Mission cryptographie

Matthieu Giraud
LIMOS, Université Clermont Auvergne
Email : matthieu.giraud@uca.fr

Pascal Lafourcade
LIMOS, Université Clermont Auvergne
Email : pascal.lafourcade@uca.fr

***Résumé*—Nous proposons une activité pédagogique à destination des élèves de lycée dans le but de leur faire découvrir des notions cryptographiques historiques (chiffrement de César, chiffrement de Vigenère) et modernes (partage de secret de Shamir, fonctions de hachage). L'activité est constituée de dix lettres chiffrées laissées par un agent secret. Le but de l'activité est de décrypter ces 10 lettres une-à-une afin de découvrir l'identité de l'agent secret.**

I. Introduction

Depuis les révélations d'Edouard Snowden en juin 2013, le grand public a pris conscience que la sécurité informatique est une discipline à part entière et qu'elle concerne tout le monde. Faire découvrir la sécurité informatique et la cryptographie est clairement une activité qui intéresse beaucoup d'élèves. Cette activité est conçue pour que de jeunes élèves découvrent par eux-mêmes des mécanismes cryptographiques aussi bien historiques que modernes. Cela peut paraître ambitieux mais les différentes expériences en classe ont montré qu'en s'amusant en groupe et en autonomie les élèves sont capables de comprendre et de résoudre de nombreux défis. L'activité appelée *Mission Crypotgraphie* [1] consiste pour les élèves en groupe de six à décrypter dix lettres laissées par un agent secret.

II. Objectif de l'activité

La *cryptographie* remonte à l'antiquité. C'est une discipline qui appartient aujourd'hui aussi bien aux mathématiques qu'à l'informatique. L'objectif de cette activité est de présenter sous forme ludique des primitives cryptographiques historiques et des notions en sécurité informatique aux jeunes élèves. Pour cela les notions de cryptanalyse, de chiffrement par substitution, de chiffrement par transposition ainsi que de partage de secret sont abordées.

III. Choix didactique et pédagogique

Pour ne pas dévoiler tous les secrets de chaque lettre, nous présentons uniquement les concepts théoriques associés aux différentes activités faites dans cette mission cryptographie. Ces choix ont été faits pour permettre aux élèves de comprendre par eux-mêmes le fonctionnement des différents chiffrements historiques proposés.

1. http://sancy.univ-bpclermont.fr/~lafourcade/MissionCrypto/Lettre0/

A. Chiffrement par substitution

La technique, appelée chiffrement par substitution, consiste à changer l'alphabet pour chiffrer un message. Elle était déjà utilisée du temps des romains sous le nom de *chiffrement de César* [SC01]. Pour chiffrer un message, il faut décaler de trois lettres dans l'alphabet chaque lettre du message à transmettre. Pour décoder un message chiffré, il suffit de décaler chacune des lettres de trois positions dans le sens inverse de l'alphabet. Nous présentons un exemple d'un message chiffré par cette méthode : `YHQL YLGL YLFL`. En appliquant la méthode exposée ci-dessus pour déchiffrer ce message, nous retrouvons la célèbre phrase que prononça Jules César après sa victoire sur Pharnace roi du Borsphore à Zéla : `VENI VIDI VICI`.

B. Chiffrement de Vigenère

Le chiffrement de Vigenère [SC01] (XVIème siècle) est un autre chiffrement par substitution. Il s'agit d'une forme plus évoluée du chiffrement de César : des chiffrements par substitutions sont appliqués dans un certain ordre. Cet ordre correspond à un mot ou une phrase connue de l'expéditeur et du récepteur du message. Cette information partagée constitue une *clef* qui permet d'effectuer dans le bon ordre les différents chiffrements par substitution. Ainsi, la même clef permet à la fois de chiffrer et de déchiffrer un message. Notons que, dans une langue donnée, une étude de fréquence d'apparition des lettres de l'alphabet dans un texte fournit une aide précieuse pour "casser" les chiffrements par substitutions. Possédant un texte d'une longueur suffisante, il est alors possible de deviner les lettres les plus utilisées, et ainsi de commencer à déchiffrer le message.

C. Chiffrement par transposition

Une des premières techniques cryptographiques est le chiffrement par transposition. Pour chiffrer un message, l'ordre des lettres du message original est permuté. Pour le déchiffrer, il suffit d'appliquer la méthode inverse. Un des premiers exemples connus d'un tel chiffrement est la *scytale* spartiate [SC01], utilisée au Vème siècle avant J-C par les grecs. La scytale consiste en un bâton autour duquel est enroulée une lanière de cuir. L'expéditeur écrit son message sur la lanière, puis une fois terminé la déroule et l'envoie. Le récepteur enroule à son tour la lanière reçue sur un bâton de même diamètre, ce qui lui permet ainsi de retrouver le texte original.

D. Partage de secret

L'objectif de cette technique inventée par Adi Shamir en 1979 [Sha79] est de permettre à k participants parmi n d'accéder à un secret seulement si au moins k participants sont d'accord. L'idée est de cacher le nombre secret dans le terme constant d'un polynôme de degré $k-1$. Ensuite il suffit de distribuer n points d'un polynôme de degré $k-1$ aux n participants. Ainsi, il faut qu'au moins k participants collaborent pour retrouver le polynôme en résolvant un système de k équations à k inconnus ou en utilisant par exemple la méthode d'interpolation de Lagrange [Sha04]. Une fois le polynôme trouvé, nous avons trouvé le terme constant. Dans la mission, un polynôme de degré 1 et un autre polynôme de degré 2 sont utilisés.

E. Deviner des mots de passe

Lors de fuite de certaines bases de données de mots de passe comme *ROCK YOU*, des milliers de mots de passe ont fuit car ils étaient stockés en clair. D'autres bases de données de mots de passe qui stockaient les mots de passe hachés ont fuit comme la base de données *Adobe*. Rappelons qu'une fonction de hachage cryptographique H [MvOV96], prenant en entrée une chaîne binaire arbitrairement longue et ayant pour sortie une chaîne binaire de longueur fixée, a les propriétés suivantes :

Résistance à la première pré-image Il n'est pas possible de retrouver x à partir de $H(x)$.

Résistance à la seconde pré-image Il n'est pas possible de trouver x' différent de x à partir de $H(x)$ et tel que $H(x) = H(x')$.

Résistance aux collisions Il n'est pas possible de trouver x et x' différents tel que $H(x) = H(x')$.

Normalement il n'est pas possible de retrouver les mots de passe à partir des hachés sauf en appliquant la fonction de hachage sur tous les mots de passe possibles, ce qui prendrait beaucoup de temps. Toutefois, en analysant la base de données *Adobe*, il a été remarqué que la base de mots de passe contenait les logins, les mots de passe hachés mais aussi un champ "indice" qui permet aux propriétaires des mots de passe de les aider à retrouver les mots de passe en cas d'oubli [HN17].

Ainsi plusieurs hachés ayant la même valeur correspondent au même mot de passe. Avec les différents indices laissés par les utilisateurs, il est possible de deviner le mot de passe et d'en avoir la certitude en appliquant la fonction de hachage correspondante. Par exemple, avec les indices "super héro" et "Araignée", il est possible de deviner que le mot de passe est "Spiderman".

IV. Présentation de l'activité

L'activité est constituée de dix lettres que les élèves doivent réussir à décoder. Elle est accessible en ligne [2] avec le login *Mission* et le mot de passe *Crypto*. La première lettre est la suivante :

2. http://sancy.univ-bpclermont.fr/~lafourcade/MissionCrypto/Lettre0/

Le 11 octobre 2018 à Aubière.

À qui de droit,

Si vous lisez cette lettre, c'est que mes ennemis m'auront retrouvé et que j'ai dû fuir. Rassurez-vous, j'ai laissé des indications et le code pour ouvrir mon coffre plein de trésors se révélera à ceux qui seront assez persévérants. Cela ne sera pas simple, j'ai utilisé tous mes codes secrets afin d'égarer les curieux et mes ennemis.

Bonne chance !

Agent0111

Post-Scriptum 1 : Décryptez-moi ces jeux bien plus vite que SHERLOCK et WATSON pour finir et gagner !

Post-Scriptum 2 : Pour la version en ligne, le mot de passe de la lettre 1 est égal à mon login. Pour la lettre 2, utilisez le nom d'une personne célèbre en majuscules obtenu dans la lettre 1.

Partant de cette première lettre les élèves vont découvrir lettre après lettre différents aspects de la cryptographie et de la sécurité informatique. Pour donner un aperçu des lettres, la prochaine lettre est chiffrée comme suit :

Oh 11 rfwreuh 2018 d Dxelhuh

D txl gh gurlw,

Mh yrlv txh yrxv dyhc frpsulv oh irqfwlrqqhphqw gx frgh gh Fhvdu, txl frqvlvwh d ghfdohu fkdtxh ohwwuh gh wurlv srvlwlrqv yhuv od gurlwh gdqv o doskdehw.

Uhwhqhc fh suhplhu srlqw vhfuhw g devflvvh prlqv flqt hw g rugrqqhh prlqv ylqjw wurlv.

Djhqw0111

Srvw-Vfulswxp 1 : Ghfubswhc prl fhv mhxa elhq soxv ylwh txh VKHUORFN hw ZDWVRQ srxu ilqlu hw jdjqhu !

Srvw-Vfulswxp 2 : Uhwurxyhc ohv wurlv prwv gh sdvvh d sduwlu gx ilfklhu gh prwv gh sdvvh (ohwwuh ghxa).

Il n'est donc pas possible de la lire sans avoir compris la méthode de chiffrement utilisée. Afin que les élèves arrivent à déchiffrer, cette lettre a la même structure que la première. Cette simple observation permet aux élèves d'avoir certaines parties du texte en clair et leurs chiffrés correspondant. Cela leur permet ainsi de découvrir la méthode de chiffrement utilisée qui dans le cas présent date du temps des romains. L'observation que le post-scriptum est un pangramme peut faciliter la résolution des dites lettres.

Après cette initiation à la cryptanalyse, les défis s'enchaînent lettre après lettre pour, *in fine*, découvrir dans la lettre dix l'identité de l'agent secret, l'auteur fictif des dix lettres. Toutes les lettres ne sont pas chiffrées, certaines nécessitent de faire des calculs pour résoudre des systèmes d'équations, ou de calculer des fonctions de hachage simples pour déduire des mots de passe ou encore de manipuler des chaines de caractères pour reconstituer un texte.

Dans la version en ligne, toutes les lettres sont aussi protégées par un login et mot de passe pour éviter qu'elles ne soient obtenues dans le mauvais ordre. Dans l'expérimentation faite avec les classes, les lettres étaient distribuées dans le bon ordre par l'animateur de la séance.

V. Éléments d'analyse *a posteriori*

Cette activité est le résultat de plusieurs années de pratique auprès des jeunes élèves pour expliquer les concepts cryptographiques. Nous avons eu des élèves du stage mathC2+, une promotion de première année de l'IUT informatique de Clermont-Ferrand et des élèves de 6ème. À chaque fois nous avons adapté et conçu de nouvelles activités. Cette version de l'activité a été testée lors de 3 séances de 1 heure 30 avec des élèves de 1ère (filière scientifique) et de BTS durant la fête de la science 2018 à l'Université Clermont Auvergne. Les élèves étaient regroupés en groupe de 6. Il est important de mettre les élèves par groupe car certaines tâches nécessitent d'être parallélisées afin de tenir dans les 1 heure 30. Le fait d'être en groupe favorise aussi les échanges et les idées pour résoudre les défis. Cela crée aussi une émulation entre les élèves.

Dans les deux classes de 1ère un groupe a réussi à chaque fois l'ensemble des missions. Dans le groupe de BTS aucun groupe n'a su obtenir le code permettant d'accéder à la dernière lettre. Les élèves de BTS ont même dit vouloir continuer durant la pause déjeuner pour trouver le secret de la dernière lettre.

L'ensemble des élèves et professeurs accompagnant, qui eux aussi formaient un groupe de deux ou quatre personnes, ont pris beaucoup de plaisir pendant cette activité.

L'aspect challenge est clairement un des atouts de cette activité. Il fait presque oublier aux élèves qu'ils travaillent et font des mathématiques.

VI. Conclustion

En conclusion cette activité permet de faire découvrir des techniques qui ont été réellement utilisées au cours de l'histoire. Elle fait appel au sens de déduction, à l'observation et à la collaboration entre les membres de l'équipe. Nous avons aussi réalisé une version pour les classes de primaires ou de collège sans utiliser la notion de partage de secret et avec des textes plus courts à déchiffrer. Nous souhaitons aussi construire de nouveaux défis qui illustreraient des techniques de la cryptographie moderne. Nous sommes en cours de réalisation d'un site web pour générer les fichiers `pdf` et les pages `html` correspondant aux différentes lettres. Cela permettra à chacun de créer son propre challenge.

Remerciements: Nous tenons à remercier Cédric Lauradoux pour nous avoir inspiré et aidé à la création de cette mission cryptographie.

Références

[HN17] Olivier Heen and Christoph Neumann. On the privacy impacts of publicly leaked password databases. In *Detection of Intrusions and Malware, and Vulnerability Assessment - 14th International Conference, DIMVA 2017, Bonn, Germany, July 6-7, 2017, Proceedings*, pages 347–365, 2017.

[MvOV96] Alfred Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

[SC01] Simon Singh and Catherine Coqueret. *Histoire des codes secrets*. Le Livre de Poche, 2001.

[Sha79] Adi Shamir. How to share a secret. *Commun. ACM*, 22(11) :612–613, 1979.

[Sha04] Mordechai Shacham. Scientific computing with MATLAB : a. quarteroni, f. saleri, springer-verlag, berlin, 2003, ISBN 3-540-44363-0. *Computer Physics Communications*, 161(3) :183–185, 2004.