IUT Lyon 1

Département Informatique

2014-2015

La Cryptographie

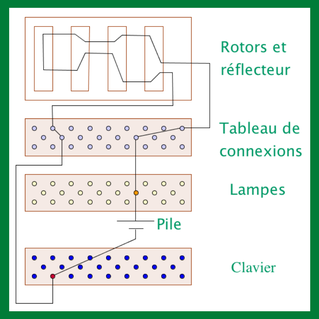
LES MACHINES DE CRYPOTGRAPHIE

La machine de cryptage la plus connue est la machine allemande Enigma, créée en 1918. Son utilisation est très simple puisqu'il suffit (après configuration) de rentrer un message lettre par lettre pour obtenir la lettre codée ou, s'il s'agit d'un message à décoder, la lettre décodée.

La machine est équipée d'un clavier pour saisir le message, de différents rotors pour le codage, d'un panneau de connexions et enfin d'un tableau lumineux pour afficher le résultat.

Lorsqu'une lettre est entrée sur le clavier, les rotors tournent, changeant la correspondance entre les lettres tapées et les lettres affichées.

Avec la rotation des rotors à chaque appui de touche ainsi que toutes les configurations de connexions possibles, les machines Enigma peuvent chiffrer un texte selon plus de 10^{20} combinaisons différentes !



La machine Enigma

1918

L'HISTOIRE DE LA CRYPTOLOGIE

Introduction:
La cryptographie a débuté dès l'antiquité, le premier document chiffré connu date du XVIeme siècle av. JC c'est un message recopié sans les consonnes et avec des voyelles modifiées Une des premières méthodes de cryptage répandue a été la technique des Hébreux (appelée aussi Atbash), au Vème siècle.

Code de César :
Plus tard le code César apparaît au Ier siècle av. JC. Son système consiste à décaler les lettres de l'alphabet d'un certain nombre, qui sera alors la clé de cryptage et décryptage. Cette méthode est peu sûre car il n'y a que 26 clés différentes possibles. Il suffit d'en connaître le principe et de tester ces 26 possibilités. Cependant il a souvent été réutilisé en raison de sa simplicité, par l'armée Russe en 1915 par exemple.

Code de Vigenère:
En 1586, le chiffre de Vigenère est créé par Blaise Vigenère. La méthode consiste à utiliser une clé que l'on choisit, composée d'une suite plus ou moins longue de lettres, qui sert à coder le message et à le décrypter.

Message à crypter	E	X	E	M	P	L	E
Clé répétée	C	L	E	C	L	E	C
Message crypté	G	I	I	O	A	P	G

- *Pour chaque lettre à crypter, on sélectionne la colonne correspondante.*
- *Pour chaque lettre à crypter correspond une lettre de la clé, on sélectionne la ligne correspondant à cette lettre de la clé.*
- *Au croisement de la ligne et de la colonne on trouve la lettre chiffrée.*
- *La lettre de la clé à utiliser est la lettre qui est placée au même endroit que la lettre à crypter, si le message à crypter a plus de lettres que la clé utilisée, alors on répète la clé.*

-1500

1978

CRYPTOLOGIE ASYMÉTRIQUE

Histoire :
Whitfield Diffie et Martin Hellman présentent le procédé en 1976. A cette époque ils n'ont pas encore d'application concrète mais estiment leur projet utile dans les années à venir.

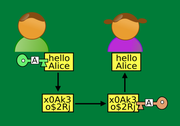
En 1978, Ronald Rivest, Adi Shamir et Leonard Adleman présentent le RSA : le système de chiffrement est basé sur le procédé asymétrique trouvé quelques années plus tôt. Le nom RSA vient des initiales des noms de ses trois créateurs : Rivest, Shamir, Adleman.

Principe :
Un grande différence existe entre le chiffrement symétrique et celui asymétrique : il faut deux clefs au lieu d'une seule.

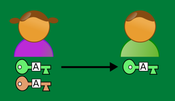
- **Une clef publique :** elle permet de chiffrer le message. Cette clef est diffusée sans aucun risque pour les messages.
- **Une clef privée :** elle permet de déchiffrer le message. Celle-ci est gardée secrète par le destinateur.

Ce système asymétrique est basé sur des propriétés mathématiques complexes, ce qui rend de décryptage compliqué. On peut chiffrer un message en ne connaissant uniquement la clef publique, mais on ne peut plus le déchiffrer.

Exemple :



Alice génère deux clés. La clé publique (verte) qu'elle envoie à Bob et la clé privée (rouge) qu'elle conserve précieusement sans la divulguer à quiconque.



Bob chiffre le message avec la clé publique d'Alice et envoie le texte chiffré. Alice déchiffre le message grâce à sa clé privée.

RSA :
Dans le système RSA, la clef est constituée de deux couples de nombres premiers. La sûreté du chiffrement dépend de leurs tailles : en général des clefs de plus de 2048 bits sont utilisées pour un minimum de sécurité.

Applications :

- Le RSA sert principalement à communiquer une clef de chiffrement symétrique qui servira à poursuivre l'échange de manière sécurisée,
- Ce système peut aussi servir à l'authentification avec signature numérique. Il est couplé à une fonction de hachage. Cette signature électronique sert à garantir l'intégralité d'un document électronique et d'en authentifier l'auteur. Elle correspond à une suite de nombres.

TRAN VAN BA Laurent ~ DUROUSSET Etienne ~ AMBROSINO Raphaël ~ SABATIE Félix ~ MARTINS Dylan ~ MICHUT Valentin