# La Cryptographie

Les messages cryptés ou cachés ont toujours existé. Ils ont d'abord servi à retranscrire des idées puis ont été largement utilisés dans le domaine militaire...

En effet, les armées devaient pouvoir transmettre des messages confidentiels de manière sécurisée, soit en en dissimulant l’existence, soit en les rendant incompréhensibles à quiconque les trouverait.

Ensuite, la science a permis l’apparition des premières machines de chiffrement électromécanique (comme Enigma) qui constituent les bases de la cryptographie, à savoir l’élaboration d’un message inintelligible aux personnes non autorisées. Avec l’avènement des nouvelles technologies (notamment de l’informatique), la cryptographie prend une nouvelle dimension. Du domaine militaire aux communications par Internet, en passant par les transactions commerciales et bancaires, il est difficile d'y échapper.

Ainsi, la cryptographie s'élargit du domaine "confidentiel" de la sécurité nationale ou de la protection des entreprises à la consommation de masse par les particuliers ( commerce électronique via Internet, confidentialité des mails, ... ).

Il est à noter que la France est resté en retard par rapport à certaines nations comme les Etats-Unis.

Alors que la cryptographie progresse, la cryptanalyse (craquage des codes cryptés), elle, change d'acteurs et d'objet. Jusqu'alors arme militaire et jeu de quelques génies, elle devient une véritable arme de vol à grande échelle (détournement de codes de carte bleue, de fonds,...) et de guerre économique (vol de secrets industriels ou commerciaux). C’est pourquoi une méthode de cryptage se doit d’être sûre.

Le but de ce T.I .P.E. est donc d’étudier les différentes méthodes de cryptage. Cette étude fait appel à deux domaines distincts que sont les mathématiques et l’informatique. Face à la diversité et au nombre de méthodes de cryptage qui existent, nous avons décidé d’insister sur 3 d’entre elles ( les plus importantes ) : le RSA, l’IDEA et le DES.

Le dossier complet en lien !

Proposé par Manue de chez notre partenaire :
NousOnLine

*Par*

**Publié sur Cafeduweb - Archives le jeudi 13 juin 2002**
Consultable en ligne : http://archives.cafeduweb.com/lire/1927-cryptographie.html