Quelques éléments d'Histoire de la Cryptographie

Par **Jacques PATARIN**
Professeur à l'Université de
Versailles-Saint-Quentin en Yvelines

En conférence le 16 décembre

Ces quelques éléments de l'histoire de la Cryptographie seront approfondis lors de ma conférence, en lien avec le logiciel de cartes historiques « Mapysto » que je développe depuis quelques années sur iPad et iPhone.

Quelques définitions

La Cryptologie est la science des communications sécurisées. Son histoire remonte à l'Antiquité et elle est massivement utilisée de nos jours, aussi bien dans le monde civil que dans le monde militaire (les applications sont de plus en plus civiles dans le monde moderne). La Cryptographie présente les techniques de défense (chiffrement, signature, authentification), alors que la Cryptanalyse présente les techniques d'attaque. La Stéganographie présente les techniques qui consistent à dissimuler l'existence même du message, alors qu'en Cryptographie l'ennemi qui capte un message chiffré va connaître l'existence du message (et éventuellement sa taille) mais ne doit pas être capable d'obtenir d'autres informations sur le contenu de ce message.

L'Antiquité

Il semble que le premier document chiffré soit une recette secrète de potier, découverte en Irak, et datant de 1550 avant J.C. environ. Hébreux, Babyloniens, Grecs et Romains utilisèrent ensuite des systèmes cryptographiques originaux. Le « carré de Polybe » (vers -150 avant J.C.) est tout particulièrement innovant pour l'époque. Le « chiffre de Jules César », qui consistait à décaler l'alphabet de trois lettres, est resté célèbre. Comme c'est Jules César qui écrit le récit de ses combats (la Guerre des Gaules), on ignore si ce système s'est réellement révélé très solide, mais c'est fort possible.

Le Moyen Âge

À partir de 1379, des systèmes de chiffrements à base de nomenclateurs sont de plus en plus utilisés.

La Renaissance

Pour la période de la Renaissance, nous verrons l'exemple des lettres chiffrées de Marie de Guise (la reine d'Écosse, mère de Marie Stuart) que je suis en train de déchiffrer avec Valérie Nachef (de l'Université de Cergy-Pontoise).
Toujours à la Renaissance, le « cabinet noir » français sous le roi François Ier était capable de déchiffrer couramment les lettres chiffrées de Charles Quint.

Marie-Antoinette

Marie-Antoinette utilisait un moyen de chiffrement qui passait à l'époque pour indéchiffrable et le « nec plus ultra » de la technique : une substitution polyalphabétique. Souvent, elle ne chiffrait qu'une lettre sur deux, mais jamais les révolutionnaires ne furent en mesure de profiter de cet affaiblissement du système. En fait, elle sera guillotinée sans que ses lettres aient été déchiffrées.

Napoléon

Napoléon Ier n'a pas fait un usage très impressionnant de la Cryptographie. Il dit ainsi, un jour, que le seul moyen d'arrêter une charge de cavalerie serait de leur demander de chiffrer ou déchiffrer des messages. Cela lui a parfois causé des problèmes certains, comme lors de la campagne de Russie, où les Russes pouvaient lire les messages français puisqu'ils étaient bien souvent non ou mal codés.

La Première Guerre mondiale

Lors de la Première Guerre mondiale, il fut très fréquent que les messages des armées ennemies soient déchiffrés. Ainsi, les Allemands furent-ils en mesure de connaître à l'avance la plupart des offensives russes, alors que les Français et les Anglais parvinrent à déchiffrer des messages allemands très importants (télégramme Zimmerman, radiogramme de la victoire par exemple).

La Seconde Guerre mondiale

La Seconde Guerre mondiale vit l'apparition des premiers ordinateurs (en 1944) qui vont permettre de casser les codes des armées allemandes (marine, aviation et armée de terre), ce qui va très significativement accélérer la fin de la guerre. Les ordinateurs vont d'ailleurs totalement transformer l'usage de la Cryptographie par la suite, aussi bien pour les attaques que pour la défense. Face aux Japonais, les Américains réussirent également de nombreux déchiffrements importants. Les avantages considérables obtenus par la Cryptographie vont faire que les Américains vont développer, après la guerre, des organismes nationaux puissants, chargés des

écoutes, alors que l'Union soviétique, qui avait davantage profité de l'espionnage durant la Seconde Guerre mondiale (orchestre rouge par exemple), va continuer à investir massivement dans l'espionnage.

L'année 1976

L'année 1976 fut une année extraordinaire pour la Cryptographie. Tout d'abord, il y eut la publication du DES (Data Encryption Standard), premier algorithme (à clé secrète) entièrement publié et recommandé par le gouvernement américain (NIST) pour les applications civiles.
Ensuite, il y eut la découverte de la Cryptographie à clé publique (avec l'algorithme de Diffie-Hellman, puis en 1977 du RSA). Les mathématiques impliquées (théorie des nombres, groupes finis) ouvrirent le domaine sur des théorèmes d'algèbres développés depuis plusieurs siècles pour leur beauté et qui, soudain, se virent ouvrir des applications totalement imprévues.
Vers 1976, la Cryptographie passe majoritairement des applications militaires (ou de diplomatie) aux applications civiles, en même temps que de plus en plus de chercheurs civils vont se consacrer au domaine.

La période actuelle

La période actuelle voit l'utilisation de la Cryptographie à une échelle massive : paiements bancaires, téléphonie mobile, télévision, satellites, cartes d'identités, cartes de sécurité sociale, *Bitcoins*, etc.
En première approximation, l'apparition de moyens de calculs massifs et automatisés a donné un grand avantage aux défenseurs face aux attaquants dans les systèmes cryptographiques. En effet, il existe des algorithmes bien connus (comme l'algorithme AES en cryptographie à clé secrète) qui sont très simples à mettre en œuvre, qui se calculent très rapidement, et qui semblent permettre de générer des messages chiffrés ou de signatures électroniques qui ne sont cassables avec les meilleurs algorithmes connus que pour des millions d'années de calculs.

Cependant, la réalité sur le terrain est bien souvent très différente de cela. En effet, le monde pullule de DVD piratés, de fraudes bancaires ou d'intrusions dans des systèmes par des pirates informatiques. De plus, récemment, l'affaire Snowden a montré que le gouvernement des États-Unis pratiquait, à grande échelle, un programme d'écoute à peine imaginable. Ceci vient principalement du fait que les failles des systèmes se sont bien souvent déplacées des algorithmes vers le matériel ou les erreurs humaines, ces erreurs humaines pouvant être volontairement provoquées (social engineering). De plus, le contrôle du matériel ou des sociétés informatiques géantes donne clairement à certains États un avantage pratique actuellement considérable.

La Cryptographie a souvent eu une grande importance dans l'histoire. L'apparition des ordinateurs a complètement transformé cette discipline, dont l'usage est devenu massif et dont les attaques se sont déplacées de l'analyse des algorithmes à l'analyse des matériels, des protocoles d'utilisation, des erreurs humaines et du contrôle des systèmes informatiques. ■