LA CRYPTOGRAPHIE

Matthieu IZAC – BTS SIO1 – 2022/2023

SOMMAIRE

Qu'est-ce qu'est la cryptographie ?

Dès que les hommes apprirent à communiquer, ils durent trouver des moyens d'assurer la confidentialité d'une partie de leurs communications : l'origine de la cryptographie remonte sans doute aux origines de l'homme. En effet, le mot cryptographie est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages c'est-à-dire de les rendre inintelligibles sans une action spécifique. Du bâton nommé « scytale » au Vie siècle avant JC, en passant par le carré de Polybe ou encore le code de César, on assista au développement plus ou moins ingénieux de techniques de chiffrement expérimentales dont la sécurité reposait essentiellement dans la confiance que leur accordaient leurs utilisateurs.

Après la première guerre mondiale a lieu une première révolution technologique. Mais ce n'est qu'à l'avènement de l'informatique et d'Internet que la cryptographie prend tout son sens. Les efforts conjoints d'IBM et de la NSA conduisent à l'élaboration du DES (Data Encryptions Standard), l'algorithme de chiffrement le plus utilisé au monde durant le dernier quart du XXème siècle. A l'ère d'Internet, le nombre d'applications civiles de chiffrement (banques, télécommunications, cartes bleues,...) explose. Le besoin d'apporter une sécurité accrue dans les transactions électroniques font naître les notions de signature et authentification électronique.

Le code Cesar

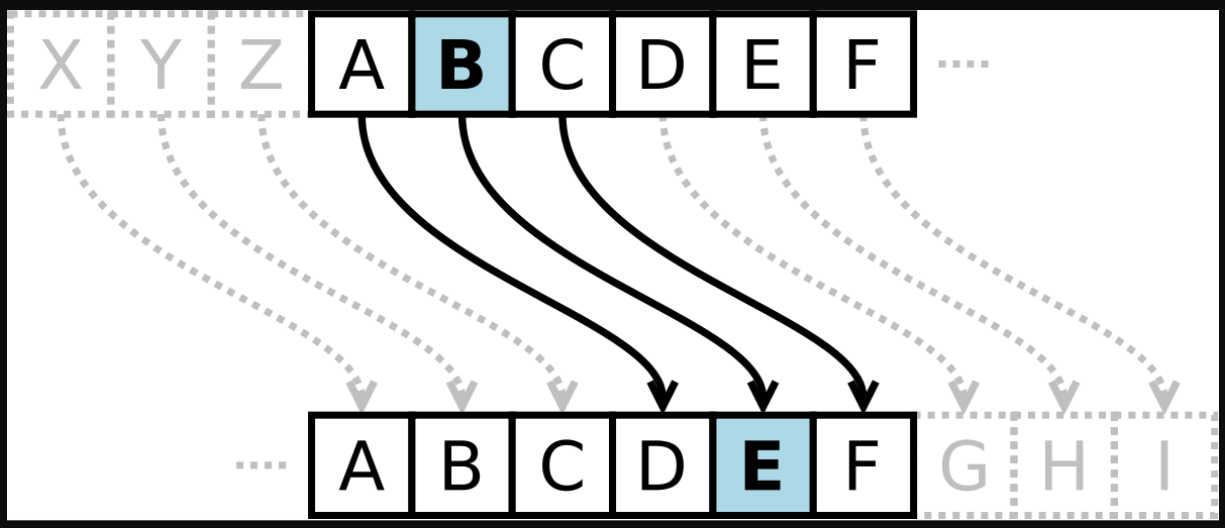
L'un des systèmes les plus anciens et les plus simples est le codage par substitution mono alphabétique (ou alphabets désordonnés). Il consiste à remplacer chaque lettre par une lettre différente. Il existe donc grâce à cette technique 26 façons de coder un message, ce qui fait que ce système a été longtemps utilisé par les armées pendant l'antiquité. Ce procédé très fiable à l'époque est tout de même problématique car il nécessite que les interlocuteurs se souviennent tous deux de la clef. De plus, il est évident que la sûreté de ce codage est quasi nulle et qu'il pourrait être déchiffré par n'importe quelle personne qui y mettrait le temps nécessaire.

Voici un exemple de substitution :

Texte clair A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Texte codé W X E H Y Z T K C P J I U A D G L Q M N R S F V B O

Malheureusement il n'y a que 26 façons différentes de chiffrer à l'aide de ce code ce qui en fait un code très peu sûr. Mais ce qui est d'autant plus insolite, c'est le fait que ce code de « César » est encore utilisé de nos jours sur Internet avec le ROT13 (rotation de 13 lettres) qui consiste à cacher des messages afin qu'ils ne soient pas lus involontairement, comme par exemple s'ils dévoilent le dénouement d'un film ou encore qui donne la réponse à une devinette.



Conclusion ?

Dans un monde quasi informatisé, où le principal actif des entreprises et des individus est l'information, qu'elle soit privée, comme les coordonnées bancaires, ou confidentielle, comme les stratégies de marché, nous avons besoin de cryptographie et de cyber sécurité pour garantir que les communications et les transferts d'informations soient aussi efficaces que possible. sûrs, et aucun intermédiaire n'essaie d'y accéder ou de les voler directement.