Decrypting Cryptography

Étienne André, Laure Petrucci
LIPN, CNRS UMR 7030
IUT de Villetaneuse
Université Paris 13, Sorbonne Paris Cité
F-93430, Villetaneuse, France
{Etienne.Andre,Laure.Petrucci}@iutv.univ-paris13.fr

***Abstract*—The main focus of the bachelor curriculum ASUR (*Administration et Sécurité des Réseaux*) is security of networks and operating systems. It necessitates to get the students familiar with the different techniques they will have to operate to secure access and communications in the networks they will be in charge of. Within the curriculum of this bachelor degree, we are in charge of two courses on *introduction to security* and *cryptography*. This domain of expertise is particularly difficult to grasp for students whose mathematical background is often insufficient. Such a subject can thus easily become somewhat boring for students, although it is a core technical skill for them. This paper shows our approach to make these courses attractive.**

Keywords*—*Security, cryptography, ciphering algorithms, pedagogy

I. Introduction

French University-based Institutes of Technology (IUT[1]) are a major player in France's higher educational system. IUTs provide technical university education, preparing students to careers in the industry and services. The main diploma is called DUT, *Diplôme Universitaire de Technologie* [8].

Designed to train mid-level technical staff in two years, IUT programmes also allow graduated students to pursue their studies with a more advanced degree, such as a *licence professionnelle* (professional bachelor degree) [9].

We prepare students for the *licence professionnelle ASUR* (standing for *Administration et Sécurité des Réseaux* – Networks Administration and Security), where the major focus is security of computer networks and operating systems.

The students registered in this curriculum have very different profiles: their background is extremely heterogeneous, resulting in very different levels in both theoretical and practical skills. The *licence professionnelle ASUR* is implemented in two different groups at the IUT de Villetaneuse (Université Paris 13, Sorbonne Paris Cité, France): the first group is dedicated to initial training and long-life learning students (the latter being generally older), while the second group is dedicated to apprenticeship students.

We are in charge of two courses in the curriculum (in both groups): *introduction to security* and *cryptography*. This complex subject is particularly difficult for our students whose mathematical background is usually rather low. Hence, even though such a subject is at the core of the curriculum, it can quickly become somewhat boring for the students. This paper aims at showing our approach to make these courses attractive, while still providing a high level of proficiency.

Indeed, a simple presentation of the existing tools that address security and cryptography is deemed insufficient since it does not provide the students with the background necessary to understand what they are actually installing or configuring. Thus, our courses aim at providing the students with the keys for understanding the vocabulary used in the security domain, and the main lines of the major techniques involved. This domain is subject to permanent evolutions. Therefore, this approach allows students both to tackle different systems and to understand new attacks against existing systems. Lab sessions aim at implementing simple symmetric and asymmetric algorithms, pointing out their difficulties and allowing for a deep understanding. Moreover, the cryptography course is illustrated with relevant problems taken from the news, related to security of communications and computer systems.

Outline: This paper is organised as follows: first, in Section II, the context introduces the main characteristics of the curriculum, and the background of the students attending the courses. In Section III, the main difficulties for learning cryptography and the pedagogical approach to overcome them are presented. The lab sessions are discussed in Section IV, while Section V shows how cryptography relates to a permanently evolving news context. Finally, Section VI concludes with possible improvements that will be implemented in the near future.

II. Teaching Context

The IUT de Villetaneuse is one of the 115 French University Technology Institutes (*Institut Universitaire de Technologie* – IUT), and is among the three IUT affiliated to University Paris 13. The university has five campuses, all of them located in the Northern suburbs of Paris. The *licence professionnelle* ASUR, a bachelor technological degree in administration and security of computer networks, is taught according to two modalities at the IUT de Villetaneuse: a traditional group of student plus long-life learning students; and a group of apprenticeship students. Each of these groups comprises 15 to 20 students. The two authors of this paper are in charge of courses *introduction to security* (20 hours) and *cryptography* (25 hours), for both groups.[2]

As the technological curriculum aims at immediate insertion in working life, the students—most of them have a

978-1-4799-1756-3/15/$31.00©2015 IEEE

[1]http://www.campusfrance.org/en/page/short-programs

[2]More precisely, we here report on the course *introduction to security* (delivered by Laure Petrucci over 2010–2012), and the course on *cryptography* (delivered by Étienne André over 2011–2015).

technical degree: BTS (*Brevet de Technicien Supérieur*) or DUT (*Diplôme Universitaire de Technologie*)—have a profile very much targeting applied studies, and hence a weak, or even very weak, mathematical and theoretical background.

III. Learning a complex domain

A. Goals for the two courses

These two courses aim at getting the students familiar with the usual problematics of security, and more specifically:

- **confidentiality:** "my communications can only be accessed by legitimate users";
- **authenticity:** "I am sure that my partner is the one he claims to be";
- **integrity:** "the data I received are indeed those that were sent";
- **non-repudiation:** "I cannot pretend not to have sent the data";
- **availability:** "the service is operational at all times".

These two modules must thereafter provide solutions to these problematics, using notions of *symmetric and asymmetric ciphering*, *hash functions*, *signature*, and more generally of *public key infrastructure*. They must also point out at which levels attacks can take place, and provide the basic knowledge to understand the functioning of the systems detecting them.

Two mistakes are to be avoided: on the one hand the danger of having a too practical course (moreover redundant with other teaching modules, in particular *networks protection* or *attack techniques*, which are significantly practical) and, on the other hand, the converse, i.e. a too theoretical course, not suited for our students (which also have a well-known aversion for everything that is more or less mathematical). Hence, any attempt to make students understand notions of circular permutations, substitution within a set, or congruence over the set of integers has remained vain. Similarly, an alphabet, will never be a set of symbols used in set theory, but will remain the set of the 26 letters from A to Z.

B. Modules content

We here detail the contents of both modules. In the schedule of the curriculum, the module introduction to security precedes the module on cryptography.

1) The "introduction to security" module: The first module aims at introducing the basic concepts of security, and give the necessary elements for a better understanding of the subsequent modules. It therefore states the vocabulary and draws a picture that are both keys to understanding the techniques used to guarantee systems and computer networks security.

First of all, presenting the terminology provides a general framework to tackle the security problems. The usual approach comprises three steps: *prevention*, *detection* and *reaction*. *Intrusions* aim at exploiting the operating systems or the computer network *vulnerabilities*. A short highlight of the history of security shows that the problematics is ancient, in contexts that are of course not computer related and allows for stories as illustrations. Still as part of the terminology, desired properties to ensure security are defined, illustrated by a simple practical example.

In a second part, the course addresses the notion of data exchange protocols. A first simple example points out the difficulties encountered to design such a protocol, and also to prove its robustness. The example of the Needham-Schroeder protocol [10] is traditional for this purpose. The basic characteristics of protocols based on symmetric and asymmetric keys are introduced together with a few examples of the main protocols implementing them.

The third part of this module presents the differences and how intricate are the concepts of *vulnerability*, *attack* and *intrusion*. They are characterised by a taxonomy of attacks based on their *target*, *vector* and *vulnerability exploiting type*.

Finally, a quick picture of *Intrusion Detection Systems* (IDS for short) shows how they are placed within the architecture (network IDS or system IDS) as well as the detection systems they use (with scenarios or with behavioural anomalies).

Getting deep into the technical details is out of the scope of this introductory module. It is only concerned with providing the students with a big picture for a better understanding of what is taught in the subsequent modules. The major part of this introductory module is given as lectures, and it is followed by a project (which will be detailed in Section IV).

2) The "cryptography" module: The first part of the cryptography module tackles symmetric ciphering[3]. The course uses very simple historical algorithms, i.e. Caesar cipher (where the Latin alphabet is rotated for a certain number of steps), and substitution cipher (where each letter of the Latin alphabet is substituted by another one), so as to instantiate the formal definitions of symmetric cryptosystems and their expected properties.

These two algorithms enjoy the possibility of being simple enough to be executed manually, and to make more concrete the notions of key, key space size, complexity, cryptanalysis, thus avoiding the numerous abstruse mathematical definitions.

Moreover, frequency analysis (proposed by Al-Kindi in as early as the ninth century to break the substitution cipher, based on the number of occurrences of letters in natural languages) is performed manually during exercise courses, making the cryptanalysis concept attractive. This cryptanalysis using letters frequency shows that even though a large keys space (very large in the case of substitution cipher) is necessary for a cryptosystem to be reliable, it is not sufficient.

Then, the cryptography module introduces asymmetric cryptography[4] and the underlying mathematical principles (in particular large integers factorisation).

Part of the module is then briefly dedicated to hash functions[5]; contrarily to the other notions in this cryptography

[3]This class of cryptosystems, used for millennia, is based on the shared knowledge of a secret, or *key*, by a group of legitimate users. The problem here lies in the way the key can securely be exchanged.

[4]This class of cryptosystems, proposed at the end of the 1970s [12], relies on a pair public key/private key. Thus, exchanging the key is no more (or way less) critical. Numerous applications make use of asymmetric cryptography, such as credit cards, electronic voting, secure online payment, etc.

[5]These functions associate an infinite set of objects (integers, strings) with a finite set of identifiers or *fingerprints*. Several properties (non-invertibility, avalanche effect, etc.) should be satisfied by hash functions for the security of the cryptosystem to be guaranteed.

course, we mathematically formalise these functions. The students know or have at least heard of these functions (typically the MD5 hash function), but do not know much about their properties.

Finally, the goal is for the students to guess how the different techniques introduced (symmetric and asymmetric ciphering, hash functions) can be combined in order to cipher, decipher, sign, and authenticate communications. This module tries to abstract as much as possible from technological aspects because first the domain is in constant evolution, and second concrete technologies are the topic of other modules. Lab sessions (see Section IV-B) allow for combining functions that provide symmetric and asymmetric ciphering, as well as hash functions, so as to obtain ciphering, deciphering, signature, and authentication.

The course also insists on the notions of *strong passwords*, giving hints on their complexity, on how easy it is to *break* relatively strong ones, quoting examples of recent events (more specifically a stolen database of the passwords that were supposedly securely encrypted on the server side[6] of LinkedIn in June 2012, and of which 90 % could be retrieved in clear within one week). The *strength* of a password is particularly critical in cryptography since such a password is generally the basis for the security of any cryptosystem. For example, as far as asymmetric cryptography is concerned, the private key is often protected by a password, which should not be easily guessed.

The course concludes by a perspective (see Section V) on hot news related to cryptography and networks security, a particularly active subject since June 2013 with the NSA scandal.

C. Pedagogic handouts

As concerns the pedagogy, the introductory module is mainly based, after presenting the concepts during lectures, on a bibliographic project, studying an existing tool. A handout synthesizing all the notions introduced is provided to the students [11].

The cryptography module is organised with sessions mixing both lectures and exercises, practical sessions and projects. The printed lecture handouts given to the students (as well as the PDF files available on the Web under a Creative Commons licence[7] [7]) are copies of the slides with "holes" (missing parts): it contains most information, except some important ones (algorithms, important notes, etc.). The students should copy this important missing information from the slides projected during the lecture. Even though this is not really appreciated by the students (satisfaction index for this kind of slides: 39, Fig. 1) and may seem relatively scholarly, we deem it interesting from a pedagogical perspective so that *i*) the students do not have to copy everything (as most of the text is already present on the paper copy), *ii*) their attention is always solicited (the missing parts are not really obvious from the paper copy), and *iii*) it allows for assimilation of concepts by handwriting them (which is a recognised pedagogical concept).

[6]Technically, these passwords were stored as fingerprints.

[7]More precisely, the Creative Commons BY-NC-SA license, that is *Attribution*, *non-commercial* usage, *share* under the same conditions; see https://creativecommons.org/licenses/by-nc-sa/3.0/deed.en.

Evaluation method

An anonymous questionnaire is distributed to the students at the end of the last session in the module. The data presented here is the means of the two groups for the academic year 2013/2014. For several questions, the students were proposed 4 possible answers: *completely disagree*, *disagree*, *agree*, and *completely agree*. The indices given in this paper correspond to the mean % of these four choices, respectively counted as 0, 33, 66, and 100. Thus an index greater than 66 indicates a good to very good satisfaction.

Figure 1. Evaluation method for the cryptography module

IV. Lab sessions

Even though the cryptography module tries as much as possible to abstract away from technologies or concrete tools, the intrinsic nature of the technological bachelor degree requires the students to have a lot of hands-on sessions. Therefore, two lab sessions and a group project are proposed to the students.

As concerns the introductory module, it does not include any hands-on session, but is concluded by a bibliographic project on Intrusion Detection Systems.

A. Implementing ciphering algorithms

Part of the lab sessions in the cryptography module address the implementation of two simple symmetric algorithms in Python: Caesar cipher, and substitution cipher. After having ciphered and deciphered a few small texts written in natural language, the students have to propose a method for automatic cryptanalysis of a text ciphered by rotation (where the key is of course unknown).

Beyond the attractive aspects that motivates the students, implementing even extremely simple algorithms gives a feeling for what a ciphering algorithm is, and how it is possible to perform attacks. Cryptanalysis of the substitution cipher, manually performed during the exercise courses, was however not proposed as practical work, due to complexity issues.

B. Using Unix functions

The second part of lab sessions within the cryptography module consists of using predefined Unix functions to generate pairs of asymmetric keys, symmetric keys, cipher and sign documents both symmetrically and asymmetrically. Then students had to send them to their neighbour, who had to decipher them or authenticate them.

Only the lower-level functions are permitted: for example, instead of using a predefined function for signing a file, students have to apply the *theoretical* approach to the signature mechanism, that has been explained during the lectures: first generate the file fingerprint, then cipher it using the private key, and finally send the file and its ciphered fingerprint.

The goal is thus to gain a deep understanding of the mechanisms at stake in higher-level software (for example email encryption or files signature). Lab sessions are generally appreciated by the students (satisfaction index: 75).

C. Group projects

1) The cryptography module: The projects achieved in small groups at the end of the cryptography module are on the contrary quite concrete, and require existing and realistic solutions to problems such as:

- proposing a documents sharing system that guarantees confidentiality, authenticity and integrity;
- propose a video-conferencing system that guarantees confidentiality, authenticity and integrity;
- set up an electronic voting system that guarantees confidentiality, authenticity, integrity and non-repudiation.

Note that the project subjects have been chosen without a solution predefined by the teacher: there does not always exist a satisfactory solution, and most likely never a perfect one. The key point is for students to be able to pinpoint the limits of the approach they propose. In particular, the electronic voting system was (curiously) never subject to a satisfactory and simple solution, and even quite the contrary gave rise to completely bizarre ones, among which the use of the commercial, USA-based Web site doodle.com, that guarantees neither confidentiality, authenticity, integrity nor non-repudiation.

2) The introduction to security module: In the context of the introductory module, the students, grouped by three to four, perform a bibliographic study of an Intrusion Detection System. Each group studies a different IDS, chosen among a proposed list. They then have to give an oral presentation highlighting the main characteristics of the tool: architecture, detection mechanism that is operated, type of attacks handled, etc. They can thus manipulate the concepts presented during the lectures. They also report about how easy it is to use and configure the tool, as well as its efficiency according to the types of attacks. Amongst the IDS studied are the following: bro [2], chkrootkit [4], orchids [5], ossec [6], rkhunter [1], snort [3].

The project concludes by an oral presentation in the class, where students are enticed to ask questions to their comrades. Thus, they get a better view of the capabilities of different tools. Moreover, at best, the students succeeded in installing the system and play with the configuration parameters[8]. The project was particularly appreciated[9], and more specifically their active participation in the different oral presentations which allowed them to have a panorama of several IDS targeting different vulnerabilities and attacks.

V. Cryptography in the news

In order to open new perspectives, but also to place cryptography within a larger context and motivate its importance, the last part of the cryptography module is dedicated to hot (if possible) news: most recent attacks against symmetric cryptography and their consequences; the NSA scandal, accused worldwide of massive spying, in particular with its programs PRISM and XKeyscore, as well as the British GCHQ's program Tempora.

Evaluation of the cryptography module

Criterion	Satisfaction
Interesting course	78
Clear course	65
Useful course	78
Interesting lab sessions	75
Useful lab sessions	66
Likes slides "with holes"	39

Figure 2. Evaluation of the cryptography module (2013/2014)

Pointing out the most recent attacks against asymmetric cryptography provides the students with insight as to the breaking possibilities of such techniques in a more or less near future, and also encourages them to keep up-to-date. Thus the course mentions the advances of quantum computing and its threats towards asymmetric algorithms such as RSA [12] and their applications (credit cards, HTTPS), but also, the consequences that would be induced by solving the famous problem $P = NP$[10] (specifically in case of equality of these two complexity classes).

The NSA scandal is a blessing for the cryptography teacher: it becomes easy to motivate the necessity of encrypting data, students understand the effects of the corrupt RDRAND function for Intel chipsets (key generation being less random and cryptanalysis made easier); the dangers of ignoring security announcements (*hijacking* of the European parliament Wi-Fi in 2013); critique of our politicians' behaviour (with top-end politicians using completely unsecured Wi-Fi access points in a famous American coffee-shop).

VI. Conclusion and perspectives

A. Conclusion

In this paper, we presented the contents of two courses in the technological bachelor degree ASUR, i.e. introduction to security and cryptography, as well as the approach we use to make it interesting for students rather allergic to formal notions.

As a result, students appreciated both courses. The evaluation of the cryptography module (see Fig. 2) shows a very high general satisfaction index (78), despite a lower mark for clarity (65)[11].

Moreover, considering the feedback from students and colleagues, the articulation with other courses (networks security and protection, attack techniques) is smooth. In particular, the informal introductory approach not only provides the technical basics for understanding[12], but also a general context in which

[8]This is not always easy, first because students must have access to an adequate platform which varies from one tool to the other, but also because the more academic tools are often not ergonomic enough.

[9]When the course took place, the satisfaction questionnaire was not available yet. Hence this statement is solely based on the informal feedback from students, and their eagerness to ask questions during the presentations.

[10]One of the most important open problems in computer science and mathematics.

[11]The moderate usefulness of lab sessions is actually a mean between the group of regular plus long-life learning students (59) and apprentices (72). The second group had an improved version of the lab sessions in 2013/2014, thus the evolution is quite positive.

[12]These technical basics are often repeated during the subsequent modules, but differently, by another teacher, and quicker than what happened in the past. Repetition is far from being a problem, but a tool for assimilation.

it is easy to navigate.

B. Evolution and perspectives

Possible improvements for the cryptography course include understanding and implementing recent algorithms (such as RSA), in a simplified form; the set up, during lab sessions, of a public key infrastructure, which was not treated until this year due to lack of time, but is being treated in 2014/2015[13], benefiting from a few additional hours of courses.

Finally a new small project will be proposed in the cryptography module starting from 2015, consisting in sending to the teacher an encrypted and/or signed email, and be able to decrypt and/or authenticate the teacher's reply. Even though there is no real theoretical difficulty in encrypting emails (the intrinsic techniques being the same as those studied during the lectures), it seems to us absolutely necessary for students in this curriculum to know how to encrypt or decrypt an email. This was not studied up to now because of a lack of time, and had to be done as homework.

Concerning the evaluation of the course, our evaluation system was not used before we became responsible of this course, hence we cannot directly evaluate the possible benefits of our approach. However, this evaluation system will be helpful in the future to monitor the evaluation by the students of future changes made to the form and the content of our courses. Furthermore, it would be interesting to compare our pedagogical choices with other implementations of the LP ASUR in other IUT, possibly using a unified evaluation scheme.

Acknowledgements

We are grateful to the anonymous reviewers for valuable comments and suggestions.

References

[1] http://rkhunter.sourceforge.net/.

[2] https://www.bro.org/.

[3] https://www.snort.org/.

[4] http://www.chkrootkit.org/.

[5] http://www.lsv.ens-cachan.fr/Software/orchids/.

[6] http://www.ossec.net/.

[7] Étienne André. Ressources du cours de cryptographie (2013-2014), 2014. Available at http://lipn.univ-paris13.fr/~andre/enseignement/crypto/2013-2014/.

[8] Assemblée des directeurs d'IUT (ADIUT) et Union nationale des présidents de conseils d'IUT. Livre blanc sur le système IUT, 2007. http://www.iut-fr.net/files/fck/File/documents/publications/livre_blanc_iut_2007.pdf.

[9] Thierry Malan. Implementing the Bologna process in France. *European Journal of Education*, 39(3):289–297, 2004.

[10] Roger M. Needham and Michael D. Schroeder. Using encryption for authentication in large networks of computers. *Communications of the ACM*, 21(12):993–999, 1978.

[11] Laure Petrucci. Cours de sécurité et surveillance des réseaux, 2011. Available at http://lipn.univ-paris13.fr/~petrucci/cours_secu.pdf.

[12] Ron L. Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[13] The course is still being taught at the time of writing, and could hence not be integrated to this teaching report.