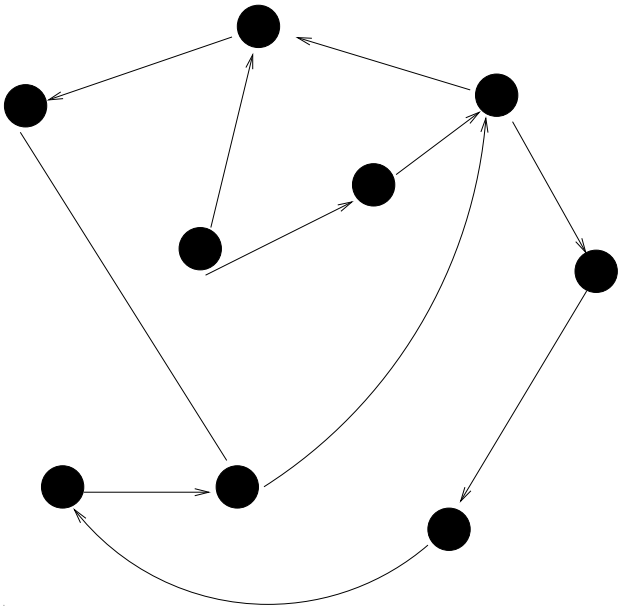
$$\begin{aligned} e(d_{ID}, U) &= e(sQ_{ID}, U = e(sQ_{ID}, rP) = e(Q_{iD}, P)^{sr} \\ &= eQ_{ID}, sP)^r = e(Q_{ID}, P_{\text{PUB}} = g_{ID}^r \end{aligned}$$

et donc $H_2\big(e(d_{ID}, U)\big) = H_2\big(g_{ID}^r\big)$ et par conséquent, comme $\oplus$ est involutif, Alice a bien récupéré le message en clair envoyé par Bob.

En pratique on choisit une courbe elliptique, E, sur un corps fini, $\mathbb{F}_q$. Comme groupe G_1 on prend un sous-groupe, $E[n] = G_1$, cyclique de $E(\mathbb{F}_q)$ d'ordre élevé engendré par un point $P \in E(\mathbb{F}_q)$ comme groupe G_2 le groupe $\mu_n = G_2$. On prend comme couplage e une modification de l'accouplement de Weil.



Système hiérarchique de Tiers de Confiance



Système non-hiérarchique de Tiers de Confiance

Chapitre 10

Fonctions de Hachage.

Les procédures de signature précédentes ont un coût prohibitif pour signer des longs messages car la signature est aussi longue que le message. On double donc la longueur du texte à crypter.

Pour réduire la longueur de la signature on peut utiliser une ***fonction de hachage*** cryptographique (***hash function*** en anglais), h, ou fonction de condensation. C'est une fonction à sens unique qui sera publique dans les applications.

Les fonctions de hachage ont d'autres applications cryptographiques que la signature, cf le chapitre 11 page 133 sur les protocoles cryptographiques.

Une fonction de hachage est une fonction rapide à calculer mais dont l'image réciproque est dans la classe des problèmes calculatoirement difficiles (la classe NP). Ell transforme un message de longueur arbitraire en une ***empreinte numérique*** ou ***code d'authentification*** du message de taille fixée, 160 bits en général actuellement. Pour des raisons de sécurité on tend à augmenter la taille de l'empreinte.

Le schéma de calcul d'une signature avec une fonction de hachage est le suivant:

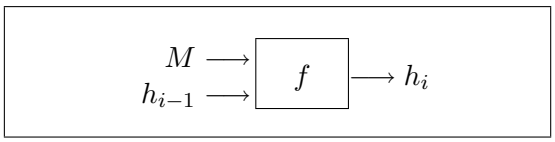
message	x	longueur arbitraire
	$\downarrow$	
empreinte numérique	$z = h(x)$	160 bits
	$\downarrow$	
signature	$y = \mathrm{sign}_K(z)$	320 bits

En réalité une fonctions de hachage prend un message x de taille inférieure à N fixé qu'elle transforme en une empreinte de taille 160 bits (ou 256 ou 384 ou 512).

Il existe des techniques classiques, cf. [31], pour étendre les fonctions de hachage de domaine de départ fini (***fonction de compression***) $\leq N$ en des fonctions de hachage dont le domaine de départ est constitué de messages de longueur arbitraire. Elles sont appelées alors ***fonctions de hachage itérées***. La principe pour l'itération est le suivant. On suppose que la fonction h peut recevoir deux entrées

- une empreinte h_{i-1}
- un bloc M de taille N

et donner en sortie une empreinte h_i.



On peut supposer que cette extension des fonctions de hachage est déjà faite.

Lorsqu'Alice souhaite envoyer un message signé, x, elle calcule d'abord l'empreinte numérique, $z = h(x)$, elle signe avec $y = \text{sign}_K(z)$ et transmet le couple (x, y) par le canal de communication.

Tout le monde peut vérifier la signature en calculant l'empreinte $z = h(x)$ et en utilisant le procédé de vérification de la signature $\text{ver}_K(z, y)$.

10.1 Construction des fonctions de hachage.

La fonction de hachage doit être construite avec soin pour qu'elle n'affaiblisse pas le protocole de signature. Un opposant comme Martin ne doit pas pouvoir forger la signature d'Alice.

Comme une fonction de hachage n'est évidemment pas injective, il existe des couples de messages x' et x tels que $h(x') = h(x)$. L'attaque la plus évidente consiste pour Martin à partir d'un message signé (x, y) authentique $(y = \text{sign}_K(x))$ précedemment calculé par Alice à calculer $z = h(x)$ et à chercher $x' \neq x$ tel que $h(x) = h(x')$. Si Martin y parvient (x', y) est un message valide.

Donnons tout d'abord quelques définitions de qualités que l'on peut exiger d'une fonction de hachage.

Définition 10.1.1. *Une fonction de hachage h est à* **collisions faibles difficiles** *si étant donné un message x, il est calculatoirement difficile d'obtenir un message $x' \neq x$ tel que $h(x) = h(x')$.*

Définition 10.1.2. *Une fonction de hachage h est à* **collisions fortes difficiles** *s'il est calculatoirement difficile d'obtenir deux messages différents x et x' tels que $h(x) = h(x')$*

Définition 10.1.3. *Une fonction de hachage est une* **fonction de hachage à sens unique** *si étant donnée une empreinte numérique z, il est calculatoirement difficile de trouver un message x tels $h(x) = z$*

Si une fonction de hachage est à collisions fortes difficiles elle est bien sûr à collisions faibles difficiles, mais aussi à sens unique.

10.1.1 Attaques des anniversaires.

Une fonction de hachage doit aussi résister aux ***attaques des anniversaires***.

Une méthode simple pour obtenir des collisions, i.e. des messages x et x' tels que $h(x) = h(x')$ est l'attaque des anniversaires décrite ci-dessous.

On a une fonction de hachage $h : X \to Z$ où $|X| = m < +\infty$ et $|Z| = n$ et $m \geq 2n$. Dans ces conditions il y a au moins n collisions.

On va trouver la borne inférieure de la probabilité de trouver une collision en tirant k messages aléatoires distincts. Cette borne dépend de k et n mais pas de m. On fait l'hypothèse simplificatrice que $|h^{-1}(z)| \approx m/n$.

Il est alors facile de calculer la probabilité pour que k éléments $z_i \in Z$ soient tous distincts si l'on tire au hasard k éléments $x_i \in X$.

On ordonne les z_i en z_1,..., z_k. Le premier tirage z_1 est arbitraire; la probabilité pour que $z_2 \neq z_1$ est $1 - \dfrac{1}{n}$; la probabilité pour que z_3 soit distinct de z_1 et z_2 est $1 - \dfrac{2}{n}$, etc...
La probabilité de non-collision est donc

$$\Big(1 - \frac{1}{n}\Big)\Big(1 - \frac{1}{n}\Big) \dots \Big(1 - \frac{k-1}{n}\Big) = \prod_{i=1}^{k-1} \Big(1 - \frac{i}{n}\Big)$$

avec un peu d'analyse élémentaire on voit facilement en utilisant l'approximation

$$e^{-x} \approx 1 - x \text{ si } x \text{ petit}$$

que:

$$\prod_{i=1}^{k-1}\left(1-\frac{i}{n}\right) \approx \prod_{i=1}^{k-1} e^{-\frac{i}{n}} = e^{-\frac{k(k-1)}{2n}}$$

La probabilité d'une collision est donc $1 - e^{-\frac{k(k-1)}{2n}}$. Si l'on veut que cette probabilité soit inférieure à ε alors il suffit de prendre

$$k \geq \sqrt{2n \log \frac{1}{1-\varepsilon}}$$

Par exemple dans une assemblée de 23 personnes la probabilité d'avoir deux dates d'anniversaire égales est supérieure à 1/2.

Une empreinte de 40 bits est vulnérable à une attaque des anniversaires avec probabilité supérieure à 1/2 en utilisant seulement 2^{20} messages aléatoires. Pour une empreinte de 128 bits il faut 2^{64} messages aléatoires. Le choix d'une empreinte de 160 bits donne une bonne résistance aux attaques anniversaires. Mais l'augmentation de la puissance de calcul disponible pour un attaquant pousse à augmenter la taille des empreintes, c'est pourquoi AES prévoit des empreintes de 256 à 512 bits.

10.1.2 Exemple académique de fonction de hachage.

Fonction de hachage de Chaum-van Heijst-Pfitzmann. Elle n'est pas utilisée en pratique car trop lente.

Soit $p = 1 + 2q$ un grand nombre premier tel que q soit aussi premier. Soit α et β deux éléments primitifs de $(\mathbb{Z}/p\mathbb{Z})^*$. La valeur de $\log_\alpha \beta$ n'est pas publique et l'on suppose qu'elle est calculatoirement difficile à obtenir.

On démontre que la fonction de hachage

$$\begin{aligned} h : \{0, 1 \ldots, q-1\} \times \{0, 1 \ldots, q-1\} &\longrightarrow (\mathbb{Z}/p\mathbb{Z})^* \\ (x_1, x_2) &\longmapsto h(x_1, x_2) = \alpha^{x_1} \beta^{x_2} \end{aligned}$$

résiste aux collisions si le calcul de $\log_\alpha \beta$ est difficile.

10.1.3 Fonction de hachage standard.

Un standard actuel en matière de fonction de hachage est ***SHA-1*** (***Secure Hash Algorithm***) avec une empreinte de taille 160 bits, faisant suite aux standard MD4 (1990), MD5 (1992), SHA (1995), cf. [31].

Depuis 2001, une nouvelle version de SHA-1, SHA-2, ainsi que les versions SHA-256, SHA-384 et SHA-512 sont en cours de validation (256, 384, 512 est la taille en bits de l'empreinte).

Description sommaire de SHA:

1. Le message est complété pour que longueur soit un multiple de 512 bits; pour cela on ajoute un bit à 1, un certain nombres de bits à 0, et un entier sur 64 bits représentant la longueur du message avant remplissage.

2. On initialise les registres A, B, C, D et E avec des constantes fixées

3. Pour chaque bloc de 512 bits du message

   (a) on copie A, B, C, D et E respectivement dans AA, BB, CC, DD et EE

   (b) on applique la fonction de compression, donnée ci dessous, à AA, BB, CC, DD et EE pour le bloc courant

   (c) on ajoute les valeurs trouvées à A, B, C, D et E

4. le résultat est la concaténation de A, B, C, D et E

Fonction de compression

1. Les 512 bits du bloc courant sont scindés en 16 mots de 32 bits $(W^{(0)}, \ldots, W^{(15)})$

2. on réalise une expansion par

   $$\forall\, i \in \{16, \ldots, 79\},\ W^{(i)} = \mathrm{ROL}_1\big(W^{(i-3)} \oplus W^{(i-8)} \oplus W^{(i-14)} \oplus W^{(i-16)}\big)$$

   où ROL_k représente un décalage circulaire de k-bits vers la gauche et $\oplus$ l'addition modulo 2 bit à bit et sans retenue (=ou exclusif).

3. Ces 80 mots de 42 bits sont utilisés pour modifier les 5 variables d'état $A^{(i)}$, $B^{(i)}$, $C^{(i)}$, $D^{(i)}$, $E^{(i)}$

   - on initialise

     $$\big(A^{(0)}, B^{(0)}, C^{(0)}, D^{(0)}, E^{(0)}\big) = \big(AA, BB, CC, DD, EE\big)$$

- pour i variant de 0 à 79

$$A^{(i+1)} = \mathrm{ADD}\big(W^{(i)}, \mathrm{ROL}_5(1^{(i)}, f^{(i)}(B^{(i)}, C^{(i)}, D^{(i)}, E^{(i)}, K^{(i)})\big)$$
$$B^{(i+1)} = A^{(i)}$$
$$C^{(i+1)} = \mathrm{ROL}_{30}(B^{(i)})$$
$$D^{(i+1)} = C^{(i)}$$
$$E^{(i+1)} = D^{(i)}$$

où

- ADD représente l'addition modulo 2^{32}
- Les $K^{(i)}$ sont des constantes fixées et les fonctions $f^{(i)}$ sont définies par

i	$f^{(i)}$	$K^{(i)}$
$0-19$	$(X \wedge Y) \vee (X \wedge Z)$	$5A827999$
$30-39$	$X \oplus Y \oplus Z$	$6ED9EBA1$
$40-59$	$(X \wedge Y) \vee (X \wedge Z) \vee (Y \wedge Z)$	$8F1BBCDC$
$60-79$	$X \oplus Y \oplus Z$	$CA62C1D6$

où $\vee$ représente le *ou inclusif* et $\wedge$ le *et*

l'architecture est représentée par le schéma 10.1

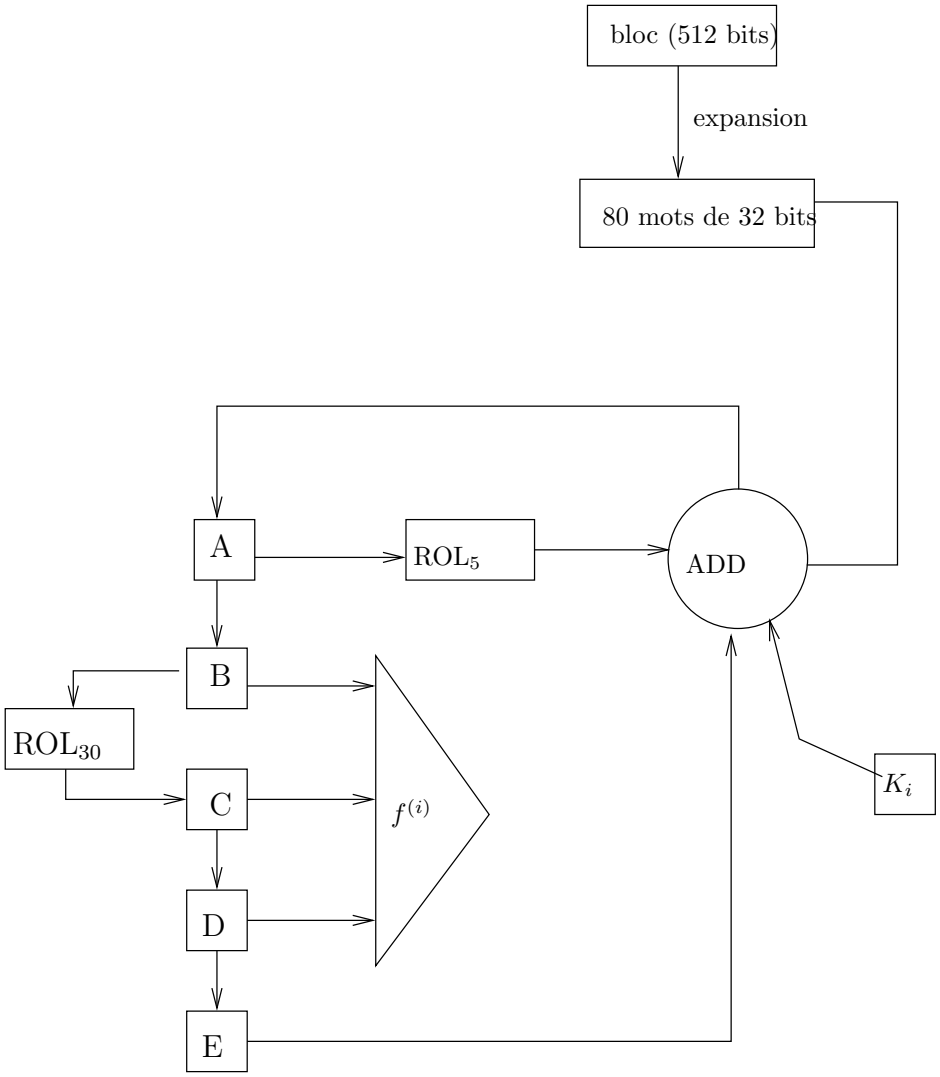


Figure 10.1: Architecture du SHA

Chapitre 11

Quelques protocoles cryptographiques.

11.1 Protocoles de signature.

Nous avons déjà décrit des protocoles de signature RSA et El Gamal. Nous allons décrire un protocole de signature utilisable avec les cryptosystèmes symétriques et nous allons rappeler le protocole de signature pour un cryptosystème à clef publique déjà décrit.

11.1.1 Protocole de signature à clef privée.

Signature d'un document à l'aide d'un cryptosystème à clef secrète et d'un ***arbitre*** ou ***tiers de confiance***.

Les utilisateurs d'un cryptosystème à clef publique se choisissent un arbitre, Yvan, c'est à dire une entité (personne, organisation, machine) en qui ils ont toute confiance.

Yvan communique avec Alice et Bob. Il partage une clé secrète K_A avec Alice et une clé secrète K_B avec Bob.

Le protocole de signature est alors le suivant

1. Alice chiffre son message pour Bob avec la clé K_A et envoie le résultat à Yvan.
2. Yvan déchiffre le message avec K_A et garde l'original.
3. Yvan assemble le message avec un avis certifiant que le message vient d'Alice. Il chiffre le tout avec K_B et l'envoie à Bob.
4. Bob déchiffre le message d'Yvan avec K_B. Il lit le message et le certificat d'Yvan.

5. Comme il a confiance en Yvan, il admet que le message reçu est conforme à l'original et vient bien d'Alice.

Ce protocole est-il sûr?
Les 3 qualités que l'on demande à un cryptosystème sont-elles bien présentes:

- Intégrité des données.
- Identités des différents interlocuteurs.
- Non-répudiation.

Bien sûr on suppose qu'Alice garde bien secrète la clef qu'elle partage avec Yvan et qu'Yvan est vraiment un tiers de confiance.

1. La signature est authentique car Yvan est respecté et seul Alice et lui connaissent K_A donc la message vient bien d'Alice.
2. La signature est infalsifiable. Seule Alice (et Yvan qui est insoupçonnable) connait K_A, donc seule Alice peut envoyer le message codé avec K_A.
3. La signature n'est pas réutilisable pour un autre message. Si Bob essaie de prendre le certificat d'Yvan et de l'associer à un autre message censé provenir d'Alice, cette dernière crierait à l'imposture. L'arbitre demandera alors à Bob de produire le texte en clair. Il le chiffrerait avec K_A et comparerait avec le message original d'Alice. Il verra qu'ils sont différents et en informera qui de droit.
4. Le document est immuable. Si Bob falsifiait le message après l'avoir reçu, Yvan pourrait dévoiler l'imposture comme ci-dessus.
5. La signature ne peut pas être reniée. Si Alice prétend ne pas avoir envoyé le message, le certificat d'Yvan prouverait le contraire (tout le monde a confiance en Yvan).

Bob pourrait nier avoir reçu le message mais alors un système d'accusé de réception permettrait d'éviter ce problème.

11.1.2 Protocole de signature à clef publique.

Le protocole est simple

1. Alice chiffre le document d'une part avec sa clé privée, signant ainsi le document, et d'autre part avec la clé publique de Bob

2. Alice envoie les deux document à Bob.

3. Bob déchiffre le premier document avec la clé publique d'Alice et le second avec sa clé privée. Si les deux sont identiques il est sûr qu'Alice est l'expéditeur.

Ce protocole est-il sûr?
Les 3 qualités que l'on demande à un cryptosystème sont-elles bien présentes:

- Intégrité des données.
- Identités des différents interlocuteurs.
- Non-répudiation.

Bien sûr on suppose que chacun des correspondants ne communique à personne sa clé secrète

1. La signature est authentique: quand Bob vérifie le message avec la clé publique d'Alice, il est sûr que seule Alice pouvait l'avoir crypté avec sa clé privée.

2. La signature est infalsifiable. Seule Alice connait sa clé privée.

3. La signature n'est pas réutilisable. La signature est une fonction du document et elle ne peut pas être transférée sur n'importe quel autre document.

4. Le document est immuable. Si Bob falsifiait le message après l'avoir reçu, il ne pourrait pas le signer car la clé privée d'Alice n'est connue que d'elle seule.

5. La signature ne peut pas être reniée. Bob n'a pas besoin de l'aide d'Alice pour vérifier sa signature.

11.2 Protocoles de datation.

Dans certaines circonstances Bob peut duper Alice.

Il peut réutiliser le document (par exemple un chèque signé) et le présenter plusieurs fois à la banque. Pour l'éviter les signatures numériques comportent souvent une datation (date+heure). Cette datation de la signature est attachée au message et signée avec lui.

La banque stocke ces datations dans une base de données.

11.2.1 Protocole de datation.

On peut confier la datation des documents à un service officiel de datation. Bob veut dater une signature du message x. Il dispose d'une fonction de hachage à sens unique, h. Il suit alors le protocole suivant

1. Bob calcule $z = h(x)$ et $y = sig_K(z)$
2. Bob soumet (z, y) au service de datation.
3. Le service de datation ajoute la date D et signe le triplet (z, y, D)

Bob peut aussi dater un document, x, seul. Pour cela il collecte un certain nombre d' informations publiques récentes (qui n'auraient pas pu être prédites auparavant), notée ***pub***. Par exemple les derniers résultats des courses hippiques et les cours actuels de la bourse. Il dispose aussi d'une fonction de hachage publique à sens unique, h. Bob suit alors le protocole suivant:

1. Bob calcule $z = h(x)$
2. Bob calcule $z' = h(z||\text{pub})$
3. Bob calcule $y = sig_K(z')$
4. Bob publie (z, pub, y) dans le prochain quotidien

La date de la signature de Bob est comprise entre la date des informations ***pub*** et la date de parution du quotidien.

11.3 Protocole de signature à clef publique et fonction de hachage.

Les algorithmes à clef publique sont trop lents pour signer de longs documents.

Pour gagner du temps les protocoles de signature numérique sont souvent réalisés avec des fonctions de hachage à sens unique.

Au lieu de signer le document Alice signe l'empreinte du document en suivant le protocole suivant:

1. Alice calcule à l'aide de la fonction de hachage à sens unique, l'empreinte du document.

2. Alice chiffre, à l'aide de l'algorithme de signature numérique, cette empreinte avec sa clef privée, signant par la même occasion le document.

3. Alice envoie le document et l'empreinte signée à Bob (à l'aide de la clef publique de Bob).

4. Bob calcule, à l'aide de la fonction de hachage à sens unique, l'empreinte du document qu'Alice lui a envoyé. Ensuite à l'aide de l'algorithme de signature numérique, il déchiffre l'empreinte signée avec la clef publique d'Alice. La signature est valide si l'empreinte de la signature est la même que l'empreinte qu'il a produite.

Avantage de ce procédé:

- rapidité de la transmission et de la comparaison des empreintes car une empreinte ne comporte que 160 bits ou au plus 512.
- confidentialité car la signature peut être gardée à part du message. On peut donc vérifier l'existence du document sans stocker son contenu.

11.4 Fonction de hachage et mot de passe.

Pour accéder à un ordinateur (ou à un distributeur de billet) on utilise souvent un mot de passe qui doit être reconnu par l'ordinateur. S'il est stocké dans l'ordinateur il y a danger pour la sécurité car un ordinateur peut être facilement infiltré (virus). Grâce à la fonction de hachage on peut résoudre à ce problème:

On dispose d'une fonction de hachage à sens unique, h. L'ordinateur ne stocke pas le mot de passe $\boldsymbol{mp}$ d'Alice mais le résultat de la fonction de hachage à sens unique appliquée à $\boldsymbol{mp}$. Le protocole est donc le suivant:

1. Alice envoie son mot de passe $\boldsymbol{mp}$ à l'ordinateur.

2. L'ordinateur calcule $h(\mathrm{mp})$

3. L'ordinateur compare le résultat de ce calcul à celui qu'il a dans sa base de données.

Ce protocole permet de se défendre contre le vol de la base des données des mots de passe des utilisateurs.

En fait on peut encore améliorer ce protocole avec les protocoles de preuve sans transfert de connaissance.

11.5 Preuve sans transfert de connaissance.

Un jeu de ***Pile ou face par Téléphone***. Considérons la situation suivante, cf. [37].

Alice et Bob viennent de divorcer et habitent dans des villes différentes et veulent par téléphone tirer à pile ou face pour savoir à qui va échoir la voiture, la machine à laver, les livres, etc...

Mais Bob hésite à dire à Alice ***face*** pour s'entendre dire ***voilà je jette une pièce***,..., ***elle retombe***,..., ***pas de chance c'est pile***.

Ils veulent un protocole qui évite toute tricherie.

Ils se donnent un ensemble E par exemple $E = \{0, 1, \ldots, n\}$ et une partition $E = X_0 \cup X_1$ de E , X_0 sera les entiers pairs de E et X_1 les entiers impairs de E. Puis ils se mettent d'accord sur une fonction à sens unique, f, de E dans un ensemble F.

On considère le protocole suivant

1. Alice choisit un élément $x \in E$ aléatoirement (c'est le jet de la pièce), calcule $y = f(x)$ et communique y à Bob (Bob ne peut pas retrouver x à partir de y car f est à sens unique).
2. Bob choisit son bit aléatoire $b \in \{0, 1\}$ et l'annonce à Alice
3. Alice déclare qui a gagné suivant que $x \in X_b$ ou non: elle prouve sa bonne foi en révélant x
4. Bob se convainc qu'il n'y a pas eu tricherie en vérifiant que $y = f(x)$

Ce protocole est-il sûr:

1. Si la fonction f est bien choisie la donnée de $f(x)$ n'apprend rien à Bob sur x.
2. Pour qu'Alice ne puisse pas tricher, il faut s'assurer qu'elle ne peut pas fabriquer deux entiers $x_0 \in X_0$ et $x_1 \in X_1$ tels que $f(x_0) = f(x_1)$, par exemple on peut prendre f bijective car l'ensemble est de taille réduite.
3. f doit être à sens unique en un sens fort pour que la connaissance de $f(x)$ n'apprenne rien à Bob sur l'appartenance de x à X_0 ou X_1

Ce protocole met en évidence la notion d'***engagement***: Alice s'engage sur x en publiant $f(x)$. Cela ne révèle rien sur x mais force Alice à ne pas modifier son choix.

11.5.1 Protocole de preuve sans transfert de connaissances.

Le protocole précédent peut être utilisé dans beaucoup de situation où l'on veut prouver que l'on connait un secret sans avoir besoin de le révéler.

Pour accéder à un ordinateur on donne son mot de passe qui est reconnu par l'ordinateur et donc stocké dedans. Si l'ordinateur auquel on se connecte est lointain, le mot de passe circule (crypté) sur des canaux qui risquent d'être espionnés.

Pour la sécurité il faudrait le changer souvent. Si la connexion est coupée accidentellement, il faut le redonner sans avoir la possiblité d'en changer.

Le clavier sur lequel on compose le mot de passe peut être espionné.

Il y a donc un intérêt à avoir un système de reconnaissance sans envoi de mot de passe même crypté.

Pour cela il faut disposer d'un secret personnel s et d'un protocole qui permet de persuader l'ordinateur (ou la personne) auquel on se connecte (s'adresse) qu'on connait s sans avoir à le révéler et ce à chaque fois à l'aide de messages différents.

De tels protocoles existent ce sont des applications des idées de ***complexité calculatoire*** et de fonctions à sens unique.

***Exemple* 11.5.1** (Preuve de possession d'un logarithme discret)**.** Cet exemple est tiré de [37]. On se donne p un nombre premier et g une racine primitive modulo p (théorème 13.3.17 page 172) qui sont publics et tels que le problème du logarithme discret soit un problème calculatoirement difficile.

Supposons que P (le prouveur) détienne le nombre secret s et soit identifié par $I = g^s \mod p$. Il s'agit de convaincre V (le vérificateur) que P connait s.

Considérons le protocole suivant:

1. P choisit un $r \mod p-1$ aléatoire, il calcule $t = \alpha^r \pmod p$ et le communique à V.

2. V choisit un bit aléatoire $\varepsilon = 0, 1$ et le communique à P

3. P donne x à V où $\begin{cases} x \equiv r \mod p-1 & \text{si } \varepsilon = 0 \\ x \equiv r + s & \text{si } \varepsilon = 1 \end{cases}$

V vérifie alors que $\begin{cases} \alpha^x = t \mod p & \text{si } \varepsilon = 0 \\ \alpha^x \equiv It \mod p & \text{si } \varepsilon = 1 \end{cases}$.

Comme dans le protocole de pile ou face P s'est engagé sur r en communiquant $t = \alpha^r$.

Que peut faire un imposteur P^* qui ne connait pas s et veut se faire passer pour P auprès de V.

- Il peut suivre le protocole et espérer que $\varepsilon = 0$; dans le cas contraire il ne saura pas quel y communiquer à **V**.
- Il peut au contraire choisir un r aléatoire et communiquer à V la quantité $t' = \dfrac{\alpha^r}{I}$. Si V choisit $\varepsilon = 1$ alors P^* donne $x' = r$ et survit à la vérification $\alpha^{x'} = t'I$. Mais si $\varepsilon = 0$ alors P^* ne sait que faire.

Donc quel que soit la manière dont P^* s'y prenne il n'a qu'une chance sur deux de donner la bonne réponse.

1. Au bout de k applications du protocole, V est convaincu avec probabilité de $1 - \dfrac{1}{2^k}$ que son interlocuteur détient un logarithme de I
2. L'information révélée à V n'est qu'une liste d'entiers modulo p aléatoires et de leurs images par l'exponentielle $x \longmapsto \alpha^x$. Le vérificateur V aurait pu aussi bien se la constituer seul en choisissant au hasard des entiers modulo p et en les exponentiant modulo p.
3. P n'a révélé aucune information sur son secret le logarithme de I.

C'est un exemple de ***protocole interactif*** et sans transfert de connaissance (zero knowledge proof).

Il y a d'autres protocoles qui permettent par exemple de réaliser un ***transfert inconscient***.

11.5.2 Transfert inconscient.

Alice dispose d'un ensemble de m secrets $\{s_1, s_2, \ldots, s_m\}$. Alice est prête à en donner (vendre) un à Bob.

Bob aimerait obtenir le secret s_i, mais il ne souhaite pas révéler à Alice lequel des secrets l'intéresse. Il existe des protocoles, [37], qui donnent une solution à ce problème:

1. ils permettent à Bob de disposer de s_i
2. ils ne lui donnent aucune information sur les autres secrets s_j, $j \neq i$
3. ils ne permettent pas à Alice de savoir quel secret elle a livré à Bob

Chapitre 12

La cryptographie et le droit.

Le droit joue un rôle important en cryptographie comme dans beaucoup de techniques liées aux aspects régaliens du rôle de l'État. Le droit vient au secours de l'État et des citoyens quand une technique menace leur intérêt et au contraire vient au secours d'une technique quand ses limitations ne lui permettent pas de remplir de manière transparente et sûre les missions qui lui sont confiées.

Par exemple s'il existait une cryptographie inviolable elle pourrait premettre des usages frauduleux qui ne pourrait pas être détectés (transferts de capitaux, espionnage,...). Au contraire s'il n'existait pas de cryptographie sûre les États auraient du mal à communiquer de manière confidentielle avec leur ambassadeurs. Dans un cas comme dans l'autre les États édictent des lois soit pour interdire l'utilisation libre d'une cryptographie inviolable soit pour limiter l'usage de la cryptanalyse.

12.1 Quelques textes juridiques sur la cryptographie.

12.1.1 LOI n° 96-659 du 26 juillet 1996 .

LOI n° 96-659 du 26 juillet 1996 de réglementation des télécommunications (1)

Article 17. - L'article 28 de la loi n° 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications est ainsi modifié :

I. - Le I est ainsi modifié :
1° Le premier alinéa est complété par une phrase ainsi rédigée :

> On entend par moyen de cryptologie tout matériel ou logiciel conçu ou modifié dans le même objectif.

2° Les deuxième, troisième, quatrième et cinquième alinéas sont remplacés par les dispositions suivantes :

Pour préserver les intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, tout en permettant la protection des informations et le développement des communications et des transactions sécurisées :

1° L'utilisation d'un moyen ou d'une prestation de cryptologie est :

a) Libre :

- si le moyen ou la prestation de cryptologie ne permet pas d'assurer des fonctions de confidentialité, notamment lorsqu'il ne peut avoir comme objet que d'authentifier une communication ou d'assurer l'intégrité du message transmis,

- ou si le moyen ou la prestation assure des fonctions de confidentialité et n'utilise que des conventions secrètes gérées selon les procédures et par un organisme agréés dans les conditions définies au II ;

b) Soumise à autorisation du Premier ministre dans les autres cas ;

2° La fourniture, l'importation de pays n'appartenant pas à la Communauté européenne et l'exportation tant d'un moyen que d'une prestation de cryptologie :

a) Sont soumises à autorisation préalable du Premier ministre lorsqu'ils assurent des fonctions de confidentialité ; l'autorisation peut être subordonnée à l'obligation pour le fournisseur de communiquer l'identité de l'acquéreur,

b) Sont soumises à la déclaration auprès du Premier ministre dans les autres cas ;

3o Un décret fixe les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations. Ce décret prévoit :

a) Un régime simplifié de déclaration ou d'autorisation pour certains types de moyens ou de prestations ou pour certaines catégories d'utilisateurs ;

b) La substitution de la déclaration à l'autorisation pour les opérations portant sur des moyens ou des prestations de cryptologie, dont les caractéristiques techniques ou les conditions d'utilisation, tout en justifiant, au regard des intérêts susmentionnés, un suivi particulier, n'exigent pas l'autorisation préalable de ces opérations ;

c) La dispense de toute formalité préalable pour les opérations portant sur des moyens ou des prestations de cryptologie, dont les caractéristiques techniques ou les conditions d'utilisation sont telles que ces opérations ne sont pas susceptibles de porter atteinte aux intérêts mentionnés au deuxième alinéa ;

d) Les délais de réponse aux demandes d'autorisation.

II. - Le II est remplacé par un II et un III ainsi rédigés :

II. - Les organismes chargés de gérer pour le compte d'autrui les conventions secrètes de moyens ou prestations de cryptologie permettant d'assurer des fonctions de confidentialité doivent être préalablement agréés par le Premier ministre.

Ils sont assujettis au secret professionnel dans l'exercice de leurs activités agréées.

L'agrément précise les moyens ou prestations qu'ils peuvent utiliser ou fournir.

Ils sont tenus de conserver les conventions secrètes qu'ils gèrent. Dans le cadre de l'application de la loi no 91-646 du 10 juillet 1991 relative au secret

des correspondances émises par la voie des télécommunications ainsi que dans le cadre des enquêtes menées au titre des chapitres premier et II du titre II du livre premier du code de procédure pénale, ils doivent les remettre aux autorités judiciaires ou aux autorités habilitées, ou les mettre en oeuvre selon leur demande.

Lorsque ces organismes remettent les conventions secrètes qu'ils gèrent dans le cadre des enquêtes menées au titre des chapitres premier et II du titre II du livre premier du code de procédure pénale, suite aux réquisitions du procureur de la République, ils informent les utilisateurs de cette remise.

Ils doivent exercer leurs activités agréées sur le territoire national.

Un décret en Conseil d'Etat fixe les conditions dans lesquelles ces organismes sont agréés ainsi que les garanties auxquelles est subordonné l'agrément ; il précise les procédures et les dispositions techniques permettant la mise en oeuvre des obligations indiquées ci-dessus.

III. - a) Sans préjudice de l'application du code des douanes, le fait de fournir, d'importer de pays n'appartenant pas à la Communauté européenne ou d'exporter un moyen ou une prestation de cryptologie sans avoir obtenu l'autorisation préalable mentionnée au I ou en dehors des conditions de l'autorisation délivrée est puni de six mois d'emprisonnement et de 200 000 F d'amende.

Le fait de gérer, pour le compte d'autrui, des conventions secrètes de moyens ou de prestations de cryptologie permettant d'assurer des fonctions de confidentialité sans avoir obtenu l'agrément mentionné au II ou en dehors des conditions de cet agrément est puni de deux ans d'emprisonnement et de 300 000 F d'amende.

Le fait de fournir, d'importer de pays n'appartenant pas à la Communauté européenne, d'exporter ou d'utiliser un moyen ou une prestation de cryptologie en vue de faciliter la préparation ou la commission d'un crime ou d'un délit est puni de trois ans d'emprisonnement et de 500 000 F d'amende.

La tentative des infractions prévues aux alinéas précédents est punie des mêmes peines.

b) Les personnes physiques coupables des infractions prévues au a encourent les peines complémentaires prévues aux articles 131-19, 131-21 et 131-27 et, à titre définitif ou pour une durée de cinq ans au plus, les peines prévues aux articles 131-33 et 131-34 du code pénal.

III. - Le III devient IV. Son dernier alinéa est ainsi rédigé :

Est puni d'un emprisonnement de six mois et d'une amende de 200 000 F le fait de refuser de fournir les informations ou documents ou de faire obstacle au déroulement des enquêtes mentionnées au présent paragraphe.

Après le mot *autorisations* sont insérés les mots *et déclarations*.

V. - Il est ajouté un VI ainsi rédigé :

VI. - Les dispositions du présent article ne font pas obstacle à l'application du décret du 18 avril 1939 fixant le régime des matériels de guerre, armes et munitions, à ceux des moyens de cryptologie qui sont spécialement conçus ou modifiés pour permettre ou faciliter l'utilisation ou la mise en oeuvre des armes.

VI. - Le V devient VII.

VII. - Le présent article est applicable aux territoires d'outre-mer et à la collectivité territoriale de Mayotte.

12.1.2 LOI n° 2004-575 du 21 juin 2004.

LOI n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

TITRE III

DE LA SÉCURITÉ DANS L'ÉCONOMIE NUMÉRIQUE

Chapitre Ier

Moyens et prestations de cryptologie

Article 29 On entend par moyen de cryptologie tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité.

On entend par prestation de cryptologie toute opération visant à la mise en oeuvre, pour le compte d'autrui, de moyens de cryptologie.

Section 1

Utilisation, fourniture, transfert, importation et exportation de moyens de cryptologie

Article 30 I. - L'utilisation des moyens de cryptologie est libre.

II. - La fourniture, le transfert depuis ou vers un Etat membre de la Communauté européenne, l'importation et l'exportation des moyens de cryptologie assurant exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont libres.

III. - La fourniture, le transfert depuis un Etat membre de la Communauté européenne ou l'importation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont soumis à une déclaration préalable auprès du Premier ministre, sauf dans les cas prévus au b du présent III. Le fournisseur ou la personne procédant au transfert ou à l'importation tiennent à la disposition du Premier ministre une description des caractéristiques techniques de ce moyen de cryptologie, ainsi que le code source des logiciels utilisés. Un décret en Conseil d'Etat fixe :

a) Les conditions dans lesquelles sont souscrites ces déclarations, les conditions et les délais dans lesquels le Premier ministre peut demander communication des caractéristiques du moyen, ainsi que la nature de ces caractéristiques ;

b) Les catégories de moyens dont les caractéristiques techniques ou les conditions d'utilisation sont telles que, au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, leur fourniture, leur transfert depuis un Etat membre de la Communauté européenne ou leur importation peuvent être dispensés de toute formalité préalable.

IV. - Le transfert vers un Etat membre de la Communauté européenne et l'exportation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont soumis à autorisation du Premier ministre, sauf dans les cas prévus au b du présent IV. Un décret en Conseil d'Etat fixe :

a) Les conditions dans lesquelles sont souscrites les demandes d'autorisation ainsi que les délais dans lesquels le Premier ministre statue sur ces demandes ;

b) Les catégories de moyens dont les caractéristiques techniques ou les conditions d'utilisation sont telles que, au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, leur transfert vers un Etat membre de la Communauté européenne ou leur exportation peuvent être soit soumis au régime déclaratif et aux obligations d'information prévus au III, soit dispensés de toute formalité préalable.

Section 2

Fourniture de prestations de cryptologie

Article 31 I. - La fourniture de prestations de cryptologie doit être déclarée auprès du Premier ministre. Un décret en Conseil d'Etat définit les conditions dans lesquelles est effectuée cette déclaration et peut prévoir des exceptions à cette obligation pour les prestations dont les caractéristiques techniques ou les conditions de fourniture sont telles que, au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, cette fourniture peut être dispensée de toute formalité préalable.

II. - Les personnes exerçant cette activité sont assujetties au secret professionnel, dans les conditions prévues aux articles 226-13 et 226-14 du code pénal.

Article 32 Sauf à démontrer qu'elles n'ont commis aucune faute intentionnelle ou négligence, les personnes fournissant des prestations de cryptologie à des fins de confidentialité sont responsables au titre de ces prestations, nonobstant toute stipulation contractuelle contraire, du préjudice causé aux personnes leur confiant la gestion de leurs conventions secrètes en cas d'atteinte à l'intégrité, à la confidentialité ou à la disponibilité des données transformées à l'aide de ces conventions.

Article 33 Sauf à démontrer qu'ils n'ont commis aucune faute intentionnelle ou négligence, les prestataires de services de certification électronique sont responsables du préjudice causé aux personnes qui se sont fiées raisonnablement aux certificats présentés par eux comme qualifiés dans chacun des cas suivants:

1° Les informations contenues dans le certificat, à la date de sa délivrance, étaient inexactes ;

2° Les données prescrites pour que le certificat puisse être regardé comme qualifié étaient incomplètes ;

3° La délivrance du certificat n'a pas donné lieu à la vérification que le signataire détient la convention privée correspondant à la convention publique de ce certificat ;

4° Les prestataires n'ont pas, le cas échéant, fait procéder à l'enregistrement de la révocation du certificat et tenu cette information à la disposition des tiers.

Les prestataires ne sont pas responsables du préjudice causé par un usage du certificat dépassant les limites fixées à son utilisation ou à la valeur des transactions pour lesquelles il peut être utilisé, à condition que ces limites figurent dans le certificat et soient accessibles aux utilisateurs.
Ils doivent justifier d'une garantie financière suffisante, spécialement affectée au paiement des sommes qu'ils pourraient devoir aux personnes s'étant fiées raisonnablement aux certificats qualifiés qu'ils délivrent, ou d'une assurance garantissant les conséquences pécuniaires de leur responsabilité civile professionnelle.

Section 3

Sanctions administratives

Article 34 Lorsqu'un fournisseur de moyens de cryptologie, même à titre gratuit, ne respecte pas les obligations auxquelles il est assujetti en application de l'article 30, le Premier ministre peut, après avoir mis l'intéressé à même de présenter ses observations, prononcer l'interdiction de mise en circulation du moyen de cryptologie concerné.

L'interdiction de mise en circulation est applicable sur l'ensemble du territoire national. Elle emporte en outre pour le fournisseur l'obligation de procéder au retrait :

1° Auprès des diffuseurs commerciaux, des moyens de cryptologie dont la mise en circulation a été interdite ;

2° Des matériels constituant des moyens de cryptologie dont la mise en circulation a été interdite et qui ont été acquis à titre onéreux, directement ou par l'intermédiaire de diffuseurs commerciaux.

Le moyen de cryptologie concerné pourra être remis en circulation dès que les obligations antérieurement non respectées auront été satisfaites, dans les conditions prévues à l'article 30.

Section 4

Dispositions de droit pénal

Article 35 I. - Sans préjudice de l'application du code des douanes :

1° Le fait de ne pas satisfaire à l'obligation de déclaration prévue à l'article 30 en cas de fourniture, de transfert, d'importation ou d'exportation d'un moyen de cryptologie ou à l'obligation de communication au Premier ministre prévue par ce même article est puni d'un an d'emprisonnement et de 15 000 EUR d'amende;

2° Le fait d'exporter un moyen de cryptologie ou de procéder à son transfert vers un Etat membre de la Communauté européenne sans avoir préalablement obtenu l'autorisation mentionnée à l'article 30 ou en dehors des conditions de cette autorisation, lorsqu'une telle autorisation est exigée, est puni de deux ans d'emprisonnement et de 30 000 EUR d'amende.

II. - Le fait de vendre ou de louer un moyen de cryptologie ayant fait l'objet d'une interdiction administrative de mise en circulation en application de l'article 34 est puni de deux ans d'emprisonnement et de 30 000 EUR d'amende.

III. - Le fait de fournir des prestations de cryptologie visant à assurer des fonctions de confidentialité sans avoir satisfait à l'obligation de déclaration prévue à l'article 31 est puni de deux ans d'emprisonnement et de 30 000 EUR d'amende.

IV. - Les personnes physiques coupables de l'une des infractions prévues au présent article encourent également les peines complémentaires suivantes:

1° L'interdiction, suivant les modalités prévues par les articles 131-19 et 131-20 du code pénal, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés, et d'utiliser des cartes de paiement;

2° La confiscation, suivant les modalités prévues par l'article 131-21 du code pénal, de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution;

3° L'interdiction, suivant les modalités prévues par l'article 131-27 du code pénal et pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise;

4° La fermeture, dans les conditions prévues par l'article 131-33 du code pénal et pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés;

5° L'exclusion, dans les conditions prévues par l'article 131-34 du code pénal et pour une durée de cinq ans au plus, des marchés publics.

V. - Les personnes morales sont responsables pénalement, dans les conditions prévues par l'article 121-2 du code pénal, des infractions prévues au présent article. Les peines encourues par les personnes morales sont:

1° L'amende, suivant les modalités prévues par l'article 131-38 du code pénal;

2° Les peines mentionnées à l'article 131-39 du code pénal.

VI. - L'article L. 39-1 du code des postes et télécommunications est complété par un 4° ainsi rédigé:

> 4° De commercialiser ou de procéder à l'installation d'appareils conçus pour rendre inopérants les téléphones mobiles de tous types, tant pour l'émission que pour la réception, en dehors des cas prévus à l'article L. 33-3.

12.1.3 LOI n° 2006-961 du 1er août 2006.

LOI n° 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information

Article 13 Dans la section 2 du chapitre Ier du titre III du livre III du code de la propriété intellectuelle, il est inséré un article L. 331-5 ainsi rédigé:

Art. L. 331-5. - Les mesures techniques efficaces destinées à empêcher ou à limiter les utilisations non autorisées par les titulaires d'un droit d'auteur ou d'un droit voisin du droit d'auteur d'une oeuvre, autre qu'un logiciel, d'une interprétation, d'un phonogramme, d'un vidéogramme ou d'un programme sont protégées dans les conditions prévues au présent titre.

On entend par mesure technique au sens du premier alinéa toute technologie, dispositif, composant qui, dans le cadre normal de son fonctionnement, accomplit la fonction prévue par cet alinéa. Ces mesures techniques sont réputées efficaces lorsqu'une utilisation visée au même alinéa est contrôlée par les titulaires de droits grâce à l'application d'un code d'accès, d'un procédé de protection tel que le cryptage, le brouillage ou toute autre transformation de l'objet de la protection ou d'un mécanisme de contrôle de la copie qui atteint cet objectif de protection.

Un protocole, un format, une méthode de cryptage, de brouillage ou de transformation ne constitue pas en tant que tel une mesure technique au sens du présent article.

Les mesures techniques ne doivent pas avoir pour effet d'empêcher la mise en oeuvre effective de l'interopérabilité, dans le respect du droit d'auteur. Les fournisseurs de mesures techniques donnent l'accès aux informations essentielles à l'interopérabilité dans les conditions définies aux articles L. 331-6 et L. 331-7.

Les dispositions du présent chapitre ne remettent pas en cause la protection juridique résultant des articles 79-1 à 79-6 et de l'article 95 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication.

Les mesures techniques ne peuvent s'opposer au libre usage de l'oeuvre ou de l'objet protégé dans les limites des droits prévus par le présent code, ainsi que de ceux accordés par les détenteurs de droits.

Les dispositions du présent article s'appliquent sans préjudice des dispositions de l'article L. 122-6-1 du présent code.

Chapitre 13

Rappels Mathématiques.

13.1 Théorie de l'information.

La théorie de l'information est due à Claude Shannon dans un article fondateur paru en 1948, [25]. Elle permet de donner un sens à la notion de d'information contenue dans un message. A partir de cette théorie , il définit en 1949, [26], la notion de secret. Son approche utilise quelques notions de probabilité qui sont rappelées ci-dessous.

13.1.1 Rappels de probabilités discrètes.

Définition 13.1.1. *Une* **variable aléatoire discrète**, $\mathbf{X}$, *consiste en un ensemble X, une distribution de probabilités discrètes $(p_x)_{x\in X}$ sur X et de la donnée $\mathbf{Pr}[\mathbf{X} = x]$: la probabilité que X se réalise en x. Par définition on a*

$$\forall\, x \in X,\ 0 \leq \mathbf{Pr}[\mathbf{X} = x] \leq 1, \quad et \quad \sum_{x\in X} \mathbf{Pr}[\mathbf{X} = x] = 1$$

***Exemple* 13.1.1.** Le jet d'une pièce de monnaie est une variable aléatoire, $\mathbf{X}$, définie sur l'ensemble $X = \{\text{pile}, \text{face}\}$, la probabilité associée étant $\mathbf{Pr}[\mathbf{X} = \text{pile}] = \mathbf{Pr}[\mathbf{X} = \text{face}] = \dfrac{1}{2}$

***Exemple* 13.1.2.** Jet aléatoire d'une paire de dés. On peut le modéliser par la variable aléatoire $\mathbf{Z}$ sur l'ensemble

$$Z = \{1, 2, 3, 4, 5, 6\} \times \{1, 2, 3, 4, 5, 6\}$$

muni de la probabilité $\mathbf{Pr}[\mathbf{Z} = (i, j)] = \mathbf{Pr}[(i, j)] = \dfrac{1}{36}$. Si on veut calculer la probabilité pour que la somme des deux dés lors d'un lancer soit 4. Cette

valeur correspond à l'évènement

$$S_4 = \{(1,3),(2,2),(3,1)\} \Longrightarrow \mathbf{Pr}[S_4] = \frac{3}{36} = \frac{1}{12}$$

Pour définir la confidentialité parfaite on introduit les définitions suivantes:

Définition 13.1.2. *Soient deux variables aléatoires* $\mathbf{X}$ *et* $\mathbf{Y}$ *définies sur des ensembles finis* X *et* Y *respectivement. La* **probabilité mutuelle** $\mathbf{Pr}[\mathbf{X} = x, \mathbf{Y} = y] = \mathbf{Pr}[x, y]$ *est la probabilité pour que* $\mathbf{X}$ *se réalise en* x *et* $\mathbf{Y}$ *se réalise en* y*.*

La **probabilité conditionnelle** $\mathbf{Pr}[\mathbf{X} = x|\mathbf{Y} = y] = \mathbf{Pr}[x \mid y]$ *est la probabilité que* $\mathbf{X}$ *se réalise en* x *sachant que* $\mathbf{Y}$ *s'est réalisé en* y*.*

Définition 13.1.3. *Les variables aléatoires* $\mathbf{X}$ *et* $\mathbf{Y}$ *sont dites des* ***variables aléatoires indépendantes*** *si* $\mathbf{Pr}[x, y] = \mathbf{Pr}[x|y]$ *pour tout* $x \in X$ *et tout* $y \in Y$

On a la proposition

Proposition 13.1.4. *On a la relation entre probabilité mutuelle et probabilité conditionnelle*

$$\mathbf{Pr}[x, y] = \mathbf{Pr}[x|y]\,\mathbf{Pr}[y]$$

Démonstration*:* C'est évident. □

On a le théorème important suivant

Théorème 13.1.5 (Théorème de Bayes)**.** *Si* $\mathbf{Pr}[y] > 0$*, on a*

$$\mathbf{Pr}[x|y] = \frac{\mathbf{Pr}[x]\,\mathbf{Pr}[y|x]}{\mathbf{Pr}[y]}$$

Démonstration*:* D'après la proposition 13.1.4 on a

$$\mathbf{Pr}[x, y] = \mathbf{Pr}[x|y]\,\mathbf{Pr}[y]$$

et en échangeant x et y on aussi $\mathbf{Pr}[x, y] = \mathbf{Pr}[y|x]\,\mathbf{Pr}[x]$. □

13.1.2 Confidentialité parfaite.

On considère un cryptosystème $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ (définition 4.0.2 page 35) et on suppose qu'une clef $K \in \mathcal{K}$ n'est utilisée qu'une fois.

On suppose que l'espace des textes clairs $\mathcal{P}$ est muni d'une distribution de probabilités associée à une variable aléatoire $\mathbf{x}$ sur $\mathcal{P}$, on définit $\mathbf{Pr}[\mathbf{x} = x]$ comme étant la ***probabilité a-priori d'occurence du texte clair*** x.

De même on suppose que l'espace des clefs $\mathcal{K}$ est muni d'une distribution de probabilités associée à la variable aléatoire $\mathbf{K}$ sur l'espace des clefs $\mathcal{K}$, on définit $\mathbf{Pr}[\mathbf{K} = K]$ la ***probabilité pour que la clé*** K ***soit utilisée*** (souvent on suppose les clés équiprobables).

Rappelons que la clef est toujours choisie par Alice et Bob avant de savoir quel message Alice va transmettre. On peut donc supposer que les variables aléatoires $\mathbf{x}$ et $\mathbf{K}$ sont indépendantes.

Les deux distributions de probabilités sur $\mathcal{P}$ et $\mathcal{C}$ induisent une distribution de probabilité sur l'espace des messages chiffrés $\mathcal{C}$ associée à la variable aléatoire $\mathbf{y}$. Un tel système sera dit probabilisé.

On pose pour $K \in \mathcal{K}$ fixé et pour $e_K \in \mathcal{E}$ la fonction de chiffrement associée

$$C(K) = \{e_K(x) : x \in \mathcal{P}\}$$

$C(K)$ est l'ensemble des messages chiffrés avec la clef K. Pour tout $y \in \mathcal{C}$ on a

$$\mathbf{Pr}[\mathbf{y} = y] = \sum_{K \in \mathcal{K}, y \in C(K)} \mathbf{Pr}[\mathbf{K} = K] \, \mathbf{Pr}[x = d_K(y)]$$

où $d_K \in \mathcal{D}$ est la fonction de décodage associée à la clé K.

On a par application du théorème de Bayes

$$\mathbf{Pr}[\mathbf{x} = x | \mathbf{y} = y] = \frac{\mathbf{Pr}[\mathbf{x} = x] \times \sum_{K \in \mathcal{K}, y \in C(K)} \mathbf{Pr}[\mathbf{K} = K]}{\sum_{K \in \mathcal{K}, y \in C(K)} \mathbf{Pr}[\mathbf{K} = K] \, \mathbf{Pr}[x = d_K(y)]}$$

On pose la définition

Définition 13.1.6. *Un système cryptographique probabilisé* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *assure une* **confidentialité parfaite** *si* $\mathbf{Pr}[x|y] = \mathbf{Pr}[x]$ *pour tout* $x \in \mathcal{P}$ *et tout* $y \in \mathcal{C}$*, c'est à dire si la probabilité a-posteriori que le texte clair soit* x *sachant que le texte chiffré est* y *est égale à la probabilité a-priori que le texte clair soit* x*.*

On démontre les théorèmes suivants

Théorème 13.1.7. *Si les vingt-six clefs d'un chiffrement par décalage (code de Cesar) sont utilisées avec la même probabilité* $\frac{1}{26}$ *alors pour toute distribution d'un bloc de texte clair on a confidentialité parfaite.*

Théorème 13.1.8. *Un système cryptographique probabilisé* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *tel que* $|\mathcal{K}| = |\mathcal{C}| = |\mathcal{P}|$ *assure une confidentialité parfaite si et seulement si chaque clef est utilisée avec la même probabilité* $\dfrac{1}{|\mathcal{K}|}$ *et si pour chaque* $x \in \mathcal{P}$ *et chaque* $y \in \mathcal{C}$*, il existe une clef* K *unique telle que* $e_K(x) = y$

Ce théorème est une mise en forme des remarques faites lors de l'étude du code de Vernam. On voit bien la différence qu'il y a entre confidentialité parfaite et code incassable. Un code de César est à confidentialité parfaite d'après le théorème précédent pourtant il est facilement cassable.

13.1.3 Entropie.

Pour étudier la situation plus réaliste où une clé est utilisée plusieurs fois, Claude Shannon a introduit la notion d'***entropie*** qui permet de modéliser l'information révélée à un opposant lors d'utilisations multiples d'une même clé.

Une chaîne de transmission numérique comporte la ***source du message***, le ***milieu de transmission*** et le ***destinataire du message***. Un message numérique est une suite d'éléments émis par la source pouvant prendre chacun une valeur parmi q valeurs possibles d'un ***alphabet*** noté $\mathscr{Q} = \{x_1, x_2, \ldots, x_q\}$. Les éléments de $\mathscr{Q}$ peuvent être considérés comme des variables aléatoires discrètes.

On supposera que la source est sans mémoire c'est à dire qu'elle est supposée émettre des messages qui sont des suites aléatoires tirées d'après une loi de probabilité, $\mathbf{Pr}(x_i)_{1 \leq i \leq q}$ indépendante du temps. Autrement dit la source est une variable aléatoire discrète notée $\mathbf{X}$. On nopte

$$\mathrm{supp}(\mathbf{X}) = \{x \in \mathscr{Q} \mid \mathbf{Pr}(x) > 0\}$$

La théorie de l'information part de la remarque simple

Plus l'événement donné par la source est probable, moins la quantité d'information correspondante est grande

On doit donc avoir un lien entre la quantité d'information fournie par une source et la distribution de probabilité de l'alphabet de cette source. Ce qui conduit à la définition suivante

Définition 13.1.9. *Soit* $\mathbf{X}$ *une variable aléatoire définie sur un ensemble fini* X*. La* **quantité d'information** *d'un élément* $x \in \mathrm{supp}(\mathbf{X})$ *est définie*

par:

$$I(x) = -\ln_2 \mathbf{Pr}(x) = \ln_2 \frac{1}{\mathbf{Pr}(x)}$$

L'entropie de la variable aléatoire $\mathbf{X}$ *est définie comme étant la quantité*

$$H(\mathbf{X}) = -\sum_{x \in X} \mathbf{Pr}[x] \ln_2 \mathbf{Pr}[x]$$

autrement dit c'est la valeur moyenne de l'information fournie par l'ensemble des éléments $x \in \mathrm{supp}(\mathbf{X})$.

C'est une notion qui vient de la thermodynamique.

On définit l'entropie conditionnelle de la source $\mathbf{X}$ connaissant l'événement $Y = y$

Définition 13.1.10. *Soient* $\mathbf{X}$ *et* $\mathbf{Y}$ *deux sources discrètes. L'entropie conditionnelle de* $\mathbf{X}$ *étant donné l'événement* $\mathbf{Y} = y$ *est défini par*

$$H(\mathbf{X} \mid \mathbf{Y} = y) = -\sum_{x \in \mathrm{supp}(\mathbf{X} \mid y)} \mathbf{Pr}(x \mid y) \ln_2 \mathbf{Pr}(x \mid y)$$

L'entropie conditionnelle de la source $\mathbf{X}$ *étant donné* $\mathbf{Y}$ *est définie par*

$$H(\mathbf{X} \mid \mathbf{Y}) = -\sum_{y \in \mathrm{supp}(\mathbf{Y})} \mathbf{Pr}(y) \ln_2 H(\mathbf{X} \mid \mathbf{Y} = y)$$

***Exemple* 13.1.3.** Si $\mathbf{X}$ est une source binaire qui émet 0 avec une probabilité p et 1 avec la probabité $1 - p$ alors

$$H(\mathbf{X}) = -p \ln_2 p - (1-p) \ln_2 (1-p)$$

On définit ensuite l'entropie $H(L)$ d'un langage naturel L comme le français ou l'anglais. On essaye de quantifier les informations qu'apporte le fait qu'en français le Q est presque toujours suivi du U et qu'un S est assez souvent suivi d'un autre S etc...
On se donne un cryptosystème $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ en langue naturelle L. On définit sa ***redondance***

$$R_L = 1 - \frac{H_L}{\ln_2 |\mathcal{P}|}$$

On choisit une clef et un ensemble fini de messages clairs que l'on chiffre avec cette clé. On appelle ***clefs parasites*** les clefs de $\mathcal{K}$ qui donnent les mêmes messages chiffrés pour le même ensemble de message.

Considérons un message M chiffré en C à partir d'une clé K (symétrique ou asymétrique). On dit que le secret du message M est parfait si la connaissance de C ne fournit aucune information sur M autrement dit M doit rester aussi imprévisible que l'on connaisse C ou pas. De manière mathématique cela se traduit par l'égalité

$$H(M \mid C) = H(M)$$

On peut montrer que dans tout cryptosystème à clef secrète qui fournit un secret parfait, l'incertitude sur la clé secrète doit au moins être aussi grande que l'incertitude sur le texte en clair M. Ce résultat donne donc une borne inférieure sur la taille minimale de la clé K supposée choisie aléatoirement et de manière uniforme: Le nombre de bits de K doit êre au moins aussi grand que le nombre de bits d'information dans le texte clair M.

On montre que le secret d'un système à clé publique parfait ne peut pas être modélisé par la théorie de l'information de Shannon: ce secret ne vient pas de l'incertitude sur la clé privée K_d mais sur la difficulté intrinsèque à calculer K_d à partir de la clé publique K_e et du message codé C. L'outil mathématique permettant de caractériser cette difficulté est la ***théorie de la complexité algorithmique***.

Définition 13.1.11. *La distance d'unicité d'un cryptosystème est la plus petite valeur n, notée n_0, telle que le nombre moyen de clefs parasites soit nul. C'est la quantité de texte chiffré nécessaire à un opposant disposant de suffisamment de temps de calcul pour déterminer la clef.*

On montre que $n_0 \sim \dfrac{|\mathcal{K}|}{R_L \ln_2 |\mathcal{P}|}$. Par exemple pour le chiffrement par substitution sur les 26 lettres de l'alphabet $|\mathcal{P}| = 26$, $|\mathcal{K}| = 26!$, si l'on prend $R_L = 0,75$ qui est une valeur admise pour l'anglais, il vient $n_0 \sim 25$. Ceci montre que pour un message de 25 lettres il n'y a en principe (en moyenne) qu'un seul déchiffrement possible (cf. les alphabets T9 sur les portables).

13.2 Théorie de la complexité.

Le but de cette théorie est de classifier les problèmes algorithmiques en fonction de leur difficulté.

Il faut donc un modèle d'ordinateur. Le modè le plus utilisé est celui des ***machines de Turing*** (Alan Turing, 1912-1954).

Une machine de Turing est la donnée de

1. un alphabet fini Σ

2. une bande infinie dans les deux sens formée de cases. Dans chaque case peut être inscrit au plus un symbole de Σ. Les cases vides sont marquées par un symbole spécial $\emptyset$. On pose $\Sigma' = \Sigma \cup \emptyset$. la bande modélise la mémoire de l'ordinateur. A chaque instant seul un nombre fini de cases de la bande contient un symbole de Σ.

3. une tête de lecture/écriture qui se déplace d'une case à l'autre.

4. un ensemble fini d'états Q, l'un d'entre eux étant appelé l'état initial.

5. un programme ou fonction de transition, composé d'un tableau, indexé par Q et Σ'.

Pour chaque couple $(q, s) \in Q \times \Sigma'$ le programme possède au plus une instruction qui sera exécutée quand la machine sera dans l'état q et que la tête de lecture lira le symbole s.

Cette instruction est codée

$$(q', s', d) \text{ avec } q' \in Q,\ s' \in \Sigma'$$
$$d \in \{\text{gauche,droite}\}.$$

Son exécution consiste à écrire le symbole s' à la place de s à déplacer la tête de lecture dans la direction d et à placer la machine dans l'état q'.

Pour faire fonctionner la machine de Turing on inscrit une suite finie de symboles $\in \Sigma$ sur la bande. On place la machine dans l'état initial et on positionne la tête de lecture sur la première case à gauche contenant un symbole de Σ.

Ensuite la machine exécute le programme et s'arrête quand elle ne possède pas d'instructions correspondant au symbole lu et l'état où elle se trouve.

***Exemple* 13.2.1.** Testeur de parité. Cette machine teste la parité du nombre de 1 dans un nombre n écrit en base 2. Elle s'arrête dans l'état q_i si n a un nombre impair de 1 et elle s'arrête dans l'état q_p si n possède un nombre pair de 1.

$\Sigma = \{0, 1\}$, $Q = \{q_0, q_1, q_p, q_i\}$, état initial q_0, fonction de transition

	0	1	$\emptyset$
q_0	$(q_0, \emptyset, \text{droite})$	$(q_1, \emptyset, \text{droite})$	$(q_p, \emptyset, \text{droite})$
q_1	$(q_1, \emptyset, \text{droite})$	$(q_0, \emptyset, \text{droite})$	$(q_i, \emptyset, \text{droite})$

Exercices. 1

13.2.1. Vérifier que la machine de Turing de l'exemple 13.2.1 compte bien la parité du nombre de 1 de l'écriture en base 2 d'un entier.

Il y a aussi des machines de Turing non déterministes qui peuvent avoir plusieurs instructions possibles pour un couple de (Q, Σ'). La machine choisit "au hasard" quelle instruction exécuter.

13.2.2 Décidabilité.

On introduit les définitions suivantes

Définition 13.2.1. *Soit Σ un alphabet et Σ^* l'ensemble des mots sur Σ. Un langage sur Σ est une partie de Σ^**

Définition 13.2.2. *Soit M une machine de Turing sur l'alphabet Σ et q_y un état de M. On dit que M accepte la donnée x (par l'état q_y) si M s'arrête dans l'état q_y lorsque la donnée est x.*

L'ensemble des mots acceptés par M s'appelle le langage reconnu par M que l'on note

$$L_{q_y}(M) = L(M)$$

Le complémentaire de $L(M)$ dans Σ^* est l'ensemble des mots pour lesquels soit M ne s'arrête pas soit M s'arrête dans un état $\neq q_y$.

Définition 13.2.3. *Un problème de décision $\mathcal{D}$ appartient à la classe* **P** *s'il existe une machine de Turing déterministe qui le résoud en un temps polyomial en fonction de la taille des données (i.e. du nombre de symboles de*

Σ *apparaissant dans la donnée). Si* $\Sigma = \{0, 1\}$ *alors le problème de décision appartient à la classe* **P** *des* **problèmes polynomiaux en temps** *si*

$$\forall\, x \in \mathcal{D} \Rightarrow \mathcal{C}_{temps}(x) = O(\textit{polynôme en } \ln_2(x))$$

Un problème de décision $\mathcal{D}$ *appartient à la classe* **NP** *des* **problèmes non polynomiaux en temps** *s'il existe une machine de Turing non-déterministe qui le résoud en un temps polynomial*

Conjecture 1. P≠NP.

Autrement dit il existe au moins un problème pour lequel on peut montrer qu'il n'existe pas de machine de Turing déterministe pour le résoudre en temps polynomial et qui peut être résolu en temps polynomial par une machine de Turing non-déterministe.

13.2.3 Complexité algorithmique.

Si on veut exécuter un algorithme sur une donnée x deux coûts sont à envisager.

- le ***coût en temps*** $\mathcal{C}_{\text{temps}}(x)$, c'est à dire le nombre d'opérations effectuées pour obtenir le résultat final ou plus formellement le nombre de déplacements de la tête de lecture/écriture avant arrêt de la machine de Turing modélisant l'ordinateur.

- le ***coût en espace***, $\mathcal{C}_{espace}(x)$ est la taille de la mémoire utilisée, plus formellement le nombre de case de la bande écrite au moins une fois.

On distingue essentiellement deux notions de complexité algorithmique la ***complexité polynomiale*** et la ***complexité non polynomiale*** (sous entendu en fonction de la taille des données).

Quel est le coût acceptable pour un problème donné. Il n'y a ni réponse claire ni réponse absolue. En 2000 on estimait que

- 2^{40} opérations élémentaires est accessible à un particulier s'il est patient.

- 2^{56} opérations élémentaires est accessible avec de gros moyens.

- 2^{80} opérations élémentaires est hors de portée de quiconque.

Rappelons qu'une année comporte $3,2 \cdot 10^7$ secondes.
Soit un algorithme dont le nombre d'opérations élementaires en fonction de la taille n de l'entrée est décrit par la fonction f. On dispose d'un ordinateur faisant 10^9 opérations élémentaires par secondes. Le temps pris par l'algorithme suivant les instances de f est:

f	$\ln_2(n)$	$\ln_2^3(n)$	n	$n \ln_2(n)$	n^2	2^n
$n = 100$	$6,6 \cdot 10^{-9}$ s	$4,4 \cdot 10^{-7}$ s	10^{-7} s	$6,7 \cdot 10^{-7}$ s	10^{-5} s	$4 \cdot 10^{13}$ ans
$n = 10^5$	$1,7 \cdot 10^{-8}$ s	$5,2 \cdot 10^{-6}$ s	10^{-4} s	$1,7 \cdot 10^{-3}$ s	10 s	$\geq 10^{30086}$ ans
$n = 10^{10}$	$3,3 \cdot 10^{-8}$ s	$3,5 \cdot 10^{-5}$ s	10 s	330 s	3 siècles	$\geq 10^{3 \cdot 10^9}$ ans
$n = 10^{20}$	$6,6 \cdot 10^{-8}$ s	$2,3 \cdot 10^{-4}$ s	30 siècles	$\geq 10^5$ ans	$\geq 10^{23}$ ans	!!!

13.2.4 Algorithmes polynomiaux en fonction de la taille des données.

On décompose tout algorithme arithmétique en ***opérations élémentaires***.

L'opération élémentaire est l'addition de 3 chiffres en base 2 et le report de la retenue

$$\textbf{retenue} + \textbf{chiffre 1} + \textbf{chiffre 2} = \textbf{résultat} + \textbf{retenue}$$

Définition 13.2.4. *On dit qu'un algorithme est* **polynomial en fonction de la taille des données** *s'il peut être décomposé en un nombre d'opérations élémentaires majoré par une fonction polynomiale du nombre de chiffres des données.*

***Exemple* 13.2.2.** Montrons que l'addition de deux nombres de tailles $\leq k$ est une fonction polynomiale de k

	1	1	1	1				***retenue***
		1	1	1	1	0	0	0 ***ligne 1***
+		0	0	1	1	1	1	0 ***ligne 2***
	1	0	0	1	0	1	1	0 ***résultat***

On suppose que le plus grand des entiers a k chiffres. Décomposons la somme en opérations élémentaires

1. Regarder dans la colonne i ($1 \leq i \leq k+1$) les chiffres des lignes ***lignes 1, 2 et retenue***
2. S'il y a 0 dans les ***lignes 1, 2 et retenue*** mettre 0 dans la ligne ***résultat*** et aller à la colonne $i+1$
3. S'il y a un 0 dans deux des ***lignes 1 et 2 et retenue*** on reporte 1 dans la ligne ***résultat*** et on passe à la colonne $i+1$
4. S'il y a un 1 dans deux des ***lignes 1 et 2 et retenue*** on reporte 0 dans la ligne ***résultat*** on met 1 dans la ligne ***retenue*** à la colonne $i+1$ et on passe à la colonne $i+1$
5. S'il y a un 1 dans les 3 ***lignes 1 et 2 et retenue*** on reporte 1 dans la ligne ***résultat*** on met 1 dans la ligne ***retenue*** à la colonne $i+1$ et on passe à la colonne $i+1$

On admet en première approximation que le temps nécessaire pour faire k opérations élémentaires est proportionnel à k avec une constante dépendant de l'ordinateur et de l'implantation de l'algorithme.

Exemples d'algorithmes polynomiaux en fonction de la taille des entrées:

- L'addition de deux entiers $n \leq m$ de longueur $\leq k$ est polynomial en fonction de la taille des entrées car (en première approximation) il faut

  $$C \cdot k \stackrel{\text{déf}}{=} O(k) = O(log_2(m)) \text{ opérations}$$

  Ajouter deux entiers de 100 chiffres en base 10 avec un ordinateur faisant 10^9 opérations par secondes nécessite $\sim 300 \cdot 10^{-9}$sec $\sim 3\mu$sec.

- La multiplication de deux entiers $n \leq m$ de taille k et ℓ nécessite

  $$2 \cdot k\ell = O\big(\ln_2^2(m)\big) \text{ opérations}$$

  Multiplier deux entiers de 100 chiffres en base 10 nécessite $\sim 90000 \cdot 10^{-9}$sec $\sim 10\mu$ sec.

- Calcul du PGCD de deux entiers, $n \geq m$ de taille $k \geq \ell$ nécessite

  $$O(k^3) = O\big(\ln_2^3(n)\big) \text{ opérations}$$

  Trouver le PGCD de deux entiers de 100 chiffres en base 10 nécessite $\sim 27000000 \cdot 10^{-9} \sim 0,027$ sec.

- Calculer $b^m \mod n$ nécessite $O\big(\ln_2^3(n)\big)$ opérations.
- Décider si un nombre entier n de taille k est premier ou non nécessite

$$O\big(k^{6+\varepsilon}\big) = O\big(\ln_2^{6+\varepsilon}(n)\big) \text{ opérations}$$

Tester si un entier de 100 chiffres en base 10 est premier nécessite avec l'algorithme polynomial $\sim 10^{26}\mu$ sec $\sim 10^9$ années. Il y a des algorithmes pour tester la primalité d'un entier non polynômiaux et/ou non déterministes qui sont plus efficaces pour des nombres pas trop grands.

le dernier exemple montre que si le polynôme est de degré trop élevé (≥ 3, un algorithme polynomial peut avoir un coût prohibitif.

Exemples d'algorithmes non polynomiaux en fonction de la taille des entrées

- Calcul de $n! = 1 \cdot 2 \ldots (n-1) \cdot n$, si l'on calcule brutalement il faut environ

$$C \cdot n^2 \ln_2^2 n = O(n^2 \ln_2^2 n) \text{ opérations}$$

Calculer $\Big(10^{100}\Big)!$ nécessite $\sim 10^{190}\mu$ sec $\sim 10^{180}$ années!!!

- Recherche d'un diviseur d'un entier n, les meilleurs algorithmes nécessitent

$$0\Big(e^{C\sqrt{\ln_2 n \ln_2 \ln_2 n}}\Big) \text{ opérations}, \quad C \leq 2$$

Trouver un diviseur d'un nombre de 100 chiffres en base 10 nécessite $\sim e^{30} \cdot 10^{-9} \sim 10^5$ sec $\sim 1,1$jours. Un tel algorithme est dit sous-exponentiel.

13.3 Rappels d'arithmétique.

Ainsi qu'on l'a vu dans la description des cryptosystèmes à clé publique RSA et El Gamal, leur principe est basé sur de l'arithmétique élémentaire.

13.3.1 La division euclidienne.

Les entiers naturels $\mathbb{N} = \{1, 2, 3 \ldots\}$ sont munis de deux opérations internes l'addition, notée $+$, et la multiplication, notée $\times$ ou $\cdot$ ou même sans symbole, et d'une relation d'ordre total, notée $\leq$, compatible avec l'addition et la multiplication c'est à dire

$$\big(\forall\, a, b \in \mathbb{N},\ a \leq b\big) \Longrightarrow \forall\, c \in \mathbb{N};\ a + c \leq b + c$$

$$\big(\forall\, a, b \in \mathbb{N},\ a \leq b\big) \Longrightarrow \forall\, c \in \mathbb{N};\ a \times c \leq b \times c$$

On définit sur $\mathbb{N}$ la division euclidienne.

Théorème 13.3.1. *Si a et b sont deux entiers ($b \neq 0$) il existe un unique couple d'entiers q et r tel que*

$$a = b \cdot q + r \quad et \begin{cases} ou\ bien & r = 0 \\ ou\ bien & 1 \leq r \leq b-1 \end{cases}$$

Démonstration*:* On considère l'ensemble des entiers $k \times b$ pour $k \in \mathbb{N}$,. Les axiomes qui définissent les entiers imosent qu'il existe nécessairemment un entier q tel que

$$b \times q \leq a < b \times (q+1)$$

et donc si l'on pose $a - bq = r$ on a $0 \leq r < b$. Nous avons donc montré l'existence d'un couple (q, r) avec $0 \leq r < b$ tel que $a = bq + r$. Il reste à montrer l'unicité.

Supposons que nous ayons deux couple (q, r) et (q', r') tels que

$$\begin{aligned} a &= bq + r, \quad 0 \leq r < b \\ a &= bq' + r', \quad 0 \leq r' < b \end{aligned}$$

alors en soustrayant membre à membre

$$0 = b(q - q') + (r - r')$$

Comme $-b < r - r' < b$ on en déduit que $q - q' = 0$ et donc que $r - r' = 0$ d'où l'unicité. □

Définition 13.3.2. *Soient a et b des entiers naturels avec $b \neq 0$. Faire la* **division euclidienne** *de a par b c'est trouver l'unique couple (q, r) d'entiers naturels (dont l'existence est assurée par le théorème* 13.3.1*) tel que*

$$a = b \cdot q + r \quad et \begin{cases} ou\ bien & r = 0 \\ ou\ bien & 1 \leq r \leq b-1 \end{cases} \tag{13.1}$$

la relation (13.1) *s'appelle l'***égalité de la division euclidienne**
On dit que b est un **diviseur** *de a s'il existe $q \in \mathbb{N}$ tel que $a = bq$, on note $a \,|\, b$ pour dire a divise b.*

Tout entier a possède au moins deux ***diviseurs triviaux*** 1 et lui-même car on a toujours

$$a = 1 \cdot a, \quad a = a \cdot 1$$

Mais il peut en avoir d'autres par exemple

$$6 = 2 \cdot 3,\ 28 = 4 \cdot 7 = 2 \cdot 2 \cdot 7 = 2 \cdot 14$$

donc 1, 2, 3 et 6 sont des diviseurs de 6 et 1, 2, 4, 7, 14 et 28 sont des diviseurs de 28.

La division euclidienne implique que $\mathbb{Z}$, les entiers relatifs, est un ***anneau euclidien***, i.e. qu'il est muni de deux lois de composition interne l'addition et la multiplication qui possédent certaines propriétés et d'une division euclidienne, cf. [28],

1. La loi + est commutative (pour tout $(a,b) \in \mathbb{Z}^2$ on a $a+b=b+a$), associative (pour tous $(a,b,c) \in \mathbb{Z}^3$ on a $(a+b)+c=a+(b+c)$, il y a un élément neutre, 0, tel que pour tout $a \in \mathbb{Z}$ on a $a+0=0+a=a$, tout élément $a \in \mathbb{Z}$ possède un opposé $b=-a$ tel que $a+b=b+a=0$.

2. La loi $\times$ est commutative ($a \times b = b \times a$), associative ($(a \times b) \times c = a \times (b \times c)$), il y a un élément neutre, 1, ($a \times 1 = 1 \times a = a$), la multiplication est distributive par rapport à l'addition ($(a+b) \times c = (a \times c) + (b \times c)$

Dans les entiers naturels on distingue

- 1 qui est une ***unité***, c'est à dire que 1 possède un inverse pour la multiplication (il existe $b \in \mathbb{N}$ tel que $1 \times b = b \times 1 = 1$) qui est 1.

- les ***nombres premiers*** qui n'ont pas d'autres diviseurs que les diviseurs triviaux i. e. 1 et eux-même (e.g. 2,3,5,7,...,37,....).

Proposition 13.3.3. *Un nombre entier $n > 0$ est premier s'il n'est divisible par aucun entier inférieur ou égal à $\sqrt{n}$.*

Démonstration*:* Si n n'est pas premier alors par définition on a $n = n_1 n_2$ avec $n_i \neq 1$ pour $i = 1, 2$. Si $n_1 > \sqrt{n}$ et $n_2 > \sqrt{n}$ alors $n_1 n_2 > \sqrt{n}^2 = n$ ce qui est absurde. □

Proposition 13.3.4. *Soit p un nombre premier et a, b deux entiers non nuls. Si p divise le produit ab alors il divise au moins l'un des deux nombres a ou b.*

Démonstration*:* Supposons que p ne divise pas a et écrivons la division euclidienne de b par p

$$b = pq + r \quad \text{et} \quad \begin{cases} \text{ou bien} & r = 0 \\ \text{ou bien} & 1 \leq r \leq p-1 \end{cases}$$

si p ne divisait pas b on aurait $r \neq 0$ et donc par multiplication par a

$$a \cdot b = apq + ar \quad \text{et } 1 \leq ar \leq ap - a < ap$$

On a donc écrit l'égalité de la division euclidienne de ab par ap et par l'unicité du quotient et du reste on devrait avoir $ar = 0$ ce qui contredit $ar \geq 1$. Donc nécessairement p divise b. □

Le théorème suivant qui découle de l'existence de la division euclideienne est appelé le théorème fondamental de l'arithmétique

Théorème 13.3.5. *Tout nombre entier différent de* 1 *possède une unique décomposition en facteurs premiers à l'ordre près des facteurs, certains facteurs peuvent être répétés.*

***Exemple* 13.3.1.** On a $2 = 2$, $4 = 2^2$, $6 = 2 \times 3$, $12 = 2^2 \times 3$

Démonstration*:* On raisonne par récurrence. Il est clair que 2 possède une unique décomposition en facteurs premiers. On suppose que tous les entiers inférieurs strictement à n possèdent une unique décomposition en facteurs premiers (éventuellement réduite à un élément si le nombre est premier).. Montrons que n aussi possède une unique décomposition en facteurs premiers.

Si n est premier c'est clair, sinon $n = a \times b$ avec $1 < na, b < n$ et donc $1 < a < n$ et $1 < b < n$. D'après l'hypothèse de récurrence on a

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i}, \quad p_1, p_2 \dots, p_i \text{ premiers}$$
$$b = q_1^{\beta_1} q_2^{\beta_2} \dots q_j^{\beta_j}, \quad q_1, q_2 \dots, q_j \text{ premiers}$$

et donc

$$n = \ell_1^{\lambda_1} \ell_2^{\lambda_2} \dots \ell_k^{\lambda_k}, \quad \lambda_r = \begin{cases} p_s, \\ \text{ou} \\ q_t \end{cases}$$

On a donc montré que n possède une décomposition en facteurs premiers. il reste à montrer l'unicité.

On suppose que

$$n = p_1 p_2 \dots p_i = q_1 q_2 \dots q_j$$
$$\text{avec } p_1, p_2, \dots, p_i, q_1, q_2, \dots, q_j \text{ premiers non nécessairement distincts}$$

Comme p_1 divise n donc p_1 divise le produit $q_1 q_2 \dots q_j$. D'après la proposition 13.3.4 p_1 divise nécessairement un des facteurs de ce produit. Comme tous les facteurs de ce produit sont des nomnres premiers on en déduit qu'il existe m tel que $p_1 = q_m$. On peut supposer que $m = 1$ et donc $p_1 = q_1$. On conclut alors par récurrence. □

Autrement dit si $a \in \mathbb{N}$, $a \leq 2$, alors il existe des nombres premiers p_1, p_2,..., p_{n_a} non nécessairement distincts tels que

$$a = p_1 \times p_2 \times \dots \times p_n, \quad p_i \text{ premier pour } 1 \leq i \leq n$$

l'entier n dépend de a. L'unicité à l'ordre près des facteurs impose que si on a une égalité

$$a = q_1 \times q_2 \times \dots \times q_m, \quad q_j \text{ premier pour } 1 \leq j \leq m$$

alors nécessairement $n = m$ et il existe une permutation ψ des entiers de 1 à n_a telle que

$$p_1 = q_{\psi(1)},\ p_2 = q_{\psi(2)}, \ldots,\ p_n = q_{\psi(n)}.$$

On peut écrire la décomposition en facteurs premiers de $a \in \mathbb{N}$ en regroupant tous les nombres premiers égaux, alors

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_\ell^{\alpha_\ell} \text{ avec } p_1 < p_2 < \cdots < p_\ell, \quad p_i \text{ premier pour } 1 \leq i \leq \ell$$

L'unicité à l'ordre près des facteurs impose que si on a une égalité

$$a = q_1^{\beta_1} q_2^{\beta_2} \ldots q_k^{\beta_k} \text{ avec } q_1 < q_2 < \cdots < q_\ell, \quad q_j \text{ premier pour } 1 \leq j \leq k$$

alors

$$\ell = k \text{ et } \alpha_i = \beta_i, \text{ pour } 1 \leq i \leq \ell$$

***Exemple* 13.3.2.** $10780 = 2^2 \cdot 5 \cdot 7^2$, $4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11$

Théorème 13.3.6. *L'ensemble des nombres premiers est infini*

Démonstration*:* Si l'ensemble des nombres premiers était fini, notons p_1,..., p_n les nombres premiers rangé par ordre croissant. Le nombre

$$1 + p_1 p_2 \ldots p_n$$

est plus grand que p_n. Il n'est pas premier donc d'après le théorème 13.3.5 il possède des diviseur premiers. Or il n'est pas divisible par p_i pour $1 \leq i \leq n$. □

13.3.2 Plus Grand Commun Diviseur ou PGCD.

Le ***plus grand commun diviseur PGCD*** en français et ***GCD*** (Greatest Common Divisor) en anglais est défini de la manière suivante

Définition 13.3.7. *Le plus grand commun diviseur de deux nombres entiers a et b est le plus grand des entiers qui divisent à la fois a et b, on le note PGCD(a, b) ou $a \wedge b$ ou encore (a, b).*

Si le PGCD de a et b vaut 1 on dira que a et b sont **premiers entre eux** *ou sont des* **nombres relativement premiers**

L'ensemble $\left\{ d \in \mathbb{N} \;\middle|\; d \text{ divise } a \text{ et } d \text{ divise } b \right\}$ est non vide, car 1 divise toujours a et b, et il est borné par le plus grand des deux entiers a et b, donc le PGCD existe et de plus il est toujours supérieur ou égal à 1.
Attention bien distinguer entre nombres relativement premiers et nombres qui ne se divisent pas.

***Exemple* 13.3.3.** 35 et 49 ne se divisent pas car $49 = 35 \cdot 1 + 14$ et $35 = 0 \times 49 + 35$, mais ils ne sont pas premiers entre eux car 7 divise à la fois 35 et 49.

Proposition 13.3.8. *Le plus grand commun diviseur de a et de b, entiers naturels, s'obtient de la manière suivante. Si*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r},\ b = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r},\ \textit{avec } \alpha_i, \beta_i \geq 0$$

sont leur décomposition en facteurs premiers, alors le PGCD de a et de b est:

$$a \wedge b = p_1^{\inf\{\alpha_1,\beta_1\}} p_2^{\inf\{\alpha_2,\beta_2\}} \dots p_r^{\inf \alpha_r,\beta_r}$$

Démonstration*:* Pour la preuve voir [13] □

Pour calculer le PGCD ni la définition 13.3.7 ni la proposition 13.3.8 ne sont efficaces car elles nécessitent l'une comme l'autre de trouver des diviseurs de a et de b. Or les meilleurs algorithmes connus pour trouver un diviseur non trivial de a ou pour décomposer a en facteurs premiers ce qui revient au même sont en $O(e^{C\sqrt{\ln_2(a)\ln_2\ln_2(a)}}$. Ces algorithmes ne sont donc pas polynomiaux en temps en fonction de la taille des données, leur coût est prohibitif pour des grands nombres entiers (500 chiffres en base 10 par exemple) même avec des ordinateurs très puissants.

***Exemple* 13.3.4.** Le PGCD de $4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7$ et de $10780 = 2^2 \cdot 5 \cdot 7^2 \cdot 11$ est

$$\text{PGCD}(4200, 10780) = 4200 \wedge 10780 = 2^2 \cdot 5 \cdot 7 = 140$$

Par contre l'algorithme de la division euclidienne fournit grâce au théorème de Bézout un algorithme très efficace, polynomial en temps en fonction de la taille des données, pour calculer le PGCD de deux entiers naturels.

13.3.3 Algorithme du plus grand commun diviseur ou algorithme du PGCD.

Considérons le problème suivant:

Soit $a \geq b$ deux entiers de taille k au plus. Trouver le PGCD $a \wedge b$ de a et de b et évaluer le nombre d'opérations élémentaires nécessaires.

Proposition 13.3.9. *On écrit les divisions euclidiennes successives*

$$\begin{array}{cc} a = bq_0 + r_1 & b = q_1 r_1 + r_2 \\ r_1 = q_2 r_2 + r_3 & \dots \\ \vdots & r_{j-2} = q_{j-1} r_{j-1} + r_j \\ r_{j-1} = q_j r_j + r_{j+1} & r_j = q_{j+1} r_{j+1} \end{array} \tag{13.2}$$

avec $0 \leq r_1 < b$, $0 \leq r_2 < r_1$, $0 \leq r_3 < r_2$,..., $0 \leq r_j < r_{j+1}$.

On arrête l'algorithme dès qu'un reste est nul et alors

$$a \wedge b = r_{j+1}$$

Démonstration*:* En effet la dernière identité de division enclidienne de (13.2) montre que r_{j+1} divise r_j, l'avant dernière identité de division enclidienne de (13.2) montre que r_{j+1} divise r_j et r_{j-1}. Puis par récurrence on montre que r_{j+1} divise a et b.

Donc r_{j+1} est un diviseur commun de a et de b, est-ce le plus grand? Considérons un diviseur commun de a et de b noté d. Par définition d divise a et b donc d'après la première des identités de division enclidienne de (13.2) on a $\mid r_1$, alors la deuxième des identités de division enclidienne de (13.2) implique que $d \mid r_2$ puis par récurrence on montre que $d \mid r_{j+1}$.

On a donc montré que tout diviseur d commun de a et de b est un diviseur de r_{j+1} et comme r_{j+1} est un diviseur de a e de b c'est le plus grand, autrement dit $r_{j+1} = a \wedge b$. □

Cet algorithme nécessite $O\big(\ln_2^3(n)\big)$ opérations élémentaires.

***Exemple* 13.3.5.** Trouver le PGDCD de 4200 et 10780:

$$10780 = 2 \times 4200 + 2380;\ 4200 = 2380 + 1820;$$
$$2380 = 1 \times 1820 + 560, 1820 = 3 \times 560 + 140,\ 560 = 4 \times 140$$
$$\mathrm{PGCD}(10780, 4200) = 140$$

L'algorithme de la division euclidienne donne aussi une version effective du théorème de Bézout, autrement dit une version effective du calcul du générateur de l'idéal $\langle a, b\rangle$ engendré par a et b.

Théorème 13.3.10 (Théorème de Bézout)**.** *Soit a et b deux entiers naturels de PGCD: $a \wedge b = d$. Alors il existe deux entiers relatifs u, v tels que*

$$d = au + bv$$

u et v sont appelés les coefficients de Bézout.

Démonstration*:* On reprend l'algorithme du PGCD à partir de la fin. On écrit avec les notations précédentes

$$\begin{aligned}
d = r_{j+1} &= r_{j-1} - q_j r_j = r_{j-1}u_{j-1}(1) - r_j v_j(q_j) \\
&= r_{j-1} - q_j\big(r_{j-2} - q_{j-1}r_{j-1}\big) \\
&= r_{j-1}\big(1 + q_j q_{j-1}\big) - q_j r_{j-2} \\
&= -u_{j-2}(q_j)r_{j-2} + r_{j-1}v_{j-1}(q_{j-1}, q_j) \\
&= \big(r_{j-3} - q_{j-2}r_{j-2}\big)\big(1 + q_j q_{j-1}\big) - q_j r_{j-2} \\
&= r_{j-3}\big(1 + q_j q_{j-1}\big) - r_{j-2}\Big(q_{j-2}\big(1 + q_j q_{j-1}\big) + q_j\Big) \\
d &= r_{j-3}u_{j-3}(q_j, q_{j-1}) - r_{j-2}v_{j-2}(q_{j-2}, q_{j-1}, q_j) \\
&\vdots \\
&= (-1)^{j+1}au_0(q_1, \ldots, q_j) + (-1)^j b v_0(q_0, \ldots, q_j)
\end{aligned}$$

On a une relation de récurrence facile sur u_j et v_j.

$$\begin{aligned}
u_{j+1} &= u_{j-1} - q_{j+1}u_j \\
v_{j+1} &= v_{j-1} - q_{j+1}v_j
\end{aligned}$$ □

***Exemple* 13.3.6.** Relation de Bézout entre 10780 et 4200:

$$\begin{aligned}
140 &= 1820 - 3 \times 560 = 1820 - 3 \times (2380 - 1820) \\
&= 4 \times 1820 - 3 \times 2380 = 4 \times (4200 - 2380) - 3 \times 2380 \\
&= 4 \times 4200 - 7 \times 2380 = 4 \times 4200 - 7 \times (10780 - 2 \times 4200) \\
&= 18 \times 4200 - 7 \times 10780 = 75600 - 75460
\end{aligned}$$

***Remarque* 13.3.1.** Le couple $(u, v))$ tel que $au + bv = d = a \wedge b$ dont l'existence est garantie par le théorème de Bézout n'est pas unique car si (u_0, v_0) est un tel couple et si (x_1, y_1) est une solution en nombres entiers relatifs de l'équation

$$ax_1 + by_1 = 0$$

alors on a encore

$$a(u + x_1) + b(v + y_1) = d$$

Par contre on a unicité au signe près si on impose

$$1 \leq |u| \leq b, \quad 1 \leq |v| \leq a$$

Algorithme d'Euclide.

On donne une version de type programme de l'algorithme d'Euclide.

- Entrée 2 entiers positifs a et b non tous deux nuls
- Sortie $a \wedge b$
  - Tant que $b \neq 0$ faire

$$a \wedge b := b \wedge (a \mod b)$$

  - si $b = 0$ retourner a et fin

Algorithme d'Euclide étendu.

On donne une version récursive de type programme de l'algorithme d'Euclide étendu qui donne les coefficients de Bézout pour le PGCD de deux entiers.

1. Entrée 2 entiers positifs a et b non tous nuls
2. Sortie 3 entiers u, v, d tels que $au + bv = a \wedge b = d$
   (a) Variables entières u_1, v_1, u_2, v_2, u_3, v_3, q, r
   (b) Si $a = 0$ retourner $(0, 1, b)$ et fin
   (c) sinon $Au_1 + Bv_1 = a$ et $Au_2 + Bv_2 = b$ où A et B sont les valeurs initiales de a et b
   (d) Faire
$$(u_1, v_1) := (1, 0) \qquad (u_2, v_2) := (0, 1)$$
   (e) Tant que $b \neq 0$ faire

$(q, r) :=$ quotient et reste de la division euclidienne de a par b
$(u_3, v_3) := (u_1 - qu_2, v_1 - qv_2)$
$(u_1 v_1, a) := (u_2, v_2, b)$
$(u_2, v_2, b) := (u_3, v_3, r)$

3. si $b = 0$ retourner (u_1, v_1, a).

13.3.4 Les Congruences.

Les cryptosystèmes RSA et El Gamal reposent sur la théorie des congruences ou ***arithmétique modulaire***.

Définition 13.3.11. *Soit a, b et m trois entiers. On dit que a est congru à b modulo m et on écrit*

$$a \equiv b \mod m$$

si la différence $a - b$ est divisible par m

Une autre manière de dire la même chose

Corollaire 13.3.12. *Soit m un entier non nul, alors a et b sont congrus modulo m si et seulement si les restes de la division euclidienne de a par m et de b par m sont les mêmes*

Démonstration*:* C'est immédiat. □

***Exemple* 13.3.7.** Prenons $m = 2$ alors deux entiers a et b sont congrus modulo 2 s'il sont soit tous les deux pairs soit tous les deux impairs.

Prenons $m = 5$ alors 5 est congru à 0 modulo 5 (car $5 - 0 = 5$ est divisible par 5) ou à -700 modulo 5 (car $5 - (-700) = 705$ est divisible par 5), 3 est congru à -2 modulo 5 (car $3 - (-2) = 5$ est divisible par 5) ou à 38 modulo 5 (car $3 - 38 = -35$ est divisible par 5)

On montre facilement que

Proposition 13.3.13. *La relation de congruence est une* **relation d'équivalence** *sur les entiers.*

c'est à dire que

- $a \equiv a \mod m$ (reflexivité)
- $a \equiv b \mod m \Longrightarrow b \equiv a \mod m$ (symétrie)
- $\big(a \equiv b \mod m \text{ et } b \equiv c \mod m\big) \Longrightarrow a \equiv c \mod m$ (transitivité)

Démonstration*:* C'est évident. □

Proposition 13.3.14. *L'addition et la multiplication sont compatibles à la relation de conguence sur les entiers; autrement dit:*

$$\Big(\big(a \pmod m\big) + \big(b \pmod m\big) \pmod m\Big) = \big(a + b \pmod m\big)$$
$$\Big(\big(a \pmod m\big) \times \big(b \pmod m\big) \pmod m\Big) = \big(a \times b \pmod m\big)$$

Démonstration*:* Pour la preuve cf. [13] □

***Exemple* 13.3.8.** Si $m = 2$ alors la proposition signifie simplement que la somme de deux nombres pairs est paire, que la somme de deux nombres impairs est paire, que la somme d'un nombre pair et d'un nombre impair est impaire et que le produit de deux nombres pairs est pair, celui de deux nombres impairs est impair, celui d'un nombre pair et d'un nombre impair est pair.

Si $m = 5$ on constate que

$$5 + 3 \equiv -700 - 2 \equiv 0 + 38 \equiv 3 \mod 5, \quad 5 \times 3 \equiv 0 \times 3 \equiv 5 \times 38 \mod 5$$

On fixe m et on décide de ne pas distinguer deux éléments congrus modulo m. L'ensemble des éléments de $\mathbb{Z}$ qui sont congrus modulo m à un entier fixé s'appellera une ***classe de congruence modulo*** m. Un élément d'une classe de congruence s'appelle un ***représentant de la classe de congruence***. Parmi les réprésentant d'une classe de congruence, il y en a toujours un, unique, compris entre 0 et $m - 1$.

On notera $\mathbb{Z}/m\mathbb{Z}$ l'ensemble des classes de congruence de $\mathbb{Z}$ modulo m. D'après la proposition 13.3.14 on peut munir $\mathbb{Z}/m\mathbb{Z}$ des deux lois $+$ et $\times$ puisque que le résultat modulo m de ces deux opérations ne dépend pas des représentants choisis dans une classe de congruences.

Corollaire 13.3.15. *Tout élément de $\mathbb{Z}/m\mathbb{Z}$ possède un opposé pour l'addition. Les éléments de $\mathbb{Z}/m\mathbb{Z}$ qui ont un inverse multiplicatif sont ceux dont les représentants dans $\mathbb{Z}$ sont premiers à m.*

Démonstration*:* Facile par Bézout. En effet si $a \wedge m = 1$ alors il existent $u, v \in \mathbb{Z}$ tels que $au+mv = 1$ et donc on a $au \equiv 1 \pmod m$. Réciproquement si a est inversibledans $\mathbb{Z}/m\mathbb{Z}$ alors il existe $u \in \mathbb{N}$ tel que $au \equiv 1 \pmod m$ ce qui équivant à:

Il existe $v \in \mathbb{Z}$ tel que $au = 1 + mv$ ce qui équivaut par Bézout à $a \wedge m = 1$.

□

Théorème 13.3.16. *Si p est premier $\mathbb{Z}/p\mathbb{Z}$ est un corps fini à p éléments, c'est à dire que tout élément différent de la classe de zéro possède un inverse multiplicatif. On le note $\mathbb{F}_p$*

Démonstration*:* facile d'après le corollaire précédent. □

Si p est un nombre premier, on peut montrer que pour chaque entier $r \geq 1$ il existe un seul corps fini à $q = p^r$ éléments à isomorphisme de corps près, noté $\mathbb{F}_{p^r} = \mathbb{F}_q$. Ils s'obtiennent en considérant les quotients

$$\mathbb{F}_q \simeq \mathbb{F}_p[X]/P(x)\mathbb{F}_p[X], \quad P(X) \in \mathbb{F}_p[X], \text{irréductible, de degré r}$$

cf. la section 13.6. Le théorème suivant est du à C.F. Gauss

Théorème 13.3.17. *Si p est premier, le groupe multiplicatif*

$$\big(\mathbb{Z}/p\mathbb{Z}\big)^* = \{\textit{éléments inversibles de } \big(\mathbb{Z}/p\mathbb{Z}, \times\big)\}$$

est cyclique, i.e. il existe g premier à p tel que

$$\{1, \ldots, p-1\} \equiv \{g^n,\, 0 \leq n \leq p-2\}$$

Un générateur g du groupe cyclique $\mathbb{Z}/p\mathbb{Z}$ s'appelle une **racine primitive modulo** *p.*

De même si $q = p^r$ avec p premier le groupe multiplicatif, $\mathbb{F}_q^*$, des éléments inversibles de $\mathbb{F}_q$ est cyclique.

Démonstration*:* Rappelons que dans un corps K un polynôme $P(x) \in K[x]$ de degré $n \geq 0$ a au plus n racines.

Tout élément g de $\mathbb{F}_q^*$ a un ordre d c'est à dire que $g^d = 1$ avec $d \geq 1$ minimal et il y $\varphi(d)$ éléments d'ordre d, cf. infra. De plus on a

$$\sum_{d \mid n} \varphi(d) = n$$

En effet dans $(\mathbb{Z}/n\mathbb{Z}, +)$ il y a un seul sous-groupe additif d'ordre d c'est l'ensemble des éléments $k\frac{n}{d}$ pour $0 \leq k \leq d-1$, noté C_d. On note Φ_d l'ensemble des générateurs de C_d. Comme tout élément de $(\mathbb{Z}/n\mathbb{Z}, +)$ engendre un des C_d le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est union disjointe des Φ_d et on a

$$n = \mathrm{Card}(\mathbb{Z}/n\mathbb{Z}, +) = \sum_{d \mid n} \Phi_d = \sum_{d \mid n} \varphi(d)$$

Soit alors d un diviseur de $q-1$ le cardinal de $\mathbb{F}_q^*$. S'il existe $x \in \mathbb{F}_q^*$ d'ordre d le sous-groupe multiplicatif $\langle x \rangle = \{1, x, \ldots, x^{d-1}\}$ engendré par x est cyclique d'ordre d et comme l'équation $X^d = 1$ a au plus d solutions dans le corps $\mathbb{F}_q$. Donc tout élément y tel que $y^d = 1$ appartient à $\langle x \rangle$.

En particulier les seuls éléments d'ordre d de $\mathbb{F}_q^*$ sont les générateurs de $\langle x \rangle$ qui sont en nombre $\varphi(d)$. Donc le nombre d'éléments de $\mathbb{F}_q^*$ d'ordre d est 0 ou $\varphi(d)$. Si c'était 0 pour un d, la formule $n = \sum_{d \mid n} \varphi(d)$ montrerait que le nombre d'éléments de $\mathbb{F}_q^*$ est $< (q-1$, ce qui est absurde. Il existe donc au moins un élément $x \in \mathbb{F}_q^*$ d'ordre $q-1$ et donc $\langle x \rangle = \mathbb{F}_q^*$ ce qui équivaut à $\mathbb{F}_q^*$ est cyclique. □

Le théorème suivant joue un rôle extrèmement important en arithmétique modulaire et en particulier pour le décodage du cryptosystème RSA, ainsi que pour la mise en oeuvre du cryptosystème El Gamal

Théorème 13.3.18 (petit théorème de Fermat)**.** *Soit p un nombre premier. Tout entier a vérifie la congruence $a^p \equiv a \pmod{p}$, et si $a \wedge p = 1$ on a aussi $a^{p-1} \equiv 1 \pmod{p}$.*

***Exemple* 13.3.9.** $p = 7$, $a = 3$ alors

$$\begin{aligned}\Big(3^6 \pmod 7\Big) &= \Big(3^{2+4} \pmod 7\Big)\\ &= \Big(3^2 \pmod 7\Big)\Big((3^2)^2 \pmod 7\Big)\\ &= \Big(2 \times 4 \pmod 7\Big) = \Big(1 \pmod 7\Big)\end{aligned}$$

Remarquer la manière de calculer une puissance: écrire l'exposant en base 2 et procéder par élévations au carré successives.

Démonstration*:* Les éléments inversibles de $\mathbb{N}$ modulo p plus petits que p sont 1, 2,...,$(p-1)$. Considérons a premier à p donc inversible modulo p et considérons l'ensemble

$$\{a,\, 2a,\, 3a, \ldots,\, (p-1)a\} \mod p$$

c'est une permutation de l'ensemble $\{1, 2, \ldots, (p-1)\}$ car a est inversible modulo p. Donc:

$$\begin{gathered}a \cdot 2a \cdot 3a \ldots (p-1)a \equiv 1 \cdot 2 \cdot 3 \ldots (p-1) \mod p\\ \Updownarrow\\ (a^{p-1} - 1)\big((p-1)!\big) \equiv 0 \mod p\end{gathered}$$

Comme $(p-1)!$ est premier à p donc inversible modulo p on a

$$a^{p-1} \equiv 1 \mod p \qquad \square$$

Le théorème suivant est appelé: Théorème des restes chinois

Théorème 13.3.19. *Soient m_1, m_2,...m_r des entiers naturels deux à deux premiers entre eux (i. e. $m_i \wedge m_j = 1$ si $i \neq j$) et soient a_1, a_2,...a_r des entiers relatifs. Le système de congruences*

$$\text{(13.3)} \qquad \begin{cases} x \equiv a_1 \mod m_1, & x \equiv a_2 \mod m_2\\ \quad\vdots & \quad\vdots\\ \ldots & x \equiv a_r \mod m_r \end{cases}$$

a toujours une solution et deux solutions quelconques sont congrues modulo $M = m_1 m_2 \ldots m_r$

***Exemple* 13.3.10.** Prenons $r = 2$, $m_1 = 15$, $m_2 = 14$, $a_1 = 6$, $a_2 = 9$. On veut donc résoudre simultanément

$$\text{(13.4)} \qquad x \equiv 6 \mod 15 \text{ et } x \equiv 9 \mod 14$$

La première équation impose que x est de la forme $x = 6 + 15k$ avec $k \in \mathbb{Z}$ et la deuxième impose que x est de la forme $x = 9 + 14\ell$ $\ell \in \mathbb{Z}$ et par connséquent on doit avoir

$$6 + 15k = 9 + 14\ell \Longleftrightarrow 15k - 14\ell = 3$$

Comme $14 \wedge 15 = 1$ le théorème de Bézout indique qu'il existe $(u, v) = (1, -1)$ tel que $15u + 14v = 1$ et donc en prenant $k = \ell = 3$ on a une solution $x = 51$ du système de congruences (13.4)

Démonstration*:* Unicité (mod M) de la solution au système de congruences. Si x_1 et x_2 sont deux solutions alors $x = x_1 - x_2 \equiv 0 \pmod{m_i}$ pour $1 \leq i \leq r$ et donc $x \equiv 0 \pmod{M}$.

Soit $M_i = \frac{M}{m_i}$, clairement $M_i \wedge m_i = 1$ donc il existe un entier N_i tel que $M_i N_i \equiv 1 \pmod{m_i}$ et de plus $m_i \mid M_j$ si $i \neq j$. Alors

$$x = \sum_{i=1}^{r} a_i M_i N_i \Longrightarrow x \equiv a_i \mod m_i, \quad 1 \leq i \leq r \qquad \square$$

Ce théorème permet de remplacer un système de congruences modulo les m_i par une congruence unique modulo $M = m_1 \cdots_r$.

Corollaire 13.3.20. *Avec les notations du théorème* 13.3.19*, le système de congruences* (13.3)

$$\begin{cases} x \equiv a_1 \mod m_1, & x \equiv a_2 \mod m_2 \\ \quad \vdots & \quad \vdots \\ \ldots & x \equiv a_r \mod m_r \end{cases}$$

équivaut à la congruence unique

$$y \equiv x \mod M$$

Démonstration*:* C'est évident. □

***Remarque* 13.3.2.** Ce corollaire exprime que l'on a

$$\prod_{i=1}^{r} \mathbb{Z}/m_i\mathbb{Z} \simeq \mathbb{Z}/M\mathbb{Z}$$

où l'isomorphisme est un isomorphisme d'anneau.

Définition 13.3.21. *Si m est un entier positif on note $\varphi(m)$ le nombre d'entiers $b < m$ et premiers à m, ou de manière équivalente $\varphi(m)$ est le nombre d'entiers $b < m$ inversibles modulo m*

La fonction φ est appelée l'***indicatrice d'Euler***.

Proposition 13.3.22. *Si $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ est la décomposition de m en facteurs premiers distincts alors*

$$\varphi(m) = p_1^{\alpha_1 - 1}(p_1 - 1) p_2^{\alpha_2 - 1}(p_2 - 1) \dots p_r^{\alpha_r - 1}(p_r - 1) \tag{13.5}$$

Démonstration*:* Il est clair que $\varphi(1) = 1$, que si p est premier $\varphi(p) = p - 1$ et que $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$. Par le théorème des restes chinois si m est premier à n alors

$$\varphi(mn) = \varphi(m) \times \varphi(n) \qquad \square$$

Théorème 13.3.23 (Théorème d'Euler)**.** *Soit $m > 1$ un entier et soit a un entier premier à m, alors on a: $a^{\varphi(m)} \equiv 1 \pmod{m}$*

Démonstration*:* Même preuve que pour le petit théorème de Fermat $\square$

En particulier si p et q sont premiers,

$$\varphi(pq) = (p-1)(q-1) \tag{13.6}$$

et

$$a^{(p-1)(q-1)} \equiv 1 \mod pq \tag{13.7}$$

Il est facile de montrer à partir du théorème d'Euler le corollaire important suivant qui est un cas particulier d'un théorème de Lagrange, [28],

Corollaire 13.3.24. *Soit $m \in \mathbb{N}$ et soit $a \in \mathbb{N}$ tel que $a \wedge m = 1$ alors le plus petit entier $e \geq 1$ tel que $a^e \equiv 1 \pmod{m}$ est un diviseur de $\varphi(m)$.*

Démonstration*:* Supposons que e ne soit pas un diviseur de $\varphi(m)$ et écrivons l'identité de la division euclidienne de $\varphi(m)$ par e

$$\varphi(m) = e \times q + r \text{ avec } 0 < r \leq e - 1$$

on a $r \neq 0$ car e ne divise par $\varphi(m)$. Alors

$$a^r = a^{varphi(m) - eq} = a^{\varphi(m)} \times a^{eq} = a^{\varphi(m)} \times (a^e)^q \equiv 1 \mod m$$

Or comme $1 \leq r \leq e - 1$ ceci contredit la définition de e. $\square$

Résidus quadratiques modulo p.

On va étudier les ***résidus quadratiques*** modulo un nombre premier p c'est à dire les carrés modulo un nombre premier p. Cette étude joue un rôle important dans les tests de primalité probabilistes ou non.

Définition 13.3.25 (Symbole de Legendre)**.** *On pose si p est premier impair*

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{si } a \text{ est premier à } p \text{ et est un carré} \pmod p \\ -1 & \text{si } a \text{ est premier à } p \text{ et n'est pas un carré} \pmod p \\ 0 & \text{si } a \text{ n'est pas premier à } p \end{cases}$$

Le symbole $\left(\frac{a}{p}\right)$ *est appelé le* **symbole de Legendre**.

C'est un caractère du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$ à valeur dans $\{\pm 1\} \cup \{0\}$ de période p autrement dit:

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$

$$\left(\frac{a}{p}\right) = \left(\frac{a+p}{p}\right)$$

Théorème 13.3.26 (Euler)**.** *Si p est premier impair et a premier à p alors*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p, \quad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Démonstration*:* Pour la démonstration voir [13]. □

Théorème 13.3.27 (Loi de ***réciprocité quadratique***)**.** *Soit p et q des premiers impairs alors*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Démonstration*:* Pour la démonstration voir [13]. □

Ce théorème (un des plus célèbres de l'arithmétique) est du à C. F. Gauss, il se généralise au symbole de Jacobi ci-dessous. Sa preuve est délicate.

Définition 13.3.28 (Symbole de Jacobi)**.** *On pose si* $m = \prod_{p_i \,|\, m} p_i^{\alpha_i}$ *est impair et* $n \in \mathbb{Z}$

$$\left(\frac{n}{m}\right) = \begin{cases} \prod_{p_i \,|\, m} \left(\frac{n}{p_i}\right)^{\alpha_i} & \text{si } m \wedge n = 1 \\ 1 & \text{si } m = 1 \\ 0 & \text{si } m \wedge n \neq 1 \end{cases}$$

Le symbole de Jacobi possède les propriétés suivantes. Si m est un entier impair

$$n_1 \equiv n_2 \mod m \Longrightarrow \left(\frac{n_1}{m}\right) = \left(\frac{n_2}{m}\right) \tag{13.8}$$

$$\left(\frac{2}{m}\right) = \begin{cases} +1 & \text{si } m \equiv \pm 1 \pmod 8 \\ -1 & \text{si } m \equiv \pm 3 \pmod 8 \end{cases} \tag{13.9}$$

$$\left(\frac{n_1 n_2}{m}\right) = \left(\frac{n_1}{m}\right)\left(\frac{n_2}{m}\right) \tag{13.10}$$

Il vérifie aussi une ***loi de réciprocité quadratique***: Si m et n sont entiers impairs:

$$\left(\frac{n}{m}\right) = \begin{cases} -\left(\frac{m}{n}\right) & \text{si } m \equiv n \equiv 3 \pmod 4 \\ +\left(\frac{m}{n}\right) & \text{sinon} \end{cases} \tag{13.11}$$

Exercices. 1

13.3.1. Calculer en utilisant la loi de réciprocité quadratique le symbole de Jacobi $\left(\frac{7411}{9283}\right)$.

13.4 Tests de primalité.

Pour les cryptosystèmes à clef publique on a besoin de disposer de grands nombres premiers. il est donc important de disposer de méthodes rapides pour dresser des listes de nombres premiers.

Pour tester si n est premier on pourrait essayer de le diviser par tous les entiers $< n$. En fait on remarque que tout nombre entier non premier

possède au moins un diviseur $d \neq 1$ strictement inférieur à $\sqrt{n}$. En effet, si n n'est pas premier on peut écrire $n = dd'$ avec $d, d' > 1$, si $d, d' < \sqrt{n}$ alors $dd' < n$ ce qui contredit $dd' = n$.

Cette remarque est à la base de la méthode du ***crible d'Eratosthenes***. Pour tester si un nombre, n, est premier on teste sa divisibilité par tous les entiers $m < \sqrt{n}$. S'il n'est divisible par aucun entier $< \sqrt{n}$ il est premier.

Cette méthode est impraticable dès que n est grand car $\sqrt{n}$ n'est pas majoré uniformément par un polynôme en $\ln n$.

Le temps de calcul devient vite prohibitif. On a vu en effet qu'une division de n par un entier inférieur demande $O(\ln^3 n)$ opérations élémentaires donc cette méthode nécessitera

$$O\Big(\sum_{i=1}^{\sqrt{n}} \ln^3 n\Big) = O(\sqrt{n}\ln^3 n) \text{ opérations}$$

Ce n'est donc pas un algorithme polynomial en temps.

Parmi les tests de primalité certains parmi les plus utilisés sont basés sur le petit théorème de Fermat, ou sur les propriétés du symbole de Legendre et sur la théorie des résidus quadratiques.

Agrawal-Kayal-Saxena ont montré en 2002, [1], que le problème décisionnelle

> n est-il premier?

appartient à la classe **P** des problème soluble en temps polynomial en fonction de la taille des données.

Leur preuve fournit des tests de primalité, basés sur le petit théorème de Fermat, qui sont polynomiaux en temps (actuellement en $O\big(\ln^{12}(n)\big)$ et même $O\big(\ln^6(n)\big)$). Mais pour l'instant ils sont moins performants que des tests probabilistes comme ceux décrits ci-dessous.

Pour tester si n est premier on procède souvent en pratique de la manière suivante dans les logiciels de calcul formel.

1. Vérifier que n n'est pas divisible par des petits facteurs premiers.
2. Puis pour des a choisis au hasard et tels que $1 \leq a \leq n$ et $a \wedge n = 1$ calculer $a^{n-1} \mod n$.
3. Si $a^{n-1} \not\equiv 1 \mod n$ pour au moins un a alors n n'est pas premier.

4. Sinon on ne peut pas conclure (cf. nombres de Carmichaël, par exemple 561). On dit que n est pseudo premier.

Pour avoir un résultat sûr on peut utiliser le ***test de Lucas***

Théorème 13.4.1 (Lucas)**.** *Si a est premier à n et si pour tout diviseur premier p de $n-1$ on a $a^{\frac{n-1}{p}} \not\equiv 1 \mod n$ alors n est premier*

Démonstration*:* La preuve de ce résultat est immédiate. □

Ce résultat n'est utilisable en pretique car il nécessite de décomposer en facteurs premiers $n-1$ et actuellement on ne dispôse pas d'algorithme polynomiaux en temps.

On peut aussi utiliser les propriétés des symboles de Legendre et de Jacobi.

Pour tester si p est premier on utilise les remarques suivantes

1. On choisit b premier à n avec $1 \leq b \leq n-1$ et on calcule $b^{\frac{p-1}{2}} \pmod p$.
2. Si p est premier on doit avoir $b^{\frac{p-1}{2}} \equiv \left(\frac{b}{p}\right) \pmod p$ pour tout b (théorème 13.3.26 page 176.
3. Si p n'est pas premier alors on a $b^{\frac{p-1}{2}} \not\equiv \left(\frac{b}{p}\right) \pmod p$ pour au moins 50% des b premiers à n.

On aboutit ainsi au ***test de primalité de Solovay-Strassen***

1. Tirer un entier aléatoire a, $1 \leq a \leq n-1$
2. Si $\left(\frac{a}{n}\right)$ $\begin{cases} \equiv a^{\frac{n-1}{2}} \pmod n & n \text{ est probablement premier} \\ \not\equiv a^{\frac{n-1}{2}} \pmod n & n \text{ est décomposable} \end{cases}$
3. Si $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod n$ choisir un autre a et recommencer.

La loi de réciprocité quadratique rend ce test probabiliste très efficace. Elle évite en effet pour calculer le symbole de Jacobi d'avoir à factoriser a et n.

***Exemple* 13.4.1.** Testons la primalité de 547. On choisit $a = 5$.

On calcule d'une part

$$\left(\frac{5}{547}\right) = \left(\frac{547}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1$$

d'autre part

$$5^{\frac{547-1}{2}} \mod 547 \equiv 5^{1+2^4+2^8} \mod 547 \equiv 5 \cdot 113 \cdot 395 \mod 547$$
$$\equiv -1 \mod 547$$

Donc 547 a une chance d'être premier. Pour se conforter on recommence avec 7 au lieu de 5, etc.

Actuellement on est capable de prouver la primalité d'un nombre sans symétrie particulière de 2000 à 3000 chiffres en base 10 en un mois de CPU sur une station de travail. On prouve aussi la primalité de nombres tests comme les nombres de Mersenne $(2^p - 1)$ ayant plusieurs millions de chiffres.

Pour construire de grands nombres premiers on couple les résultats précédents avec des théorèmes sur la répartition des nombres premiers.

On sait par exemple que le nombre de nombres premiers inférieurs à x, $\pi(x) \sim \frac{x}{\ln x}$. On en déduit qu'il y a toujours un nombre premier entre n et $2n$ (en fait on sait plus). On prend un nombre n au hasard et on teste s'il est premier, s'il ne l'est pas on passe à $n+1$, etc.

13.5 Méthode de factorisation.

Principe d'un algorithme très utilisé pour factoriser de grand nombres entiers, le ***crible quadratique***. Il est fondé sur la proposition suivante

Proposition 13.5.1 (Fermat)**.** *Soit n un entier positif impair. Il y a une bijection entre les décompositions de n sous la forme $n = ab$ avec $a \geq b \geq 0$ entiers et les représentations de n sous la forme $n = t^2 - s^2$, où s et t sont des entiers positifs ou nuls. La bijection est donnée par les équations*

$$t = \frac{a+b}{2}, \quad s = \frac{a-b}{2}, \quad a = t+s, \quad b = t-s$$

***Exemple* 13.5.1.** Soit à factoriser $n = 23360947609$

$$n = 23360947609 \Longrightarrow E(\sqrt{n}) = 152843$$

On pose $t = 152843$. On teste s'il existe i pas trop grand tel que

$$(t+i)^2 - n = (152843+i)^2 - 23360947609$$

est un carré.

On trouve que pour $i = 2$ on a

$$152845^2 - 23360947609 = 804^2$$

et donc $n = pq$ avec $\begin{cases} p = 152845 + 804 = 152649 \\ q = 152845 - 804 = 152041 \end{cases}$. On vérifie aisément que p et q sont premiers.

Cette méthode ne marche pas à coup sûr, on l'a raffinée de diverses manières mais la factorisation d'un nombre reste encore un problème difficile.

Dans la proposition précédente on utilise le fait que l'on a

$$t^2 \equiv s^2 \mod n \text{ et } t \not\equiv \pm s \mod n$$

Ces deux relations impliquent que l'on trouve alors un diviseur non trivial de n en calculant $\mathrm{PGCD}(t+s, n)$ et $\mathrm{PGCD}(t-s, n)$. En effet $n \mid t^2 - s^2$ et $n \not| t+s$, $n \not| t-s$, donc $a = \mathrm{PGCD}(t+s, n)$ est un diviseur non trivial de n et $b = \frac{n}{a}$ divise $a = \mathrm{PGCD}(t-s, n)$.

***Exemple* 13.5.2.** On veut factoriser 4633. On remarque que

$$118^2 \equiv 25^2 \mod 4633,$$
$$\mathrm{PGCD}(118+25, 4633) = 41, \quad \mathrm{PGCD}(118-25, 4633) = 113$$

On constate que $4633 = 41 \times 113$.

Pour mettre cette remarque en oeuvre on cherche une famille finie de nombres premiers $\mathcal{B} = \{p_1, p_2, \ldots, p_h\}$, où $p_1 = -1$ et des entiers b_i tels que le plus petit représentant de $(b_i^2 \mod n)$ noté $\{b_i^2\}$ (i.e le représentant compris entre $-\frac{n}{2}$ et $+\frac{n}{2} - 1$) s'écrive $\{b_i^2\} = \prod_{j=1}^{h} p_j^{\varepsilon_{j,i}}$ avec pour tout j, $\sum_i \varepsilon_{j,i} \equiv 0 \pmod 2$.

On pose alors

$$\gamma_j = \frac{1}{2} \sum_i \varepsilon_{j,i}$$

et

$$\{b\} = \prod_i b_i \mod n, \text{ et } c = \prod_{p \in \mathcal{B}} p^{\gamma_j}$$

Si $b \not\equiv \pm c \mod n$ on a gagné et on a un diviseur de n par la remarque précédente. Sinon il faut recommencer avec un autre choix pour $\mathcal{B}$ ou pour les b_i.

La factorisation des entiers reste un problème difficile. En 1994 il a fallu le travail combiné de 600 personnes pendant 8 mois pour factoriser un nombre

de 129 chiffres proposé 17 ans plus tôt et pour cela il fallu développer dans l'intervalle de nouvelles méthodes de factorisation.

En 1999 il a fallu 8 mois de travail pour factoriser un nombre de 155 chiffres. Il a fallu en plus de l'augmentation de puissance des ordinateurs développer et perfectionner de nouvelles méthodes de factorisation.

En 2005 on a factorisé des nombres de 200 chiffres en base 10 en utilisant le crible quadratique et 80 ordinateurs travaillant en parallèle pendant plusieurs mois.

Pour des généralisations des codes RSA ainsi que pour des procédés de factorisation et des tests de primalité, on utilise l'arithmétique sur les courbes elliptiques qui est une sorte de généralisation de l'arithmétique modulaire .

13.6 Rappels d'algèbre.

Ainsi qu'on l'a vu à la section 8.5 page 82 la description d'AES nécessite celle des extensions de corps finis comme quotient d'anneaux de polynômes.

13.6.1 Groupes, anneaux, corps

Nous rappelons quelques définition sur les groupes, les anneaux et les corps on trouvera plus d'informations dans [28].

Définition 13.6.1. *Un* **groupe**, G, *est un ensemble muni d'une loi de composition interne notée* $*$

$$\begin{aligned} G \times G &\longrightarrow G \\ (a,b) &\longmapsto c = a * b \end{aligned}$$

telle que

1. *Il existe un élement noté* 1 *tel que pour tout* $a \in G$ *on a* $a*1 = 1*a = a$, *il est appelé l'***élément neutre pour l'addition**.
2. *Pour tout* $a \in G$ *il existe* $a' \in G$ *tel que* $a * a' = a' * a = 1$, a' *est noté aussi* a^{-1}, *appelé l'***inverse** *de* a
3. *Pour tous* $a, b, c \in G$ *on a* $((a * b)) * c) = (a * (b * c))$, **associativité**

Si de plus la loi interne est **commutative** *c'est à dire que*

$$a * b = b * a$$

pour tous $a, b \in G$ on dit que G est un **groupe abélien** *ou commutatif. Dans ce cas la loi est souvent notée $+$, l'élément neutre est noté 0, et l'inverse de a est appelé l'opposé de a et noté $-a$.*

Définition 13.6.2. *Si $(G, \times)$ est un groupe l'***ordre d'un élément** *$g \in G$ est le plus petit entier $n \geq 1$ tel que $g^n = 1$. Un groupe, $(G, \times)$, est* **cyclique** *s'il existe un élément $g \in G$ tel que tout élément $a \in G$ soit de la forme g^n; autrement dit G est isomorphe à $(\mathbb{Z}, +)$ ou à $(\mathbb{Z}/m\mathbb{Z}, +)$.*

Théorème 13.6.3. *Si G est un groupe fini de cardinal (on dit aussi d'ordre) $= |G|$ alors l'ordre de tout élément $g \in G$ est un diviseur de n.*

Démonstration*:* Pour la preuve voir [28]. On a donné une preuve pour les groupe abélien au corollaire 13.3.24. □

Théorème 13.6.4. *Un groupe abélien fini est de la forme*

$$\mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_s\mathbb{Z}$$

où $m_i \,|\, m_{i+1}$ pour $1 \leq i \leq s-1$. Les entiers m_i sont déterminés de manière unique.

Définition 13.6.5. *Un* **anneau** *est un ensemble A muni de deux lois internes (c'est à dire des applications de $A \times A$ dans A). La première notée $+$ est appelée addition, la seconde notée multiplicativement, $\times$ ou $\cdot$, est appelée multiplication. L'addition détermine sur A une structure de groupe abélien. La multiplication possède les propriété suivantes*

1. *elle est associative: pour tous $a, b, c \in A$ on a*

$$((a \times b) \times c) = (a \times (b \times c))$$

2. *elle est distributive par rapport à l'addition: pour tous $a, b, c \in A$ on a*

$$a(b + c) = a \cdot b + a \cdot c$$

3. *il y a un* **élément unité** *noté 1 tel que $a \cdot 1 = 1 \cdot a = a$*

4. *si la multiplication est commutative, pour tous $a, b \in A$ $a \cdot b = b \cdot a$, on dit que l'anneau est commutatif.*

***Exemples* 13.6.1.** Les entiers relatifs $\mathbb{Z}$ forment un anneau commutatif.

Si m est un entier naturel non nul les entiers modulo m, $\mathbb{Z}/m\mathbb{Z}$, est un anneau commutatif. Le corps des nombres rationnels, $\mathbb{Q}$, est un aneau commutatif.

Les polynômes à coefficients rationnels $\mathbb{Q}[X]$, resp. réels $\mathbb{R}[X]$, resp. complexes $\mathbb{C}[X]$, forme un anneau commutatif.

Si K est un corps et $P(X)$ un polynômes non nul de $K[X]$, $K[X]/P(X)K[X]$ est un anneau commutatif.

Définition 13.6.6. *Un élément a de l'anneau A est* **inversible** *s'il existe $a' \in A$ tel que $a \times a' = a' \times a = 1$, a' est l'***inverse** *de a.*

***Exemples* 13.6.2.** Dans les entiers relatifs $\mathbb{Z}$ seuls 1 et -1 sont inversibles, comme dans tout anneau.

Dans $\mathbb{Z}/m\mathbb{Z}$ les éléments inversibles sont exactement ceux qui proviennent d'entiers premiers à m.

Dans $\mathbb{Q}[X]$, resp. $\mathbb{R}[X]$, resp. $\mathbb{C}[X]$, les éléments inversibles sont les éléments non nuls de $\mathbb{Q}$, resp. $\mathbb{R}$, resp. $\mathbb{C}$.
les éléments inversibles de $K[X]/P(X)K[X]$ sont les polynômes premiers à $P(X)$.

Définition 13.6.7. *Un* **corps** *est un anneau dans lequel tout élément non nul, c'est distinct de l'élément neutre pour l'addition, a un inverse pour la multiplication, autrement dit:*

Pour tout $a \neq 0$, il existe a' tel que $aa' = a'a = 1$.

On remarque que dans un corps $1 \neq 0$ et de plus $0 \times a = 0$ pour tout élément a du corps, cf. [28].

***Exemples* 13.6.3.** $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des corps.

$\mathbb{Z}/m\mathbb{Z}$ est un corps si et seulement si m est un nombre premier.

Si K est un corps alors $K[X]/P(X)K[X]$ est un corps si et seulement si $P(X)$ est un polynôme premier de $K[X]$.

Définition 13.6.8. *Soit K un corps et k un sous-corps. On dit que K est une* **extension***de k.*

Proposition 13.6.9. *Soit K un corps et k un sous-corps, alors le corps K est un espace vectoriel sur le corps k.*

Démonstration*:* Pour la preuve voir [28] □

Définition 13.6.10. *Soit K un corps et k un sous-corps. On dit que K est une* **extension algébrique***de k si tout élément $x \in K$ est racine d'une équation algébrique à coefficents dans k. Autrement si*

> *Pour tout $x \in K$ il existe un polynôme non nul $P(X) \in k[X]$ tel $P(x) = 0$.*

Un corps K est **algébriquement clos** *si tout polynôme de $K[X]$ a au moins une racine dans K. On appelle* **clôture algébrique** *d'un corps k une extension algébrique de k qui est algébriquement close.*

Théorème 13.6.11. *Tout corps k possède une clôture algébrique K. elle est unique à k-isomorphisme de corps près c'est à dire que si K' désigne une autre clôture algébrique de k il existe une bijection*

$$\varphi : \ K \longrightarrow K'$$

telle que pour tous x, y de K

$$\begin{aligned} &\varphi(x+y) = \varphi(x) + \varphi(y) \\ &\varphi(1_K) = 1_{K'} \\ &\varphi(xy) = \varphi(x)\varphi(y) \end{aligned}$$

Démonstration*:* Pour la preuve cf. [28]. □

On note souvent $\bar{K}$ une clôture algébrique de K.

Définition 13.6.12. *Soit K un corps on pose pour $m \in \mathbb{N}$*

$$c(m) = \underbrace{1 + 1 + \cdots + 1}_{m \text{ fois}}$$

où l'addition est faite dans le corps K.

S'il existe un entier $m \neq 0$ tel que $c(m) = 0$, on notera p le plus petit entier non nul tel que $c(p) = 0$ et on dira que le corps K est de **caractéristique finie** *que sa caractéristique est p. Si $c(m) \neq 0$ pour tout entier $m \neq 0$ on dira suivant les auteurs que K est de* **caractéristique infinie** *ou que K est de* **caractéristique zéro**

Proposition 13.6.13. *La caractéristique d'un corps est soit infinie et si elle est finie c'est nécessairement un nombre premier p*

Démonstration*:* Si K est de caractéristique finie p et si p n'est pas un nombre premier alors il existe des entiers $k, \ell > 1$ tels que $p = k\ell$. Par définition de la caractéristique on $c(k) \neq 0$, $c(\ell) \neq 0$. Donc $c(k)$ et $c(\ell)$ ont des inverses dans K, notés $c(k)^{-1}$ et $c(\ell)^{-1}$. On a alors

$$\begin{aligned}[c(k)c(k)^{-1}][c(\ell)c(\ell)^{-1}] &= 1 \\ &= [c(k)c(\ell)][c(k)^{-1}c(\ell)^{-1}] \\ &= 0 \times [c(k)^{-1}c(\ell)^{-1}] \\ &= 0\end{aligned}$$

ce qui est contraire à $0 \neq 1$. □

Proposition 13.6.14. *Si K est un corps de caractéristique p alors*

$$\underbrace{x + x + \cdots + x}_{p \text{ fois}} = px = 0$$

Démonstration*:* C'est évident. □

Théorème 13.6.15. *Si K est un corps de caractéristique p alors pour tous $a, b \in K$ on a:*

$$(a + b)^{p^n} = a^{p^n} + b^{p^n}$$

Démonstration*:* Pour la preuve cf. [28]. □

13.6.2 Anneaux des polynômes sur un corps

Soit $\mathbb{K}$ un corps, par exemple $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ou un corps fini comme $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z}$ avec p premier.

Définition 13.6.16. *L'anneau des polynômes à coefficients dans $\mathbb{K}$, noté $\mathbb{K}[X]$, est l'ensemble des suites finies d'éléments de $\mathbb{K}$,*

$$P = P(X) = (a_0, a_1, \ldots, a_n)$$

appelées polynômes. Deux polynômes

$$P(X) = (a_0, a_1, \ldots, a_n) \in \mathbb{K}[X], \quad Q(X) = (b_0, b_1, \ldots, b_m) \in \mathbb{K}[X]$$

(avec $m \geq n$) sont égaux si $a_i = b_i$ pour $0 \leq i \leq n$ et $b_j = 0$ pour $n + 1 \leq j \leq m$, en particulier

$$P(X) = (a_0, a_1, \ldots, a_n) = \underbrace{(a_0, a_1, \ldots, a_n, 0, 0, \ldots, 0)}_{n+h \text{ éléments}}$$

Considérons les polynômes

$$P(X) = (a_0, a_1, \ldots, a_n) \in \mathbb{K}[X], \quad Q(X) = (b_0, b_1, \ldots, b_m) \in \mathbb{K}[X]$$

On définit la somme $P(X) + Q(X)$ *par*

$$P(X)+Q(X) = R(X) = (c_0, c_1 \ldots, c_n) = \big((a_0+b_0), (a_1+b_1), \ldots, (a_n+b_n)\big)$$

et le produit $P(X) \times Q(X) = P \cdot Q = PQ$ *par*

$$P(X) \times Q(X) = (d_0, d_1 \ldots, d_{m+n}) = \big((a_0b_0), (a_0b_1 + a_1b_0), \ldots \\ \ldots, \underbrace{(a_jb_0 + a_{j-1}b_1 + \cdots + a_{j-k}b_k + \cdots + a_0b_j)}_{\text{avec } a_\ell=0 \text{ si } \ell>n,\ b_\lambda=0 \text{ si } m>\lambda} + \cdots + (a_nb_m)\big)$$

***Notations* 13.6.1.** On adopte les notations classiques suivantes

- Le polynôme $(0, 0, \ldots, 0)$ sera noté 0 et on a $P(X) + 0 = 0 + P(X) = P(X)$ et $0 \times P(X) = P(X) \times 0 = 0$. Le polynôme $(1, 0, 0 \ldots, 0)$ sera noté 1 et on a $1 \times P(X) = P(X) \times 1 = P(X)$.
- Le polynôme $P(X) = (0, 1, 0, \ldots, 0)$ sera noté X et appelé l'***indéterminée*** ou la ***variable***.
- Le polynôme $P(X) = \underbrace{(0, 1, 0, \ldots, 0) \times \cdots \times (0, 1, 0, \ldots, 0)}_{n \text{ facteurs}}$ sera noté X^n,
- Si $P(X) \neq 0$ alors il existe un indice n tel que si

  $$P(X) = (a_0, a_1, \ldots, a_m)$$

  on ait $a_\ell = 0$ pour $\ell \geq n + 1$. L'entier n sera appelé le ***degré du polynôme*** P et sera noté $\deg(P)$. Le degré du polynôme 0 n'est pas défini, on lui donne parfois par convention le degré $-\infty$.
- Avec ces notations on écrira le polynôme $P(X) = (a_0, a_1, \ldots, a_n)$ de degré n sous la forme $P(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$, le terme a_iX^i, $0 \leq i \leq n$ sera appelé le ***terme de degré*** i de $P(X)$. On remarque que l'on a aussi $P(X) = a_0 + a_1X + \cdots + a_nX^n + 0x^{n+1} + \cdots + 0x^m$
- Un polynôme non nul, $P(X)$, sera dit ***unitaire*** si le coefficent de son terme de plus haut degré est 1.

Muni de ces deux opérations $\mathbb{K}[X]$ est un anneau commutatif unitaire, cf. [28], muni d'une division euclidienne définie de la manière suivante

Définition 13.6.17 (Division euclidienne)**.** *Si $A(X)$ et $B(X)$ sont deux polynômes de $\mathbb{K}[X]$ ($B \neq 0$) il existe un unique couple de polynômes $Q(X)$ et $R(X)$ tel que*

$$A(X) = B(X)Q(X) + R(X) \text{ et} \begin{cases} \text{ou bien} & R = 0 \\ \text{ou bien} & 0 \leq \deg(R) \leq \deg(B) - 1 \end{cases}$$

On dit que $B(X)$ est un **diviseur** *de $A(X)$ s'il existe $Q(X) \in \mathbb{K}[X]$ tel que $A(X) = B(X)Q(X)$, on note $B(X) \mid A(X)$.*

On dit que deux polynômes non nuls $A(X)$ et $B(X)$ sont **associés** *s'il existe $a \in \mathbb{K}^*$ tel que $A(X) = a \times B(X)$.*

La notion de divisibilté fournit une relation d'ordre partielle sur l'anneau des polynômes.

Tout polynôme $A(X) = a_0 + a_1X + \cdots + a_nX^n$ a au moins comme diviseurs les éléments non-nuls de $\mathbb{K}$ et lui-même car si $a \neq 0 \in \mathbb{K}$ alors a^{-1} existe et on a

$$A(X) = a\Big((a_0a^{-1}) + (a_1a^{-1})X + \cdots + (a_na^{-1})X^n\Big),\ A(X) = 1 \times A(X)$$

Mais il peut en avoir d'autres par exemple:

$$X^2 - 1 = (X - 1)(X + 1)$$

$X^2 - 1$ a donc comme diviseurs les constantes non nulles ($=\mathbb{K}^*$), les polynômes $X-1$ et $X+1$ à une constante multiplicative non nulle près et lui-même à une constante multiplicative non nulle près.

Un polynôme, $P(X)$, est appelé une ***unité de*** $\mathbb{K}[X]$ s'il est réduit à un élément de $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$, autrement dit si P^{-1} existe dans $\mathbb{K}[X]$

Définition 13.6.18. *Un polynôme $P(X) \in \mathbb{K}[X]$ est appelé un* **polynôme premier** *ou* **polynôme irréductible** *si ses seuls diviseurs sont lui-même et les élements de $\mathbb{K}^*$*

***Exemple* 13.6.4.** Dans $\mathbb{Q}[X]$ le polynôme X^2+1 est irréductible, par contre dans $\mathbb{F}_2[X]$ il ne l'est pas car sur $\mathbb{F}_2$ on a $X^2 + 1 = (X + 1)^2$.

Proposition 13.6.19. *Tout polynôme non nul $A(X) \in \mathbb{K}[X]$ possède une décomposition en un* **produit de polynômes premiers**

$$A(X) = a \cdot P_1(X)P_2(X)\dots P_m(X)$$
$$\text{où } a \in \mathbb{K}^*,\ P_j(X) \text{ premier pour } 1 \leq j \leq m$$

Cette décomposition est unique à l'unité a près et à l'ordre près des facteurs P_j. Si l'on regroupe tous les polynômes P_j associés la décomposition en produit de polynômes premiers prend la forme suivante

$$A(X) = a \cdot P_1(X)^{\alpha_1}P_2(X)^{\alpha_2}\dots P_\ell(X)^{\alpha_\ell}, \quad \alpha_i \in \mathbb{N},$$
$$\text{où } a \in \mathbb{K}^*,\ P_j(X) \text{ premier pour } 1 \leq j \leq \ell,$$
$$P_i \text{ et } P_j \text{ ne sont pas associés pour } i \neq j$$

sous cette forme la décomposition est unique à l'unité a près et à l'ordre des facteurs si on choisit les P_j unitaires et les $\alpha_i \geq 1$ (c'est à dire qu'on s'interdit des exposant nuls).

Démonstration*:* La preuve repose sur l'algorithme de division euclideienne, cf. [28]. □

On définit alors comme dans le cas de $\mathbb{Z}$ la notion de Plus Grand Commun Diviseur (PGCD) de deux polynômes. Les degrés des diviseurs unitaires communs à A et B forment un ensemble majoré par le maximum des degrés de A et de B.

Définition 13.6.20. *Le PGCD de deux polynômes $A(X)$ et $B(X)$ de $\mathbb{K}[X]$ est le polynôme unitaire de plus grand degré $D(X)$ qui divise à la fois $A(X)$ et $B(X)$. On note $PGCD(A, B) = A \wedge B$*

Proposition 13.6.21. *Soient $A(X)$ et $B(X)$ des polynômes non nuls. On peut toujours supposer, quitte à modifier les unités a et b et à utiliser des exposants, que leurs décomposition en produit de facteurs premiers unitaires est*

$$A(X) = a \times P_1(X)^{\alpha_1}P_2(X)^{\alpha_2}\dots P_r^{\alpha_r},$$
$$B(X) = b \times P_1(X)^{\beta_1}P_2(X)^{\beta_2}\dots P_r(X)^{\beta_r},\ \text{avec } \alpha_i, \beta_i \geq 0$$

alors le PGCD de A et de B est:

$$A(X) \wedge B(X) = P_1(X)^{\inf\{\alpha_1,\beta_1\}}P_2(X)^{\inf\{\alpha_2,\beta_2\}}\dots P_r(X)^{\inf \alpha_r,\beta_r}$$

Démonstration*:* Pour la démonstration voir [28]. □

Ni la définition ni la proposition 13.6.21 ne fournissent d'algorithmes très effecaces pour calculer le PGCD de deux polynômes, $A(X)$ et $B(X)$.

Par contre l'algorithme de la division euclidienne en fournit un très efficace.

Proposition 13.6.22. *Le PGCD des polynômes A et B est donné par l'algorithme suivant. On écrit les divisions euclidiennes successives*

$$\begin{cases} A(X) = B(X)Q(X)_0 + R_1(X) \\ B(X) = Q_1(X)R_1(X) + R_2(X) \\ R_1(X) = Q_2(X)R_2(X) + R_3(X) \\ \vdots \\ R_{j-2}(X) = Q_{j-1}(X)R_{j-1}(X) + R_j(X) \\ R_{j-1}(X) = Q_j(X)R_j(X) + R_{j+1}(X) \\ R_j(X) = q_{j+1}(X)r_{j+1}(X) \end{cases} \tag{13.12}$$

avec ($0 \leq \deg(R_1) < \deg(B)$ *ou* $R_1 = 0$*), (*$0 \leq \deg(R_2) < \deg(R_1)$ *ou* $R_2 = 0$*),* $0 \leq \deg(R_3) < \deg(R_2)$*,...,* $0 \leq \deg(R_j) < \deg(R_{j+1})$*.*

On arrête l'algorithme dès qu'un reste est nul et alors

$$A(X) \wedge B(X) = R_{j+1}(X)$$

Démonstration*:* La dernière identité de division enclidienne de (13.12) montre que R_{j+1} divise R_j, l'avant dernière identité de division enclidienne de (13.12) montre que R_{j+1} divise R_j et R_{j-1}. Puis par récurrence on montre que R_{j+1} divise A et B.

Donc R_{j+1} est un diviseur commun de A et de B, est-ce le plus grand? Considérons un diviseur commun de A et de B noté D. Par définition D divise A et B donc d'après la première des identités de division enclidienne de (13.12) on a $D \,|\, R_1$, alors la deuxième des identités de division euclidienne de (13.12) implique que $D \,|\, R_2$ puis par récurrence on montre que $D \,|\, R_{j+1}$.

On a donc montré que tout diviseur D commun de A et de B est un diviseur de R_{j+1} et comme R_{j+1} est un diviseur de A et de B c'est le plus grand, autrement dit $R_{j+1} = A \wedge B$. □

L'arithmétique de $\mathbb{K}[X]$ est donc tout à fait parallèle à celle de $\mathbb{Z}$.

- Les deux sont des anneaux munis d'une division euclidienne.
- On définit sur $\mathbb{K}[X]$ une notion de factorisation en facteurs premiers,
- On peut définir le PGCD de deux polynômes,
- Il y a sur $\mathbb{K}[X]$ une relation de Bezout, un algorithme d'Euclide étendu pour calculer le PGCD.

- etc..

On a le théorème de Bézout comme dans le cas des entiers

Théorème 13.6.23 (Théorème de Bézout)**.** *Soit $A(X), B(X) \in \mathbb{K}[X]$, alors il existe des polynômes $U(X), V(X) \in \mathbb{K}[X]$ tels que*

$$A(X)U(X) + B(X)V(X) = A(X) \wedge B(X) = D(X) \tag{13.13}$$

Démonstration*:* La preuve est la même que sur $\mathbb{Z}$. On reprend l'algorithme du PGCD (13.12) à partir de la fin. On écrit avec les notations précédentes

$$\begin{aligned}
D = R_{j+1} &= R_{j-1} - Q_j R_j = R_{j-1}U_{j-1}(1) - R_j V_j(Q_j) \\
&= R_{j-1} - Q_j\big(R_{j-2} - Q_{j-1}R_{j-1}\big) \\
&= R_{j-1}\big(1 + Q_jQ_{j-1}\big) - Q_jR_{j-2} \\
&= -U_{j-2}(Q_j)R_{j-2} + R_{j-1}V_{j-1}(Q_{j-1}, Q_j) \\
&= \big(R_{j-3} - Q_{j-2}R_{j-2}\big)\big(1 + Q_jQ_{j-1}\big) - Q_jR_{j-2} \\
&= R_{j-3}\big(1 + Q_jQ_{j-1}\big) - R_{j-2}\Big(Q_{j-2}\big(1 + Q_jQ_{j-1}\big) + Q_j\Big) \\
d = R_{j-3}U_{j-3}(Q_j, Q_{j-1}) &- R_{j-2}V_{j-2}(Q_{j-2}, Q_{j-1}, Q_j) \\
&\vdots \\
= (-1)^{j+1}aU_0(Q_1, \ldots, Q_j) &+ (-1)^j bV_0(Q_0, \ldots, Q_j)
\end{aligned}$$

On a une relation de récurrence facile sur U_j et V_j.

$$\begin{aligned}
U_{j+1} &= U_{j-1} - Q_{j+1}U_j \\
V_{j+1} &= V_{j-1} - Q_{j+1}V_j
\end{aligned}$$

□

On définit alors les congruences entre polynômes comme dans le cas des entiers

Définition 13.6.24. *Si $P(X) \in \mathbb{K}[X]$ et si $A(X)$, $B(X)$ appartiennent à $\mathbb{K}[X]$ on dit que A et B sont* **congrus modulo** *P s'il existe $Q \in \mathbb{K}[X]$ tel que $A - B = PQ$. On écrira $A \equiv B \mod P$ et on dira que A et B appartiennent à la même classe d'équivalence modulo P.*

On vérifie aisément que c'est une relation d'équivalence sur l'anneau des polynômes qui est compatible aux opérations sur les polynômes.

Proposition 13.6.25. *Soit $P(X) \in K[X]$ de degré $f \geq 0$, alors tout polynôme $A(X) \in K[X]$ possède un unique représentant dans sa classe d'équivalence modulo $P(X)$ unitaire et de degré $\leq f - 1$. Autrement dit pour tout polynôme $A(X) \in K[X]$ il existe un unique polynôme unitaire $R(X) \in K[X]$ de degré $\leq f - 1$ tel que $A(X) \equiv R(X) \mod P(X)$.*

Démonstration*:* Utiliser la division euclidienne. □

Proposition 13.6.26. *L'addition et la multiplication sont compatibles à la relation de congruence sur les polyômes; autrement dit si $P(X)$ est un polynôme fixé et si $A(X), B(X) \in \mathbb{K}[X]$ alors*

$$\Big(\big(A(X) \pmod{P(X)}\big) + \big(B(X) \pmod{P(X)}\big) \pmod{P(X)}\Big) = \big(A(X) + B(X) \pmod{P(X)}\big)$$

$$\Big(\big(A(X) \pmod{P(X)}\big) \times \big(B(X) \pmod{P(X)}\big) \pmod{P(X)}\Big) = \big(A(X) \times B(X) \pmod{P(X)}\big)$$

Démonstration*:* Pour la preuve cf. [28] □

Proposition 13.6.27. *Soit $P(X) \in K[X]$, l'ensemble des classes d'équivalence modulo $P(X)$ est noté*

$$\mathbb{K}[X]/P(X)\mathbb{K}[X] \text{ ou } \mathbb{K}[X]/P(X)$$

C'est un anneau commutatif unitaire et c'est un corps si et seulement si P est irréductible dans $K[X]$ ou de manière équivalente si $P(X)$ est un polynôme premier de $K[X]$.

Démonstration*:* Pour la première partie cf. [28]. Si P est irréductible alors par définition si $A(X) \not\equiv 0 \pmod{P(X)}$ on a $A(X) \wedge B(X) = 1$. Donc d'après le théorème de Bezout, il existe $U(X), V(X) \in \mathbb{K}[X]$ tels que

$$A(X)U(X) + P(X)V(X) = 1$$

et donc

$$A(X)U(X) \equiv 1 \mod P(X)$$

Donc si $P(X)$ est irréductible tout élement non nul de $\mathbb{K}[X]/P(X)$ possède un inverse multiplicatif, autrement dit c'est un corps. □

Proposition 13.6.28. *Un système complet de représentants de*

$$\mathbb{K}[X]/P(X)\mathbb{K}[X]$$

est l'ensemble des restes de la division euclidienne des polynômes de $\mathbb{K}[X]$ par $P(X)$.

Démonstration*:* C'est immédiat. □

Si $\mathbb{K}$ est un corps fini, $\mathbb{F}_p$, et si P est un polynôme irréductible sur $\mathbb{F}_p$ alors $\mathbb{F}_p[X]/P(X)$ est un corps fini qui contient $\mathbb{F}_p$. Sur tout corps fini il y a des polynômes irréductibles de degré n pour tout n, [28].

***Exemple* 13.6.5.** Sur $\mathbb{F}_2$ le polynôme $P = X^2+X+1$ est irréductible car il n'est divisible par aucun polynôme de degré 1. En effet les seuls polynômes de degré 1 de $\mathbb{F}_2[X]$ sont X et $X+1 = X-1$ et il est clair que dans $\mathbb{F}_2[X]$ les équations

$$X^2+X+1 = X(X+b), \quad X^2+X+1 = (X+1)(X+b)$$

n'ont pas de solution.

Donc $\mathbb{F}_2[X]/X^2+X+1$ est un corps noté $\mathbb{F}_2^2$ dont on va donner les éléments

$$\mathbb{F}_2^2 = \mathbb{F}_2[X]/(X^2+X+1)\mathbb{F}_2[X] = \{0, 1, X, X+1\}$$

Rappelons que dans $\mathbb{F}_2$ on a $0+1 = 1+1 = 0$, $0+1 = 1+0 = 1$, $0\times 0 = 0\times 1 = 0\times 0 = 0$ et $1\times 1 = 1$ et donc que dans $\mathbb{F}_2$, $1 = -1$ et $1+1 = 2 = 0$.

L'addition sur $\mathbb{F}_2^2$ est donnée par la table suivante

$+$	0	1	X	$X+1$
0	0	1	X	$X+1$
1	1	0	$X+1$	X
X	X	$X+1$	0	1
$X+1$	$X+1$	X	1	0

Cette table est évidente.

La multiplication sur $\mathbb{F}_2^2$ est donnée par la table suivante

$\times$	0	1	X	$X+1$
0	0	0	0	0
1	0	1	X	$X+1$
X	0	X	$X+1$	1
$X+1$	0	$X+1$	1	X

Les seules choses à montrer sont

$$X\times X = X^2 \equiv X+1 \mod X^2+X+1$$

$$X \times X + 1 = X^2 + X \equiv 1 \mod X^2 + X + 1$$
$$(X + 1) \times (X + 1) = (X + 1)^2 \equiv X + 1 \mod X^2 + X + 1$$

ce qui est vrai car

$$X^2 - (X + 1) = X^2 + X + 1 \equiv 0 \mod X^2 + X + 1$$
$$X^2 + X - 1 = X^2 + X + 1 \equiv 0 \mod X^2 + X + 1$$
$$(X + 1)^2 - (X + 1) = X^2 + X + 1 \equiv 0 \mod X^2 + X + 1$$

Donc dans $\mathbb{F}_2^2$ l'inverse multiplicatif de $X + 1$ est X.

Le théorème des restes chinois se généralise sans difficulté à $\mathbb{K}[X]$ avec la même preuve.

Corollaire 13.6.29. *Si p est un nombre premier et si $P(x)$ est un polynôme irréductible de degré f de $\mathbb{F}_p[X]$ alors $\mathbb{F}_p[X]/P(X)\mathbb{F}_p[X]$ est le corps fini $\mathbb{F}_q$ à $q = p^f$ éléments. En particulier si $p = 2$ et $P(X) = X^8 + X^4 + X^3 + X + 1$ alors $\mathbb{F}_2[X]/P(X)\mathbb{F}_2[X]$ est le corps fini à $2^8 = 256$ éléments.*

Démonstration*:* Il suffit de remarquer que $\mathbb{F}_p[X]/P(X)\mathbb{F}_p[X]$ est un $\mathbb{F}_p$ espace vectoriel dont une base est constituée des classes de 1, X,..., X^i,..., X^{f-1}, et donc le cardinal de $\mathbb{F}_p[X]/P(X)\mathbb{F}_p[X]$ est $p^f = q$. □

On a vu que $\mathbb{F}_q^*$ est un groupe multiplicatif cyclique à $q - 1$ éléments. On peut donc considérer des cryptosystèmes El Gamal utilisant le groupe $\mathbb{F}_q^*$, par exemple

***Exemple* 13.6.6.** Considérons $p = 3$, on montre facilement que le polynôme $P(X) = X^3 - X + 1$ est un polynôme irréductible de $\mathbb{F}_3[X]$. En effet sinon on aurait nécessairement une décomposition

$$X^3 - X + 1 = (X + a)(X^2 + bX + c), \text{ avec } a, b, c \in \mathbb{F}_3 \simeq \mathbb{Z}/3\mathbb{Z}$$

avec un facteur de degré 1 au moins. Autrement dit le polynôme $P(X)$ aurait au moins une racine dans $\mathbb{F}_3$, or on vérifie aisément avec le petit théorème de Fermat que

$$P(0) = P(1) = P(2) = 1$$

Donc $\mathbb{F}_3[X]/(X^3 - X + 1)\mathbb{F}_3[X]$ n'est autre que le corps $\mathbb{F}_{3^3}$ à 27 éléments.

On a vu que son groupe multiplicatif $\mathbb{F}_{3^3}^*$ est cyclique. Trouvons un générateur g sous forme polynomiale. Montrons que que la classe de X modulo $X^3 - X + 1$ engendre $\mathbb{F}_{3^3}^*$.

Il suffit pour cela de donner le tableau (ci-dessous) des puissances successives de $X \pmod{X^3 - X + 1}$. On prend comme système de représentant de $\mathbb{F}_3$, $\{0, 1, 2\}$ (en fait d'après le théorème de Lagrange 13.6.3 ou le corllaire 13.3.24 il suffit de vérifier que $X^{13} \neq 1 \pmod{X^3 - X + 1}$).

i	0	1	2	3
X^i	1	X	X^2	$X+2$
i	4	5	6	7
X^i	X^2+2X	$2X^2+X+2$	X^2+X+1	X^2+2X+2
i	8	9	10	11
X^i	$2X^2+2$	$X+1$	X^2+X	X^2+X+2
i	12	13	14	15
X^i	X^2+2	2	$2X$	$2X^2$
i	16	17	18	19
X^i	$2X+1$	$2X^2+X$	X^2+2X+1	$2X^2+2X+2$
i	20	21	22	23
X^i	$2X^2+X+1$	X^2+1	$2X+2$	$2X^2+X$
i	24	25	26	
X^i	$2X^2+2X+2$	$2X^2+2$	1	

Exercices.

13.6.1. On pose $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$. Trouvez l'inverse multiplicatif de $X^3 + 3X - 1$ modulo $X^5 + X + 1$ considérés comme des polynômes de $\mathbb{F}_5[X]$.

13.6.2. On considère le corps à 3 éléments $\mathbb{Z}_3/3\mathbb{Z}_3$ que l'on notera $\mathbb{F}_3$. On peut le représenter par les 3 entiers $\{0, 1, 2\}$ muni des lois d'addition et de multiplication modulo 3 données par les tables

1. Montrer que le polynôme $P(X) = X^3+2X^2+1 \in \mathbb{F}_3[X]$ est irréductible et donc que $\mathbb{F}_3[X]/P(X)\mathbb{F}_3[X]$ est un corps.
2. Montrer que $\mathbb{F}_3[X]/P(X)\mathbb{F}_3[X]$ contient 27 éléments que l'on peut représenter par les polynômes de degré inférieur ou égal à 2 de $\mathbb{F}_3[X]$. On notera $\mathbb{F}_{27}$ l'ensemble $\mathbb{F}_3[X]/P(X)\mathbb{F}_3[X]$.
3. Montrer que

$$X^3 = X^2 + 2 \text{ dans } \mathbb{F}_{27}\big(\Leftrightarrow X^3 \equiv X^2 + 2 \mod (X^3 + 2X^2 + 1)\mathbb{F}_3[X]\big)$$

$X^4 = X^3 + 2X = X^2 + 2X + 2$ dans $\mathbb{F}_{27}$
$X^5 = x^3 + 2X^2 + 2X = 2X + 2$ dans $\mathbb{F}_{27}$

4. Écrire les puissances successives de X pour des exposants allant de 0 à 26. Déduisez-en que la suite $n \mapsto x^n$ est périodique de période 26 dans $\mathbb{F}_{27}$ et que tout élément non nul de $\mathbb{F}_{27}$ est représentable d'une et une seul manière par une puissance de x (autrement dit le groupe multiplicatif des éléments non nuls de $\mathbb{F}_{27}$ est cyclique).

5. Comme $\mathbb{F}_{27} - \{0\} = \mathbb{F}_{27}^*$ contient 26 éléments on peut coder les 26 lettres de l'alphabet par un élément et un seul de $\mathbb{F}_{27}^*$ de la manière suivante

$A \leftrightarrow 1$	$B \leftrightarrow 2$	$C \leftrightarrow x$	$D \leftrightarrow x+1$
$E \leftrightarrow x+2$	$F \leftrightarrow 2x$	$G \leftrightarrow 2x+1$	$H \leftrightarrow 2x+2$
$I \leftrightarrow x^2$	$J \leftrightarrow x^2+1$	$K \leftrightarrow x^2+2$	$L \leftrightarrow x^2+x$
$M \leftrightarrow x^2+x+1$	$N \leftrightarrow x^2+x+2$	$O \leftrightarrow x^2+2x$	$P \leftrightarrow x^2+2x+1$
$Q \leftrightarrow x^2+2x+2$	$R \leftrightarrow 2x^2$	$S \leftrightarrow 2x^2+1$	$T \leftrightarrow 2x^2+2$
$U \leftrightarrow 2x^2+x$	$V \leftrightarrow 2x^2+x+1$	$W \leftrightarrow 2x^2+x+2$	$X \leftrightarrow 2x^2+2x$
$Y \leftrightarrow 2x^2+2x+1$	$Z \leftrightarrow 2x^2+2x+2$		

   Montrer que l'on peut alors utilser $\mathbb{F}_{27}^*$ pour construire un système El Gamal avec pour générateur $g = x$ et exposant $\alpha = 11$.

   On code avec ce cryptosystème lettre à lettre : à quelles lettres correspondent les couples $(y_1, y_2) = (K, H)$, $(y_1, y_2) = (F, A)$.

13.7 Courbes elliptiques.

Les courbes elliptiques définies sur un corps $\mathbb{K}$ sont des courbes décrites par l'ensemble des solutions de certaines équations polynomiales à deux inconnues $f(x, y) \in \mathbb{K}[X, Y]$. Pour plus de précisions on pourra consulter [31] ou [33].

Définition 13.7.1. *Soit $\mathbb{R}$ le corps des réels et soit $a, b \in \mathbb{R}$ tels que $\Delta(a, b) = 4a^3 + 27q^2 \neq 0$. Une* **courbe elliptique non singulière** *définie sur $\mathbb{R}$ est l'ensemble E des points P de $\mathbb{R}^2$ dont les coordonnées (x, y) sont des solutions de l'équation*

$$y^2 = x^3 + ax + b$$

plus un point spécial, noté $\mathcal{O}$ ou ∞, appelé le **point à l'infini**.

La condition $4a^3 + 27q^2 \neq 0$ assure que la courbe est sans point double. Si $4a^3 + 27q^2 = 0$ on a affaire à une ***courbe singulière***.

***Exemple* 13.7.1.** La courbe $y^2 = x^3 - 4x$ est une courbe elliptique car $\Delta(-4, 0) \neq 0$, voir la figure 13.1 page 199.

13.7.1 Groupe des points d'une courbe elliptique

Si E est une courbe elliptique non-singulière on définit sur les points de E une addition notée $+$ qui fera de l'ensemble des points de E un groupe abélien.

- $\forall\, P \in E$, par définition $P + \mathcal{O} = \mathcal{O} + P = P$.
- Si $P, Q \in E$ avec $P = (x_1, y_1)$, $Q = (x_2, y_2)$ on considère les 3 cas
  1. $x_1 \neq x_2$
  2. $x_1 = x_2$ et $y_1 = -y_2$
  3. $x_1 = x_2$ et $y_1 = y_2$

  – Dans le cas 1, on note L la droite passant par P et Q. Elle coupe E en 3 points dont deux, P et Q, sont déjà connus, on note $R' = (x', y')$ le troisième point d'intersection. On prend le symétrique de R' par rapport à l'axe des abscisses. On obtient un point $R = (x', -y') = (x, y)$ qui est encore sur E. On pose par définition

  $$P + Q = R$$

  Par un calcul sans mystère on trouve l'équation de L

  $$y = \lambda x + \nu = \Big(\frac{y_2 - y_1}{x_2 - x_1}\Big)x + \Big(y_1 - \frac{y_2 - y_1}{x_2 - x_1}x_1\Big)$$

  on obtient alors les coordonnées de R

  $$x = \lambda^2 - x_1 - x_2 = \big(\frac{y_2 - y_1}{x_2 - x_1}\Big)^2 - x_1 - x_2$$
  $$y = \lambda(x_1 - x_2) - y_1 = \big(\frac{y_2 - y_1}{x_2 - x_1}\Big)(x_1 - x_2) - y_1$$

  – Dans le cas 2, on définit si $P = (x, y) \in E$, $-P = (x, -y)$

  $$(x, y) + (x, -y) = \mathcal{O}$$

– Le cas 3 se ramène au cas 2 en considérant que la droite L est la tangente en P à E. On trouve que l'équation de L est

$$y = \lambda x + \nu = \Big(\frac{3x_1^2 + a}{2y_1}\Big)x + \Big(y_1 - \Big(\frac{3x_1^2 + a}{2y_1}\Big) \cdot x_1\Big)$$

ensuite le calcul de R est identique.

On montre que la loi ainsi définie est

1. stable sur E: si P et Q appartiennent à E, $P + Q \in E$
2. associative: P, Q et R appartiennent à E alors $(P + Q = +R = P + (Q + R)$
3. commutative: $P + Q = Q + P$
4. possède un élément neutre, $\mathcal{O}$: $P + \mathcal{O} = \mathcal{O} + P = P$
5. Chaque point de E admet un opposé pour cette addition: $\forall\, P \in E\ \exists\, Q \in E$ tel que $P + Q = \mathcal{O}$

Cette loi fait donc des points de E définis sur $\mathbb{K}$ un groupe abélien.

Tout ceci est résumé par les figures 13.1 et 13.2:
On remarque que les formules donnant les coordonnées de la somme de deux points P et Q sur la courbe elliptique E sont des fonctions rationnelles à coefficients dans $\mathbb{Z}$ de leurs coordonnées.

Cette remarque montre que l'appartenance des coordonnées de P et Q à $\mathbb{R}$ ne joue aucun rôle. Ce qui importe est de pouvoir effectuer des additions, multiplications, soustraction, division des coordonnées. Autrement dit on peut définir la somme de deux points sur une courbe elliptique dès que leurs coordonnées appartiennent à un corps.

Définition 13.7.2. *Soit K un corps et E une courbe elliptique définie sur le corps K, c'est à dire que l'équation $y^2 = x^3 + ax + b$ qui dfinit la courbe elliptique est coefficients dans K, $a, b \in K$, et $\Delta(a, b) = 4a^3 + 27b^2 \neq 0$. On note $E(K)$ l'ensemble des couples $(x, y) \in K^2$ tels que $y^2 = x^3 + ax + b$.*

On vérifie aisément que si P et Q appartiennent à $E(K)$ c'est à dire que leurs coordonnées appartiennent à K et vérifient l'équation de la courbe alors les coordonnées de $R = P + Q$ appartiennent à K et vérifent aussi l'équation $y^2 = x^3 + ax + b$.

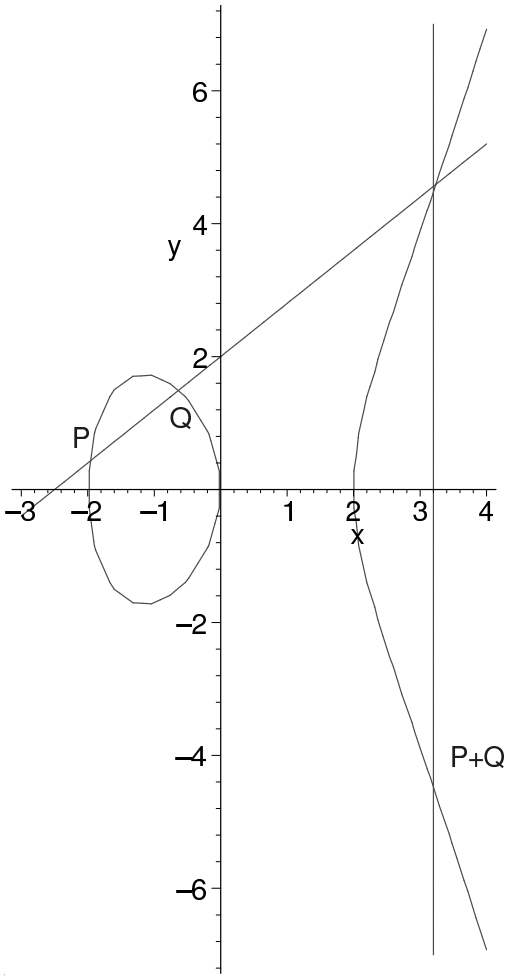


Figure 13.1: courbe elliptique sur $\mathbb{R}$, $y^2 = x^3 - 4x$

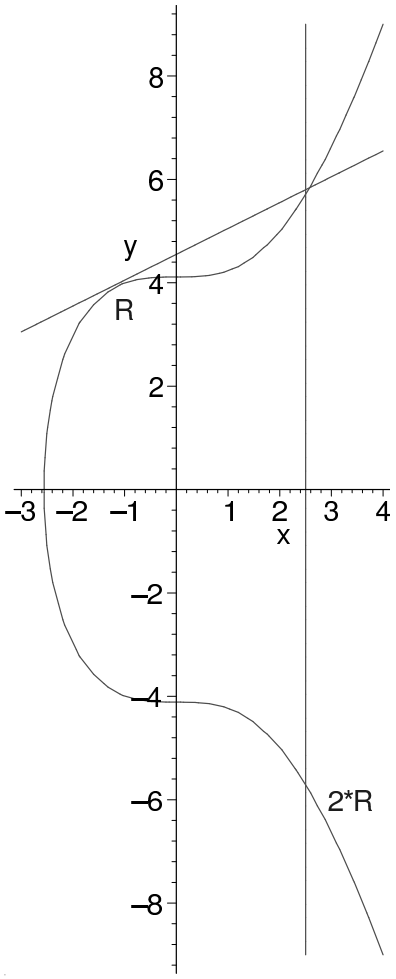


Figure 13.2: courbe elliptique sur $\mathbb{R}$, $y^2 = x^3 + 17$

***Exemple* 13.7.2.** La courbe $y^2 = x^3 - 4x$ peut tre considre comme une courbe elliptique sur $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, mais aussi sur le corps fini $\mathbb{F}_p$ pour p premier, $p \neq 2$. En effet $\Delta(-4, 0) = -2^8$ qui est diffrent de zro dans $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ et $\mathbb{F}_p$ pour p premier, $p \neq 2$.

13.7.2 Endomorphismes d'une courbe elliptique

Soit K un corps et E une courbe elliptique définie sur K et soit $\bar{K}$ une clôture algébrique de K.

Définition 13.7.3. *Une* **endomorphisme d'une courbe elliptique** E *définie sur* K *est un homomorphisme* α *de la courbe*

$$\alpha : \ E(\bar{K}) \longrightarrow E(\bar{K})$$

qui est donné par des applications rationnelles.

Autrement dit α *est une application de* $E(\bar{K})$ *dans lui-même telle que*

$$\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2), \ \textit{pour tous points } P_1, P_2 \in E(\bar{K})$$

et il existe des fonctions rationnelles $R_1(x, y)$ *et* $R_2(x, y)$ *à coefficients dans* $E(\bar{K})$ *telles que*

$$\alpha(x, y) = \big(R_1(x, y), R_2(x, y)\big)$$

pour tout $P = (x, y) \in E(\bar{K})$.

***Exemple* 13.7.3.** Soit E d'équation $y^2 = x^3 + ax + b$ et soit $\alpha(P) = 2P$. Alors α est un homomorphisme et

$$\alpha(x, y) = \big(R_1(x, y), R_2(x, y)\big)$$

avec

$$R_1(x, y) = \left(\frac{3x^2 + a}{2y}\right)^3 - 2x$$
$$R_2(x, y) = \left(\frac{3x^2 + a}{2y}\right)\left(3x - \left(\frac{3x^2 + a}{2y}\right)^2\right) - y$$

et donc α est un endomorphisme de E.

On montre que tout endomorphisme de E peut s'écrire sous la forme

$$\alpha(x, y) = \big(r_1(x), r_2(x)y\big)$$

où $r_i(x)$ est une fonction rationnelle. on posera

$$r_1(x) = \frac{p(x)}{q(x)}, \quad p(x) \wedge q(x) = 1$$

Le ***degré de*** α est défini par

$$\deg(\alpha) = \max\{\deg p(x), \deg q(x)\}$$

On dira que α est ***séparable*** si $r_1'(x)$ n'est pas identiquement nul.

Si $K = \mathbb{F}_q$ avec $q = p^n$ est le corps fini à q éléments et si E est une courbe elliptique définie sur K il y a un endomorphisme important: l'***endomorphisme de Frobenius*** ϕ_q

$$\phi_q(x, y) = \left(x^q, y^q\right), \quad (x, y) \in E(\bar{K})$$

Il n'est pas séparable, il est de degré q

13.7.3 Courbes Elliptiques sur un corps fini

D'après la remarque précédente le fait que le corps de base soit $\mathbb{R}$ ne joue pas un grand rôle dans les calculs précédents (sauf pour pouvoir dessiner les courbes).

Si maintenant on a un corps fini $\mathbb{F}_q$ où $q = p^f$ avec p un nombre premier on peut refaire la théorie en supposant que l'on cherche des solutions dans $\mathbb{F}_q^2$ (on peut prendre $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$).

Définition 13.7.4. *Soit $\mathbb{F}_q$ un corps fini avec $p \geq 5$ et soit $a, b \in \mathbb{F}_q$ tels que $4a^3 + 27b^2 \neq 0$. Une* **courbe elliptique non singulière définie sur** $\mathbb{F}_q$ *est l'ensemble $E = E(\mathbb{F}_q)$ des points P de $\mathbb{F}_q^2$ dont les coordonnées (x, y) sont des solutions de l'équation*

$$y^2 = x^3 + ax + b$$

plus un point spécial $\mathcal{O}$ appelé point à l'infini.

Les points de $E(\mathbb{F}_q)$ sont appelé les **points définis sur** $\mathbb{F}_q$ *de la courbe elliptique E.*

***Exemple* 13.7.4.** Calculons par exemple les points de la courbe elliptique $y^2 = x^3 + x + 6$ dans $\mathbb{F}_{11}$

x	$x^3+x+6 \mod 11$	résidu quadratique?	y
0	6	non	
1	8	non	
2	5	oui	4,7
3	3	oui	5,6
4	8	non	
5	4	oui	2,9
6	8	non	
7	4	oui	2,9
8	9	oui	3,8
9	7	non	
10	4	oui	2,9

Cette courbe sur $\mathbb{F}_{11}$ admet 13 points y compris celui à l'infini.

Comme l'ensemble $E(\mathbb{F}_q)$ des points définis sur $\mathbb{F}_q$ de la courbe elliptique E est un sous ensemble de $\mathbb{F}_q^2$ c'est un ensemble fini. Le cardinal de cet ensemble est soumis à des limitations sévèress. On a le théorème important

Théorème 13.7.5 (Hasse)**.** *Soit p un nombre premier supérieur à 3 et soit $q = p^f$. Soit E une courbe elliptique définie sur le corps fini $\mathbb{F}_q$. On note $\#E$ le nombre de points de E définis sur $\mathbb{F}_q$. On a*

$$q + 1 - 2\sqrt{q} \leq \#E \leq q + 1 + 2\sqrt{q}$$

Le calcul de $\#E$ est difficile mais il existe un algorithme performant pour le faire l'***algorithme de Schoof***.

Pour pouvoir utiliser le groupe des points d'une courbe elliptique sur un corps fini, E, il faut ensuite trouver un sous-groupe cyclique aussi gros que possible afin de pouvoir transposer le schéma de codage El-Gamal. Il y a des algorithmes efficaces pour cela.

Avec des sous-groupes cycliques de E à 2^{160} éléments on a une très bonne sécurité si l'on prend quelques précautions pour éliminer des courbes elliptiques indésirables pour lesquelles le problème du logarithme discret est facile.

L'avantage des cryptosystèmes basés sur les courbes elliptiques est, entre autre, la possibilité d'avoir des clés courtes pour une bonne sécurité.

13.7.4 Points de torsion sur une courbe elliptique

Soit E une courbe elliptique définie sur un corps K et soit $\bar{K}$ une cloture algébrique de K. Soit n un entier positif. on note

$$E[n] = \left\{P \in E(\bar{K}) \mid nP = \underbrace{P + P + \cdots + P}_{n \text{ fois}} = \mathcal{O}\right\}$$

***Exemple* 13.7.5.** Prenons $y^2 = x^3 + ax + b$ l'équation de la courbe E. on peut écrire

$$y^2 = (x - e_1)(x - e_2)(x - e_3), \quad e_i \in \bar{K}$$

un point P vest de 2-torsion si $2P = \mathcal{O}$ autrement dit si la tangente en P est verticale ce qui équivaut à $y = 0$. Donc

$$E[2] = \left\{\mathcal{O}, (e_1, 0), (e_2, 0), (e_3, 0)\right\}$$

On a le théorème suivant qui décrit $E[n]$

Théorème 13.7.6. *Soit E une courbe ellitique sur un corps K et soit n un entier positif. Si la caractéristique de K ne divise pas n ou est infini, alors*

$$E[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$$

Si la caractéristique de K est $p > 0$ et si $p \mid n$ on écrit $n = p^r n'$ avec $p \wedge n' = 1$. Alors

$$E[n] \simeq \begin{cases} \mathbb{Z}/n'\mathbb{Z} \oplus \mathbb{Z}/n'\mathbb{Z} \\ ou \\ \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n'\mathbb{Z} \end{cases}$$

Démonstration*:* Pour la preuve voir [33]. □

13.7.5 L'accouplement de Weil

L'accouplement de Weil est un outil essentiel pour l'étude des courbes elliptiques et aussi pour les crypto-systèmes elliptiques ainsi que pour le chiffrement basé sur l'identité.

Soit K un corps et E une courbe elliptique définie sur K et soit n un entier premier à la caractéristique de K. Alors $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. Soit

$$\mu_n = \left\{x \in \bar{K} \mid x^n = 1\right\}$$

le groupe des racines $n$ièmes de l'unité dans $\bar{K}$. Un générateur ζ de μ_n est appelé une racine primitive n-ième de l'unité. On a le théorème suivant

Théorème 13.7.7. *Soit K un corps et E une courbe elliptique définie sur K et soit n un entier premier à la caractéristique de K. Alors il existe un accouplement (c'est à dire une forme bilinéaire non dégénérée)*

$$e_n : \quad E[n] \times E[n] \longrightarrow \mu_n$$

*appelé l'***accouplement de Weil** *qui vérifie les proprités suivantes:*

1. *e_n est bilinéaire par rapport à chacune des variables, c'est à dire que*

$$e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T)$$
$$e_n(S, T_1 + t_2) = e_n(S, T_1)e_n(S, T_2)$$

   pour tous $S, S_1, S_2, T, T_1, T_2 \in E[n]$

2. *e_n est non dégénérée par rapport à chaque variable, c'est à dire que*

$$e_n(S, T) = 1 \text{ pour tout } T \in E[n] \Longrightarrow S = \mathcal{O}$$
$$e_n(S, T) = 1 \text{ pour tout } S \in E[n] \Longrightarrow T = \mathcal{O}$$

3. *$e_n(T, T) = 1$ pour tout $T \in E[n]$*

4. *$e_n(S, T) = e_n(T, S)^{-1}$ pour tout $S, T \in E[n]$*

5. *$e_n(\sigma(S), \sigma(T)) = \sigma\big(e_n(S, T)\big)$ pour tout automorphisme σ de $\bar{K}$ qui laisse invariant les coefficients de l'équation, $y^2 = x^3 + ax + b$, de E, c'est à dire $\sigma(a) = a$ et $\sigma(b) = b$.*

6. *$e_n\big(\alpha(S), \alpha(T)\big) = e_n(S, T)^{\deg(\alpha)}$ pour tout endomorphisme séparable α de E. Si les coefficients de E sont dans un corpd finis $\mathbb{F}_q$, alors le résultat est vrai si α est l'endomorphisme de Frobenius ϕ_q.*

Démonstration*:* Pour la preuve voir [33] □

Corollaire 13.7.8. *Si $E[n] \subset E(K)$ alors $\mu_n \subset K$*

Sites internet

cryp1 http://cryptosec.lautre.net/index.php3;
donne un resumé et des références sur divers aspects de la cryptographie

hist1 http://histoirecrypto.ifrance.com/histoirecrypto/ ;
site historique

prim1 http://www.utm.edu/research/primes/ ;
donne des renseignements sur les nombres premiers (records, tests de primalité,...)

cryp2 http://www.securite.org/db/crypto/ ;
donne un resumé et des références sur divers aspects de la cryptographie

aes1 http://www.securiteinfo.com/crypto/aes.shtml:
donne une description succincte d'AES et de sa comparaison avec triple DES

aes2 http://www.cryptageaes.com/:
présente des produits commerciaux utilisant AES

aes3 http://www.bibmath.net/crypto/moderne/aes.php3:
donne une description succincte d'AES

Bibliographie

[1] Manindra Agrawal, Neeraj Kayal & Nitin Saxena, PRIMES is in P, *Annals of Mathematics* **160**, n°2, (2004), 781-793.

[2] François Arnault, *Théorie des nombres et Cryptographie*, cours DEA Université de Limoges, **2000**.

[3] Thomas Baignres, Pascal Junod, Yi Lu, Jean Monnerat & Serge Vaudenay, *A Classical Introduction to Cryptography Exercice Book*, Springer, **2006**

[4] Christophe Bidan, *Cryptographie et Cryptanalyse*, Cours, http://www.supelec-rennes.fr/ren/perso/cbidan/cours/crypto.pdf

[5] I.F Blake, G. Seroussi, N. P. Smart, *Elliptic curves in cryptography*, London Mathematical Society Lecture Note Series, **265** Cambridge University Press **1999**.

[6] D. Boneh & M. Franklin, Identity based encryption from the Weil pairing. In *Advances in Cryptology- Crypto'2001,* pages 213-229, Springer-Verlag, 2001, Lecture Notes on Computer Sciences, n°2139.

[7] Johannes A. Buchmann, *Introduction to cryptography*, Springer, Undergraduate Texts in Mathematics, **2000**.

[8] Joan Daemen & Vincent Rijmen, *The design of Rijndael* Springer Verlag, Berlin Heidelberg New-York, **2002**.

[9] W. Diffie, M.E. Helman, New Directions in Cryptography, IEEE Transactions on Information Theory, 22 , 644-654, **1976**.

[10] Gilles Dubertet, *Initiation à la Cryptographie*, éditions Vuibert.

[11] Touradj Ibrahimi, Franck Leprévost, Bertrand Warusfel, *Enjeux de la sécurité multimédia*, Hermès Science Lavoisier, **2006**

[12] Touradj Ibrahimi, Franck Leprévost, Bertrand Warusfel, *Cryptographie et sécurité*, Hermès Science Lavoisier, **2006**

[13] G.H.Hardy, E.M. Wright, *Une Introduction à la théorie des nombres*, Springer-Verlag, SCOPOS 15, **2005**.

[14] Robert Harris, *Enigma*, éditions Pocket.

[15] Howard M. Heys, *A tutorial in Linear and differential cryptanalysis*, disponible sur internet l'URL

http://www.engr.mun.ca/~howard/Research/Papers/ldc_tutorial.html

[16] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, GTM, **1990**.

[17] Auguste Kerckhoffs, La cryptographie militaire, *Journal des sciences militaires*, vol. IX, pp. 5-83, Jan. 1883, pp. 161-191, Feb. 1883, disponible à: http://www.petitcolas.net/fabien/kerckhoffs/

[18] Neal Koblitz, *A Course in Number Theory and Cryptography*, 2nd edition, Springer, Graduate Texts in Mathematics n°114, , **1994**.

[19] Neal Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, GTM 97, **1987**.

[20] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied cryptographie*, Discrete Mathematics and its applications, CRC Press, **1997**.

[21] Jean-Louis Pons, *Introduction à la Cryptographie*, cours ENSAM Aix en Provence, **2003**.

[22] La Recherche, n°386 (05/2005), n°383 -(02/2005), n°382 (01/2005), n°381 (12/2004), n°377 (07/2004, n°377 (07/2004), n°371 (01/2004), n°370 (12/2003), n°366 (07/2003), n°365 (06/2003), n°362 (03/2003), n°361 (02/2003), n°360 (01/2003), n°352 (04/2002), n°351 (03/2002), n°328 (02/2000), n°327 (01/2000), n°310 (06/1998).

[23] Pour la Science

[24] Guy Robin, *Algorithmique et cryptographie*, éditions Ellipses.

[25] Claude E. Shannon, Communication Theory of secrecy systems, *Bell Systems Technical Journal*, **27** (1948), 379-423 & 623-665.

[26] Claude E. Shannon, A mathematical theory of communication, *Bell Systems Technical Journal*, **28** (1949), 656-715.

[27] Bruce Schneier, *Cryptographie Appliquée*, éditions Thomson Publishing.

[28] Lionel Schwartz, *Mathématiques pour la Licence, Algèbre*, Dunod, Paris, **1998**.

[29] Simon Singh, *Histoire des codes secret*, JC Lattès, **1999**.

[30] Jacques Stern *La Science du Secret*, Odile Jacob, Paris, **1998**.

[31] Douglas Stinson, *Cryptographie, théorie et pratique*, éditions Vuibert 2e édition, **2003**.

[32] Serge Vaudenay, *A Classical Introduction to Cryptography*, Springer, **2006**

[33] Lawrence C. Washington, *Elliptic Curves, Number Theory and Cryptography*, Discrete Mathematics and its applications, Chapman & Hall/CRC, **2003**.

[34] Benne de Weger, *Cryptographic Systems*, cours Technische Universiteit Eindhoven **2005**; http://www.win.tue.nl/ bdeweger/

[35] Encyclopédie Wikipédia, *Problème du sac à dos*

[36] V. V. Yaschenko, *Cryptography: An Introduction*, Moscow Center for Continuous Mathematics Education, Editor AMS, **2002**.

[37] Gilles Zémor, *Cours de cryptographie*, éditions Cassini, **2002**.

Index