
# Cryptologie et arithmétique

## L2 Informatique - UFR S.A.T

Pr. Ousmane THIARE

ousmane.thiare@ugb.edu.sn
http://www.ousmanethiare.com

10 mai 2024

# Cryptologie et arithmétique

# Chapitre III : Cryptologie et arithmétique



## 1 Méthode de cryptage "à clé publique"

**Principe**

Supposons qu'un individu A soit obligé de transmettre à un autre individu B un message M en utilisant un réseau de communication public, par exemple les ondes hertziennes. N'importe quel individu peut se mettre à l'écoute et intercepter le message.
Le problème est donc :

- le message doit être inintelligible pour tout individu autre que A et B.

**Principe**

Supposons qu'un individu A soit obligé de transmettre à un autre individu B un message M en utilisant un réseau de communication public, par exemple les ondes hertziennes. N'importe quel individu peut se mettre à l'écoute et intercepter le message.
Le problème est donc :

- le message doit être inintelligible pour tout individu autre que A et B.
- B doit pouvoir le comprendre.

## Principe

Supposons qu'un individu A soit obligé de transmettre à un autre individu B un message M en utilisant un réseau de communication public, par exemple les ondes hertziennes. N'importe quel individu peut se mettre à l'écoute et intercepter le message.
Le problème est donc :

- le message doit être inintelligible pour tout individu autre que A et B.
- B doit pouvoir le comprendre.
- B doit pouvoir s'assurer que le message provient bien de A (et non d'un plaisantin quelconque).

## Principe

L'idée est de doter tous les participants de la même méthode de cryptage. Les résultats du cryptage d'un même message par divers individus sont cependant différents, car chacun d'entre eux emploie une "clé" qui lui est propre.

**Exemple :** Lorsque l'on remplace 'a' par 'c', 'b' par 'd', etc. . . , la méthode de cryptage est "décalage des lettres de l'alphabet" et la clé est la longueur du décalage, ici 2.

La méthode de cryptage est fondée sur l'existence de fonctions f, dépendant d'un paramètre (la "clé" ), inversibles, mais pour lesquelles la détermination de l'inverse est matériellement impossible, en l'état actuel des connaissances humaines.

## Principe

Soit $f_A$ la fonction de cryptage qui utilise la clé propre à l'individu A.

- La clé de A est publique, ainsi n'importe qui est en mesure d'appliquer la fonction $f_A$ à un message M quelconque.
- Par contre, seul A connaît la fonction inverse $f_A^{-1}$ qui permet de retrouver le message initial.

Au message M , A applique en fait $f_A^{-1}$ (il est le seul à pouvoir le faire). Puis, à ce message $f_A^{-1}(\mathrm{M})$, il applique la fonction de cryptage de B, soit $f_B$ (il peut le faire, la clé de B est publique), pour obtenir $f_B \circ f_A^{-1}(M)$, incompréhensible car les clés sont évidemment uniques, et donc $f_B \circ f_A^{-1}$ n'est pas l'identité.

**Principe**

C'est ce message "doublement" crypté qui est envoyé. B le reçoit et lui applique aussitôt $f_B^{-1}$, ce qu'il est le seul à pouvoir faire, pour obtenir $f_A^{-1}(\mathrm{M})$, auquel il applique $f_A$ : si le résultat est compréhensible, B est sûr que le message lui était bien destiné, et qu'il a bien été envoyé par A.

**Résultat de base**

Diverses fonctions « à inverse difficile à déterminer » ont été proposées. Les plus satisfaisantes sont celles qui utilisent le résultat suivant :

## Propriété

*S'il est très facile d'obtenir un très grand nombre entier composé par produit de deux nombres premiers eux-mêmes grands, la décomposition en facteurs premiers d'un nombre composé est très difficile.*

## Méthode de cryptage

La méthode de cryptage est la suivante :

- Soit donc n pq un entier, produit de deux nombres entiers premiers, par exemple tels que $p \equiv q \equiv 2[3]$.
- Soit M le message, préalablement chiffré (sans précautions particulières, par exemple en remplaçant les lettres par leurs codes ASCII).
- Si $M \geq n$, on décompose M en plusieurs sous-messages, ses "chiffres" en base n, par exemple.
- Si n est la clé choisie par A,et pour M<n, $f_A$(M)=C, avec $C \equiv M3[n]$. Comme n est connu de tous, n'importe qui peut calculer C tre ?s rapidement. Par contre, les facteurs premiers p et q de n sont soigneusement tenus secrets par A.

## Méthode de cryptage

La méthode de cryptage est la suivante (suite) :

1. Un résultat (élémentaire) d'arithmétique indique que, comme n n'a pas de facteur carré, si M est premier avec n, alors $M^{\phi(n)} \equiv 1[n]$ (dans cette expression, $\phi$ est la fonction indicatrice d'Euler, c'est-à-dire que $\phi(n)$ est le nombre de nombres strictement positifs inférieurs à n qui sont premiers avec n).
2. Un autre résultat (élémentaire) d'arithmétique dit que, comme n=pq, avec p et q premiers, $\phi(n) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$.
3. On a donc, en combinant ces deux résultats, $M^{(p-1)(q-1)} \equiv 1[n]$, donc $M^{2(p-1)(q-1)} \equiv 1[n]$, et finalement $M^{2(p-1)(q-1)+1} \equiv M[n]$.

## Méthode de cryptage

La méthode de cryptage est la suivante (suite) :

1. Comme on a choisi $p \equiv q \equiv 2[3], (p-1)(q-1) \equiv 1[3], 2(p-1)(q-1) \equiv 2[3]$ et $2(p-1)(q-1)+1 \equiv 0[3]$. Il s'agit donc d'un multiple de 3, on peut poser 2(p-1)(q-1)+1=3k, et on a $M^{3k} \equiv M[n]$.
2. Or $M^{3k} \equiv (M^3)^k$, donc, si le message crypté est $C \equiv M^3[n]$, $C^k \equiv M[n]$ et la connaissance de $k = \frac{2(p-1)(q-1)+1}{3}$ permet de retrouver le message original.