Cryptographie et théorie des nombres

ARSIC Marko et ROBACHE William

22/01/2021

---

1 Introduction

La cryptographie moderne s'est developpée simultanéement aux recherches et aux avancées sur la théorie des nombres.Cette branche des mathématiques a emergé au milieu du XXème 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 Vigénère

Le codage Vigénère 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 les clé entre les protagonistes de la communication. Ces cryptosytèmes 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 retrover 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'usager 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.

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 un clé secrète.
Soit donc f_C la fonction de cryptage utilisée pour la transmission. Le récepteur R possède grâce à sa trappe une fonctio 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 reçoive 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 m 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.

3.2.3 Principe de chiffrement authentifié

Pour un chiffrement authentifié, l'émetteur et le récepteur communiquent leur fonction de cryptage. Pour envoyer un message, il suffit alors de le signer avec sa propre fonction de décryptage, puis, de crypter le résultat avec la fonction publique de cryptage du récepteur. Le récepteur, quant à lui, utilise sa fonction de décryptage privée pour déchiffrer le message. Ensuite, pour lire le message, il lui suffit de l'authentifier en utilisant la fonction de cryptage publique de l'émetteur.

3.3 Le système RSA

Ce système a été créé par Rivest, Shamir etAdleman en 1978. Son principe repose sur une fonction à sens unique avec trappe; il peut donc être utilisé comme mécanisme de chiffrement ou de signature.

La confidentialité du système est basé sur la difficulté de factoriser un nombre qui est le produit de deux grands nombres premiers. Ce problème fait effectivement parti des problèmes dits difficiles en mathématiques.

La fonction de cryptage est l'exponentation à la puissance e modulo n, où e est appelé clé d'encryptage et n est le modulo du cryptage (il s'agit d'un cryptage par bloc).

La fonction de décryptage est l'exponentation à la puissance d modulo n, où d est appelé clé de décryptage.

Pour que le système fonctionne, il faut que n soit choisi de façon à être le produit de deux nombres premiers p et q.

Ensuite e et d doivent être choisis de façon à ce que

$$e.d \equiv 1[(p-1)(q-1)]$$

Bien sûr, puisque e est connu de façon publique, et que l'inverse d'un nombre modulo n est facilement trouvable en utilisant l'algorithme d'Euclide, il faut qu'il soit difficile de trouver p et q.

Donc effectivement, tout est basé sur la difficulté de factoriser le modulo n et de retrouver les nombres premiers p et q qui le composent.

Bien sûrr, ce système peut être utilisé à la fois pour du chiffrement ou de la signature numérique.

- Avantage : on peut utiliser RSA sur internet à partir du moment o'u l'on est sur que la clé publique provient bien de l'émetteur.
- Inconvénient : ce protocole est relativement lent pour crypter des données et il est difficile d'échanger en direct sur internet par exemple. Les systèmes de cryptage à clé symétriques sont bien plus rapides.

3.4 Le système RSA authentifié

Le système RSA authentifié est un système de cryptage entre un émetteur Alfred et un récepteur Bertrand. Les échanges sont à la fois cryptés et donc uniquement lisibles par le récepteur, mais aussi signés par l'émetteur de sorte que le récepteur est sûr que le message provient de l'émetteur.

Chacun des participants utilise un cryptage RSA. L'émetteur A choisit donc sa base de cryptage n_A et sa clé d'encryptage e_A et il possède sa clé privée d_A.

Le récepteur B, quant à lui, choisit sa base de cryptage n_B et sa clé d'encryptage e_B et il possède sa clé privée d_B.

- Remarque : Le modulo du cryptage réel doit être inférieur au min de n_A et n_B sinon certains messages se coderont de la même façon et le cryptage ne sera pas bijectif.

L'émetteur signe alors son message en utilisant sa fonction de signature (qui n'est autre que sa fonction de décryptage privée) et trouve M. Il crypte alors le message M en utilisant la clé publique du récepteur et peut envoyer son résultat au récepteur.

Pour retrouver le message initial, le rcepteur doit décrypter classiquement son message en utilisant sa fonction de décryptage. Puis il lui reste à authentifier la provenance en utilisant la fonction de vérification qui n'est autre que la fonction de cryptage publique donnée par l'émeteur.

3.5 Méthode de Diffie et Hellman

La méthode de Diffie et Hellman (1976) permet à deux interlocuteurs de se mettre d'accord sur une clé privée commune.

L'intérêt du mécanisme est que les échanges d'information peuvent se faire de façon publique. Appelons Alex et Barbara les interlocuteurs, le processus est le suivant :

Alex et Barbara se mettent tout d'abord d'accord sur un grand nombre premier n commun. De plus, ils choisissent un entier (clé publique) p.

Ensuite Alex choisit A sa clé privée et Barbara choisit B sa clé privée.

Alex envoie alors $\beta = pA$ modulo n et Barbara envoie $\alpha = p^B$ modulo n.

Il reste à Alex à calculer $\alpha^A[n]$ pour obtenir la clé privée commune à Alex et Barbara.

De même Barbara obtient la même clé en calculant $\beta^p[n]$.
Cette clé commune est donc $p^{AB}[n]$. Ce principe est utilisable par exemple sur le réseau internet.

4 Cryptage en ligne

Pour le cryptage en ligne, il n'est pas possible d'utiliser des systèmes du type RSA car ils sont trop demandeurs en calculs pour les processeurs actuels. On utilise donc généeralement un système d'échange de clé par une procédure type RSA ou Diffie et Hellman. Puis on utilise un système de cryptage à clé symétrique de type transposition ou utilisant des opérateurs booléens comme par exemple DES (algorithme un peu vieux) ou triple DES ou AES.

5 Et l'informatique quantique ?

La démocratisation des ordinateurs quantiques pourrait changer la façon de penser la cryptographie, en introduisant un nouveau modèle de computation.

Shor a trouvé des algorithmes en temps polynômiaux pour la factorisation des entiers et le problème du logarithme discret sur un ordinateur quantique hypothétique.

Dans le monde post-quantique, RSA ainsi que la cryptographie à courbes elliptiques s'effondreront, alors que la cryptographie à base de réseaux (ainsi que certains systèmes utilisant des codes correcteurs d'erreurs, entre autres) ont une chance de survie.

Pour le moment, il s'agit de voir si un ordinateur quantique fiable sera réalisé de notre vivant, et quelles en seront les conséquences pratiques.

Références

[1] David Kohel & Igor E.Shparlinski, “Théorie des nombres et cryptographie”
[2] Pierre Rouchon, “Cryptographie et théorie des nombres”
[3] James S.Kraft & Lawrence C.Washington, ”An Introduction to Number Theory with Cryptography