# LE CHIFFREMENT RSA

Dans la fiche n° 3 sur les procédés de chiffrement par substitution, nous avons vu qu'il existait un mode de chiffrement inviolable, qui ne pouvait pas être décrypté : le chiffrement à l'aide d'un tableau de Vigenère avec une *clef aléatoire utilisée une seule fois*.

Cependant, ce procédé présente des inconvénients pratiques majeurs : la communication des clés en toute sécurité et de façon simple entre les expéditeurs et les destinataires des messages est assez difficile. De plus, si le volume des messages est important, il nécessite un nombre considérable de clés, ce qui complique encore plus leur communication. Lorsque le destinataire est une unité militaire sur le terrain ou un sous-marin, on voit bien le problème logistique qui est posé avec en plus le risque de l'interception des clefs lors de leur communication aux destinataires.
En résumé, c'est le problème bien connu en cryptographie de *la distribution de la clef.*

## 1. Les précurseurs : l'algorithme d'échange de clés Diffie-Hellman-Merkle

Dans les exemples donnés sur le fonctionnement de ces chiffrements, il y a trois personnages imaginaires : Alice, Bob et Ève. Alice envoie des messages à Bob et Ève les espionne.

Whitley Diffie et Martin Hellman et Ralph Merkle sont des cryptographes américains. En 1976, ils ont inventé un système fonctionnant de la façon suivante :

Alice veut envoyer un message à Bob. Elle met ce message dans un coffret en fer, met un cadenas et l'envoie à Bob. Lorsqu'il reçoit le coffret, Bob ajoute son propre cadenas et le renvoie à Alice. Alice reçoit donc le coffret muni de deux cadenas. Elle retire le sien, en ne laissant que le cadenas de Bob. Enfin elle le retourne à Bob, qui peut ouvrir son propre cadenas avec sa propre clef.

On a bien compris l'analogie : les cadenas sont un procédé de chiffrement. Alice chiffre son message avec sa clé et l'envoie à Bob. Bob le chiffre et le renvoi à Alice. Alice le déchiffre et le renvoie à Bob qui le déchiffre. Mais il y a un problème : si ça fonctionne en théorie, en pratique ce n'est pas possible car l'ordre dans lequel intervient les chiffrement et les déchiffrements a son importance. Il doit obéir à la loi : *« dernier mis, premier enlevé »*.Autrement dit , le dernier chiffrement effectué doit être le premier à être enlevé. Si la chronologie des chiffrements avec la clef n'est pas respectée, ce qui est le cas dans le schéma proposé, ça ne fonctionne pas.

Comme ce système à deux cadenas ne pouvait pas s'appliquer, Diffie et Hellmann passèrent des mois à essayer trouver une solution pour contourner le problème. Ils concentrèrent leurs efforts sur diverses fonctions mathématiques, en particulier les fonctions à sens unique.

Si l'on considère une fonction classique y = 2x + 3, il est facile de calculer y avec une valeur de x donnée. Si l'on veut inverser la fonction, c'est à dire trouver x avec une valeur donnée de y, la fonction devient x = (y-3) / 2. Il n'est pas difficile de l'inverser.

Ce qui intéressait Diffie et Hellman, c'était *les fonctions à sens unique,* c'est à dire une fonction qu'il est impossible d'inverser : une fonction non-réversible. Une fonction modulo, par exemple, est une fonction à sens unique. Ils travaillèrent donc sur les fonctions modulo.

L'arithmétique modulo est relativement simple : le résultat d'une fonction modulo est le reste de la division de 2 nombres entiers.

Exemple : 17 modulo 6 est égal à 5, parce que 17 divisé par 6 = 2 , que 6 x 2 = 12 et 17 - 12 =5. Donc le reste de la division de 17 par 6 est égal à 5.

Autre exemple : 99 (mod 13) = 8 puisque 99 divisé par 13 = 7, et 7 x 13 = 91. Donc le reste de la division est égal à 99 – 91 = 8

Considérons maintenant la fonction $f(x) = 3^x \pmod 7$ et calculons sa valeur pour x = 1, 2, 3 etc.

Le tableau suivant nous donne la valeur de f(x) :

| X | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $3^x$ | 3 | 9 | 27 | 81 | 243 | 729 | 2 187 | 6 561 | 19 683 | 59 049 | 177 147 | 531 441 |
| $3^x \bmod 7$ | 3 | 2 | 6 | 4 | 5 | 1 | 3 | 2 | 6 | 4 | 5 | 1 |

Essayons maintenant de calculer la valeur de la fonction réciproque à partir d'une valeur de x.

Si l'on suppose f(x) = 2, c'est à dire $3^x$ (modulo 7) = 2, on voit qu'il y a plusieurs solutions : x = 2, x = 8 etc. Si l'on travaille sur des petits nombres, il est relativement facile trouver x, même si le calcul est un peu fastidieux.

Mais si au lieu de $f(x) = 3^x \pmod 7$ on prend la fonction

$$f(x) = 453^x \pmod{21\,997}$$

les choses se compliquent un peu : on voit qu'il est relativement facile d'attribuer une valeur à x et de calculer f(x), mais si l'on attribue une valeur à f(x), par exemple 5 787, et que l'on écrit :

$$f(x) = 453^x \pmod{21\,997} = 5\,787$$

il sera quasi impossible de trouver la valeur de x. On ne peut pas inverser cette fonction, c'est une fonction à sens unique.

Au printemps 1976, après deux ans de travail sur ces fonctions, Hellman parvint à résoudre le problème de l'échange de clefs. Il prouva qu'en utilisant les propriétés des fonctions à sens unique, *Alice et Bob pouvaient établir une clef secrète, sans se rencontrer*. A partir de 2 nombres échangés entre eux, plus un nombre choisi par Alice et un nombre choisi par Bob, chacun gardant secret son nombre. Alice et Bob peuvent définir une même clef qu'ils peuvent utiliser pour chiffrer un message.

Si Ève, la méchante, intercepte les messages, elle aura connaissance des nombres échangés, mais pas des deux nombres secrets, et il lui sera impossible de déchiffrer ces messages.

Cette découverte est fondamentale, car elle est totalement *contraire à l'intuition scientifique.* Elle obligea les cryptographes à réviser complètement les règles du chiffrement.

Pour ne pas alourdir cette fiche qui est une initiation, nous ne décrirons pas mathématiquement ce procédé de calcul que l'on trouve par ailleurs facilement sur Internet ou dans le livre *Histoire des codes secrets* de Simon Singh. Il est plus important de comprendre les concepts qui régissent ces types de chiffrement. Par contre, nous verrons en détail l'aspect mathématique du procédé de chiffrement RSA, qui en est dérivé, dans le paragraphe suivant.

*Hellman a renversé un des piliers fondamentaux de la cryptographie et prouvé qu'Alice et Bob n'avaient pas besoin d'échanger une clef commune.* Ensuite, il suffisait de trouver un schéma un petit peu plus efficace pour que le problème de la distribution des clefs soit totalement surmonté. Ce fut Whitfield Diffie qui le trouva.

Whitfield Diffie eut l'idée géniale d'un nouveau type de chiffre, qui utilisait *une clef asymétrique.*

Voici le principe :

Le destinataire du message créé une clé publique et une clé privée. La personne qui veut lui adresser un message le chiffre avec la clé publique que tout le monde connaît et envoie le message. A la réception, le destinataire déchiffre avec sa clé privée connue de lui seul.

Soyons encore plus clair : dans un système de chiffrement traditionnel, l'expéditeur chiffre le message avec une clef et l'adresse au destinataire. Ce destinataire connaît la clef de chiffrement, qui a été échangée avec l'expéditeur, et déchiffre le message. Dans le chiffrement RSA, ce n'est pas l'expéditeur qui chiffre avec sa clé : il chiffre avec une clef donnée par le destinataire et connue de tous.

Prenons une analogie avec une boite et des cadenas :

N'importe qui peut fermer un cadenas en appuyant dessus. Mais seule la personne qui a la clé du cadenas peut l'ouvrir. Tout le monde peut verrouiller (chiffrement), mais seul le possesseur de la clé peut déverrouiller (déchiffrement).

L’idée de Diffie est que la clé qui sert à chiffrer n’a aucune raison d’être semblable à la clé qui sert à déchiffrer. De ce fait la clé qui sert à chiffrer peut-être connue de tous, et même le message chiffré. Seule la clef privée permettra de déchiffrer.

Cela dit, s’il avait conçu le concept général de chiffre asymétrique, Diffie n’avait aucun exemple concret à proposer. Le concept était génial, mais personne ne savait comment le mettre en musique.

Il fallait trouver une fonction mathématique qui fasse le même travail et qui puisse être intégrée dans un système opérationnel de chiffrement.

Diffie publia les grandes lignes de son idée au cours de l’été 1975. D’autres mathématiciens se mirent à la recherche de la fonction requise pour créer un chiffrement asymétrique. Diffie, Helman et Merkle poursuivirent leurs recherches à l’université de Stanford (Californie). Ils ne réussirent pas à trouver de solution. Ce furent trois autres chercheurs qui y parvinrent : Ron Rivest, Adi Shamir et Leonard Adleman.

## 2. Le chiffrement RSA

Ron Rivest, Adi Shamir et Leonard Adleman étaient chercheurs et travaillaient tous les trois au Laboratoire d’informatique du MIT (Massachusetts Institute of Technology) près de Boston.


Ronald **R**ivest, Adi **S**hamir et Leonard **A**dleman

Les initiales de leurs noms ont formé le nom du mode de chiffrement.

Ils travaillèrent plusieurs années à la recherche d'une fonction à sens unique pour résoudre le problème d'une clef asymétrique. En avril 1977, une nuit, Rivest eut une inspiration sur la façon de générer un chiffre asymétrique. Il passa la fin de la nuit à formaliser son idée et le matin il avait rédigé un texte. C'était Rivest qui a fait la découverte, mais comme ils travaillaient ensemble depuis plus d'un an sur le problème, Rivest insista pour signer l'article de leurs trois noms.

**Le concept du chiffrement RSA :**

Dans tous les systèmes de chiffrement classiques, on utilise la même clef pour chiffrer et déchiffrer un message. C'est un chiffrement dit « symétrique ».

*Le chiffrement RSA repose sur le principe suivant :*

Reprenons nos trois personnages : on convient que Alice est destinataire des messages et souhaite en recevoir de la part de Bob et d'autres personnes. Il y a toujours Ève, la méchante, qui veut intercepter le message.

Alice souhaite recevoir des messages : elle va fabriquer des centaines de cadenas tous identiques, mais seule sa clef pourra les ouvrir. Alice envoie ces cadenas dans des bureaux de postes partout à travers le monde. Bob veut envoyer un message à Alice. Il le met dans une boîte, va à son bureau de poste, demande un cadenas d'Alice et verrouille la boite avec la cadenas. Il expédie la boite. A sa réception, seule Alice peut ouvrir la boite. Si Ève intercepte la boîte, elle ne peut pas l'ouvrir, elle n'a pas la clé.

On a bien compris l'analogie : les cadenas distribués partout sont la clé publique d'Alice et la clé du cadenas est sa clé privée.

Reste à trouver l'algorithme, c'est à dire les opérations mathématiques qui vont réaliser la chose ! C'est ce que réalisa Ron Rivest.

**3. Concrètement, les mathématiques du chiffrement RSA :**

**Création de clefs par Alice**

Afin de pouvoir recevoir des messages, Alice va donc créer une *clé publique*.
Pour se faire, elle choisit deux nombres entiers et premiers, p et q. Elle effectue leur produit pour déterminer un nombre N tel que :

$$N = p \times q$$

Pour illustrer, nous allons prendre par exemple p = 17 et q = 11, soit N = 17 x 11 = 187.

*L'essentiel de la méthode est déjà présent* : il repose sur le fait que connaissant N, il est très difficile et très long de calculer p et q. Dans l'exemple, c'est facile. Mais dans la réalité, p et q sont des

nombres de 100 chiffres, donc N fait 200 chiffres. Et là, il faut un temps quasi infini à un ordinateur pour décomposer N en deux facteurs premiers.

Alice va ensuite choisir un autre nombre, **e**, qui est plus petit que le nombre (p-1)(q-1) et qui est premier avec (p-1)(q-1). C'est à dire tel que le PGCD de **e** et de (p-1)(q-1) soit égal à 1. Prenons par exemple **e = 7.**
Dans l'exemple, on calcule aisément (p-1)(q-1) = 160

**Ces deux nombres, N et e, constituent la clef publique d'Alice.** Alice peut publier sa clé sur un annuaire, par exemple Internet. Dans l'exemple, elle va publier : **RSA, 187, 7.**

Ensuite, Alice va calculer sa clef secrète, **d**. Ce nombre d est tel que

$$(e \times d) \bmod [(p-1)(q-1)] = 1$$

C'est à dire dans notre exemple (7 x d) mod (160) = 1

**Ce nombre d est la clef privée d'Alice et elle la garde secrète.**

Dans l'exemple, on aura **d = 23.** On a en effet 23 x 7 = 161 et 161 (mod 160) = 1. Calculer la valeur de **d** n'est pas immédiat, mais l'algorithme d'Euclide permet à Alice de trouver **d** facilement et sûrement. L'important est que puisque p et q sont inconnus de tous, il n'y a qu'Alice qui puisse calculer le produit (p-1)(q-1) et donc sa clef secrète **d.**

**2. Chiffrement et envoi du message par Bob**

Bob veut envoyer un message à Alice. Supposons le message

Clair : VIVE LES VACANCES

Il le transforme en nombres en remplaçant chaque lettre par son rang dans l'alphabet :

Clair : 22 09 22 05 12 05 19 22 01 03 01 14 03 05 19

Désignons par « blocs B» ces nombres de 2 chiffres dont chacun représente une lettre. Bob va chiffrer chaque nombre B à l'aide du nombre N et du nombre e d'Alice (qui sont publiques) en le transformant en un nombre C selon la relation :

$$C = B^{e} \pmod N \quad \text{c'est à dire} \quad C = B^{7} \pmod{187}$$

Le message clair est donc chiffré ainsi :

Chiffré : 044 070 044 146 177 146 145 044 001 130 001 108 130 146 145

Bob adresse ce message chiffré à Alice

### 3. Réception et déchiffrement du message par Alice

A la réception du message, Alice va inverser le processus à l'aide de sa clé secrète d.

A partir de chaque nombre chiffré C, elle va calculer B selon la formule :

$$B = C^d \pmod N \quad \text{c'est à dire } B = C^{23} \pmod{187}$$

Avec ce calcul, le message chiffré : 44 70 44 146 177 146 145  044 001 130 001 108 130 146 145

redevient : 22 09 22 05 12 05 19 22 01 03 01 14 03 05 19 , c'est à dire :

V I V E L E S VACANCES

Une calculatrice ordinaire peut difficilement calculer $145^{23} \pmod{187}$. Si l'on est intéressé, on pourra aisément effectuer les calculs sur le site dcode.fr : https://www.dcode.fr/chiffre-rsa

Remarquons que dans l'exemple précédent, on a chiffré de la même façon les 3 V, les 3 E et les 2 S et les 2 A de « Vive les vacances ». Dans la pratique, pour casser une éventuelle analyse de fréquence, on crée des blocs de taille différente des nombres à chiffrer, par exemple les nombres de 2 chiffres sont regroupé par blocs de 3 et chiffrés comme tels. De plus, les blocs sont des très grands nombres.

On voit que cette méthode de chiffrement évite totalement un échange de clefs entre Alice et Bob.
Le chiffrement repose pour l'instant sur l'impossibilité actuelle de factoriser un très grand nombre (plus de 200 chiffres) en deux nombres premiers eux aussi très grands, ainsi que sur la non-réversibilité des fonctions modulo.

**Remarque cryptograhique :**

Pour l'instant, on ne sait pas factoriser, c'est à dire décomposer en facteurs, un très grand nombre qui est le produit de 2 nombres premiers. Mais il est possible que quelqu'un dans un organisme de cryptographie, à la NSA ou en Russie par exemple, y soit parvenu et que le secret soit bien gardé pour pouvoir espionner les petits camarades. Le secret du déchiffrement d'Enigma a été gardé pendant 40 ans. C'est le monde de la cryptographie.

**Remarque mathématique :**

Si l'on pose la question sur Google : combien y a-t-il d'atomes dans tout l'Univers visible ? on obtient une réponse, selon les sites Internet consultés, qui est un nombre de l'ordre de $10^{80}$ atomes. Pourtant le nombre 80 ne paraît pas très grand… Ceci pour dire qu'avec des nombres de l'ordre de $10^{100}$ ou $10^{200}$ , on est totalement en dehors du réel, ou du moins d'un réel physique quantifiable qui ait un sens concret. C'est juste une remarque au passage.

**Conclusion**

45 ans après sa création, le chiffrement RSA est toujours très utilisé,  pour les paiements par cartes bancaires entre autres.

Pour une utilisation grand public, les chiffrements modernes concernent principalement les problèmes de signature électronique. On utilise pour cela des fonctions de hachage, qui réalisent des résumés d'un message, sous forme d'une suite de bits, généralement en numérotation hexadécimale.

Pour chiffrer, il existe aussi la méthode de chiffrement par blocs et de chiffrement par flots, en cryptographie symétrique (clé identique pour l'expéditeur et le destinataire)

Actuellement, la recherche en cryptographie s'oriente vers des chiffrements du type RSA, mais encore plus subtils. Il existe par exemple des chiffrements effectués à partir des courbes elliptiques : à partir de points sur la courbe, on détermine une clé secrète et une clé publique. On estime qu'une clef de 200 bits pour les courbes elliptiques est plus sûre qu'une clef de 1024 bits pour le chiffrement RSA. Cette technologie est utilisées pour les cartes à puces et a fait l'objet de nombreux dépôts de brevets à travers le monde.

Si vous êtes passionnés par le Chiffre et que vous souhaitez écrire sur ce site Internet quelques pages à propos de l'un de ces sujets, vous serez le bienvenu. Et si vous persévérez loin dans cette voie, c'est peut être vous qui écrirez les prochains chapitres de l' Histoire  de la Cryptographie à travers votre métier.

*******
*****
***
*