

Cryptographie et théorie des nombres

ARSIC Marko et ROBACHE William

15/01/2021

1.Introduction

La cryptographie moderne s'est développée simultanément aux recherches et aux avancées sur la théorie des nombres. Cette branche des mathématiques a émergé au milieu du XX^{ème} siècle dans la recherche en technologie de l'information, en et à joué notamment un rôle important dans la théories des codes et la cryptographie.

La cryptographie qui, autrefois, était un domaine réservé aux militaires a trouvé de nombreuses applications dans le domaine du grand public. Elle a vu son utilisation se démocratiser et s'expandre dans de nombreux secteurs d'activité. Elle est notamment utilisée pour garantir la confidentialité des échanges sur Internet, pour protéger des données sensibles dans les entreprises, pour garantir l'identité des parties contractantes en introduisant des protocoles de signature en particulier sur Internet. Les chaînes de télévision utilisent des systèmes de cryptage pour pouvoir faire payer leurs téléspectateurs. Le secteur bancaire est sûrement le secteur qui utilise le plus la cryptographie. L'existence même des banques directes n'a été rendue possible que grâce aux avancées dans le domaine de la cryptographie (notamment le cryptage asymétrique à clé publique).

2.Cryptage à clé symétrique On parle de cryptage à clé symétrique lorsque la connaissance de la clé de codage permet directement d'en déduire la procédure de décryptage. Ainsi en cryptographie symétrique une seule clé secrète sert à la fois pour le chiffrement et le déchiffrement des messages.

2.1 Codage César Le système du codage César est un système dit de substitution. C'est l'ancêtre des systèmes de cryptage. Comme son nom l'indique il est attribué à Jules César qui l'utilisait pour communiquer secrètement avec ses armées.

Le système revient à faire un décalage sur l'alphabet. On choisit une clé qui correspond à une lettre. On code la lettre en chiffre en prenant l'ordre de l'alphabet $A = 0$ $B = 1$ etc...

Ensuite, on décale chaque lettre de l'alphabet en ajoutant la clé. Lorsque la lettre codée dépasse Z , on revient au début de l'alphabet. On peut bien sûr utiliser ce cryptage uniquement avec des nombres en prenant le congru modulo 26.

A l'origine César utilisait un alphabet de 31 lettres puisqu'il y ajoutait les symboles espace , . et ? et il utilisait la clé D puisqu'il ajoutait 3 aux lettres.

2.2 Codage Vigenère Le codage Vigenère est une complication du codage César. Le principe est le même sauf que le décalage sur les lettres dépend de la position de la lettre. On choisit donc une clé qui est un mot.

Exemple : BBC

La clé choisie est de taille 3, ce qui veut dire que toutes les lettres modulo 3 se codent suivant le même décalage sur l'alphabet.

2.3 Les limites du cryptage à clé symétrique Le principal défaut d'un système de cryptage à clé symétrique est la transmission de la clé. Effectivement, pour pouvoir recevoir des messages cryptés, il faut transmettre la clé de cryptage et ce de façon secrète.

Par conséquent, les protagonistes doivent d'abord avoir accès à un canal sécurisé pour établir la clé secrète commune dont ils se serviront pour communiquer plus tard. Le canal sécurisé prend typiquement la forme d'une réunion face-à-face, mais peut être un courrier fiable qui transporte la clé entre les protagonistes de la communication. Ces cryptosystèmes sont sûrs et efficaces, mais le besoin d'un canal sécurisé limite leur utilité dans de nombreuses situations pratiques. De plus la connaissance de la clé de cryptage est aussi suffisante pour décrypter tous les messages.

3. Cryptage à clé asymétrique

Le système de cryptage à clé symétrique peut être comparé à un système de coffre-fort dans lequel on peut mettre des messages. Pour pouvoir y mettre un message ou lire un message on utilise la même clé. Le système à clé asymétrique peut, quant à lui, être comparé à un système de boîte aux lettres. N'importe qui peut laisser un message au récepteur, mais seul le récepteur peut lire les messages en vérifiant sa boîte avec sa clé privée.

3.1 Fonctions à sens unique On appelle fonction à sens unique une fonction qui à x associe $f(x)$ dont la bijection réciproque est difficilement exprimable. Autrement dit, connaissant $f(x)$ on ne peut pas retrouver x bien que connaissant f . En fait, il est presque toujours théoriquement possible de retrouver la clé, en procédant par exemple de façon itérative. On définit donc différents niveaux de difficulté de ce type de problème mathématiques.

Exemple d'utilisation :

Pour protéger l'accès à votre ordinateur, ce dernier vous demande un mot de passe. Une solution pour vérifier l'identité de l'utilisateur serait donc de contrôler directement l'exactitude du mot de passe. Cependant, cette solution nécessiterait d'écrire quelque part sur votre disque dur ce mot de passe. Un pirate averti aurait tout le loisir de le trouver sur votre disque dur et le système ne serait pas fiable. La solution retenue est donc d'utiliser une fonction à sens unique, d'appliquer cette fonction au mot de passe entré par l'utilisateur et de le comparer au résultat écrit sur votre disque dur. Même si un pirate pouvait trouver ce résultat, il ne pourrait pas en déduire votre mot de passe initial, étant donné qu'il s'agit d'une fonction à sens unique. Autre illustration... CB

3.2 Fonction à sens unique avec trappe On dit qu'une fonction à sens unique est avec trappe lorsque l'inversion est impossible sauf avec une clé secrète.

Soit donc f_C la fonction de cryptage utilisée pour la transmission. Le récepteur R possède grâce à sa trappe une fonction de décryptage f_D .

3.2.1 Principe de chiffrement Le récepteur du message annonce publiquement sa fonction de cryptage f_C et conserve dans un lieu secret sa fonction de décryptage f_D .

Tout émetteur peut alors envoyer un message m en procédant ainsi :

Au lieu d'envoyer le message m par la poste en prenant le risque que quelqu'un n'intercepte le message, il envoie $M = f_C(m)$.

Ainsi, toute personne interceptant ce message ne peut le lire, le seul récepteur peut décrypter ce message en utilisant sa fonction de décryptage privée f_D .

Effectivement,

$$f_D(M) = f_D[f_C(m)] = m$$

3.2.2 Principe de signature Un procédé de signature numérique consiste à adjoindre au texte clair un petit nombre de bits qui dépendent simultanément du message et de son auteur. Pour que ce système soit efficace, il faut bien sûr que tout le monde puisse vérifier la provenance de la signature et que personne ne puisse l'imiter. Il y a donc une fonction de signature privée et une fonction de vérification.

Un schéma de signature garantit donc :

- l'identité de la personne émettrice

- l'intégrité des données reçues, et donc l'assurance que le message n'a pas été modifié ou altéré

- il faut aussi qu'il soit impossible à l'auteur de nier le contenu du message.

Au niveau juridique, la signature numérique est une preuve au même titre que la signature manuscrite depuis la loi du 13 mars 2000.

Le même système que précédemment peut alors être utilisé par le récepteur R pour apposer une signature numérique.

En effet, supposons que R veuille envoyer un message afin que la personne P qui reçoit ce message soit sûre que celui-ci provienne de R .

Dans ce cas, il suffit à R d'envoyer $f_D(m)$. P reçoit alors ce message et il applique la procédure f_C sur ce message pour authentifier l'expéditeur. Si le message provient bien de R alors il retrouve un message cohérent.

La fonction de signature est donc la fonction privée de décryptage f_D . La fonction de vérification ou d'authentification est la fonction publique de cryptage f_C .