Synthèse documentaire : La Cryptographie.

I. Introduction :

Aujourd'hui dans cette synthèse, je vais expliquer de manière globale qu'est-ce la cryptographie et déborder un peu sur la cryptanalyse.
Nous aborderons en premier la notion de cryptographie (et son historique), pour enchainer sur un rapide exposé des différentes méthodologies de chiffrement dont l'existence a permis que la cryptographie devienne ce qu'elle est maintenant. Ensuite, expliquer les deux grandes familles de cryptosystèmes.

Par la suite nous enchainerons sur la notion de sécurité et cassage en lient avec la Cryptographie ; pour terminer des applications concrètes et sur les possibilités futures de ce domaine d'expertise.

II. La Cryptographie au fil du temps :

La cryptographie est une discipline permettant d'assurer la confidentialité, l'authenticité du contenu de leurs missives entre deux entités (personnes, organisation, institution, etc.).
Ainsi en utilisant des méthodes de chiffrement. On peut transmettre un message, souvent écrit, via un canal de communication peu sûr et avoir l'assurance qu'aucun autre individu ne peut comprendre le message.

Cette discipline existait déjà à l'Antiquité que ce soit :

- En Égypte il y a 2000 ans av.J, un scribe avait gravé des hiéroglyphes différents pour rendre le texte, relatant la vie de Khumhotep II sur sa pierre tombale, indéchiffrable.
- Pendant la Guerre des Gaules, où Jules César inventa une procédure de chiffrement de type substitution qu'on nommera Chiffre de César.
  Concrètement, il décalait la lettre qui voulait écrire de 3 par rapport à l'ordre de ceux-ci dans l'alphabet. Pour écrire a, il mettait D b devient E, X devient....

En outre, les avancées en cryptographie se font tout au long des différentes périodes. Que ce soit au Moyen Âge où les auteurs d'ouvrages dont le contenu serait en désaccord avec l'Église chiffrent leur nom pour qu'on ne les relie pas à leurs ouvrages.
Quant à l'époque de la Renaissance, il y a une explosion des connaissances qui se fait. Cela s'explique par l'invention de l'imprimerie, on reconnait la méthodologie par transposition et substitution comme des principes indissociable en cryptographie....

Ensuite vient l'époque des deux grandes guerres où la discipline est devenue une arme indispensable. L'exemple le plus parlant est la machine Enigma que l'état-major allemand développe pour automatiser les procédures de chiffrements.
Donc de la mécanique nous sommes passés à l'ordinateur engendrant ainsi des appareils de plus en plus performant dans le déchiffrement des messages chiffrés.

Ex. :
Les Bombes rapides pouvant réaliser 20 280 essais par seconde, ce qui permettait en moyenne de décrypter en 50 secondes les messages de l'Egnima à 3 rotors et en 20 minutes ceux de l'Enigma M4 (la possibilité de combinaison allait à 159. 10^{18})

III. Les systèmes chiffrement classiques et les deux grandes familles de cryptosystèmes.

Dans ce que l'on nomme par systèmes rudimentaires de chiffrement ce sont des procédures de chiffrement/déchiffrement qu'on utilise plus actuellement, mais ont permis de faire avancer la cryptographie.
Il existe deux types de chiffrements anciens : la substitution et la transposition.

Un chiffrement par substitution c'est le fait que lorsqu'on écrit le contenu du message qu'on envoie, écrit dans un alphabet. On va changer un caractère du message par un autre pour créer le message caché. Et donc pour rendre mon message caché en un message clair, on substitute le caractère changé dans le message par le bon caractère.

Il y en a quatre types de substitution en cryptographie classique :

- Le simple
- L'homophonique
- La polygamique
- La polyalphabétique

Un chiffrement par transposition se traduit par permuter l'entièreté de mon message clair en un message caché. Dès lors ce n'est pas un caractère ou un ensemble qu'on change, mais tous les caractères de mon message.

Voici deux procédés ayant pour base un chiffrement par transposition :

- Le XOR
- Le Masque jetable/One-Time Pad.

En ce qui concerne les deux grandes familles de chiffrement qui sont de véritable cryptosystème, ce sont : Chiffrement symétrique (ou chiffrement à clef secrète) et chiffrement asymétrique (ou chiffrement à clef publique).

Un chiffrement symétrique part du principe que la clef de chiffrement et de déchiffrement est la même et donc l'algorithme permettant de transmettre mon message caché et de retranscrire le message clair est le même.

Ex : DES, AES, masque jetable...

Et on divise cette famille en deux catégories : — Chiffrement par flots
— Chiffrement par blocs

Un chiffrement asymétrique part du principe que la clef de chiffrement et de déchiffrement est totalement différente. Ainsi A qui va envoyer un message va utiliser une clef publique pour crypter le message clair, alors que B va utiliser une clef privée pour décrypter le message caché.
De ce fait si quelqu'un récupère la clef publique, il ne pourra pas déchiffrer le message caché.

Ex. : RSA, DSA....

IV. Sécurité et Cassage.

En cryptographie on utilise des cryptosystèmes pour sécuriser des messages.
La question que l'on doit se poser en premier serait : comment protéger mon système contre ceux qui voudraient s'attaquer à lui ? Et en deuxième : Quelles méthodes que les attaquants utiliseraient pour le faire ?

Et c'est la qu'entre en compte la notion de Sécurité du système et les familles d'attaques cryptanalytique.

Pour savoir quel serait le niveau de sécurité d'un cryptosystèmes, on a inventé une classification :

> « *1) "Total break" : on est capable de trouver la clef K telle que* $C = D_K(M)$.
> *2) "Déduction globale" : l'attaquant est capable de trouver un algorithme alternatif pour le déchiffrement sans connaissance de la clef (c.-à-d., l'algorithme produit* D_K *[C] sans connaissance de K).*
> *3) "Déduction locale" (cassage ou craquage d'une instance) : l'attaquant est capable de trouver le message clair à partir du message chiffré.*
> *4) "Déduction partielle" : l'attaquant est capable d'obtenir une information partielle sur la clef ou le message clair. Par exemple, cela peut être la connaissance de quelques bits de la clef. »* [1]

En ce qui concerne les différentes familles d'attaque en cryptanalyse[2]. Il y en a beaucoup, mais les principales sont : l'analyse fréquentielle, l'indice de coïncidence, l'attaque par mot probable, l'attaque par dictionnaire, la taque par force brute et l'attaque par paradoxe des anniversaires.

I. Applications et futur de la cryptographie :

En terme d'application, la cryptographie était utilisée avant tout dans le domaine de la diplomatie et du militaire. Maintenant, elle est presque partout :

- Dans le domaine bancaire pour assurer la sécurité des échanges.
- La sécurité des réseaux informatiques.
- La sécurisation des moyens de communication comme les Emails, les téléphones, etc.

Pour le futur de la cryptographie, actuellement il y a la cryptographie quantique et le chiffrement harmonique qui est en train de se développer.

---

1 Cours1_FondementCrypto.pdf

2 Cryptanalyse : c'est la discipline opposer à la cryptographie qui a pour objectif d'accéder au message clair par le message caché en n'ayant pas la clef de déchiffrement.