La cryptographie décryptée

Étienne ANDRÉ, Laure PETRUCCI
Université Paris 13, Sorbonne Paris Cité, IUT de Villetaneuse, F-93430, Villetaneuse, France
Mél. : {Etienne.Andre,Laure.Petrucci}@iutv.univ-paris13.fr

***Résumé*—Le domaine d'intérêt majeur de la licence professionnelle ASUR (administration et sécurité des réseaux) est la sécurité des systèmes et des réseaux. Il est nécessaire de familiariser les étudiants avec les différentes techniques qu'ils seront amenés à mettre en œuvre pour sécuriser les accès et les communications sur les réseaux dont ils auront la charge. Dans le programme de cette licence professionnelle, nous sommes en charge de deux modules d'introduction à la sécurité et à la cryptographie. Ce domaine particulièrement complexe est difficile à appréhender pour les étudiants, lesquels ont souvent un bagage mathématique insuffisant. Un tel sujet peut donc aisément devenir rébarbatif pour les étudiants alors qu'il fait partie de leur cœur de compétences. Cet article montre la démarche adoptée pour rendre ces cours attractifs.**

***Index Terms*—Sécurité, cryptographie, algorithmes de chiffrement, pédagogie**

I. INTRODUCTION

Le domaine d'intérêt majeur de la licence professionnelle ASUR (administration et sécurité des réseaux) est la sécurité des systèmes et des réseaux. Il est nécessaire de familiariser les étudiants avec les différentes techniques qu'ils seront amenés à mettre en œuvre pour sécuriser les accès et les communications sur les réseaux dont ils auront la charge.

Une simple présentation des outils existants nous semble insuffisante car, si elle leur permet de mettre en place un système via une interface, elle ne leur donne pas le bagage nécessaire pour comprendre ce qu'ils installent vraiment, ni ce que la solution retenue garantit ou ne garantit pas.

Dans le programme de la licence professionnelle ASUR, nous sommes en charge de deux modules d'introduction à la sécurité et à la cryptographie. Ce domaine particulièrement complexe est difficile à appréhender pour les étudiants, lesquels ont souvent un bagage mathématique insuffisant. De tels modules peuvent donc aisément devenir rébarbatifs pour les étudiants alors qu'ils font partie de leur cœur de compétences. Ces modules visent à donner aux étudiants les clés (sic) leur permettant de comprendre le vocabulaire utilisé dans le domaine et les grandes lignes des principales techniques. Les évolutions étant permanentes, cette approche permet aux étudiants d'appréhender les différents systèmes, de comprendre les principales caractéristiques de nouveaux systèmes cryptographiques, et de comprendre les nouvelles attaques contre les systèmes existants. Des travaux pratiques sur l'implémentation d'algorithmes de chiffrement simples permettent à la fois d'en pointer les difficultés et d'en avoir une compréhension approfondie. De plus, le cours de cryptographie est illustré par des problèmes issus de l'actualité en lien avec la sécurité des communications et des systèmes informatiques.

Plan: Après avoir rappelé le contexte de l'enseignement en section II, cet article présente dans la section III les difficultés d'apprentissage de la cryptographie et la pédagogie mise en œuvre. Les travaux pratiques sont présentés dans la section IV. La section V décrit comment nous replaçons la cryptographie dans un contexte d'actualité permanente. Enfin, la section VI conclut et décrit l'articulation de ce module de cours avec ceux abordant d'autres aspects des problématiques de sécurité. Elle montre également les améliorations envisagées pour les prochaines sessions.

II. CONTEXTE DE L'ENSEIGNEMENT

L'IUT (institut universitaire de technologie) de Villetaneuse est l'un des 115 IUT français, et l'un des trois IUT de l'Université Paris 13, laquelle est située sur cinq campus en Seine-Saint-Denis. La licence professionnelle ASUR existe en deux déclinaisons à l'IUT de Villetaneuse, l'une en formation initiale et formation continue, l'autre en formation par l'alternance. Chacun des deux groupes comporte entre 15 et 20 étudiants. Les deux auteurs de l'article sont responsables des modules « introduction à la sécurité » (volume horaire : 20h) et « cryptographie » (25h), dans les deux déclinaisons de la licence. [1]

De par la nature professionnalisante de la licence professionnelle, les étudiants – titulaires d'un BTS (brevet de technicien supérieur) ou DUT (diplôme universitaire de technologie) pour la plupart – ont un profil relativement appliqué, et en général un bagage mathématique et théorique faible voire très faible.

III. L'APPRENTISSAGE D'UN DOMAINE COMPLEXE

A. Objectifs des deux modules

Le but de ces deux modules est de familiariser les étudiants avec les problématiques générales de la sécurité, plus particulièrement :

confidentialité : « mes communications ne sont accessibles que par les interlocuteurs légitimes » ;

authenticité : « j'ai la garantie que mon interlocuteur est celui qu'il prétend être » ;

1. Plus précisément, nous relatons ici notre expérience relative au module « introduction à la sécurité » (effectué par Laure PETRUCCI sur les années 2010–2012), et au module « cryptographie » (effectué par Étienne ANDRÉ sur les années 2011–2014).

intégrité : « les données que j'ai reçues sont bien celles qui ont été envoyées » ;

non-répudiation : « je ne peux pas prétendre ne pas avoir envoyé des données » ;

disponibilité : « le service est toujours fonctionnel ».

Ces deux modules se doivent ensuite de donner des solutions à ces problématiques à l'aide des notions de *chiffrements symétrique et asymétrique*, de *fonctions de hachage*, de *signature*, et plus largement d'*infrastructure à clé publique*. Ils doivent également montrer à quels niveaux peuvent se situer des attaques, et poser les jalons nécessaires pour comprendre le fonctionnement des systèmes permettant de les détecter.

Deux écueils sont alors à éviter, à savoir le danger d'un cours trop pratique (et redondant avec d'autres modules, notamment « protection des réseaux », ou encore « techniques d'attaques », qui sont eux fortement appliqués) et, à l'inverse, d'un cours trop théorique, notamment au vu de l'aversion notoire qu'ont nos étudiants pour tout ce qui ressemble de près ou de loin à des mathématiques. Ainsi, toute tentative de faire comprendre les notions de permutation circulaire, de substitution dans un ensemble, ou de congruence sur les entiers est restée vaine. De même, un alphabet, loin d'un ensemble de symboles utilisé en théorie des ensembles, restera à jamais nos 26 lettres latines de A à Z.

B. Contenu des modules

Nous détaillons ci-après le contenu des deux modules. Dans l'organisation du planning pédagogique, le module d'introduction à la sécurité précède le module de cryptographie.

1) Module d'introduction à la sécurité: Le premier module vise à introduire les concepts de base de la sécurité et fournir les éléments nécessaires à la compréhension des modules suivants. Par conséquent, il fixe le vocabulaire et dresse un panorama essentiels à la compréhension des techniques mises en œuvre pour assurer la sécurité des systèmes et réseaux informatiques.

Tout d'abord, la présentation de la terminologie permet de situer le cadre dans lequel se situe la problématique. L'approche classique comprend trois étapes : *prévention*, *détection* et *réaction*. Les *intrusions* visent à exploiter des *vulnérabilités* du système d'exploitation ou du réseau.

Un bref historique met en lumière l'ancienneté de la problématique, dans des contextes autres qu'informatiques et permet de l'illustrer avec quelques anecdotes.

Toujours dans le cadre terminologique, les propriétés souhaitées pour assurer la sécurité sont définies et accompagnées d'un exemple pratique simple.

Dans une seconde partie, on s'intéresse à la notion de protocole d'échange de données. Un premier exemple simple montre la difficulté d'élaborer un tel protocole, et de prouver sa robustesse. L'exemple du protocole de Needham-Schroeder [NS78] est pour cela classique. Les caractéristiques de base des mécanismes de clés symétriques et asymétriques sont introduits avec quelques exemples des principaux protocoles les mettant en œuvre.

La troisième partie du cours montre aux étudiants la différence et l'intrication entre les concepts de *vulnérabilité*, *attaque* et *intrusion*. Une taxinomie des attaques permet de les caractériser avec leurs *cible*, *vecteur* et *type d'exploitation de vulnérabilité*.

Enfin, un bref aperçu des *systèmes de détection d'intrusions* (IDS — *Intrusion Detection System*) montre leur positionnement au sein de l'architecture (IDS réseau ou IDS système) ainsi que les mécanismes de détection qu'ils emploient (par scénarios ou par anomalies de comportement).

Ce module étant introductif, il ne vise en aucun cas à rentrer dans des détails techniques, mais simplement à brosser un panorama permettant aux étudiants de mieux comprendre et situer ce qui leur est enseigné dans les modules suivants. L'essentiel du module est constitué de cours, suivi d'un projet (que nous détaillerons dans la section IV).

2) Module de cryptographie: La première partie du module de cryptographie s'intéresse au chiffrement symétrique [2]. Le cours utilise des algorithmes historiques très simples, à savoir le chiffre de César (où l'on décale l'alphabet d'un certain nombre de pas), et le chiffrement par substitution (où toute lettre de l'alphabet latin est substituée par une autre), afin d'instancier les définitions formelles des cryptosystèmes symétriques, et les propriétés qu'ils doivent vérifier. Ces deux algorithmes présentent l'avantage d'être déroulables à la main, et de rendre concrètes les notions de clé, de taille de l'espace des clés, de complexité, et de cryptanalyse, permettant ainsi d'éviter l'écueil des nombreuses définitions mathématiques absconses. En outre, l'analyse des fréquences (proposée dès le IX^{e} siècle pour casser le chiffrement par substitution, et basée sur la fréquence d'apparition des lettres dans les langages naturels) est effectuée à la main en travaux dirigés, ce qui rend ludique le concept de cryptanalyse. Cette cryptanalyse par analyse des fréquences montre que, si la taille de l'espace des clés (très grande dans le cas du chiffrement par substitution) est une condition nécessaire pour la fiabilité d'un cryptosystème, elle n'est en aucun cas suffisante.

Le module de cryptographie présente ensuite la cryptographie asymétrique [3] et le principe mathématique sous-jacent (notamment la factorisation en nombres premiers). Une partie du module est ensuite brièvement consacrée aux fonctions de hachage [4] ; à l'inverse des autres notions du cours de cryptographie, nous nous attachons tout particulièrement à formaliser d'un point de vue mathématique ces fonctions,

2. Cette classe de cryptosystèmes, utilisés depuis des millénaires, repose sur la connaissance par les interlocuteurs légitimes d'un secret commun, ou *clé*. Tout le problème repose sur la façon dont cette clé peut être échangée de façon sécurisée.

3. Cette classe de cryptosystèmes, proposée à la fin des années 1970 [RSA78], repose sur la notion d'un couple clé publique / clé privée. Ainsi, la question de l'échange de clé ne se pose plus (ou beaucoup moins). La cryptographie asymétrique est derrière de nombreuses applications, dont les cartes de crédit, le vote électronique, le paiement sécurisé sur Internet, etc.

4. Ces fonctions associent à un ensemble infini d'objets (entiers, chaînes de caractères) un ensemble fini d'identifiants ou *empreintes*. Un certain nombre de propriétés (non-inversibilité, effet avalanche, etc.) doivent être satisfaites par les fonctions de hachage afin de garantir la sécurité d'un cryptosystème.

que les étudiants connaissent tous de nom (et notamment la fonction de hachage md5), mais sans bien en connaître les propriétés.

Enfin, le but est de faire deviner aux étudiants comment combiner les éléments vus (chiffrements symétrique et asymétrique, fonctions de hachage) afin de chiffrer, déchiffrer, signer et authentifier des communications. Le module essaie autant que possible d'abstraire les technologies, d'une part en raison des rapides évolutions dans le domaine et, d'autre part, car des technologies concrètes sont vues dans d'autres modules. Les travaux pratiques (voir section IV-B) permettront une combinaison à la main des fonctions implémentant chiffrements symétrique et asymétrique ainsi que les fonctions de hachage, en vue de permettre chiffrement, déchiffrement, signature et authentification.

Le cours insiste également sur la notion de mots de passe « forts », en donnant une idée de la complexité d'un mot de passe, et de la facilité à « casser » des mots de passe relativement forts, au travers d'exemples de l'actualité récente (notamment la récupération de 90 % des mots de passe soit-disant sécurisés [5] du site LinkedIn en juin 2012). L'importance d'un mot de passe « fort » est critique en cryptographie, car la sécurité d'un cryptosystème repose généralement sur un tel mot de passe. Par exemple, en cryptographie asymétrique, la clé privée est généralement protégée par mot de passe, et celui-ci ne doit donc en aucune façon pouvoir être aisément deviné.

Une mise en perspective conclut le cours (voir la section V) grâce à l'actualité bouillonnante en matière de cryptographie et de sécurité des réseaux depuis juin 2013.

C. Supports pédagogiques

Pédagogiquement, le module d'introduction à la sécurité est majoritairement sous la forme de projets d'étude d'un outil existant, après une présentation en cours des concepts généraux. Un polycopié est fourni [Pet11], synthétisant toutes les notions introduites.

Le module de cryptographie est dispensé sous la forme de séances mixtes de cours et travaux dirigés, de séances de travaux pratiques, et de projets. Le cours se présente sous la forme de diapositives dites à trous : la copie papier distribuée aux étudiants (et placée sur le Web en PDF sous licence Creative Commons [6] [And14]) contient la plupart des informations, à l'exception de certaines informations importantes (algorithmes, notes importantes, etc.). Les étudiants doivent recopier ces informations manquantes depuis les diapositives projetées en cours. Quoique ce point soit relativement peu apprécié des étudiants (indice de satisfaction des diapositives à trous : 39, voir figure 1) et puisse paraître scolaire, il nous semble intéressant d'un point de vue pédagogique afin (i) d'éviter aux étudiants d'avoir à tout recopier, (ii) de les garder attentifs (les trous ne sont pas particulièrement marqués sur la copie papier) et (iii) de permettre l'assimilation par la copie manuscrite.

Méthode d'évaluation

Un formulaire anonyme a été distribué en fin d'enseignement (les données présentées ici sont la moyenne des deux déclinaisons en 2013–2014). Pour un certain nombre de points (cours intéressant, cours clair, diapositives à trous appréciées, etc.), les étudiants pouvaient choisir entre 4 opinions, à savoir « pas du tout d'accord », « pas trop d'accord », « assez d'accord », et « tout à fait d'accord ». Le neutre n'était pas proposé. Les indices donnés dans cet article correspondent à la moyenne sur cent de ces quatre choix, comptés respectivement comme 0, 33, 66 et 100. Un indice supérieur à 66 indique donc une satisfaction générale entre bonne et très bonne.

FIGURE 1: Méthode d'évaluation du cours de cryptographie

IV. Mise en pratique

Quoique le module de cryptographie essaie autant que possible de s'abstraire de technologies ou outils concrets, la nature même de la licence professionnelle impose de faire manipuler les étudiants de façon conséquente. Par conséquent, deux séances de travaux pratiques ainsi que des projets par groupe sont proposés aux étudiants.

Le module d'introduction, quant à lui, se prête peu à des travaux pratiques. En revanche, il donne lieu à un projet d'étude bibliographique des systèmes de détection d'intrusions.

A. Implémentation d'algorithmes de chiffrement

Une partie des travaux pratiques du module de cryptographie consiste en l'implémentation dans un langage relativement simple (en général Python) de deux algorithmes symétriques simples : le chiffre de César, et le chiffrement par substitution. Après avoir chiffré et déchiffré des petits textes en français, les étudiants doivent proposer une méthode pour cryptanalyser de façon automatique un texte chiffré par décalage (dont on ne connaît bien sûr pas la clé).

Au-delà de l'aspect ludique permettant de motiver les étudiants, implémenter des algorithmes même très simples permet de donner un aperçu aux étudiants de ce qu'est un algorithme de chiffrement, et comment il est possible de l'attaquer. La cryptanalyse du chiffrement par substitution, déroulée à la main en travaux dirigés, n'était en revanche pas proposée en travaux pratiques, pour des raisons de complexité. [7]

B. Utilisation des fonctions Unix

Une seconde partie des travaux pratiques du module de cryptographie, plus conventionnelle, consiste à utiliser les

5. En fait conservés sous forme d'empreinte.

6. Plus précisément, la licence Creative Commons BY-NC-SA, à savoir « Attribution – Pas d'utilisation commerciale – Partage dans les mêmes conditions » ; voir https://creativecommons.org/licenses/by-nc-sa/3.0/deed.fr.

7. Cette cryptanalyse (par analyse des fréquences) est simple à implémenter sans l'aide d'un dictionnaire, mais il est alors très difficile de trouver des textes français dont l'ordre des fréquences d'apparition des lettres est exactement l'ordre moyen pour la langue française. Quant à la version avec un dictionnaire (et qui fonctionne même si les fréquences varient légèrement par rapport au français moyen), elle est nettement plus compliquée à implémenter dans le cadre d'un tel cours.

fonctions prédéfinies dans un système Unix (au niveau terminal) pour générer des couples de clés asymétriques, des clés symétriques, chiffrer et signer des documents de façon symétrique ou asymétrique, et les envoyer à leur voisin, qui doit à son tour les déchiffrer ou en vérifier l'authenticité.

Seules les fonctions les plus bas niveau sont autorisées : par exemple, plutôt qu'utiliser directement une fonction prédéfinie de signature de fichier, les étudiants doivent appliquer le fonctionnement « théorique » du mécanisme de signature vu en cours, à savoir d'abord générer l'empreinte du fichier, puis chiffrer l'empreinte avec sa clé privée, et enfin envoyer manuellement le fichier et son empreinte chiffrée.

L'objectif est de comprendre comment fonctionnent précisément des logiciels de plus haut niveau (par exemple, chiffrement de courriels ou signature de fichiers). Les travaux pratiques sont généralement très appréciés (indice de satisfaction : 75).

C. Projets par groupe

1) Module de cryptographie: Les projets réalisés par petits groupes en fin de module de cryptographie sont à l'inverse beaucoup plus concrets, et demandent des solutions existantes et réalistes à des problèmes tels que :

- proposer un système de partage de documents distants garantissant confidentialité, authenticité et intégrité ;
- proposer un système de visioconférence garantissant confidentialité, authenticité et intégrité ;
- mettre en place une élection électronique garantissant confidentialité, authenticité, intégrité et non-répudiation.

Notons que les intitulés des projets ont été conçus sans solution prédéfinie par l'enseignant : il n'y avait ainsi pas toujours de bonne solution, et certainement jamais de solution parfaite. L'essentiel était que les étudiants soient capables de pointer les limites de la solution proposée. En particulier, le système de vote électronique n'a (curieusement) jamais donné lieu à une proposition satisfaisante et simple à mettre en place — et a contrario a donné lieu à des réponses très farfelues, dont… le site Web commercial doodle.com, qui ne garantit ni confidentialité, ni authenticité, ni intégrité, ni non-répudiation.

2) Module d'introduction à la sécurité: Dans le cadre du module d'introduction, les étudiants réalisent, en groupe de trois à quatre étudiants, une étude bibliographique d'un système de détection d'intrusions. Chaque groupe étudie un système différent, choisi parmi une liste qui leur est proposée, pour lequel ils doivent faire un exposé mettant en exergue les caractéristiques du fonctionnement de l'outil : architecture, mécanisme de détection, types d'attaques visées, etc. Ainsi, ils peuvent manipuler les concepts qui leur ont été présentés en cours. Ils explicitent également la facilité d'utilisation, de paramétrisation, ainsi que l'efficacité du système en fonction des attaques. Parmi les systèmes de détection d'intrusions étudiés, nous comptons : bro [IDSb], chkrootkit [IDSd], orchids [IDSe], ossec [IDSf], rkhunter [IDSa], snort [IDSc].

Le projet résulte en une soutenance en classe complète où les étudiants sont incités à poser des questions à leurs camarades. Ceci leur permet de mieux cerner les capacités de différents outils.

Par ailleurs, dans les meilleurs cas, les étudiants auront pu installer l'outil et jouer avec les paramètres de configuration [8].

Les étudiants ont apprécié le projet [9], et en particulier leur participation active aux diverses soutenances, qui leur ont montré toute une palette d'outils de détection d'intrusions adaptés à différentes vulnérabilités et attaques.

V. Cryptographie et actualité

Afin d'ouvrir des perspectives, mais également afin de replacer la cryptographie dans un contexte plus large et d'en justifier l'utilité, la dernière partie du module de cryptographie est consacrée à l'actualité, d'une part aux attaques les plus récentes contre la cryptographie asymétrique et leurs conséquences pratiques et, d'autre part, au scandale autour de la NSA (*National Security Agency*, l'Agence nationale de la sécurité des États-Unis), accusée d'espionnage massif dans le monde entier, en particulier à l'aide de son programme PRISM.

Mentionner aux étudiants les attaques les plus récentes contre la cryptographie asymétrique permet de leur donner quelques éléments de compréhension quant aux risques de cassage de ces techniques dans un avenir plus ou moins proche, et de les encourager à surveiller l'actualité scientifique. Ainsi, le cours mentionne les avancées du calcul quantique et les menaces que cela fait peser sur les algorithmes asymétriques de type RSA [RSA78] et leurs applications (cartes bancaires, HTTPS), mais également, plus en ouverture, les conséquences qu'aurait une résolution du problème $P = NP$ (surtout dans le cas de l'égalité des deux classes de complexité).

Quant au scandale de la NSA, il s'agit ni plus ni moins que de pain béni pour un enseignant en cryptographie : justification de la nécessité de chiffrer ses données, compréhension par les étudiants des implications de la corruption de la fonction RDRAND des processeurs Intel (rendant moins aléatoire la génération des clés, et donc plus facile la cryptanalyse), compréhension du danger d'ignorer un avertissement de sécurité (« piratage » du Wi-Fi du parlement européen en 2013), ou encore critique par les étudiants des comportements de nos dirigeants politiques (utilisation des points d'accès Wi-Fi entièrement non sécurisés d'une célèbre chaîne de cafés américaine).

VI. Conclusion et perspectives

A. Conclusion

Nous avons présenté ici le contenu de deux modules de la licence ASUR, à savoir le module d'introduction à la sécurité et le module de cryptographie, et les méthodes que

8. Ce n'est pas toujours facile, à la fois pour un problème d'accès à des plateformes d'installation idoines, mais aussi parce que certains outils plus académiques ne disposent pas d'une ergonomie suffisante.

9. Lorsque le module d'introduction à la sécurité a été dispensé, l'enquête de satisfaction n'était pas encore utilisée au sein du département. Cette affirmation est basée sur les retours des étudiants.

Évaluation du module de cryptographie

Critère	Indice
Cours intéressant	78
Cours clair	65
Cours utile	78
TP intéressants	75
TP utiles	66
Aimé diapositives à trous	39

FIGURE 2: Évaluation du cours de cryptographie (2013–2014)

nous mettons en œuvre afin d'intéresser nos étudiants plutôt allergiques aux notions formelles.

Au final, les étudiants ont fortement apprécié nos deux modules. L'évaluation du module de cryptographie (voir figure 2) donne un indice de satisfaction générale très élevé (78), avec un seul bémol sur la clarté (65) [10]. Nous avons même reçu un courriel fort encourageant : « J'ai beaucoup apprécié ce cours ! Il y a plein de choses concernant l'actualité que je comprends mieux ! ».

Par ailleurs, au vu des retours des étudiants et de l'équipe enseignante, l'articulation avec des modules proches (sécurité et protection réseaux, techniques d'attaque) se passe bien. En particulier, l'approche informelle introductive fournit non seulement des bases de compréhension technique [11] mais aussi un contexte général dans lequel ils peuvent facilement se replacer.

B. Évolution et perspectives

Des perspectives d'amélioration du cours de cryptographie incluent la compréhension et l'implémentation d'algorithmes actuels (tels que RSA), éventuellement dans une version simplifiée, mais aussi la mise en place en travaux pratiques d'une infrastructure à clé publique, jusqu'ici délaissée par manque de temps mais qui pourra être traitée en 2014–2015 grâce à un volume horaire légèrement augmenté. Enfin, un nouveau mini-projet sera proposé en cryptographie dès 2014–2015, consistant à envoyer à l'enseignant un courriel chiffré et/ou signé, et être à même de déchiffrer et/ou vérifier la réponse de l'enseignant. Si le chiffrement de courriel a un intérêt théorique relativement faible (car les techniques inhérentes sont les mêmes que celles vues en cours), il nous semble en revanche absolument essentiel que des diplômés de licence professionnelle ASUR soient à même de savoir le faire. Ce point n'était pas vu jusqu'ici par manque de temps, et sera à effectuer sur le temps de travail personnel des étudiants.

10. L'utilité modérée des TP est en fait la moyenne entre le groupe formation initiale et continue (59) et en alternance (72) ; le groupe en alternance ayant eu une version améliorée des TP en 2013–2014, nous jugeons que l'évolution est très positive.

11. Ces bases techniques sont souvent répétées dans les modules suivants, mais d'une autre manière, par un autre enseignant, et beaucoup plus rapidement que par le passé. La répétition n'est pas un problème, mais au contraire un outil d'assimilation certain.

Remerciements: Nous remercions l'ensemble des étudiants des deux groupes de licence professionnelle ASUR, ainsi qu'Emmanuel VIENNET pour avoir aimablement accepté de présenter cet article.

RÉFÉRENCES

[And14] Étienne André. Ressources du cours de cryptographie (2013-2014), 2014. Disponible sur http://lipn.univ-paris13.fr/~andre/enseignement/crypto/2013-2014/.

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

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

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

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

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

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

[NS78] 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.

[Pet11] Laure Petrucci. Cours de sécurité et surveillance des réseaux, 2011. Disponible sur http://lipn.univ-paris13.fr/~petrucci/cours_secu.pdf.

[RSA78] 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.