Chapitre 12 : Cryptographie et sécurisation des communications

12.1 Principe et introduction

Depuis la naissance de l'écriture l'Homme a cherché à maintenir secrètes certaines communications. Dans de nombreux domaines tels que les champs politique, militaire, économique, amoureux, etc. il est nécessaire de disposer d'une forme de communication chiffrée. Dans le cas de la cryptographie, il ne s'agit pas de dissimuler un message (par exemple dans un autre texte, dans une image ou à l'encre invisible) mais de le rendre incompréhensible à ceux qui ne possèdent pas la clé de déchiffrement.
La cryptographie est utilisée depuis l'antiquité, l'une des utilisations les plus célèbres pour cette époque est le chiffre de césar, nommé en référence à Jules César qui l'utilisait pour ses communications secrètes. Mais la cryptographie est bien antérieure à cela, une des traces les plus anciennes de messages chiffrés remonte au XVe siècle avant J.C.

Définition 1
Les principes communément adoptés pour caractériser un système de chiffrement sont au nombre de trois :

1. Le système doit être mathématiquement « indéchiffrable » (reste à definir ce que l'on entend par indéchiffrable).
2. La méthode de chiffrement n'a pas à être secrète, la méthode ou l'algorithme de chiffrement peut être divulguée sans mettre en péril le chiffrement.
3. La clé de chiffrement doit pouvoir être simple à retenir et facilement communiquable, modifiable.

Noter que les chiffrements de cesar et affine vérifient ces trois conditions s'il on accepte qu'à une époque elles étaient indéchiffrables.

12.2 Le chiffrement symétrique

a. Principe

Tous les schémas de chiffrement utilisés jusque dans les années 1970 sont dits symétriques, ce qui signifie que la même clé est utilisée pour chiffrer et pour déchiffrer. On les appelle également schémas de chiffrement à clé secrète.
Une analogie couramment utilisée est celle du coffre-fort. L'expéditeur et le destinataire utilisent un coffre-fort partagé pour s'échanger des messages. Tous deux ont accès à la clé, aussi bien pour déposer des messages que pour en retirer.

Propriété 1
Les systèmes de chiffrement symétrique sont composés de trois algorithmes :

- un algorithme de génération de clé, qui retourne en sortie une clé secrète K partagée entre les deux utilisateurs ;
- un algorithme de chiffrement, qui prend en entrée un message m (secret) et cette clé K (secrète) et renvoie un message C (chiffré) ;
- un algorithme de déchiffrement, qui prend en entrée un message chiffré C (public) et la clé K (secrète) et renvoie le message clair m (secret).