République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Ferhat Abbas Sétif 1


Faculté des Sciences
Département d'Informatique

# Notes de Cryptographie

Préparé par :
**Dr. Lemia Louail**
Maître de conférences en Informatique
Laboratoire des Réseaux et Systèmes Distribués LRSD

Destiné aux étudiants en L3 Informatique
Disponible sur Moodle

# Table des matières

# Table des figures

# Introduction à la cryptographie

## Sommaire



## 1.1 Définitions

**La cryptologie** est une science à mi-chemin entre les mathématiques et l'informatique. Le terme cryptologie vient du grec **kryptos** signifiant **caché** ou **secret** et **logos** signifiant **discours**. La cryptologie est donc la science des messages secrets.

La cryptologie comporte deux sous disciplines :

- **La cryptographie** : qui est l'ensemble des techniques (algorithmes et protocoles) permettant de chiffrer et déchiffrer des messages.
- **La cryptanalyse** : qui est la science qui consiste à tenter de trouver un message ayant été protégé par une technique de cryptographie, i.e la cryptanalyse vise à **casser** les méthodes de la cryptographie.

### Autres définitions

- **Le chiffrement** est l'opération permettant de transcrire un texte clair en un texte chiffré à l'aide d'une clé de chiffrement (voir Figure 1.1).
- **Le déchiffrement** est l'opération inverse du chiffrement (voir Figure 1.1).

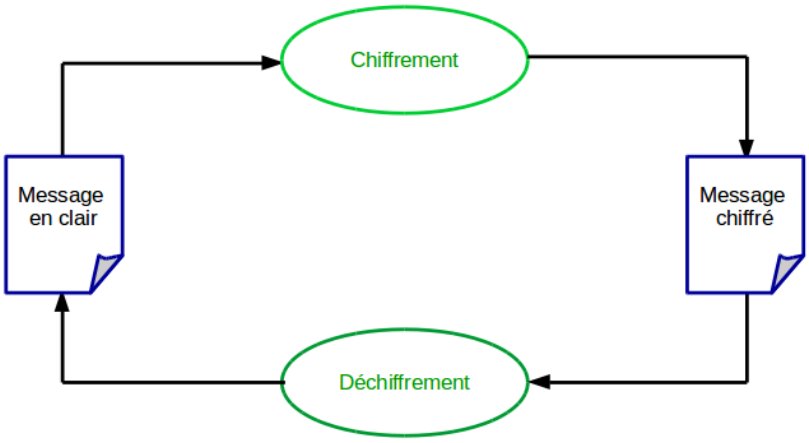


FIGURE 1.1 – Chiffrement/déchiffrement d'un message

## 1.2 Historique

### De la stéganographie à la cryptographie

Depuis l'antiquité, on cherche à envoyer des messages sans que des personnes étrangères ne puissent les intercepter.

**Stéganographie** : étymologie grecque, **Steganos** signifiant **couvert** et **Graphein** signifiant **écriture**. Il s'agit de l'art de cacher un message.

- 600 avant J.C. : Nabuchodonosor, roi de Babylone, utilisait les crânes rasés de ses esclaves pour écrire ses messages, il attendait la repousse de leurs cheveux avant qu'il les envoie à ses généraux.
- 480 avant J.C. : Dematarus (Grec) isolé en Perse utilisait des tablettes de cires pour prévenir son pays des projets de Xerxes (Perse).
- 1er siècle : apparition de l'encre invisible (fluide organique riche en carbone).

La scytale ou bâton de Pultarque (Figure 1.2) est un bâton de bois utilisé pour lire ou écrire une dépêche chiffrée. Elle est considérée comme le plus ancien dispositif de cryptographie militaire.

FIGURE 1.2 – Scytale de chiffrement/déchiffrement

## 1.3 Notations

Le message en clair **P** (Plaintext) est transformé en message chiffré **C** (Ciphertext) via la fonction de chiffrement **E** (Encrypt) et la clé **K** (Key).

$$C = E(P, K)$$

Le message chiffré **C** est transformé en message en clair **P** via la fonction de déchiffrement **D** (Decrypt) et la clé $K^{-1}$ (qui peut être égale à K ).

$$P = D(C, K^{-1})$$

## 1.4 Objectifs de la cryptographie

Le but pricipal de la cryptographie est d'assurer la sécurité des communications transmises sur un canal public en présence d'adversaires.

Il existe deux types d'adversaire :

- Adversaire passif : qui écoute les communications sans les modifier.
- Adversaire actif : qui est capable de modifier ou d'effacer les communications transmises sur le canal.

## 1.5 Qualités d'un cryptosystème

Un crypto-système doit assurer les quatres qualités suivantes :

- La confidentialité : Garantir que le contenu d'une communication ou d'un fichier n'est pas accessible aux tiers.
- L'intégrité : Garantir que le contenu d'une communication ou d'un fichier n'a pas été modifié.
- L'authentification : Garantir l'identité d'une entité (émetteur ou récepteur) ou l'origine d'une communication ou d'un fichier.
- La non-répudiation : l'émetteur ne peut pas nier avoir envoyé le message et le récepteur ne peut pas nier l'avoir reçu.

## 1.6 Classification des crypto-systèmes

Un crypto-système, comme montré dans la figure 1.3 peut être symétrique (à clé privée), asymétrique (à clé publique) ou hybride (symétrique et asymétrique).

Les trois types sont détaillés dans le reste du document.

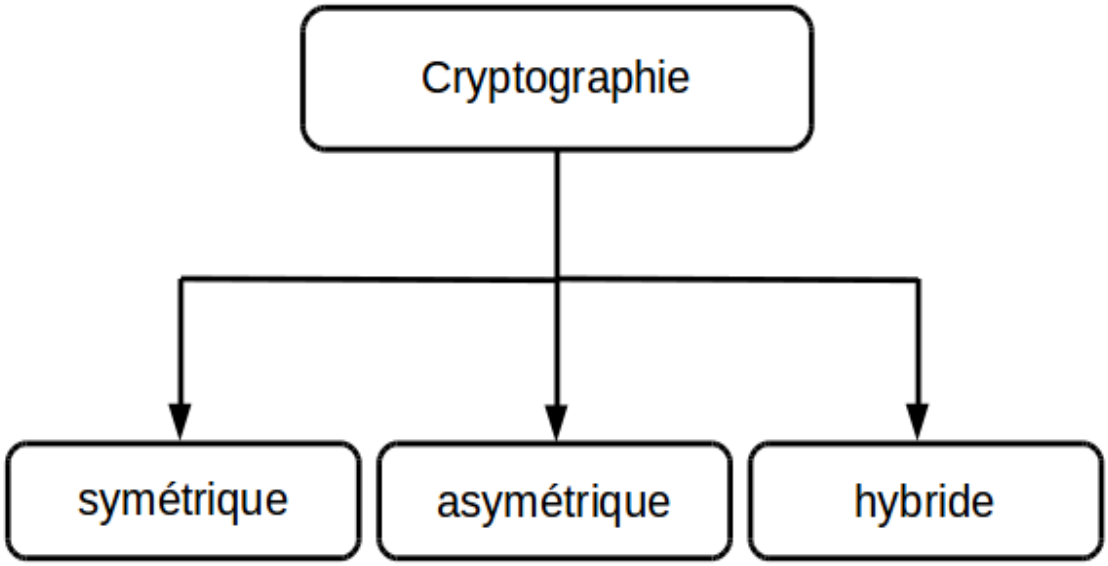


FIGURE 1.3 – Classification des crypto-systèmes

# Cryptograhie symétrique

## Sommaire



## 2.1 Introduction

Dans **la cryptographie symétrique**, appelée aussi **cryptographie à clé symétrique** ou encore **cryptographie à clé secrète** ou à **clé privée**, la clé de chiffrement est la même que celle du déchiffrement. C'est la plus ancienne méthode de cryptographie utilisée par l'Homme.

### Principe de fonctionnement

La figure 2.1 résume le principe de fonctionnement d'un cryptosystème symétrique qui est le suivant :

- Les deux interlocuteurs se mettent d'accord sur une clé secrète.
- L'émetteur chiffre son message avec la clé secrète.
- Le récepteur déchiffre le message avec la même clé.

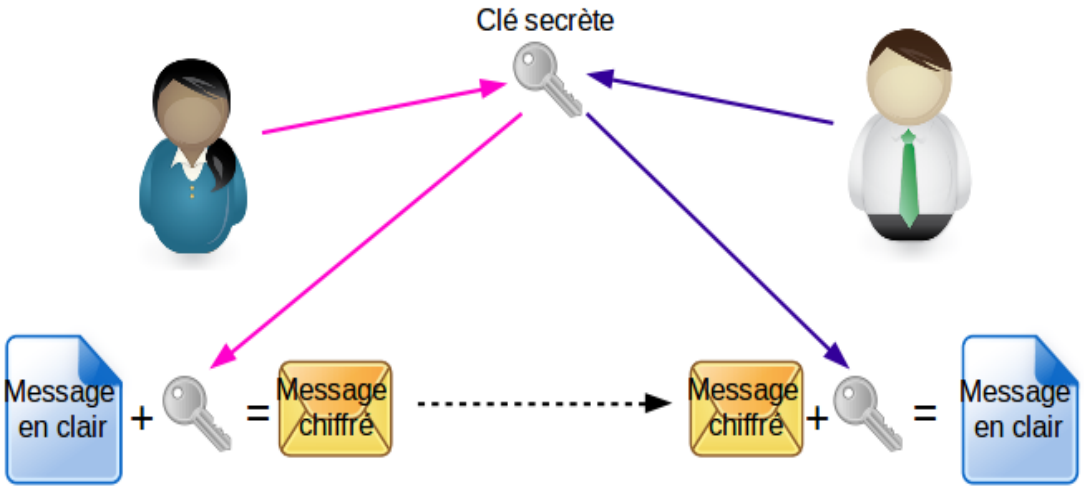


FIGURE 2.1 – Procédure de chiffrement symétrique

### Avantages de la cryptographie symétrique

- Système rapide (implantation matérielle).
- Utilise peu de ressources systèmes.
- Clé relativement courte (128 ou 256 bits).

### Inconvénients de la cryptographie symétrique

- Gestion des clés difficiles (nombreuses clés → une clé pour chaque destinataire).
- Risque lors de l'échange de la clé secrète.

## 2.2 Crypto-systèmes symétriques

Il existe plusieurs cryptosysètmes symétriques, les plus connus sont les suivants :

- le chiffrement de César,
- le chiffrement de Vigenère,
- le chiffrement par substitution,
- le chiffrement affine,
- le chifrement de Hill.

## 2.3 Chiffrement de César

Le chiffrement de César est un chiffrement **monoalphabétique par décalage**. Il utilise une permutation circulaire de l'ensemble des lettres de l'alphabet.

- On numérote les lettres de 0 (pour A) jusqu'à 25 (pour Z).
- On choisit une clé $K \in \{1, ..., 25\}$
- Pour chaque lettre en clair $\sigma \in \{0, ..., 25\}$ :

$$E(\sigma, K) = (\sigma + K)\ modulo\ 26$$

- Pour chaque lettre chiffrée $\sigma' \in \{0, ..., 25\}$ :

$$D(\sigma', K) = (\sigma' - K)\ modulo\ 26$$

Exemple :

Chiffrement du message CESAR avec la clé K=8

E(C,8) = E(2,8) = (2+8) mod 26 =10 mod 26 = 10 = K
E(E,8) = E(4,8) = (4+8) mod 26 = 12 mod 26 = 12 = M
E(S,8) = E(18,8) = (18+8) mod 26 = 26 mod 26 = 0 = A
E(A,8) = E(0,8) = (0+8) mod 26 = 8 mod 26 = 8 = I
E(R,8) = E(17,8) = (17+8) mod 26 = 25 mod 26 = 25 = Z

CESAR → KMAIZ

Déchiffrement du message KMAIZ avec la clé K=8

D(K,8) = D(10,8) = (10-8) mod 26 =2 mod 26 = 2 = C
D(M,8) = D(12,8) = (12-8) mod 26 = 4 mod 26 = 4 = E
D(A,8) = D(0,8) = (0-8) mod 26 = -8 mod 26 = 18 = S
D(I,8) = D(8,8) = (8-8) mod 26 = 0 mod 26 = 0 = A
D(Z,8) = D(25,8) = (25-8) mod 26 = 17 mod 26 = 17 = R

KMAIZ → CESAR

NB : Modulo négatif
$x\%y$ avec $x < 0 \rightarrow (y-1) - ((-x-1)\%y)$

Exemple de table de César avec un décalage de 8 :

| Alphabet en clair | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Rang alphabet | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| Rang+décalage de 8 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |
| Alphabet chiffré | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |

| Alphabet en clair | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Rang alphabet | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| Rang+décalage de 8 | 23 | 24 | 25 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Alphabet chiffré | X | Y | Z | A | B | C | D | E | F | G | H |

Le chiffrement de César peut être représenté par deux cercles (Figure 2.2) : le grand cercle représente l'alphabet en clair et le petit cercle représente les lettres chiffrées.

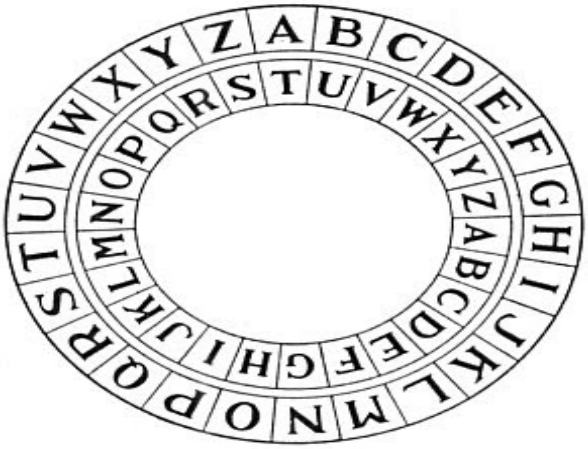

FIGURE 2.2 – Cercle de chiffrement de César

## Inconvénients

- Nombre de clés petit : taille de l'alphabet décrémentée (taille - 1).
- Attaque par force brute possible (voir section 2.8).
- Attaque par analyse fréquentielle possible (voir section 2.9).

## 2.4 Chiffrement de Vigenère

Le chiffrement de Vigenère est un chiffrement **polyalphabétique par décalage**, présenté par Blaise de Vigenère au courant du 16ème siècle.

### Principe de fonctionnement

- On choisit un message : VIGENERE
- On choisit un mot-clé : CLEF
- Le rang de chaque lettre de la clé définit un décalage à appliquer

V—I—G—E—N—E—R—E
C—L—E—F—C—L—E—F

E(V,C) = E(21,2) = (21+2) mod 26 =23 mod 26 = 23 = X

E(I,L) = E(8,11) = (8+11) mod 26 =19 mod 26 = 19 = T

E(G,E) = E(6,4) = (6+4) mod 26 =10 mod 26 = 10 = K

E(E,F) = E(4,5) = (4+5) mod 26 =9 mod 26 = 9 = J

E(N,C) = E(13,2) = (13+2) mod 26 =15 mod 26 = 15 = P

E(E,L) = E(4,11) = (4+11) mod 26 =15 mod 26 = 15 = P

E(R,E) = E(17,4) = (17+4) mod 26 =21 mod 26 = 21 = V

E(E,F) = E(4,5) = (4+5) mod 26 =9 mod 26 = 9 = J

Le chiffrement du message VIGENERE avec la clé CLEF donne :

VIGENERE → XTKJPPVJ

| Message clair | V | I | G | E | N | E | R | E |
|---|---|---|---|---|---|---|---|---|
| Rang message | 21 | 8 | 6 | 4 | 13 | 4 | 17 | 4 |
| Clé | C | L | E | F | C | L | E | F |
| Rang clé | 2 | 11 | 4 | 5 | 2 | 11 | 4 | 5 |
| Message chiffré | X | T | K | J | P | P | T | J |

## Déchiffrement

Le déchiffrement d'un message chiffré par la méthode de Vigenère se fait avec l'opération inverse : un décalage dans le sens inverse s'applique sur chaque lettre du message chiffré.

Prenons le message chiffré XTKJPPVJ avec la clé CLEF.

X—T—K—J—P—P—V—J
C—L—E—F—C—L—E—F

D(X,C) = D(23,2) = (23-2) mod 26 =21 mod 26 = 21 = V

D(T,L) = D(19,11) = (19-11) mod 26 =8 mod 26 = 8 = I

D(K,E) = D(10,4) = (10-4) mod 26 =6 mod 26 = 6 = G

D(J,F) = D(9,5) = (9-5) mod 26 =4 mod 26 = 4 = E

D(P,C) = D(15,2) = (15-2) mod 26 =13 mod 26 = 13 = N

D(P,L) = D(15,11) = (15-11) mod 26 =4 mod 26 = 4 = E

D(V,E) = D(21,4) = (21-4) mod 26 =17 mod 26 = 17 = R

D(J,F) = D(9,5) = (9-5) mod 26 =4 mod 26 = 4 = E

Le déchiffrement du message XTKJPPVJ avec la clé CLEF donne :

$$\text{XTKJPPVJ} \rightarrow \text{VIGENERE}$$

## Le carré de Vigenère

Le carré de Vigenère permet aussi de chiffrer des messages, il suffit de choisir la ligne correspondant à la lettre du message en clair et de faire l'intersection avec la colonne correspondant à la lettre de la clé pour trouver la lettre chiffrée.

Pour le même exemple de chiffrement précédant, l'intersection de la ligne V avec la colonne C donne la lettre chiffrée X comme le montre le tableau suivant :

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
Z A B C D E F G H I J K L M N O P Q R S T U V W X Y

## 2.5 Chiffrement par substitution

Le chiffrement monoalphabétique par substitution, appelé aussi **alphabets désordonnés**, utilise une permutation arbitraire de l'ensemble des lettres de l'alphabet.

Ce chiffrement peut se faire soit en associant aléatoirment à chaque lettre de l'alphabet une autre lettre, soit en utilisant un mot clé.

### Construction d'une table de substituion arbitraire

Pour chaque lettre de l'alphabet en clair, on associe aléatoirement une lettre qui ne peut pas être utilisée une deuxième fois.

| A | B | C | D | E | F | G | H | I | J | K | L | M | N |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| O | S | K | B | E | J | P | A | Y | I | M | N | Z | X |

| O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|
| H | D | W | L | C | U | V | G | R | Q | T | F |

Message en clair : BONJOUR

Message chiffré : SHXIHVL

### Construction d'une table de substitution à partir d'un mot-clé

- Choisir un mot-clé : SECURITE
- Supprimer les lettres doubles du mot-clé : SECURIT
- Faire correspondre les premières lettres de l'alphabet aux premières lettres du mot-clé

| A | B | C | D | E | F | G | H | I | J | K | L | M | N |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S | E | C | U | R | I | T | | | | | | | |

| O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | |

- Compléter la table de substitution, en supprimant les lettres présentes dans la clé, et en reprenant l'alphabet à partir de :

— la dernière lettre de la clé nettoyée,

| A | B | C | D | E | F | G | H | I | J | K | L | M | N |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S | E | C | U | R | I | T | V | W | X | Y | Z | A | B |

| O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|
| D | F | G | H | J | K | L | M | N | O | P | Q |

— ou, la première lettre de l'alphabet

| A | B | C | D | E | F | G | H | I | J | K | L | M | N |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S | E | C | U | R | I | T | A | B | D | F | G | H | J |

| O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|
| K | L | M | N | O | P | Q | V | W | X | Y | Z |

- Remplacer chaque lettre du message en clair par la lettre qui lui correspond dans l'une des deux tables précédantes.

NB : Le chiffrement de César est un cas particulier du chiffrement par substitution.

## 2.6 Chiffrement affine

Le chiffrement affine est une méthode de cryptographie basée sur **un chiffrement par substitution mono-alphabétique**.

Le principe de ce chiffrement repose sur le fait d'utiliser une fonction affine du type :

$$y = ax + b \ [modulo\ 26]$$

où $a$ et $b$ sont des constantes, et $x$ et $y$ correspondent aux rangs des lettres de l'alphabet.

Pour que le chiffrement soit possible, il faut que la fonction affine soit injective, i.e. la congruence $ax + b \equiv y(\ mod\ 26)$ doit avoir une solution unique pour $x$.
Cette congruence est équivalente à $ax \equiv y - b(\ mod\ 26)$. Cette congruence a une solution unique pour tout $y$ si et seulement si **PGCD(a,26)=1**. c'est à dire $a$ doit être premier avec 26 sinon deux lettres différentes peuvent avoir le même codage, ce qui rend le déchiffrement impossible.

Exemple :

- On choisit $a = 17$ et $b = 2$
- On veut chiffrer la lettre $K$ ayant le rang 10, donc $x = 10$
- $y = (17x + 2)\ modulo\ 26$
- $y = (17 \times 10 + 2)\ modulo\ 26$
- $y = 16 \rightarrow$ la lettre chiffrée est $Q$

$$\mathrm{K} \rightarrow \mathrm{Q}$$

NB : lorsque $a = 1$, on retrouve le chiffrement de **César** avec un décalage de $b$

### déchiffrement affine

Le déchiffrement se fait à l'aide de la fonction inverse de celle utilisée pour le chiffrement :

$$x = a^{-1}(y - b)\ [modulo\ 26]$$

$a^{-1}$ est l'inverse de $a$ dans 26 (appelé **inverse modulaire**) et peut être calculé à l'aide de l'algorithme d'Euclide étendu.

Exemple :

- Déchiffrement de la lettre Q avec $a = 17$ et $b = 2$
- Commençons par trouver l'inverse de 17 dans 26 avec **l'algorithme d'Euclide étendu** :
  - 26 = 1×17+9 ... (1) (division de 26 sur 17)
  - 17 = 1×9+8 ...(2) (division de 17 sur 9)
  - 9 = 1×8+1 ...(3) (division de 9 sur 8)
  - lorsque le reste de la division est égal à 1 on arrête les divisions, on commence par la dernière équation et on inverse :
  - 1 = 9 - 8 ... de (3)
  - 1 = 9 - (17 - 9) ... de (2)
  - 1 = 2×9 - 17 ... simplification
  - 1 = 2×(26-17) - 17 ... de (1)
  - 1 = 2×26 **-3**×17 ... simplification
  - Puisqu'on cherche l'inverse de 17, on prend le coefficient de 17 dans cette dernière étapes
  - si ce coefficient est positif c'est le résultat final ; s'il est négatif on lui ajoute 26
  - -3+26=23
  - L'inverse de 17 dans 26 est 23
- $a^{-1} = 23, b = 2 \rightarrow x = 23(y - 2)\ mod\ 26$
- $x = 23(16 - 2)\ mod\ 26 \rightarrow x = 10 = K$
- La lettre chiffré Q correspond en clair à la lettre K

## 2.7 Chiffrement de Hill

Le chiffrement de Hill (publié en 1929 par Lester S. Hill) est une méthode **polygraphique**, i.e. on ne chiffre/déchiffre pas lettre par lettre mais plutôt **bloc par bloc**. Hill considère des **blocs de deux lettres (chiffrement bigraphique)**.

### Principe de fonctionnement

- Les lettres du message en clair sont remplacées par leurs rangs dans l'alphabet.
- Le message en clair est ensuite découpé en blocs de deux lettres.
- Une clé de chiffrement est construite sous forme de matrice carrée.
- La première lettre chiffrée correspond au premier bloc du message en clair chiffré avec la première ligne de la matrice clé, la deuxième lettre chiffrée correspond au premier bloc du message en clair chiffré avec la deuxième ligne de la matrice clé, ... (en modulo 26).

Pour que le chiffrement soit possible, il faut que le déterminant de la matrice soit premier avec la taille de l'alphabet i.e. **PGCD(det,26)=1**.
Le déterminant d'une matrice :

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \quad det(M) = A \times D - C \times B$$

Exemple :
message en clair **MESSAGE** avec la matrice clé

$$M = \begin{pmatrix} 3 & 1 \\ 4 & 3 \end{pmatrix} \ mod\ 26; \quad det(M) = 3 \times 3 - 4 \times 1 = 5;\ PGCD(5, 26) = 1 \rightarrow matrice\ valide$$

Prenons le premier bloc du message→ "ME" → 12 4

12×3+4×1= 40 modulo 26 = 14 → O

12×4+4×3= 60 modulo 26 = 8 → I

le bloc **ME** devient **OI**

### Déchiffrement

Afin de déchiffrer un message chiffré avec le crypto-système de Hill, il faut calculer l'inverse de la matrice de chiffrement.
Pour une matrice :

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

L'inverse se caclule comme suit :

$$M^{-1} = \frac{1}{A \times D - B \times C} \times \begin{pmatrix} D & -B \\ -C & A \end{pmatrix}$$

Prenons, par exemple, le message chiffré **OI** avec la matrice de l'exemple précédant :

$$M = \begin{pmatrix} 3 & 1 \\ 4 & 3 \end{pmatrix} \ mod\ 26$$

$$M^{-1} = \frac{1}{3 \times 3 - 1 \times 4} \times \begin{pmatrix} 3 & -1 \\ -4 & 3 \end{pmatrix} \ mod\ 26$$

$$M^{-1} = \frac{1}{5} \times \begin{pmatrix} 3 & -1 \\ -4 & 3 \end{pmatrix} \ mod\ 26$$

L'inverse de 5 dans 26 est 21 (voir l'algorithme d'Euclide étendu section 2.6), par conséquent la matrice devient :

$$M^{-1} = 21 \times \begin{pmatrix} 3 & -1 \\ -4 & 3 \end{pmatrix} \ mod\ 26$$

$$M^{-1} = \begin{pmatrix} 63 & -21 \\ -84 & 63 \end{pmatrix} \ mod\ 26$$

Puisque nous utilisons un alphabet de 26 lettres, tous les calculs se font en modulo 26 :

$$M^{-1} = \begin{pmatrix} 11 & 5 \\ 20 & 11 \end{pmatrix} \ mod\ 26$$

Le déchiffrement du message **OI (14 8)** se fait avec la matrice inverse comme suit :

$14 \times 11 + 8 \times 5 = 194\ mod\ 26 = 12 \rightarrow$ M

$14 \times 20 + 8 \times 11 = 368\ mod\ 26 = 4 \rightarrow$ E

le bloc chiffré **OI** correspond au bloc en clair **ME**.

## 2.8 Analyse fréquentielle

L'analyse fréquentielle, ou analyse de fréquences, est une méthode de cryptanalyse consistant à examiner la fréquence d'apparition de chaque lettre d'un texte chiffré. Cette méthode est basée sur le fait que, selon la langue utilisée, certaines lettres apparaissent avec certaines fréquences. Par exemple, dans la langue française, la lettre **e** est la plus fréquente, suivie de la lettre **a** et de la lettre **s**. Ceci permet d'analyser la fréquence de chaque lettre du texte chiffré et de trouver à quelle lettre en clair elle correspond.

Le tableau suivant présente les 5 lettres les plus fréquentes dans certaines langues.

| | | | | | |
|---|---|---|---|---|---|
| **Français** | e (14,7%) | s (7,9%) | a (7,6%) | i (7,5%) | t (7,2%) |
| **Anglais** | e (12,7%) | t (9%) | a (8,2%) | o (7,5%) | i (7%) |
| **Espagnol** | e | a | o | s | r |
| **Allemand** | e | n | i | s | r |
| **Italien** | e | a | i | o | n |
| **Portugais** | a | e | i | s | r |

Le tableau suivant présente les fréquences d'apparition **moyenne** des lettres de la langue française.

| Lettre | Fréquence | Lettre | Fréquence |
|---|---|---|---|
| A | 8.40 % | N | 7.13 % |
| B | 1.06 % | O | 5.26 % |
| C | 3.03 % | P | 3.01 % |
| D | 4.18 % | Q | 0.99 % |
| E | 17.26 % | R | 6.55 % |
| F | 1.12 % | S | 8.08 % |
| G | 1.27 % | T | 7.07 % |
| H | 0.92 % | U | 5.74 % |
| I | 7.34 % | V | 1.32 % |
| J | 0.31 % | W | 0.04 % |
| K | 0.05 % | X | 0.45 % |
| L | 6.01 % | Y | 0.30 % |
| M | 2.96 % | Z | 0.12 % |

## Exemple

Voici un texte rédigé en Français et chiffré à l'aide d'un cryptosystème monoalphabétique :

E'MKMSZMHU WU XDSVZIJRIU JS MEFAMOUZ WU XARCCIUHUSZ WU XUZZU HMSRUIUUVZ GJ'RE UVZ ZIUV CMXREU WU HUHDIRVUI EU HDZ DJ E'UNFIUVVRDS JZRERVU, UZ WDSX E'MEFAMOUZ WU XARCCIUHUSZ. X'UVZ ZIUV RHFDIZMSZ, XMI VR E'UHUZZUJIWJ HUVVMHU WDRZ UXIRIU E'MEFAMOUZ WU XARCCIUHUSZ VJI JS ODJZ WU FMFRUI,XUEJR-XR FUJZ ZDHOUI USZIU EUV HMRSV WU E'USSUHR, GJR XDSSMRZ MEDIV EM XEUWU XARCCIUHUSZ UZ FUJZ WUXARCCIUI ZDJZU XDHHJSRXMZRDS GJR M UZU USXDWUUMKUX. MJ XDSZIMRIU, VR EM XEU UVZ JSRGJUHUSZ HUHDIRVUU, EUV XAMSXUV GJUE'USSUHR EM WUXDJKIU VDSZ FEJV CMROEUV.

Est-il possible de déchiffrer ce texte sans connaître ni le cryptosystème qui a permis de le chiffrer ni la clé de chiffrement ?

Oui, ceci est possible en appliquant la méthode de l'analyse fréquentielle.

Les fréquences d'apparition des lettres de ce texte sont comme suit :

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2,0 | 0,0 | 2,7 | 4,5 | 5,7 | 2,3 | 1,1 | 5,0 | 6,4 | 5,2 | 0,7 | 0,0 | 6,4 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 0,2 | 1,4 | 0,0 | 0,0 | 7,5 | 6,4 | 0,0 | 18,9 | 5,7 | 3,4 | 5,7 | 0,0 | 8,9 |

Dans ce texte, la lettre **U** a la fréquence d'apparition la plus élevée. Suivant les fréquences d'apparition des lettres de la langues française, la lettre **U** correspond à la lettre en clair **E**. Prenons, par exemple, le premier mot de ce texte chiffré **E'MKMSZMHU**. En remplaçant le **U** par le **E**, nous obtenons E'MKMSZMH**E**.

Les lettres **Z** et **M** sont aussi très fréquentes dans ce texte chiffré ; elles correspondent probablement aux lettres en clair **A**, **S** ou **T**. Grâce à l'apostrophe dans ce premier mot, nous pouvons déduire que la lettre chiffré **M** correspond à une voyelle et donc à la lettre en clair **A** et donc le mot devient E'**A**K**A**SZ**A**H**E**.

Nous pouvons aussi déduire que la première lettre avant l'apostrophe est soit un **L** soit un **J**, mais selon la table des fréquence elle correspond probablement à la lettre en clair **L**, par conséquent le mot devient **L**'**A**K**A**SZ**A**H**E**.

En procédant de la même façon, le premier mot en clair est "L'avantage" et le texte en clair est le suivant :

*L'avantage de construire un alphabet de chiffrement de cette manière est qu'il est très facile de mémoriser le mot ou l'expression utilisé, et donc l'alphabet de chiffrement. C'est très important, car si l'émetteur du message doit écrire l'alphabet de chiffrement sur un bout de papier, celui-ci peut tomber entre les mains de l'ennemi, qui connaît alors la clé de chiffrement et peut déchiffrer toute communication qui a été encodée avec. Au contraire, si la clé est uniquement mémorisée, les chances que l'ennemi la découvre sont plus faibles.*

## 2.9 Attaque par force brute

L'attaque par force brute est une méthode de **cryptanalyse** (voir section 1.1) consistant à essayer systématiquement toutes les clés possibles afin de trouver celle qui a permis de chiffrer le message. Selon la puissance de la méthode de chiffrement utilisée, cette technique peut, dans certain cas, nécessiter un temps d'exécution énorme pour trouver la bonne clé.

Prenons l'exemple d'une valise (Figure 2.3) qui se ferme avec un code. Ces codes sont généralement composés de 3 chiffres.

FIGURE 2.3 – Exemple d'un code de fermeture d'une valise

Une personne ne connaissant pas la clé pour ouvrir la valise est obligée d'essayer toute les combinaisons possibles, i.e de 000 jusqu'à 999.

Chaque combinaison possible comporte 3 chiffres et chaque chiffre varie de 0 à 9 donc le nombre de combinaisons possibles est $10^3$.

Dans le cas général, si l'espace des clés comporte $N$ clés de 1 à $N$, la notion de complexité peut être utilisée comme suit :

- dans le meilleur des cas (best case complexity), la première clé à tester correspond à la clé de chiffrement, dans ce cas un test suffit pour trouver la bonne clé.
- dans le pire des cas (worst case complexity), la dernière clé à tester est celle utilisée lors du chiffrement, dans ce cas, il faudra tester $N$ clés pour trouver la bonne.
- en moyenne (average complexity) il faut tester approximativement $\frac{N}{2}$ clés afin de trouver la clé de chiffrement.

# Cryptographie asymétrique

## Sommaire



## 3.1 Introduction

Dans la cryptographie asymétrique, appelée aussi cryptographie à **clé asymétrique** ou encore cryptographie à **clé publique**, on utilise un couple de clé (clé publique, clé privée).

Il existe deux utilisations principales de ce couple de clé :

- Le chiffrement/déchiffrement (Figure 3.1)
- La signature

#### Le chiffrement/déchiffrement

- Une personne A génère le couple de clés, elle distribue la clé publique et conserve la clé privée.
- Une personne B désire chiffrer un message et l'envoyer à A.
- B récupère la clé publique de A et chiffre son message avec cette clé.
- Lorsque A reçoit le message chiffré de B, elle le déchiffre en utilisant sa clé privée.

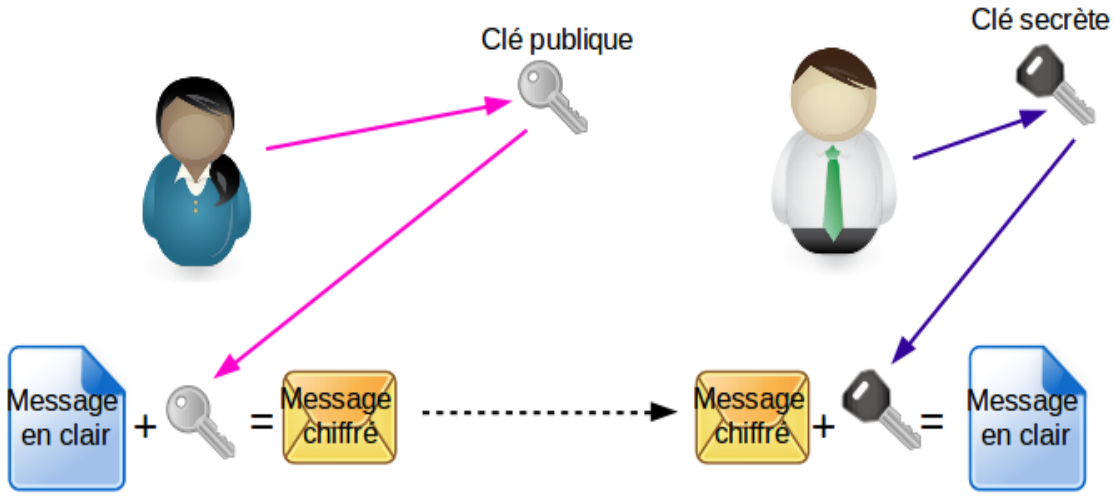


FIGURE 3.1 – Procédure de chiffrement asymétrique

### La signature numérique

La signature numérique est une application très concrète de la cryptographie asymétrique qui fut inventée dans le milieu des années 70.
La signature numérique permet :

- de garantir l'intégrité d'un message,
- d'identifier la personne qui a signé le message.

#### Principe de la signature

- A veut signer un message pour B.
- A calcule la signature en utilisant sa clé privée.
- A envoie le message et la signature à B.
- B récupère la clé publique de A.
- B vérifie la signature de A en utilisant la clé publique.
- Propriété obtenue : l'authentification.

## Avantages de la cryptographie asymétrique

- Les clés sont beaucoup plus longues que celles utilisées dans les cryptosysètmes symétriques, donc elles sont plus difficiles à trouver.

## Inconvénients de la cryptographie asymétrique

- Les algorithmes des cryptosysètmes asymétriques sont très lents et nécessitent beaucoup de ressources.

## 3.2 Chiffrement RSA (Rivest-Shamir-Adleman)

Le système RSA, publié en 1977 par Ron Rivest, Adi Shamir et Leonard Adleman, est le premier système de chiffrement à clé publique solide inventé, et le plus utilisé actuellement.

### Principe de fonctionnement

- Choisir deux grands nombres premiers $p$ et $q$
- Calculer le module RSA (module de chiffrement) $n = p \times q$
- Calculer la fonction indicatrice/génératrice d'Euler $\phi(n) = (p-1)(q-1)$
- Choisir un entier $e$ (exposant de chiffrement) tel que $e < \phi(n)$ et $PGCD(e, \phi(n)) = 1$
- Calculer $d$ l'inverse de $e$ *modulo* $\phi(n)$ : $d \times e = 1 \ mod \ \phi(n)$
- Le calcul de $d$ peut se faire par deux méthodes :
  - Par essais successifs ;
  - En utilisant l'algorithme d'Euclide étendu.

La clé publique est le couple $(n, e)$
La clé privée est le couple $(n, d)$

### RSA naif

Une personne A souhaite chiffrer un message $m$ et l'envoyer à B, elle utilise la clé publique de chiffrement :

$$c = m^e \ mod \ n$$

Lorsque la personne B reçoit le message chiffré c, elle le déchiffre en utilisant sa clé privée comme suit :

$$m = c^d \ mod \ n$$

### Force de RSA

Comment trouver $d$ en connaissant $n$ ?

- $d$ est l'inverse de $e$ *modulo* $\phi(n)$
- il faut donc pouvoir calculer $\phi(n) = (p-1)(q-1)$
- il faut donc trouver $p$ et $q$
- pour trouver $p$ et $q$ il faut factoriser $n = p \times q$

$\rightarrow$ Casser RSA revient à factoriser $n$

## Exemple

- A choisit $p = 7$ et $q = 11$
- A calcule $n = p \times q = 77$
- A calcule $\phi(n) = (p-1)(q-1) = 60$
- A choisit $e < \phi(n)$ : $e = 43$
- A calcule $d$ tel que : $d \times e = 1 \ mod \ \phi(n)$

    - Par essais successifs : essayer $d = 1$, $d = 2$, ....
    - Avec l'algorithme d'Euclide étendu :
        - $d \times 43 = 1 \ mod \ 60$
        - 60=1 × 43+17 ...(1)
        - 43=2×17+9 ...(2)
        - 17=1×9+8 ...(3)
        - 9=1×8+**1** ...(4)
        - 1=9-8 ... de (4)
        - 1=9-(17-9) ... de (3)
        - 1=2×9-17 ... par simplification
        - 1=2(43-2×17)-17 ... de (2)
        - 1=2×43-5×17 ... par simplification
        - 1=2×43-5(60-43) ...de (1)
        - 1=-5×60+7×43 ... par simplification
        - le coefficient de 43 est positif donc on le garde tel qu'il est.
        - Si le coefficient était négatif on lui ajoute $\phi(n)$
        - $d = 7$

- A possède une clé privée (77,7) qu'il garde et une clé publique (77,43) qu'il diffuse à toute personne souhaitant communiquer avec lui
- B veut chiffrer le message $m = 2$ et l'envoyer à A
- B utilise la clé publique de A (77,43)
- chiffrement : $c = 2^{43} \ mod \ 77 \rightarrow C = 30$
- B envoie le message chiffré $c = 30$ à A
- A déchiffre le message $c = 30$ avec sa clé privée : $m = 30^7 \ mod \ 77 \rightarrow m = 2$

## RSA avec signature

Après avoir généré une clé privée et une clé publique, si la personne A désire signer un message $m$ avant de l'envoyer, elle calcule la signature comme suit :

$$s = m^d \ mod \ n$$

A envoie le message $m$ et la signature $s \rightarrow (m, s)$

Lorsque la personne B reçoit le message avec la signature $(m, s)$ elle vérifie la signature en utilisant la clé publique de A :

$$s' = s^e \ mod \ n$$

- si $s' = m$ alors la signature vient de B
- si $s' \neq m$ alors la signature ne vient pas de B

**Exemple**

- A génère une clé privée (77,7) et une clé publique (77,43)
- A désire transmettre à B le message $m = 2$ avec une signature
- A calcule la signature $s = 2^7 \ mod \ 77 \rightarrow s = 51$
- A envoie à B le message avec la signature (2,51)
- En recevant le message signé, B vérifie l'authenticité du message
- B calcule $s' = s^{43} \ mod \ 77 \rightarrow s' = 51^{43} \ mod \ 77 \rightarrow s' = 2$
- Puisque $s' = m$, B est sûr que la personne qui a écrit le message est celle qui l'a signé.

## 3.3 Mise en accord de clé de Diffie-Hellman

L'échange de clé Diffie-Hellman est une méthode permettant à deux personnes de se mettre d'accord sur un nombre qu'ils peuvent utiliser comme clé de chiffrement, sans qu'une troisième personne puisse le découvrir.

### Fonctionnement

- A et B choisissent un nombre premier $p$
- A et B choisissent un générateur (une base) $g$
- A choisit un entier $a$, calcule $Ya = g^a \ mod \ p$ et l'envoie à B
- B choisit un entier $b$, calcule $Yb = g^b \ mod \ p$ et l'envoie à A
- A calcule la clé : $(g^b \ mod \ p)^a \ mod \ p$
- B calcule la clé : $(g^a \ mod \ p)^b \ mod \ p$
- $Kab = (g^b \ mod \ p)^a \ mod \ p = (g^a \ mod \ p)^b \ mod \ p$, donc A et B utilisent la même clé

#### Exemple

- A et B choisissent $p = 13$ et $g = 2$
- A choisit le nombre secret $a = 5$
- B choisit le nombre secret $b = 4$
- A calcule $2^5 \ mod \ 13 = 6$ et l'envoie à B
- B calcule $2^4 \ mod \ 13 = 3$ et l'envoie à A
- en recevant le message de B, A calcule $3^5 \ mod \ 13 = 9$
- de même pour B, il calcule $6^4 \ mod \ 13 = 9$
- A et B utilisent la même clé 9

La puissance de cette méthode repose sur un problème de logarithme discret. Il est difficile de trouver les valeurs de $a$ et $b$ même si $p$, $g$, $g^a \ mod \ p$ et $g^b \ mod \ p$ sont publiques.

### L'attaque de l'homme du milieu (man in the middle)

L'attaque de l'homme du milieu est une attaque permettant à une personne d'intercepter les communications entre deux interlocuteurs sans que ces derniers ne puissent le savoir.
Cette technique est particulièrement applicable dans la méthode d'échange de clés de Diffie-Hellman.

**Exemple**

- Supposons deux personnes A et B qui veulent se mettre d'accord sur une clé privée en utilisant la méthode de Diffie-Hellman
- Supposons aussi que le canal de transmission n'est pas sécurisé
- A et B choisissent $g = 2$ et $p = 13$
- Une troisième personne C écoute les transmissions entre A et B. Par conséquent C connaît les valeurs de $g$ et $p$
- A choisit $a = 5$, calcule $2^5 \ mod \ 13 = 6$ et envoie le résultat vers B
- B choisit $b = 4$, calcule $2^4 \ mod \ 13 = 3$ et envoie le résultat vers A
- C, se trouvant entre A et B, recevra les deux valeurs transmises sur le canal et ne les laissera pas passer
- C choisit à son tour un nombre aléatoire $c = 7$ et calcule $2^7 \ mod \ 13 = 11$
- C envoie à A 11 au lieu de 3, et envoie à B 11 au lieu de 6
- A reçoit la valeur 11 en pensant qu'elle vient de B
- B reçoit la valeur 11 en pensant qu'elle vient de A
- A calcule la clé privée $11^5 \ mod \ 13 = 7$ qu'il utilise pour chiffrer ses messages
- B calcule la clé privée $11^4 \ mod \ 13 = 3$ qu'il utilise pour chiffrer ses messages
- C calcule les deux clés privées $6^7 \ mod \ 13 = 7$ et $3^7 \ mod \ 13 = 3$
- C utilise la clé 7 pour communiquer avec A en se faisant passer pour B
- C utilise la clé 3 pour communiquer avec B en se faisant passer pour A

## 3.4 Chiffrement El Gamal

Le système d'El Gamal est un système de chiffrement asymétrique inventé par Taher El Gamal en 1984.

**Principe de fonctionnement**

- Les deux interlocuteurs A et B se mettent d'accord sur deux entiers : un générateur $g$ et une base $p$
- Génération de clés :
  - A choisit un entier $x \in ]0, p-1[$ qui est sa clé secrète
  - A calcule $y = g^x \ mod \ p$ et le diffuse
  - la clé publique est $(p, g, y)$
- Chiffrement :
  - B veut chiffrer un message $m$
  - B choisit aléatoirement un entier $k$
  - B calcule $c_1 = g^k \ mod \ p$ et $c_2 = (y^k \times m) \ mod \ p$
  - B envoie à A le message chiffré $(c_1, c_2)$
- Déchiffrement :
  - A reçoit le message chiffré $(c_1, c_2)$
  - A calcule $r = (c_1)^{p-1-x}$
  - A calcule le message en clair $m = (r \times c_2) \ mod \ p$

**Avantages**

- L'entier aléatoire $k$ est difficile à trouver.
- Un même caractère peut être chiffré avec des $k$ différents.

**Inconvénients**

- La taille du message chiffré est importante (deux fois plus grande que la taille du message initial).

**Exemple**

- Deux personnes A et B se mettent d'accord sur $p = 11$ et $g = 2$
- A choisit sa clé secrète $x = 5$ et calcule $y = 2^5 \ mod \ 11 = 10$
- La clé publique est $(11, 2, 10)$
- ===Chiffrement===
- B veut envoyer le message "bhf" à A (b=1, h=7, f=5)
- B choisit $k = 6$ et chiffre la première lettre de son message en calculant $c_1$ et $c_2$ comme suit : $c_1 = 2^6 \ mod \ 11 = 9$ et $c_2 = (10^6 \times 1) \ mod \ 11 = 1$

- B envoie à A le couple (9,1)
- B choisit $k = 4$ et chiffre la deuxième lettre de son message : $c_1 = 2^4 \ mod \ 11 = 5$ et $c_2 = (10^4 \times 7) \ mod \ 11 = 7$
- B envoie à A le couple (5,7)
- B choisit $k = 7$ et chiffre la deuxième lettre de son message : $c_1 = 2^7 \ mod \ 11 = 7$ et $c_2 = (10^7 \times 5) \ mod \ 11 = 6$
- B envoie à A le couple (7,6)
- ===Déchiffrement===
- En recevant le premier couple (9,1), A déchiffre le message de B en calculant $r = 9^{11-1-5} \ mod \ 11 = 1$ et $m = (1 \times 1) \ mod \ 11 = 1 \rightarrow$ 'b'
- A procède de la même façon pour le deuxième couple $r = 5^{11-1-5} \ mod \ 11 = 1$ et $m = (1 \times 7) \ mod \ 11 = 7 \rightarrow$ 'h'
- De même pour le dernier couple $r = 7^{11-1-5} \ mod \ 11 = 10$ et $m = (10 \times 6) \ mod \ 11 = 5 \rightarrow$ 'f'

## Signature El Gamal

- A désire signer un message $m$ et l'envoyer à B
  - A calcule $s_1 = g^n \ mod \ p$ ($n$ est un entier aléatoire)
  - A calcule $s_2$ tel que : $m = (s_1 \times x + s_2 \times n) \ mod \ (p - 1)$
  - A envoie le message m avec la signature $(s_1, s_2)$
- B reçoit le message $m$ avec $(s_1, s_2)$ et procède à la vérification de la signature
  - B calcule $(y^{s_1} \times s_1^{s_2}) \ mod \ p$ et la compare avec $g^m \ mod \ p$
  - Si les deux valeurs sont égales alors la signature est bonne
  - Sinon, la signature est falsifiée

## Exemple

- A et B se mettent d'accord sur $p = 11$ et $g = 2$
- A souhaite envoyer un message $m = 5$ signé à B
- A choisit un nombre secret aléatoire $x = 8$
- A calcule $y = 2^8 \ mod \ 11 = 3$
- La clé publique est (11,2,3)
- ===Signature===
- Pour signer le message $m = 5$, A choisit $n = 9$
- A calcule $s_1 = 2^9 \ mod \ 11 = 6$
- A calcule $s_2$ tel que $(s_1 \times x + s_2 \times n) = m \ mod \ (p - 1)$
  - $(6 \times 8 + s_2 \times 9) = 5 \ mod \ 10$
  - $9 \times s_2 = 7$
  - $s_2 = 7 \times 9^{-1}$

    - L'inverse de 9 dans 10 est 9 (voir l'algorithme d'Euclide étendu section 2.6)
    - $s_2 = 7 \times 9 = 63 \ mod \ 10$
    - $s_2 = 3$
- A envoie à B le message $m = 5$ avec la signature (6,3)
- ===Vérification de la signature===
- En recevant le message et la signature, B procède à la vérification de ces derniers
- B calcule $(y^{s_1} \times s_1^{s_2}) \ mod \ p = (3^6 \times 6^3) \ mod 11 = 10$
- B calcule également $g^m \ mod \ p = 2^5 \ mod \ 11 = 10$
- La signature correspond bien au message reçu.

# Cryptographie hybride

## Sommaire



## 4.1 Introduction

La cryptographie hybride est un système de cryptographie faisant appel aux deux grandes familles de systèmes cryptographiques : la cryptographie symétrique et la cryptographie asymétrique. Cette combinaison permet de bénéficier des avantages des deux systèmes et de pallier certains de leurs incovénients.

### Principe de fonctionnement

La figure 4.1 présente le prinicipe de fonctionnement de la plupart des systèmes de cryptographie hybride qui est le suivant :

- Une clé aléatoire est générée avec un crypto-système symétrique.
- Le destinataire génère une clé publique et une clé privée. La clé publique sert à chiffrer la clé aléatoire. Étant donné que cette dernière est courte, la chiffrer est une opération rapide, alors que chiffrer le message avec un algorithme asymétrique aurait été plus long.
- L'émetteur envoie le message chiffré (à l'aide de la clé aléatoire) accompagné de la clé chiffrée correspondante.
- Le destinataire utilise sa clé privée pour déchiffrer la clé aléatoire. Avec cette dernière, il retrouve le message via un déchiffrement symétrique.

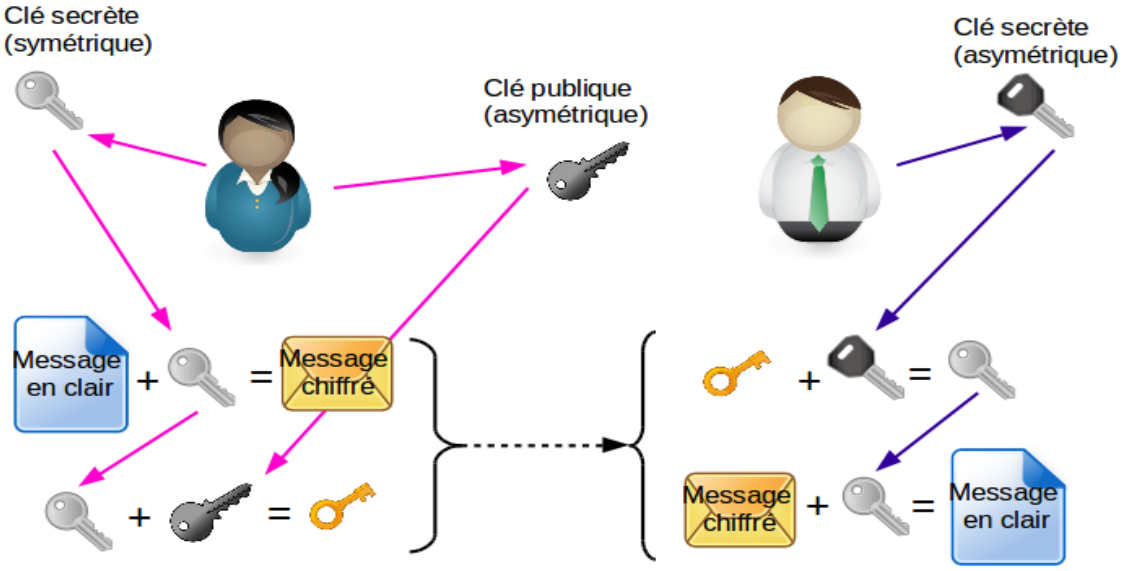


FIGURE 4.1 – Procédure de chiffrement hybride

### Exemples de crypto-systèmes hybrides

- PGP (Pretty Good Privacy) : crypto-système symétrique IDEA + crypto-système asymétrique RSA.
- S/MIME (Secure/Multipurpose Internet Mail Extensions).

## 4.2 PGP (Pretty Good Privacy)

PGP (Pretty Good Privacy) est un cryptosystème hybride développé par *Philip Zimmermann* en 1991, proposant de garantir la confidentialité et l'authentification lors des communications. Il est très utilisé dans les applications des courriers électroniques.

- L'émetteur génère un nombre aléatoire de 128 bits qu'il utilise comme clé de session pour chiffrer uniquement le message courant
- ==Chiffrement==
- Le message est chiffré avec la clé de session en utilisant un cryptosystème symétrique.
- La clé de session est chiffrée avec RSA (ou autre cryptosystème asymétrique) en utilisant la clé publique du destinataire
- ==Déchiffrement==
- Le destinataire utilise RSA avec sa clé privé afin de déchiffrer la clé de session qui a servi au chiffrement du message (cryptosystème asymétrique)
- Une fois la clé de session trouvée, le destinataire l'utilise pour déchiffrer le message (cryptosystème symétrique)

# Fonctions de hachage cryptographique

## Sommaire



## 5.1 Définition

Une fonction de hachage cryptographique est une fonction permettant de transformer une donnée de taille quelconque en une donnée de taille fixe. La donnée en question peut être du texte, une image ou sous une autre forme. Elle sera transformée en binaire avant de lui appliquer la fonction de hachage.

Notons $H$ la fonction de hachage et $M$ un message de longueur variable. La valeur $h = H(M)$ est de longueur fixe, elle est jointe au message lors de sa transmission.
Le receveur du message $M$ authentifie ce message en recalculant la valeur de $h$ qui doit être égale à celle reçue avec le message.

## 5.2 Caractéristiques d'une fonction de hachage cryptographique

Une fonction de hachage cryptographique $H$ doit avoir certaines propriétés avant d'être utilisée :

1. $H$ est applicable sur un bloc de données de taille quelconque ;
2. $H$ fournit un résultat de taille fixe ;
3. Pour un $x$ donné, il devrait être facile de calculer $H(x)$. En pratique, la fonction $H$ est implémentée matériellement ou logiquement ;
4. Pour un $y$ donné, il est difficile de trouver une image inverse $x$ tel que $y = H(x) \rightarrow$ $H$ est une fonction à sens unique ;
5. Pour tout $x$, il est difficile de trouver un $z$ tel que $H(x) = H(z) \rightarrow$ propriété de faible résistance aux collisions ;

6. Il est difficile de trouver $x, z$ tels que $x \neq z$ et $H(x) = H(z) \rightarrow$ propriété de résistance forte aux collisions ;

## 5.3 Exemples d'utilisation des fonctions de hachage cryptographiques

### Vérification des mots de passe

La vérification de mot de passe est une méthode proposée par *Roger Needham*. Dans cette méthode, au lieu de stocker les mots de passe des utilisateurs en clair, il suffit de stocker la valeur de hachage de chaque mot de passe. Ainsi, le risque de corruption du fichier des mots de passe est réduit. Lorsqu'un utilisateur procède à l'authentification, le mot de passe fournit $(x)$ est haché $(H(x))$ et est comparé avec la valeur stockée dans le serveur $(y)$. i.e. si $H(x) = y$ alors le mot de passe est correct.

### Vérification de l'intégrité des fichiers

Lors du téléchargement d'un fichier par exemple, on peut vérifier son intégrité en comparant la valeur de hachage du fichier avant et après son téléchargement. Si sa valeur de hachage n'a pas changé, le fichier n'a pas été modifié.
Certains sites web (Linux mint par exemple) affichent des valeurs de hachage obtenues par des fonctions telles que MD5, SHA-1 ou SHA-2, ce qui permettra aux utilisateurs de vérifier l'intégrité du contenu téléchargé.

# Exercices

## Exercice 1

Chiffrer le message « La rencontre est prévue à la bibliothèque » à l'aide du chiffrement par décalage avec la clé $k = 7$

## Exercice 2

Déchiffrer le message suivant qui a été chiffré en utilisant le cryptosystème de César avec une clé $k = 12$
« v'muyq xm odkbfasdmbtuq »

## Exercice 3

En utilisant le cryptosystème de Vigenère, chiffrer le message « ceci est un secret » avec la clé "attention"

## Exercice 4

Déchiffrer le message suivant en utilisant la méthode de Vigenère avec le mot clé « cours »
« esmkdjsoiwfsfrhcimv »

## Exercice 5

Chiffrer le message « je suis étudiant en informatique » en utilisant la table de substitution suivante :

| A | B | C | D | E | F | G | H | I | J | K | L | M | N |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| H | M | P | F | O | A | N | V | G | Q | X | B | W | Z |

| O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|
| I | L | E | U | K | T | D | J | C | S | R | Y |

## Exercice 6

Le texte suivant a été chiffré en utilisant le cryptosystème de César. En utilisant l'analyse fréquentielle, trouver la clé de chiffrement et le texte en clair.

WHZZHNL / MPSAYHNL : KLZ ZFULYNPLZ WVBY KLTHPU
CLYZ SL JVUJLWA KL YLUMVYJLTLUA ZLYPLS KL SH ZLJBYPAL .

H S'OLBYL VB S'VWPUPVU WBISPXBL WYLUK BUL JVUZJPLUJL HJJYBL KLZ KHUNLYZ XB'LSSL LUJVBYA, UVBZ KLCVUZ HCVPY BU YLNHYK PUJPZPM ZBY S'PTWSPJHAPVU ZLJBYPAHPYL XBP UVBZ LJOVPA. AVBAL SH XBLZAPVU KL SH ZLJBYPAL PUMVYTHAPXBL YLWVZL ZBY BU LAHA KL IPWVSHYPAL PUZAHISL : AVBA KVPA LAYL HWWHYLUA LA AVBA KVPA LAYL JHJOL, LA PUCLYZLTLUA.
WVBY KVUULY BU LELTWSL ZPTWSL, BU KPZWVZPAPM KL MPYLDHSS BWNYHKL , LU VILYHUA SLZ KPZWVUPIPSPALZ JSPLUA/ZLYCLBY , WVBYYHPA NLULYLY BU MSBZOPUN PUJVUAYVSHISL KLZ JVUZPNULZ KL ZLJBYPAL, JL XBP JVUZAPABLYHPA SL IHJRKVVY VYPMPJL PKLHS WVBY PUAYBKLYZ THSPUALUAPVUULZ.
VU CVPA HPUZP HPZLTLUA XBL SH YBWABYL ZFZALTPXBL LUAYL SH WYHEPZ JVBABTPLYL KLZ VWLYHALBYZ K'BU ZFZALTL LA SL WYVJLZZ KL ZLJBYPZHAPVU YHAPVUUHSPZLL TLA LU WLYPS SL JVUJLWA KL YLUMVYJLTLUA ZLYPLS KL SH ZLJBYPAL .
WVBY TLAAYL HB WVPUA BUL WYVJLKBYL KL YLTLKPHAPVU, QL WYLJVUPZL S'HKVWAPVU K' BUL ZAYHALNPL KLJPZPVUUHPYL LU AYVPZ ALTWZ MVYAZ :
- TLAAYL HB WVPUA BU IPSHU JYPAPXBL KL SH OPLYHYJOPZHAPVU WFYHTPKHSL KLZ KLNYLZ KL KHUNLYVZPAL
- YLUKYL VWLYHAPVUULSZ SLZ HJXBPZ WHAYPTVUPHBE LU ALYTLZ KL AYHPALTLUA LMMPJPLUA KLZ ZPABHAPVUZ KL JHAHZAYVWOL
- KLZPNULY KL MHJVU JVSSLNPHSL BUL LXBPWL JVOLYLUAL JOHYNLL K'HJJLSLYLY S'LEALYUHSPZHAPVU KLZ KPMMPJBSALZ PUOLYLUALZ HB WYVJLZZBZ JVUJLYUL

## Exercice 7

En utilisant le chiffrement par fonctions affines, donnez le texte chiffré correspondant au texte en clair P = « cibleabbattue » avec la clé k = (7,3) ; (a=7, b=3)

## Exercice 8

Dans un alphabet de 27 lettres (caractère Blanc = 26), utilisez le chiffrement affine avec clé a=13 et b=9 pour déchiffrer le texte chiffré « THRPXDH »

# Exercice 9

On suppose qu'un chiffrement affine E(x) = (ax + b) MOD 26 transforme H en X et Q en Y.
- Déterminer la fonction de chiffrement (a et b).
- Combien de fonctions de transformations affines possibles peut-on avoir dans ce cas ?
- Chiffrer le message «RDV DEMAIN».

# Exercice 10

Soit la matrice clé :

$$M = \begin{pmatrix} 3 & 1 \\ 4 & 3 \end{pmatrix}$$

Chiffrer à l'aide du cryptosystème de Hill la phrase : Message en clair.

# Exercice 11

Soit la matrice M suivante et l'alphabet alpha A,B,....Z
- Donnez le texte chiffré C correspondant au texte en clair P = DCOD

$$M = \begin{pmatrix} 2 & 3 \\ 5 & 7 \end{pmatrix}$$

- Donnez le texte en clair P correspondant au texte chiffré LN

# Exercice 12

Pour pouvoir renforcer son chiffrement, un étudiant décide de chiffrer son texte clair à l'aide des deux matrices suivantes. Le texte chiffré obtenu avec la première matrice est chiffré une deuxième fois avec la deuxième matrice.

$$A1 = \begin{pmatrix} 3 & 11 \\ 4 & 15 \end{pmatrix} \quad A2 = \begin{pmatrix} 10 & 15 \\ 5 & 9 \end{pmatrix}$$

- Donnez le texte chiffré correspondant au texte clair SEND de l'alphabet des 26 lettres
- Donnez le texte en clair correspondant au texte chiffré ZMOY
- Le renforcement du chiffrement souhaité par l'étudiant est inutile, pourquoi ? comment le rendre effectif ?

# Exercice 13

- Qu'est ce qui justifie la confiance accordée au protocole RSA lorsque les nombres p et q sont premiers de tailles importantes ?

- Pourquoi RSA ne peut être utilisé efficacement pour crypter et décrypter les communications téléphoniques via portables ?

# Exercice 14

On considère les valeurs p= 53,q= 11 et e= 3.

- Calculez la valeur publique n.
- Calculez la fonction d'Euler $\phi(n)$.
- Utilisez l'algorithme étendu d'Euclide pour calculer la valeur de la clé privée $d$.

# Exercice 15

Un professeur envoie ses notes au secrétariat par mail. La clé publique du professeur est (3,55) ; celle du secrétariat est(3,33).

- Vérifier que la clé privée du professeur (supposée connue de lui seul) est 27 ; et que celle du secrétariat est 7.
- Pour assurer la confidentialité de ses messages, le professeur chiffre les notes avec la clef RSA du secrétariat. Quel message chiffré correspond à la note 12 ?
- Pour assurer l'authenticité des messages contenant les notes, le professeur signe ses messages pour le secrétariat après les avoir chiffrés. Le secrétariat reçoit le message 23. Quelle est la note correspondante ?

# Exercice 16

Une personne utilise le protocole RSA et publie sa clé publique N= 187 et e= 3.

- Chiffrer le message m=15 avec la clé publique donnée.
- En utilisant le fait que $\phi(N) = 160$, retrouver la factorisation de N, puis la clé privée de cette personne.

# Exercice 17

Effectuer le chiffrement et le déchiffrement en utilisant l'algorithme RSA pour les valeurs suivantes :

- p = 3 ; q = 11 ; e = 7 ; M = 5
- p = 5 ; q = 11 ; e = 3 ; M = 9
- p = 7 ; q = 11 ; e = 17 ; M = 8
- p = 11 ; q = 13 ; e = 11 ; M = 7
- p = 17 ; q = 31 ; e = 7 ; M = 2

## Exercice 18

Soit un système à clé publique utilisant le RSA, vous interceptez le texte chiffré C=10 envoyé par un utilisateur dont la clé publique est e = 5 et n = 35.
Que vaut M ?

## Exercice 19

Dans un système RSA, la clé publique d'un utilisateur donné est e = 31, n = 3599. Quelle est la clé privée de cet utilisateur ?

## Exercice 20

Considérons un cryptosystème RSA modulo n=35 et l'exposant de chiffrement e=7.

- Déterminer l'exposant de déchiffrement d du receveur B.
- Soit le message M = 2, chiffrez M en M' en utilisant les paramètres RSA ci-dessus.
- Si B a envoyé M (question précédente) à A, quel sera la signature associée à M et comment B vérifierait cette signature ?

## Exercice 21

Les utilisateurs A et B utilisent Diffie-Hellman avec p=71 et g=7

- Si la clé de l'utilisateur A est 5, que vaut Ya ?
- Si la clé de l'utilisateur B est 12, que vaut Yb ?
- Que vaut Kab ?

## Exercice 22

considérez un schéma Diffie-Hellman avec p=11 et g=2.

- si Ya = 9, que vaut a ?
- si Yb = 3, que vaut Kab ?

## Exercice 23

Soient deux partenaires A et B voulant ouvrir une session de communication confidentielle sur un support de communication non sécurisé (Internet par exemple).
A et B décide de choisir le protocole d'échange de Diffie-Hellman. Ils se mettent d'accord pour choisir le nombre premier p=13 et la base ou générateur g=2.
A choisit son exposant secret a=5, tandis que B choisit b=4.
a) Donnez les étapes intermédiaires suivies par A et B pour déterminer la clé symétrique S commune.

b) Un intrus ou attaquant C se met à l'écoute pour intercepter les messages échangés entre A et B et même injecter ses propres messages. Supposons que C génère un exposant secret c=7. Expliquez comment l'attaquant C utilise sa valeur secrète c pour réaliser l'attaque de l'homme de milieu (Man in the Middle) et déterminer les différentes clés entre "C et A" et "C et B".
c) Comment résoudre ce problème ?

# Exercice 24

Soit p un nombre premier p=13 et g= 2 un générateur de F*p. Si A choisit comme nombre secret x=5, quelle est la clé publique Apub de A ?

Si B choisit comme nombre secret h=3 et désire envoyer à A le message m=4, quel sera le chiffrement m' de m et quelle sera la signature de m ?

# Exercice 25

Soit l'alphabet Zn avec n=11 formé des 10 chiffres décimaux et le point
Zn=(0,1,2,3,4,5,6,7,8,9,.).
Soient A et B désireux ouvrir une session de communication confidentielle.
Sachant que p=7 et q=3, A choisit un nombre secret 5 ; B choisit également le nombre 3.

- Donnez les clés publiques KpubA de A et KpuB de B.
- Comment s'assurer que les clés publiques KpubA et KpubB appartiennent bien à A et B ?
- B décide d'envoyer le message $M = m_1m_2 = 22$ à A, donnez le message crypté $M' = m'_1m'_2$ associé à $M$.
- Comment A peut vérifier l'authenticité de M ?
- Quel est le problème rencontré par A et B d'avoir utilisé la même valeur n ?

B se met d'accord avec A pour que le message précédent $M = m_1m_2$ représente la clé d'un chiffrement affine $(a = m_1, b = m_2)$.

- Si maintenant A veut envoyer le message 56 à B quel sera alors le ciphertext du plaintext 56 ?

# Bibliographie


- *Introduction to cryptography with coding theory*. W. Trappe. Pearson Education India 2006.
- *Initiation à la cryptographie*. G. Dubertret. Vuibert 2018.
- *Exercices et problèmes de cryptographie*. D. Vergnaud & J. Stern. Dunod 2012.
- *Cryptography and network security : principles and practice*. W. Stallings. Upper Saddle River : Pearson, pp. 92-95, 2017.
- *Notes de cryptographie*. R.M. Amadio. 2018.
- *Arithmétique modulaire et cryptologie*. P. Meunier. Cépaduès 2010.
- *A course in number theory and cryptography*. N. Koblitz. Springer Science & Business Media, Vol. 114, 1994.
- *Cryptography : The science of secret writing*. L. D. Smith. Courier Corporation 1955.
- *Handbook of applied cryptography*. J. Katz, A.J. Menezes, P.C. Van Oorschot & S.A. Vanstone. CRC press 1996.
- *A classical introduction to cryptography exercise book*. T. Baigneres, P. Junod, Y. Lu, S. Vaudenay & J. Monnerat. Springer science & business media 2006.