Chiffrement affine : définition

Le **chiffrement par décalage** est un cas particulier du **chiffrement par substitution** dans lequel on utilise une translation comme substitution. Un autre cas particulier du chiffrement par substitution est le **chiffrement affine**. Dans ce procédé, on limite les fonctions de chiffrement à certaines fonctions de la forme

$$E_{(a,b)}(x) = ax + b \mod 26 \tag{1}$$

où $a, b \in \mathbb{Z}_{26}$. Ces fonctions sont appelées des **fonctions affines**, d'où l'on a tiré le nom du procédé. On remarque que l'on retrouve le chiffrement par décalage pour $a = 1$.

Pour que l'opération de déchiffrement soit possible, il est nécessaire que la fonction affine soit bijective. Autrement dit, pour tout $y \in \mathbb{Z}_{26}$, l'équation

$$ax + b = y \mod 26 \tag{2}$$

doit avoir une, et une seule, solution x. L'équation (2) est équivalente à

$$ax = y - b \mod 26\ . \tag{3}$$

Lorsque y parcourt l'ensemble $\mathbb{Z}_{26}$, $y - b$ décrit également ce même ensemble. Donc, il suffit d'étudier l'équation $ax = z \mod 26$ pour tout $z \in \mathbb{Z}_{26}$. On démontre que cette équation admet une unique solution pour tout z fixé, si, et seulement si, $pgcd(a, 26) = 1$ (où *pgcd* est le plus grand diviseur commun de ses arguments) ; au passage on dit que a et 26 sont **premiers entre eux**. En effet si a et 26 sont premiers entre eux (et seulement dans ce cas), alors a admet un inverse $a^{-1} \in \mathbb{Z}_{26}$ (*i.e.*, $aa^{-1} = a^{-1}a = 1 \mod 26$), et l'unique solution de l'équation $ax = z \mod 26$ est $x = a^{-1}z \mod 26$. En particulier, $x = a^{-1}(y - b) \mod 26$ est l'unique solution a l'équation (2).

Supposons donc que a et 26 sont premiers entre eux. On vient de voir que, dans ce cas, l'application $E_{(a,b)}$ est inversible. Sa bijection réciproque est donnée par $D_{(a,b)}(y) = a^{-1}(y-b) \mod 26$. Nous pouvons maintenant décrire complétement le chiffrement affine. Les ensembles de textes clairs $\mathcal{P}$ et chiffrés $\mathcal{C}$ sont tous les deux égaux à $\mathbb{Z}_{26}$. L'espace des clefs secrètes est quant à lui donné par

$$\mathcal{K} := \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : pgcd(a, 26) = 1\}\ . \tag{4}$$

Pour tout $(a, b) \in \mathcal{K}$, on définit

$$E_{(a,b)}(x) := ax + b \mod 26 \tag{5}$$

et

$$D_{(a,b)}(y) := a^{-1}(y - b) \mod 26\ . \tag{6}$$

1 Exercice : Mise en œuvre du chiffrement affine (CORRECTION)

Soit $(a, b) = (7, 3)$.

1. Montrer que $(a, b) \in \mathcal{K}$ et calculer a^{-1} dans $\mathbb{Z}_{26}$. **Correction :** Pour montrer que (a, b) est une clef valide, il suffit de vérifier que a et 26 sont premiers entre eux, ce qui est ici le cas car 7 est un nombre premier.
2. Vérifier par calcul que $D_{(a,b)}(E_{(a,b)}(x)) = x$ pour x quelconque dans $\mathbb{Z}_{26}$. **Correction :** Il faut que l'on calcule $-b = -3$ dans $\mathbb{Z}_{26}$: $-b = 26 - 3 = 23 \mod 26$. Il faut également calculer $a^{-1} = 7^{-1}$. Il s'agit de trouver un élément $b \in \mathbb{Z}_{26}$ pour lequel $ab = 1 \mod 26$. Or on a $7 \times 15 = 105 = 4 \times 26 + 1$, d'où $7 \times 15 = 1 \mod 26$ et $a^{-1} = 15$. Calculons maintenant (modulo 26).

$$\begin{array}{lcl} E_{(a,b)}(x) & = & 7x + 3 \\ D_{(a,b)}(E_{(a,b)}(x)) & = & D_{(a,b)}(7x + 3) \\ & = & 15(7x + 3 + 23) \\ & = & 15(7x + 0) \\ & = & x \ . \end{array}$$

3. Chiffrer le mot *hot* avec cette clef. **Correction :** On commence par coder les lettres en élément de $\mathbb{Z}_{26}$ de la façon habituelle. On a alors $h \leftrightarrow 7$, $o \leftrightarrow 14$ et $t \leftrightarrow 19$. Puis on applique la règle de chiffrement.

$$\begin{array}{lcl} 7 \times 7 + 3 \mod 26 & = & 52 \mod 26 = 0 \ , \\ 7 \times 14 + 3 \mod 26 & = & 101 \mod 26 = 23 \ , \\ 7 \times 19 + 3 \mod 26 & = & 136 \mod 26 = 6 \ . \end{array}$$

   On obtient donc le texte chiffré 0 23 6 qui, en lettres, donne *axg*.
4. Énumérer les $a \in \mathbb{Z}_{26}$ qui sont premiers avec 26. **Correction :** Il est facile de vérifier que les éléments de $\mathbb{Z}_{26}$ qui sont premiers avec 26 sont $1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23$ et 25. En effet ce sont les seuls éléments de $\mathbb{Z}_{26}$ qui ne sont divisibles ni par 2 ni par 13 (les seuls diviseurs différents de 1 de $\mathbb{Z}_{26}$).
5. Pour chacun des éléments $a \in \mathbb{Z}_{26}$ premiers avec 26, calculer son inverse (modulo 26). **Correction** Pour $a \in \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$, il s'agit de trouver $b \in \mathbb{Z}_{26}$ tel que $ab = 1 \mod 26$ ou, en d'autres termes, $ab = q26 + 1$, pour un certain q (c'est-à-dire que le reste de ab par 26 est égal à 1, donc ab est congru à 1 modulo 26). On obtient ainsi

a	a^{-1}
1	1
3	9
5	21
7	15
9	3
11	19
15	7
17	23
19	11
21	5
23	17
25	25

(7)

6. Calculer le nombre de clefs possibles. Qu'en déduisez-vous quant à la solidité de ce procédé de chiffrement ? **Correction** Le nombre de clef possible est le nombre de a premiers avec 26 (qui est égal à 12 d'après la question précédente) multiplié par 26 (le nombre de b) soit $12 \times 26 = 312$. Le nombre de clefs est trop petits pour assurer la solidité du cryptosystème.

2 Exercice : Cryptanalyse du chiffrement affine (CORRECTION)

Dans cet exercice, on s'intéresse à une technique de cryptanalyse permettant de casser un procédé de chiffrement affine. Cette technique est basée sur l'analyse des fréquences d'occurrence des lettres dans un texte écrit dans une langue donnée (par exemple, l'anglais ou le français). Dans le cas présent, on effectue une hypothèse simplificatrice : on suppose que le texte clair est **un message rédigé en anglais sans ponctuations ni espaces**.

Plusieurs personnes ont estimé la probabilité d'apparition des vingt-six lettres de l'alphabet en faisant des statistiques sur de nombreux romans, magazines et journaux quotidiens écrits en anglais. Les estimations suivantes sur la langue anglaise ont été obtenues par Beker et Piper.

Fréquences d'occurrences des lettres dans les textes écrits en anglais (Beker & Piper)

lettre	proba	lettre	proba
a	$0,082$	n	$0,067$
b	$0,015$	o	$0,075$
c	$0,028$	p	$0,019$
d	$0,043$	q	$0,001$
e	$0,127$	r	$0,060$
f	$0,022$	s	$0,063$
g	$0,020$	t	$0,091$
h	$0,061$	u	$0,028$
i	$0,070$	v	$0,010$
j	$0,002$	w	$0,023$
k	$0,008$	x	$0,001$
l	$0,040$	y	$0,020$
m	$0,024$	z	$0,001$

Nous allons utiliser ces statistiques pour déchiffrer un cryptogramme provenant d'un message écrit en anglais. Supposons donc qu'Oscar ait intercepté le message suivant (sans espaces ni signes de ponctuation) :
FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDKAPRKDLYEVLRHHRH.

1. Calculer le nombre d'occurrences de chacune des lettres de l'alphabet dans ce mes-

sage. **Correction :**

lettre	fréquence	lettre	fréquence
A	2	N	1
B	1	O	1
C	0	P	2
D	6	Q	0
E	5	R	8
F	4	S	3
G	0	T	0
H	5	U	2
I	0	V	4
J	0	W	0
K	5	X	2
L	2	Y	1
M	2	Z	0

2. Expliquer pourquoi on peut supposer que la lettre R se déchiffre en E. **Correction :** Le caractère le plus fréquent est R (8 occurrences) suivi de D (6 occurrences), et, E, F et K (5 occurrences chacun). Comme en anglais la lettre la plus courante est E, on peut supposer que R se déchiffre en E. La seconde lettre la plus fréquence est T qui pourrait donc se chiffrer en D.

3. Supposons que la lettre D se déchiffre en T (et R en E). Trouver la clef (a, b) qui en résulte, et expliquer pourquoi cette clef n'est pas valide. **Correction :** En transformant les lettres en des nombres, dire que R se déchiffre en E est équivalent à $E_{(a,b)}(17) = 4$ ($R = 17$, $E = 4$). Dire que D se déchiffre en T signifie $E_{(a,b)}(3) = 19$ ($D = 3$, $T = 19$). En se souvenant que $E_{(a,b)}(x) = ax + b$, où a, b sont inconnus, on obtient un système de deux équations à deux inconnues

$$\begin{aligned} 4a + b &= 17 \\ 19a + b &= 3\ . \end{aligned}$$

Il nous faut résoudre ce système dans $\mathbb{Z}_{26}$. Prenons la seconde équation $19a + b = 3$ soit $a = 11(3 - b)$ (car $19^{-1} = 11$). On a donc $a = 33 - 11b = 7 - 11b \mod 26$. On injecte cela dans la première équation et il en résulte que l'on a $4(7 - 11b) + b = 17$ soit $28 - 43b = 17 \Leftrightarrow 2 - 17b = 17$ (car $28 = 2 \mod 26$ et $43 = 17 \mod 26$) ce qui est équivalent à $-17b = 15$. Or $-17 = 26 - 17 = 9$, et on a donc $9b = 15$. On résoud cela pour trouver $b = 19$ (en effet $9^{-1} = 3$, donc on doit calculer $b = 3 \times 15 = 45 = 19 \mod 26$). On trouve alors $a = 7 - 11 \times 19 \mod 26 = 6$. Cette clef n'est pas valide car a et 26 ne sont pas premiers entre eux.

4. Supposons que la lettre R se déchiffre en E, et K en T. Trouver la clef (a, b) qui en résulte, et expliquer pourquoi cette fois-ci la clef est valide. **Correction :** Cette fois on obtient $a = 3$ et $b = 5$. En effet, il s'agit de résoudre dans $\mathbb{Z}_{26}$ le système de deux équations à deux inconnues a et b :

$$\begin{aligned} 4a + b &= 17 \\ 19a + b &= 10 \end{aligned}$$

puisque la lettre K correspond au nombre 10 ($4 \leftrightarrow E$, $17 \leftrightarrow R$, $19 \leftrightarrow T$). De l'équation $19a + b = 10$, on en déduit que $a = 19^{-1}(10 - b) = 11(10 - b)$ (puisque

$19^{-1} = 11) = 110 - 11b = 6 - 11b$ (puisque $110 = 6 \mod 26$) $= 6 + 15b$ (puisque $-11 = 26 - 11 = 15 \mod 26$). En injectant cela dans l'équation $4a + b = 17$, on obtient

$$\begin{array}{rlcl} & 4(6+15b)+b & = & 17 \\ \Leftrightarrow & 24+61b & = & 17 \\ \Leftrightarrow & 24+9b & = & 17 \text{ (puisque } 61 = 9 \mod 26) \\ \Leftrightarrow & 9b & = & 17-24 \\ \Leftrightarrow & 9b & = & 17+26-24 \\ \Leftrightarrow & 9b & = & 19 \\ \Leftrightarrow & b & = & 9^{-1} \times 19 \\ \Leftrightarrow & b & = & 3 \times 19 \\ \Leftrightarrow & b & = & 57 \\ \Leftrightarrow & b & = & 5 \end{array}$$

d'où $a = 6 + 15 \times 5 = 6 + 75 = 81 = 3 \mod 26$. Enfin 3 est premier avec 26. Donc $(3, 5)$ est une clef valide.

5. En vous basant sur ce que vous avez trouvé pour a à la question précédente, calculer a^{-1} (dans $\mathbb{Z}_{26}$). Une fois cela fait, déchiffrer le message afin de vérifier qu'il s'agit bien d'un texte écrit en anglais. **Correction :** Le déchiffrement est donné par $D_{(a,b)}(y) = 9y - 19$ (car $3^{-1} = 9$ qui avait été calculé au préalable). Comme $-19 = 26 - 19 = 7 \mod 26$, on a $D_{(a,b)}(y) = 9y + 7$. On déchiffre les lettres

num	*lettre*	$D_{(a,b)}(num)$	*lettre correspondante*
0	A	7	H
1	B	16	Q
2	C	25	Z
3	D	8	I
4	E	17	R
5	F	0	A
6	G	9	J
7	H	18	S
8	I	1	B
9	J	10	K
10	K	19	T
11	L	2	C
12	M	11	L
13	N	20	U
14	O	3	D
15	P	12	M
16	Q	21	V
17	R	4	E
18	S	13	N
19	T	22	W
20	U	5	F
21	V	14	O
22	W	23	X
23	X	6	G
24	Y	15	P
25	Z	24	Y

(8)

En utilisant cette fonction de déchiffrement sur le message chiffré initial on obtient :

algorihmsarequitegeneraldefinitionsofarithmeticprocesses .

Ce message clair signifiant “ Les algorithmes définissent de manière assez générale les calculs arithmétiques ”.