SÉCURITÉ INFORMATIQUE

3ème Année Informatique

Chapitre 2 :

Initiation à la cryptographie

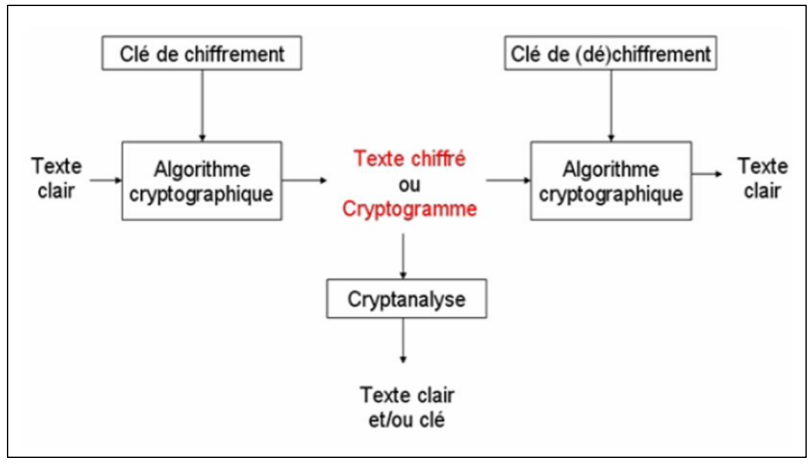
Introduction

L'objectif fondamental de la cryptographie est de permettre à deux personnes de communiquer à travers un canal peu sûr de telle sorte qu'un opposant passif ne puisse pas comprendre ce qui est échangé et que les données échangées ne puissent pas être modifiées ou manipulées par un opposant actif.

Introduction

- **La cryptologie** est une science très ancienne : les hommes ont toujours eu besoin de dissimuler des informations et de transmettre des messages en toute confidentialité.
- Le terme cryptologie vient du grec ”kruptos” signifiant secret, caché et de logos signifiant discours.
- La cryptologie est donc la science du secret. Elle regroupe la cryptographie et la cryptanalyse,
  - **La cryptographie** a pour but de concevoir des systèmes visant à assurer la sécurité des communications sur un canal public,
  - **La cryptanalyse** vise à trouver des failles dans ces systèmes..

1. Vocabulaire et définitions



Protocole de chiffrement

1. Vocabulaire et définitions

- **Cryptologie :** Il s'agit d'une science mathématique comportant deux branches : la cryptographie et la cryptanalyse.
- **Cryptographie :** La cryptographie est l'étude des méthodes donnant la possibilité d'envoyer des données de manière confidentielle sur un support donné.
- **Texte en clair(Plain text) :** Données lisibles et compréhensible sans intervention spécifique.
- **Texte chiffré(Cipher text) :**Texte inintelligible résultant du chiffrement.
- **Cryptage(chiffrement) :** Méthode permettant de crypter un texte en clair en changeantsoncontenu.Cetteopérationpermets'assurerqueseuleslespersonnesauxquel leslesinfos.Sontdestinéespourrontyaccéder.
- **Décryptage(déchiffrement):** Processus inverse de transformation du texte chiffré en texte clair.
- **Clé :** Il s'agit du paramètre impliqué et autorisant des opérations de chiffrement et/ou déchiffrement.

1. Vocabulaire et définitions

- **Cryptanalyse :** Opposée à la cryptographie, elle a pour but de retrouver le texte clair à partir de textes chiffrés en déterminant les failles des algorithmes utilisés.
- **Cryptosystème :** Il est défini comme l'ensemble des clés possibles (espace de clés), des textes clairs et chiffrés possibles associés à un algorithme donné. L'algorithme est en réalité un triplet d'algorithmes :
  - L'un générant les clés,
  - Un autre pour chiffrer le message en clair, et
  - Un troisième pour déchiffrer le texte chiffré.

Notations

• En cryptographie, la propriété de base est que :

$$\mathbf{M = D(E(M))}$$

où :

- M représente le texte clair,
- C est le texte chiffré,
- K est la clé (dans le cas d'un algorithme à clé symétrique), E_k et D_k dans le cas d'algorithmes asymétriques,
- E(x) est la fonction de chiffrement, et
- D(x) est la fonction de déchiffrement.

Principe de Kerckhoff

• En 1883 *Auguste Kerckhoffs* posa les principes de la cryptographie moderne.

• La sécurité d'un cryptosystème ne doit pas reposer sur le secret de l'algorithme de codage mais qu'elle doit uniquement reposer sur la clé secrète du cryptosystème qui est un paramètre facile à changer, de taille réduite et donc assez facile à transmettre secrètement.

• Les systèmes conçus dans le secret révèlent souvent rapidement des défauts de sécurité qui n'avaient pas été envisagés par les concepteurs.

• Si un algorithme est supposé être secret, il se trouvera toujours quelqu'un soit pour vendre l'algorithme, soit pour le percer à jour, soit pour en découvrir une faiblesse ignorée de ses concepteurs. À ce moment là c'est tout le cryptosystème qui est à changer et pas seulement la clé.

2. Attaques sur un chiffrement

• La cryptanalyse est l'ensemble des procédés d'attaque d'un cryptosystème.

• On suppose (principes de Kerckhoffs) que l'attaquant connait le système cryptographique utilisé, la seule partie secrète du cryptosystème est la clé.

• **Principaux types d'attaques**

➢ *L'attaque à texte chiffré seulement :* Le cryptanalyste dispose du texte chiffré de plusieurs messages chiffrés avec le même algorithme. La tâche du cryptanalyste est de retrouver le plus grand nombre de messages clairs possibles ou les clés qui ont été utilisées, ce qui permettrait de déchiffrer d'autres messages chiffrés avec ces mêmes clés.

➢ *L'attaque à texte clair connu :* Le cryptanalyste a non seulement accès aux textes chiffrés de plusieurs messages, mais aussi aux textes clairs correspondants. La tâche est de retrouver la ou les clés qui ont été utilisées pour chiffrer ces messages ou un algorithme qui permet de déchiffrer d'autres messages chiffrés avec ces mêmes clés.

➢ *L'attaque à texte clair choisi :* Le cryptanalyste a non seulement accès aux textes chiffrés et aux textes clairs correspondants, mais de plus il peut choisir les textes en clair. Cette attaque est plus efficace que l'attaque à texte clair connu, car le cryptanalyste peut choisir des textes en clair spécifiques qui donneront plus d'informations sur la clé.

➢ *L'attaque à texte chiffré choisi :* Le cryptanalyste peut choisir différents textes chiffrés à déchiffrer. Les textes déchiffrés lui sont alors fournis. Par exemple, le cryptanalyste a un dispositif qui ne peut être désassemblé et qui fait du déchiffrement automatique. Sa tâche est de retrouver la clé.

3. Cryptographie Classique

- La science de la cryptographie est utilisée depuis l'antiquité.
- Elle est basée sur l'utilisation des lettres de la langue pour le chiffrement des textes.
- La même clé est utilisée pour le chiffrement et pour le déchiffrement.
- Cette catégorie continué jusqu'à la fin de deuxième guerre mondiale.
- Ces cryptosystèmes sont appliques pour protéger les documents physiques dans les domaines militaires et diplomatiques.

3.1. Codes à répertoire

Ils consistent en un dictionnaire qui permet de remplacer certains mots par des mots différents. Ils sont très anciens et ont été utilisés intensivement jusqu'au début du 20-ième siècle.

• Ils ont fait l'objet d'une critique sévère de A. Kerchkoffs dans son article fondateur.

• On peut par exemple créer le dictionnaire suivant :

rendez-vous ↔ 175	demain ↔ oiseaux
midi ↔ à vendre	Villetaneuse ↔ au marché

- La phrase en clair: RENDEZ VOUS DEMAIN MIDI VILLETANEUSE

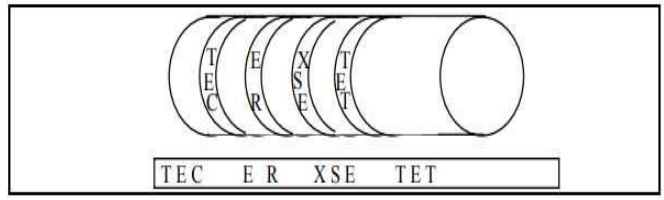
- Devient avec ce code : 175 OISEAUX À VENDRE AU MARCHÉ

3.2. Chiffrement par transposition

Les méthodes de chiffrement par transposition consistent à réarranger les données à chiffrer de façon à les rendre incompréhensibles. Il s'agit par exemple de réordonner géométriquement les données pour les rendre visuellement inexploitables.

La technique assyrienne

- Cette technique de cryptage est vraisemblablement la première preuve de l'utilisation de moyens de chiffrement en Grèce dès 600 avant Jésus Christ pour dissimuler des messages écrits sur des bandes de papyrus.



La technique assyrienne

La technique consistait à:

- enrouler une bande de papyrus sur un cylindre appelé scytale ;
- écrire le texte longitudinalement sur la bandelette ainsi enroulée

Question :

comment le destinataire déchiffrerait le message sur le scytale ?

- Le message une fois déroulé n'est plus compréhensible
- Il suffit au destinataire d'avoir un cylindre de même rayon pour pouvoir déchiffrer le message

Exemple :

Soit la matrice M(6,5)=

M	E	S	S	A	G
E		S	E	C	R
E	T		A		T
R	A	N	S	P	O
S	E	R			

Le message crypté est donc: MEERSE TAESS NRSEAS AC P GRTO

Amélioration de la technique assyrienne

-Pour pouvoir modifier le code rapidement sans toucher à son principe et pouvoir ainsi augmenter la sécurité les deux interlocuteurs peuvent décider l'ajout d'une clé.

- Le but est de pouvoir changer facilement le cryptage d'un message tout en gardant le même algorithme de codage. Pour cela on rajoute une clé secrète constituée par l'ordre de lecture des col

Exemple : Pour l'exemple précèdent on choisit la clé : CAPTER

- On numérote les colonnes en fonction du rang des lettres du mot CAPTER dans l'alphabet c'est-à-dire : **2, 1, 4, 6, 3, 5**

- Et on lit les colonnes dans l'ordre indiqué.

E□TAEMEERSSEAS□ GRTO□ SS□NR AS□P□

- On a 6! codes différents.

- Pour décoder le message précédent on range en colonne sur la grille en suivant l'ordre des colonnes donné par le mot de code :

donnes.

3.3. Chiffrement par substitution

Le chiffrement par substitution, consiste à remplacer dans un message une ou plusieurs entités (généralement des lettres) par une ou plusieurs autres entités.

- Substitution monoalphabétiques : Consiste à remplacer chaque lettre du message par une autre lettre de l'alphabet.
- Substitution polyalphabétique : consiste à utiliser une suite de chiffres monoalphabétiques réutilisée périodiquement.
- Substitution homophonique : permet de faire correspondre à chaque lettre du message en clair un ensemble possible d'autres caractères.
- Substitution de polygrammes : consiste à substituer un groupe de caractères (polygramme) dans le message par un autre groupe de caractères.

3.3.1 Chiffre de César (50 av. J-C)

- Il s'agit d'un des plus simples et des chiffres classiques les plus populaires.
- Son principe est un décalage des lettres de l'alphabet.
- Jules César pendant la guerre des Gaules avait utilisé le code de substitution par flot suivant :

lettre codée = lettre claire + 3 modulo 26

Exemple :

Le message en clair :

RENDEZ VOUS DEMAIN MIDI VILLETANEUSE

- Devient :

UHQGHC YRXV GHPDLQ PLGL YLOOHWDQHXVH

- On peut considérer toute la famille des codes :

lettre codée = lettre claire + n modulo 26

- Où n est un entier entre 0 et 25 appelé la clé du code.

Avec la clé n = 7, le texte codé du message précédent devient :

YLUKLG CVBZ KLTHPU TPKP CPSSLAHULBZLBZL

- Le décodage se fait en utilisant la relation :

lettre claire = lettre codée -n mod 26

- On a affaire à un code en continu ou par flots symétrique ou à clé secrète.

Analyse de fréquences

• Le chiffre de César repose sur une simple méthode de substitution de lettres.

• Ce sont les érudits et savants de l'empire arabe qui sont à l'origine de la cryptanalyse de ce chiffre.

• En effet Abu Yusuf Al-Kindi découvre aux alentours du IXème siècle, une méthode très simple permettant de venir à bout du chiffre de César *: l'attaque par analyse des fréquences.*

• Cette analyse des fréquences consiste à répertorier toutes les lettres du texte chiffré et de comparer leur nombre avec le tableau des fréquences des lettres de la langue correspondante.

Analyse de fréquences

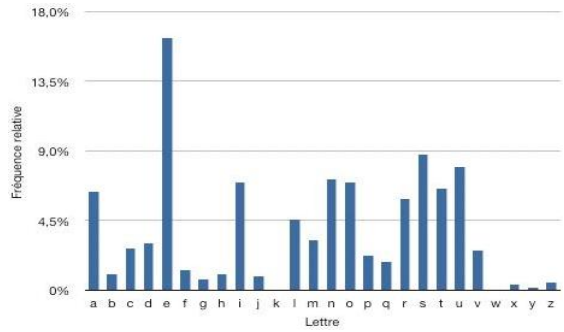


Tableau des fréquences des lettres en français.

• Ainsi, dans un texte chiffré en français, si une lettre apparaît aux environs des 16%, nous pourrons assimiler cette lettre à un E ; et ainsi de suite avec les autres lettres du texte chiffré.

• **Exemple**

- Voici par ordre décroissant des fréquences la répartition des lettres en français :

E	17,76	S	8,23	A	7,68	N	7,61	T	7,30	I	7,23
R	6,81	U	6,05	L	5,89	O	5,34	D	3,60	C	3,32
P	3,24	M	2,72	Q	1,34	V	1,27	G	1,10	F	1,06
B	0,80	H	0,64	X	0,54	Y	0,21	J	0,19	Z	0,07
K	0,01	W	0,00								

- Voici un texte chiffré en utilisant le chiffre de César ; on ne connait pas ici la clé utilisée : SEGELAZEW AOP QJ LNKFAP Z AJYUYHKLAZEA CNWPQEPA AYNEPA YKKLANWPERAIAJP

- Nous pouvons constater que c'est la lettre A qui est la plus fréquente dans le message chiffré. Celle-ci a donc de grande chance de représenter la lettre E dans le message clair.

- Nous obtiendrons dans ce cas un décalage de 22 lettres puisque l'on a supposé A = E. Muni de cette clé, nous pouvons décrypter le reste du message, ce qui nous donne :

Wikipédia est un projet d'encyclopédie gratuite écrite coopérativement

3.3.2. Chiffre de Vigenère (1568)

- C'est une amélioration décisive du chiffre de César.
- Sa force réside dans l'utilisation non pas d'un, mais de 26 alphabets décalés pour chiffrer un message. On parle du **carré de Vigenère**.
- Ce chiffre utilise une clé qui définit le décalage pour chaque lettre du message.
- Dans le carré de vigenère :

- La lettre de la clé est dans la colonne la plus à gauche.
- La lettre du message clair est dans la ligne tout en haut.
- La lettre chiffrée est à l'intersection des deux.

• Carré de Vigenère :

	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
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Exemple :

- Chiffrement du texte "CHIFFRE DE VIGENERE" avec la clé "BACHELIER" (cette clé est éventuellement répétée plusieurs fois pour être aussi longue que le texte clair).

Clair	C	H	I	F	F	R	E	D	E	V	I	G	E	N	E	R	E
Clef	B	A	C	H	E	L	I	E	R	B	A	C	H	E	L	I	E
Décalage	1	0	2	7	4	11	8	4	17	1	0	2	7	4	11	8	4
Chiffré	D	H	K	M	J	C	M	H	V	W	I	I	L	R	P	Z	I

- La grande force du chiffre de Vigenère est que la même lettre sera chiffrée de différentes manières d'où perte de la fréquence des lettres, ce qui rend inutilisable l'analyse de fréquence classique

3.3.3. Chiffre affine

- L'idée est d'utiliser comme fonction de chiffrement une fonction affine du type :

$$y = (ax + b) \bmod 26$$

- Où a et b sont des constantes, et où x et y sont des nombres correspondant aux lettres de l'alphabet (A = 0,B = 1,...).
- On peut remarquer que si a = 1, alors on retrouve le chiffre de César où b est le décalage (le k du chiffre de César).
- *Propriété de neutralité :* si b = 0, alors "a" est toujours chiffré "A" car il ne subit aucun décalage. L'alphabet de départ se retrouve chiffré par lui même, et donc ne subit aucune modification.
- Pour le chiffre affine, la clé est constituée de (k_1, k_2) où $k_1, k_2 \in [0, 25]$ et telle que :

$$\text{pgcd}(k_1, 26) = 1.$$

Sécurité informatique : Initiation à la cryptographie

- Le chiffrement en lui-même est donné par :

$$c_i = f(m_i) = k_1 * m_i + k_2 \bmod 26.$$

- Pour le déchiffrement, il vient :

$$m_i = f^{-1}(c_i) = k_1^{-1} * (c_i - k_2) \bmod 26.$$

- Par le chiffre affine, on obtient 312 clés possibles. En effet, pour respecter la propriété de k_1, il n'y a que 12 choix possibles. Et puisque k_2 peut prendre n'importe quelle valeur dans [0, 25], il vient 12 * 26 = 312.

- Exemple : Soit la clé = $(k_1, k_2) = (3, 11)$

- Transformation de chiffrement : $c_i = f(m_i) = 3 * m_i + 11 \bmod 26.$

- Transformation de déchiffrement :

$$k_1^{-1} = 3^{-1} \bmod 26 = 9 \text{ [car } 3 * 9 \bmod 26 = 1]$$

$$m_i = f^{-1}(c_i) = 9 * (c_i - 11) \bmod 26.$$

- Ainsi, pour une suite de lettres telle que 'NSA' → 13 18 0 → 24 13 11 →'YNL'.

27

Sécurité informatique : Initiation à la cryptographie

➢ **Cryptanalyse de chiffre affine**

- Il faut tout d'abord établir la fréquence relative de chaque lettre du texte chiffré, par analyse de fréquence.

- Exemple de texte chiffré : HGAHY RAEFT GAGRH DGAGM OEHIY RAAOT ZGAGJ GKFDG AZGSB INNTG KGRHE NNIRG

- On dénombre 12 fois la lettre G et 8 fois la lettre A.

- Supposons que le langage original du texte est le français. Sur base de l'analyse de fréquences, on en déduit les équations suivantes :

$$E \rightarrow G \Rightarrow f(E) = G$$

$$S \rightarrow A \Rightarrow f(S) = A$$

- Il en découle que : $4 \rightarrow 6 \Rightarrow f(4) = 6$

$$18 \rightarrow 0 \Rightarrow f(18) = 0$$

28

• On peut maintenant résoudre les équations pour retrouver k_1 et k_2 :

$$f(4) = 6, f(18) = 0$$
$$\downarrow$$
$$4 * k_1 + k_2 \equiv 6 \pmod{26}$$
$$18 * k_1 + k_2 \equiv 0 \pmod{26}$$
$$\downarrow$$
$$14\, k_1 \equiv -6 \bmod 26$$
$$\downarrow$$
$$k_1 = 7 \Rightarrow k_2 = 4.$$

• La fonction de déchiffrement est donc la suivante : $m_i = 15\ (c_i - 4) \bmod 26$.

• Et donc : HGAHYRAEFTGAGRHDGAGMOEHIYRAAOTZGAGJGKFDGAZGSB INNTGKGRHENNIRG

devient : TESTONSAPRESENTLESEQUATIONSSURDESEXEMPLESDECHIFFRE MENTAFFINE

3.3.4. Chiffrement polygraphique

• Il s'agit ici de chiffrer un groupe de n lettres par un autre groupe de n symboles. On citera notamment le chiffre de Playfair et le chiffre de Hill.

• Ce type de chiffrement porte également le nom de substitutions polygrammiques.

1. Chiffre de Playfair (1854)

• On chiffre 2 lettres par 2 autres. On procède donc par digramme. On dispose les 25 lettres de l'alphabet (W exclu car inutile à l'époque, on utilise V à la place) dans une grille de 5x5 construite sur la base d'une clé.

• La variante anglaise consiste à garder le W et à fusionner I et J.

• On remplit la grille avec les lettres du mot clé (en ignorant les doublons), ligne par ligne. Ensuite, on comble la grille avec les lettres restantes de l'alphabet.

• **Exemple :**

- Mot-clé = exemple playfair

- La grille est remplie comme suit :

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

• Il y a 4 règles à appliquer selon les deux lettres à chiffrer lors de l'étape de substitution. Pour le déchiffrement, on procède dans l'ordre inverse.

1. Si les lettres sont sur des "coins", les lettres chiffrées sont les 2 autres coins.

Ex : LA → ER , CA → BY

2. Si les lettres sont sur la même ligne, il faut prendre les deux lettres qui les suivent immédiatement à leur droite.

Ex : EM → XP , CH → DB

3. Si les lettres sont sur la même colonne, il faut prendre les deux lettres qui les suivent immédiatement en dessous.

Ex : YK → CT , MU → FM

4. Si elles sont identiques (ou s'il n'en reste qu'une), il faut insérer une nulle (habituellement le X) entre les deux pour éliminer ce doublon.

Ex : BALLON devient : "BA" "LX" "LO" "ON", ensuite on chiffre chaque digramme.

• **Exemple de chiffrement**

- Le message « Cache l'or dans la souche de l'arbre » :

CA CH EL OR DA NS LA SO UC HE DE LA RB RE

- Devient :

BY DB XE QI BF JU ER VJ TD BL BM ER AH AL

2. Chiffre de Hill (1929)

- Substitution simple par des polygrammes.
- L'algorithme remplace m lettres successives du texte en clair par m lettres chiffrées.
- La substitution se fait à l'aide de m équations linéaires où à chaque lettre est assignée une valeur numérique qui représente son rang dans l'alphabet (a=0, b=1, …, z=25).
- Les opérations de chiffrement et de déchiffrement dans le système de Hill sont définies comme suit :

$$C = E_k(P) = k.P \bmod 26$$

$$P = D_k(C) = k^{-1} . C \bmod 26 = k^{-1} K.P \bmod 26$$

- Où : P et C sont des vecteurs colonnes de taille m qui correspondent aux caractères du texte en clair et chiffré. K est une matrice (m x m) inversible qui représente la clé de chiffrement. Cette matrice est définie dans l'ensemble de l'alphabet A.

- Si on pose m = 3, on a donc :

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} \bmod 26$$

- On calcule les lettres du texte chiffré à l'aide de ces équations linéaires :

$c_1 = (k_{11}P_1 + k_{12}P_2 + k_{13}P_3) \bmod 26$

$c_2 = (k_{21}P_1 + k_{22}P_2 + k_{23}P_3) \bmod 26$

$c_3 = (k_{31}P_1 + k_{32}P_2 + k_{33}P_3) \bmod 26$

- **Exemple**

- On effectue le chiffrement par blocs de 2 lettres (m = 2).

- On cherche à chiffrer le message « TEXTEACRYPTER » en utilisant, comme clé, une matrice K dont le déterminant est premier avec 26.

- Par exemple, on utilise la matrice :

$$K = \begin{pmatrix} 3 & 5 \\ 6 & 17 \end{pmatrix}$$

dont le déterminant est 21. Comme 5 × 21 = 105 ≡ 1 (mod 26), 5 est un inverse de det(K) modulo 26.

- TEXTEACRYPTER → 19 ; 4 ; 23 ; 19 ; 4 ; 0 ; 2 ; 17 ; 24 ; 15 ; 19 ; 4 ; 17

- On regroupe les lettres par paires créant ainsi 7 vecteurs de dimension deux, la dernière paire étant complétée arbitrairement :

$$X_1 = (19;4); X_2 = (23;19); X_3 = (4;0); X_4 = (2;17); X_5 = (24;15); X_6 = (19;4); X_7 = (17;6).$$

- On multiplie (modulo 26) ensuite ces vecteurs par la matrice K, par exemple pour le premier vecteur :

$$Y_1 = \begin{pmatrix} 3 & 5 \\ 6 & 17 \end{pmatrix} \begin{pmatrix} 19 \\ 4 \end{pmatrix} \bmod 26 = \begin{pmatrix} 25 \\ 0 \end{pmatrix}$$

35

- On obtient alors 7 vecteurs, soit 14 lettres :

(25 ; 0) ; (8;19) ; (12 ; 24) ; (13 ; 15) ; (17 ; 9) ; (25 ; 0) ; (3 ; 22)

→ ZAITMYNPRJZADW

- Pour déchiffrer le cryptogramme, il faut inverser la matrice K :

$$k^{-1} = \begin{pmatrix} 17 & -5 \\ -6 & 3 \end{pmatrix}$$

et la multiplier (modulo 26) par l'inverse du déterminant de K c'est-à-dire par 5 :

$$B = \begin{pmatrix} 7 & 1 \\ 22 & 15 \end{pmatrix}$$

Connaissant les couples Y, il suffit de les multiplier (modulo 26) par la matrice B pour retrouver les couples X et réussir à déchiffrer le message. Par exemple pour le premier vecteur :

$$X_1 = \begin{pmatrix} 7 & 1 \\ 22 & 15 \end{pmatrix} \begin{pmatrix} 25 \\ 0 \end{pmatrix} \bmod 26 = \begin{pmatrix} 19 \\ 4 \end{pmatrix}$$

36

3.3.5. Chiffre de Vernam (One Time Pad - 1917)

• Le masque jetable, également appelé Chiffre de Vernam, est défini comme un chiffre de Vigenère avec la caractéristique que la clé de chiffrement a la même longueur que le message clair.

• Pour utiliser ce chiffrement, il faut respecter plusieurs propriétés :

- ➢ Choisir une clé aussi longue que le texte à chiffrer,
- ➢ Utiliser une clé formée d'une suite de caractères aléatoires,
- ➢ Protéger la clé,
- ➢ Ne jamais réutiliser une clé.

• **Exemple**

Clair	M	A	S	Q	U	E	J	E	T	A	B	L	E
Clef	X	C	A	A	T	E	L	P	R	V	G	Z	C
Décalage	23	2	0	0	19	4	11	15	17	21	6	25	2
Chiffré	J	C	S	Q	N	I	U	T	K	V	H	K	G

37

• **Exemple illustrant l'inviolabilité :**

- Soit le texte chiffré : CUSKQXWMFWITUK
- Soit le masque jetable possible : bgfbcdfbfdecdg
- Résultat : BONJOURLATERRE
- Soit un autre masque jetable : quauwtedbdisjg
- Résultat : MASQUESJETABLE
- Il est donc impossible de déterminer le bon masque.
- Le système du masque jetable, avec les précautions indiquées ci-dessus, est absolument inviolable si l'on ne connaît pas la clé.
- Le problème de ce système est de communiquer les clé de chiffrement ou de trouver un algorithme de génération de clé commun aux deux partenaires.

38

4. Machines à rotors

• Très vite après la première guerre, on s'est rendu compte que si l'on souhaitait diffuser beaucoup de documents chiffrés rapidement, et pouvoir changer de clé de chiffrement facilement, il fallait fabriquer des machines à chiffrer et à déchiffrer.

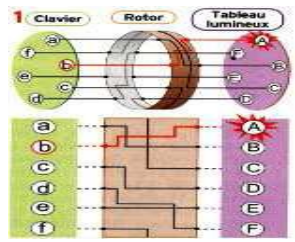
• Les machines utilisées à ces fins sont les machines à rotors (dont la plus célèbre était la machine ENIGMA à 3 rotors inventée dans les années 30).

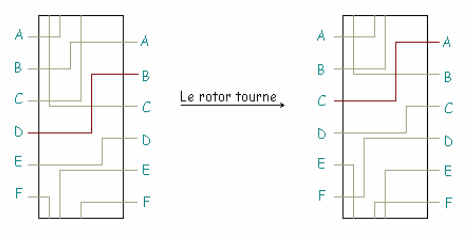
• Cette machine électrique est composée d'un clavier alphabétique, d'un écran lumineux et de trois rotors. Le système est simple : l'utilisateur tape une lettre sur le clavier et le texte chiffré apparaît alors sur l'écran. A chaque frappe sur le clavier, le premier rotor tournait d'une unité puis à la fin d'un tour complet décalait le deuxième rotor d'une unité et ainsi de suite. On positionnait initialement les rotors comme on voulait, ce qui définissait ainsi la clé.

• Pour chiffrer un message, une fois la clé fixée, il suffisait de le taper sur la machine et pour le déchiffrer de mettre les rotors dans la même position initiale et de taper le message chiffré.

39

Sécurité informatique : Initiation à la cryptographie





• Chaque message commençait par la donnée de la clé choisie par l'opérateur, qu'il cryptait elle aussi selon une liste de clé changeant tous les jours.

• La machine ENIGMA a été utilisée pendant toute la seconde guerre mondiale par l'armée allemande qui croyait en son inviolabilité.

• Une équipe de mathématiciens (spécialisée en cryptanalyse, art de déchiffrer des messages) anglais dirigée par A.Turing finit par la décrypter.

• En l'espace de quelques années, la cryptographie et la cryptanalyse sont passées de simples techniques désuètes, à véritables sciences.

40

4. Cryptographie moderne

- Il dépend de l'apparition de l'informatique dans les années 60 et l'augmentation des systèmes de communications.
- Elle est basée sur le langage machine 0/1.
- Elle est appliquée dans la majorité des applications, telles que: commerciales, financières, militaires, communications, transports, santé, etc.

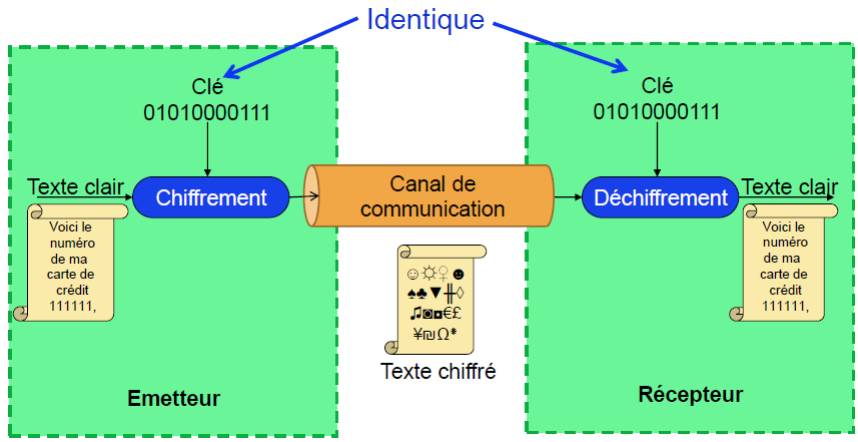
2. Histoire de la cryptographie

Avec l'apparition de l'informatique son utilisation se popularise et se vulgarise. En 1977, le standard de chiffrement symétrique DES est proposé comme standard par le NIST. En 1976, le cryptage asymétrique est né avec le chiffrement de Diffie-Hellman et en 1977 RSA une autre idée sur le cryptage asymétrique est née et mondialement utilisée. Le chiffrement AES est le standard actuel en termes de cryptographie symétrique, il est proposé en 2000.

Enfin, la Cryptographie post-quantique permet de dépasser les limites de la cryptographie mathématique.

4. Cryptographie moderne

4.1. Cryptographie symétrique (à clé secrète)



4. Cryptographie moderne

4.1. Cryptographie symétrique (à clé secrète)

La cryptographie symétrique utilise la même clé pour les processus de chiffrement et de déchiffrement ; cette clé est le plus souvent appelée "secrète" car toute la sécurité de l'ensemble est directement liée au fait que cette clé n'est connue que par l'expéditeur et le destinataire.

La cryptographie symétrique est très utilisée et se caractérise par une grande rapidité (opérations simples, chiffrement à la volée) et par des implémentations aussi bien software que hardware ce qui accélère nettement les débits et autorise son utilisation massive.

4. Cryptographie moderne

4.1. Cryptographie symétrique (à clé secrète)

l existe deux types de chiffrement à clé symétrique :

- Le chiffrement par blocs : l'opération de chiffrement s'effectue sur des blocs de texte clair.
- Le chiffrement par flots (ou par stream ou de flux) : l'opération de chiffrement s'opère sur chaque élément du texte clair (caractère, bits). On chiffre un bit/caractère à la fois.

4. Cryptographie moderne

4.1. Cryptographie symétrique (à clé secrète)

DES (IBM)	56 bits : Trop faible actuellement
IDEA (Massey et Xuejia)	128 bits : efficace mais breveté
RC4 (Ronald Rivest)	1 à 2048 bits: certaines clés sont faibles
RC5 (Ronald Rivest)	128 à 256 bits : efficace mais breveté
AES (Rijndael, Daemen, Rijmen)	128 à 256 bits : meilleur choix
Serpent (Anderson, Biham, Knudsen)	128 à 256 bits : très fort
Triple DES (IBM)	168 bits : second meilleur choix
Blowfish (Bruce Shneier)	1 à 448 bits : vieux et lent
Twofish (Bruce Shneier)	128 à 256 bits: très fort,largement utilisé

4. Cryptographie moderne

4.1.1. DES (Data Encryption Standard)

- Consiste à effectuer des combinaisons, des substitutions et des permutations entre le texte à chiffrer et la clé
- Chiffrement symétrique par bloc. La clé est codée sur 64 bits (16 blocs de 4 bits) dont 56 utiles et 8 de parité

Principe:

Fractionnement du texte en blocs de 64 bits (8 octets) ;

• Permutation initiale des blocs ;

• Découpage des blocs en 2 parties: gauche et droite (G et D) ;

• Etapes de permutation et de substitution répétées 16 fois(appelées rondes) ;

• Recollement des parties G et D et permutation initiale inverse.

4. Cryptographie moderne

4.1.2. *AES (Advenced Encryption Standard)*

• La progression de la puissance des ordinateurs a causé la mort du DES. Ce dernier n'est plus jamais utilisé lorsque la sécurité demandée est forte (utilisation militaire, documents "secrets", etc.).

• En Janvier 1997, la NIST (National Institute of Standards and Technology) lance un appel d'offre international pour remplacer le vieillissant DES : il en résulte 15 propositions.

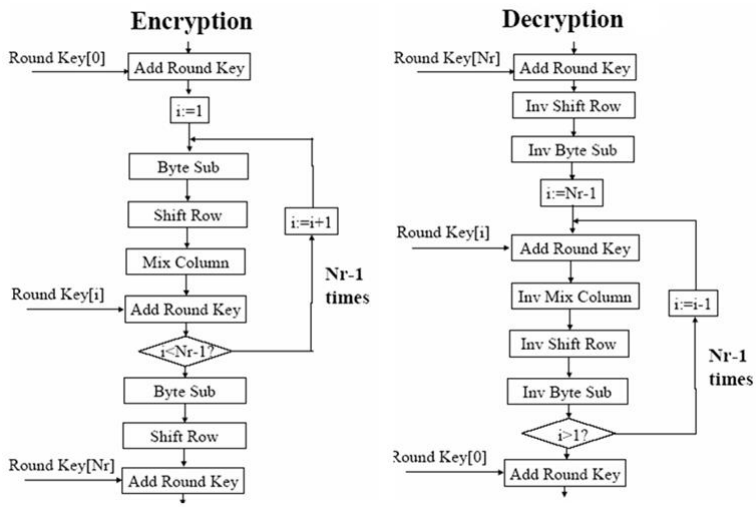
• En octobre 2000 la NIST élit Rijndael comme nouveau standard qu'on nomme aussi AES (Advanced Encryption Standard).

• Rijndael, du nom condensé de ses concepteurs Rijmen et Daemen, est un algorithme de chiffrement par blocs à plusieurs tours similaire à DES mais avec une taille de blocs et de clefs supérieures et variables, choisis entre 128, 196 et 256 bits.

Rq : AES est un sous-ensemble de Rijndael, il ne travaille qu'avec des blocs de 128 bits. La différence entre AES-128, AES-192 et AES-256 , c'est la longueur de la clé : 128, 192 ou 256 bits.

4. Cryptographie moderne

4.1.2. *AES (Advenced Encryption Standard)*



4.1.2. AES (Advenced Encryption Standard)

•Chiffrement :

- Le chiffrement AES consiste en une addition initiale de clé, notée AddRoundKey, suivie par Nr -1 rondes (nombre de rondes -1), chacune constitué de quatre étapes :

- SubBytes.
- ShiftRows.
- MixColumns.
- AddRoundKey.

- Enfin, une ronde finale FinalRound est appliquée (elle correspond à une ronde dans laquelle l'étape MixColumns est omise).

•Déchiffrement :

• La routine de chiffrement peut être inversée et réordonnée pour produire un algorithme de déchiffrement utilisant les transformations InvSubBytes, InvShiftRows, InvMixColumns, et AddRoundKey.

❖ **Table d'état du texte et des clés**

• Le message et la clé sont conservés sous forme de tables appelées tables d'états (State). Le nombre de colonnes dépend des tailles des textes et clés :

$$Nb = L_{bloc}/32$$
$$Nk = L_{clef}/32$$

• Une colonne du tableau correspond à un mot de 32 bits. Ainsi, chaque petit bloc représente 8 bits, donc 1 octet. L'input et l'output sont donc gérés comme des séquences linéaires d'octets.

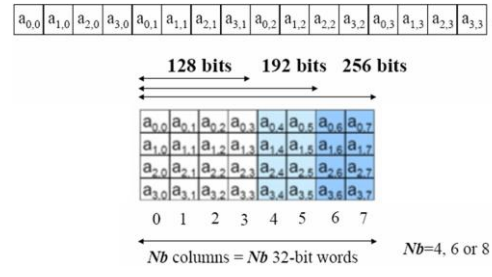


Table d'état du texte

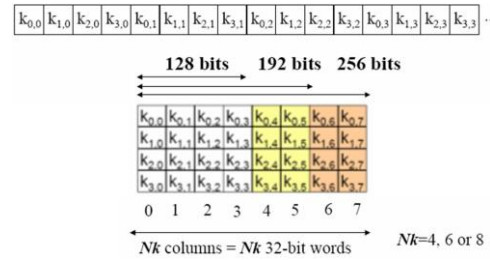
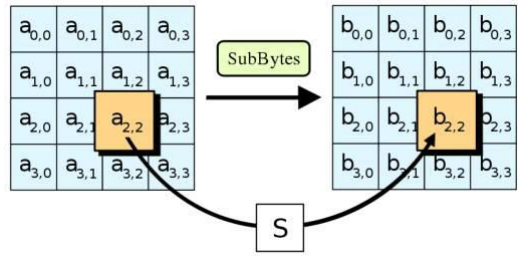


Table d'état des clés

❖ **SubByte**

• Tous les octets $a_{i,j}$ de la table d'état sont transformés en appliquant une S-Box inversible (afin de permettre un déchiffrement unique).

• Une seule S-Box est suffisante pour toute la phase de chiffrement.



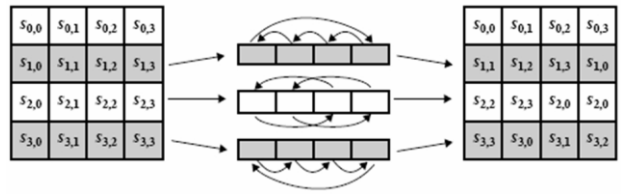
Exemple : Si $a_{i,j}$ = 53 en hexadécimal, alors $b_{i,j}$ = ED ce qui correspond à la ligne 5 et la colonne 3.

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Table S-Box

❖ **ShiftRow**

• Cette étape effectue un décalage des lignes de l'état courant (table d'état).



Etape du ShiftRow

• Selon la taille des blocs de message (la valeur de Nb), les décalages ne seront pas toujours identiques.

- La ligne 0 n'est jamais décalée.
- La ligne 1 est décalée de C1.
- La ligne 2 est décalée de C2.
- La ligne 3 est décalée de C3.

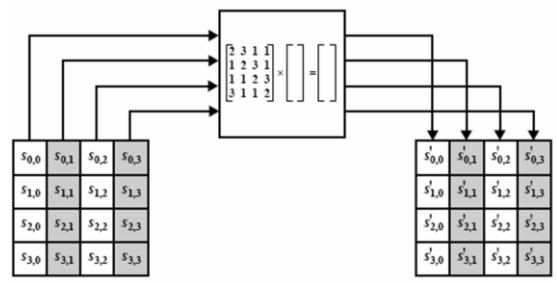
	C_1	C_2	C_3
N_B=4	1	2	3
N_B=6	1	2	3
N_B=8	1	3	4

Décalage selon la taille des blocs de messages

❖ **MixColumn :**

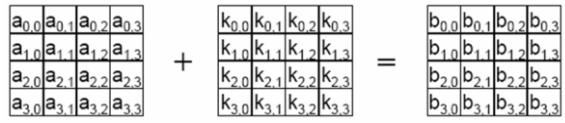
• La transformation MixColumn consiste à prendre chaque colonne de l'état et à la multiplier par la matrice suivante :

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$



Etape du MixColumn

❖ **AddRoundKey :** AddRoundKey consiste en un OU exclusif de l'état courant et de la clef du tour. Il s'agit d'additionner des sous-clés aux sous-blocs correspondants.



Add Round Key

❖ **Nombre de rondes**

• Selon la taille des blocs à traiter et la taille de la clé, le nombre de rondes évolue.

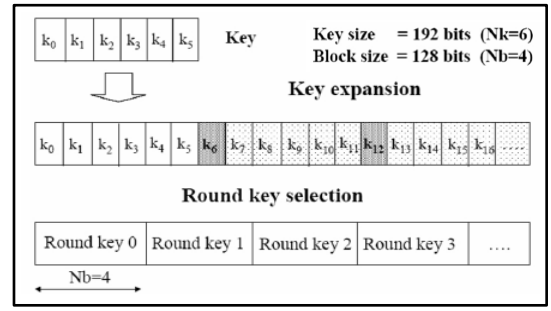
Block length	Key length: 128 bits Nk=4	192 bits Nk=6	256 bits Nk=8
128 bits Nb=4	10	12	14
192 bits Nb=6	12	12	14
256 bits Nb=8	14	14	14

Nombres de rondes à effectuer

➢ **Calcul de la clé**

• Après avoir subi une extension (Key Expansion), la clé sera découpée en sous-clés (appelées clés de rondes).

• Le nombre de sous-blocs k_i dépendra de la taille des clés et bloc du message.



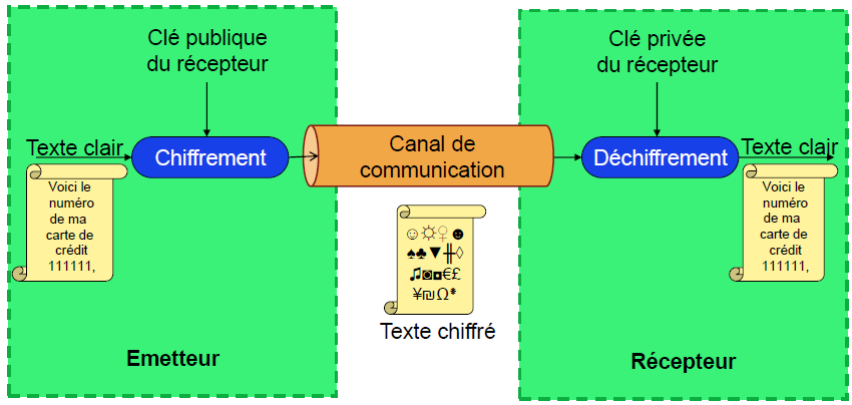
Opérations effectuées sur la clé

Avantages d'AES

- Des performances très élevées (plus performant que le DES).
- Le parallélisme peut être implémenté.
- Il ne comprend pas d'opérations arithmétiques ; uniquement des décalages et des XOR.
- Le nombre de rondes peut facilement être augmenté si c'est requis.
- Il ne possède pas de clés faibles.
- Il est résistant à la cryptanalyse différentielle et linéaire.

4. Cryptographie moderne

4.2. Cryptographie asymétrique (à clé publique)



4. Cryptographie moderne

4.2. Cryptographie asymétrique (à clé publique)

•Dans le cas des systèmes symétriques, la même clef est utilisée pour le chiffrement et le déchiffrement. Le problème essentiel de la cryptographie symétrique est la distribution des clefs : pour que n personnes puissent communiquer de manière confidentielle il faut n (n-1)/2 clefs.

• L'idée de base des cryptosystèmes à clefs publiques a été proposée dans un article fondamental de Diffie et Hellman en 1976. Le principe fondamental est d'utiliser des clefs de chiffrement et déchiffrement différentes, non reconstructibles l'une à partir de l'autre :

- Une clef publique pour le chiffrement.
- Une clef privée (secrète) pour le déchiffrement.

• Ce système est basé sur une fonction à sens unique, soit une fonction facile à calculer dans un sens mais très difficile à inverser sans la clef privée.

4. Cryptographie moderne

4.2. Cryptographie asymétrique (à clé publique)

•Le gros avantage de ce système est qu'il n'y ait pas besoin d'avoir partagé un secret au préalable pour s'échanger des messages cryptés.

• En revanche les implémentations de tels systèmes (RSA, ElGamal, …) ont un inconvénient majeur : leur lenteur par rapport à leurs homologues à clefs secrètes qui tournent eux jusqu'à près de mille fois plus vite.

4.2. Cryptographie asymétrique (à clé publique)

4.2.1. RSA (Rivest - Shamir - Adleman)

- 1978: Rivest, Shamir Adleman
- Le niveau de sécurité dépend de la difficulté de factoriser des grands nombres.
- Les clé publiques et privées sont des fonctions d'une paire de grands nombres premiers.
- Clef publique = (n, e) ; Clef privee = (n, d) , d calculé à partir de p,q (secrets)
- n produit de p q premiers
- Le chiffrement de x est

$$y = x^e \bmod n$$

- Le déchiffrement de y est

$$x = y^d \bmod n$$

- Afin d'assurer qu'il n'y ait aucune ambiguïté dans la reconstitution de x à travers le module n, il suffit de découper le message en blocs codés par des entiers m qui soient tous <= n -1.

4.2.1. RSA (Rivest - Shamir - Adleman)

Génération de clef publique « e » et secrète « d »

1. Choisir ***p*** et ***q***, deux nombres premiers distincts.
2. Calculer leur produit ***n = pq***, appelé module de chiffrement.
3. Calculer ***φ(n) = (p - 1)(q -1)*** (c'est la valeur de l'indicatrice d'Euler en *n*).
4. Choisir un entier naturel **e** premier avec φ(n) et strictement inférieur à φ(n), appelé exposant de chiffrement.
5. Calculer l'entier naturel **d**, inverse de e modulo φ(n) (c.à.d. ed ≡ 1 (mod φ(n))), et strictement inférieur à φ*(n)*, appelé exposant de déchiffrement ; *d* peut se calculer efficacement par l'algorithme d'Euclide étendu.

➢ **Exemple**

• Alice choisit p = 17 et q = 19

- On a : n = p x q = 323, φ(n) = (p-1) * (q-1) = 288

• Elle choisit e = 5 (par exemple, et on a PGCD (e,(φ(n))=1).

- On détermine, alors, que d =173 (inverse modulaire de e sur $Z_{\varphi(n)}$: 173*5= 3*288+1).

- La clé publique est donc (5, 323) et la clé privée est (173, 323).

• Supposons que Bob veut envoyer à Alice le message « BONJOUR » en se servant de la position des lettres dans l'alphabet pour les transformer en nombres. Cela donne :

B	O	N	J	O	U	R
2	15	14	10	15	21	18

• Après avoir chiffré en remplaçant chaque nombre b par (b^e mod n) on obtient le message que Bob envoie à Alice :

32	2	29	193	2	89	18

• Pour le déchiffrement, Alice calcule pour chaque nombre b du message reçu :

b = (b^d mod n) pour trouver :

2	15	14	10	15	21	18
B	O	N	J	O	U	R

qui est bien le message initial.

➢ **Sécurité du système RSA**

• RSA est basé sur la difficulté de factoriser n. En effet celui qui arrive à factoriser n peut retrouver facilement la clef secrète d'Alice connaissant seulement sa clef publique.

• Il n'est pas très astucieux de choisir d'aussi petites valeurs car on peut retrouver d très facilement. En pratique, il faut prendre de très grandes valeurs de p et q.

5. Fonctions de Hachage

• Une fonction de hachage est une fonction mathématique qui assure l'intégrité des informations qui circulent sur le réseau.

• La fonction de hachage sert à calculer une courte empreinte de taille fixe à partir d'une information de taille arbitraire.

• Le résultat d'une fonction de hachage peut être appelé : *somme de contrôle, empreinte, hash, résumé de message,* ou *condensé, ...*

• La probabilité d'avoir deux messages avec le même haché doit être extrêmement faible. Le haché ne contient pas assez d'informations en lui-même pour permettre la reconstitution du texte original. L'objectif est d'être représentatif d'une donnée particulière et bien définie (en l'occurrence le message).

• Le hachage est en effet aussi employé pour les signatures numériques.

➢ Propriétés

• Les fonctions de hachage possèdent de nombreuses propriétés :

- Elles peuvent s'appliquer à n'importe quelle longueur de message M.

- Elles produisent un résultat de longueur constante.

- Il doit être facile de calculer h = H(M) pour n'importe quel message M.

- Pour un h donné, il est impossible de trouver x tel que H(x) = h => propriété à sens unique.

- Pour un x donné, il est impossible de trouver y tel que H(y) = H(x) => résistance faible de collision.

- Il est impossible de trouver x, y tels que H(y) = H(x) => résistance forte de collision.

- En perturbant un seul bit en entrée, on obtient idéalement une sortie totalement différente, (soit environ bit sur deux sera changé) => Effet avalanche.

➢ **MD5 (Message Digest 5)**

• Conçu par Ronald Rivest, un des créateurs de RSA, est un des plus connus algorithmes de hachage. C'est le dernier d'une série (MD2, MD4). Cet algorithme produit un condensé de 128 bits.

➢ **SHA-1 (Secure Hash Algorithm)**

• Il a été conçu par NIST et NSA en 1993, et révisé 1995 pour étendre ses capacités en matière de sécurité. Contrairement au MD5 qui produit des condensés de 128 bits, le SHA produit des valeurs condensées de 160 bits.

• Jusqu'à 2005, il était l'algorithme généralement préféré pour le hachage, mais des rumeurs de cassage le font peu à peu évoluer vers des versions plus sophistiquées.

• Depuis 2001, une nouvelle version de SHA-1, SHA-2, ainsi que les versions SHA-256, SHA-384 et SHA-512 sont en cours de validation (256, 384, 512 est la taille en bits de l'empreinte).

6. La signature électronique

•La signature électronique (par fois appelée digitale/numérique) est un mécanisme de sécurité permettant de chiffrer un message ou un document en utilisant la clé privée de l'émetteur (ou l'auteur).

•La signature électronique comme signature manuscrite utilisée pour prouver l'identité du signataire (de l'émetteur) et l'intégrité du document.

•La signature électronique assure l'intégrité, l'authenticité et la non-répudiation de l'origine.

6. La signature électronique

•La signature électronique (par fois appelée digitale/numérique) est un mécanisme de sécurité permettant de chiffrer un message ou un document en utilisant la clé privée de l'émetteur (ou l'auteur).

•La signature électronique comme signature manuscrite utilisée pour prouver l'identité du signataire (de l'émetteur) et l'intégrité du document.

•La signature électronique assure l'intégrité, l'authenticité et la non-répudiation de l'origine.

6. La signature électronique

Applications des signatures numériques:

- Signer et vérifier les différents formats de document: Word, Excel et PDF.
- Effectuer des transactions en ligne sécurisées.
- Identifier les participants d'une transaction en ligne.
- Vérifier les certificats numériques (ex. X509)

6. La signature électronique

Comment fonctionne la signature numérique?

- Pour produire une signature, on utilise les fonctions de hachage et le chiffrement à clé publique.
- Une signature numérique est produite par un algorithme de génération de signature numérique.
- Lorsque le destinataire reçoit le message et la signature, il vérifie la signature par un algorithme de vérification de signature numérique.

7. Les certificats numériques

Le certificat est une carte d'identité numérique. Il permet d'associer une clé publique à une entité (une personne, une machine, ...) afin d'en assurer la validité. Un certificat est délivré par un organisme appelé autorité de certification (CA : Certification Authority).

Un certificat est un fichier émis par une CA composé de deux parties, une contenant des informations, l'autre contenant la signature de l'autorité de certification. Il comprend donc:

- Nom, prénom, adresse email + informations diverses
- Clé publique de la personne
- Date de validité
- Nom de l'autorité de certification
- Signature de l'autorité de certification

7. Les certificats numériques

L'ensemble de ces informations (informations + clé publique du demandeur) est signé par la CA. Une fonction de hachage crée une empreinte de ces informations, puis ce condensé est chiffré à l'aide de la clé privée de la CA.

La vérification du certificat se fait à l'aide de la clé publique de l'autorité de certification et de la date de validité. Pour vérifier un certificat, il suffit de connaitre la clé publique de l'autorité émettrice.

7. Les certificats numériques

La structure des certificats est normalisée par le standard X.509 de l'UIT, qui définit les informations contenues dans le certificat :

- La version de X.509 à laquelle le certificat correspond
- Le numéro de série du certificat
- L'algorithme de chiffrement utilisé pour signer le certificat
- Le nom (DN, pour Distinguished Name) de l'autorité de certification émettrice
- La date de début de validité du certificat
- La date de fin de validité du certificat
- L'objet de l'utilisation de la clé publique
- La clé publique du propriétaire du certificat
- La signature de l'émetteur du certificat

7. Les certificats numériques

exemple d'un certificat X.509 version 3

```
Certificate:
  Data:
    Version: v3 (0x2)
    Serial Number: 3 (0x3)
    Signature Algorithm: PKCS #1 MD5 With RSA Encryption
    Issuer: OU=Ace Certificate Authority, O=Ace Industry, C=US
    Validity:
      Not Before: Fri Oct 17 18:36:25 1997
      Not After: Sun Oct 17 18:36:25 1999
    Subject: CN=Jane Doe, OU=Finance, O=Ace Industry, C=US
    Subject Public Key Info:
      Algorithm: PKCS #1 RSA Encryption
      Public Key:
        Modulus:
          00:ca:fa:79:98:8f:19:f8:d7:de:e4:49:80:48:e6:2a:2a:86: [...]
    Extensions:
        Identifier: Certificate Type
          Critical: no
          Certified Usage:
            SSL Client
        Identifier: Authority Key Identifier
          Critical: no
          Key Identifier:
            f2:f2:06:59:90:18:47:51:f5:89:33:5a:31:7a:e6:5c:fb:36:
            26:c9
    Signature:
      Algorithm: PKCS #1 MD5 With RSA Encryption
      Signature:
        6d:23:af:f3:d3:b6:7a:df:90:df:cd:7e:18:6c:01:69:8e:54:65:fc:06: [...]
```


8. Autorités de certification et PKI

Une Infrastructure à clés publiques ou Infrastructure de Gestion de Clefs ou encore Public Key Infrastructure (PKI), est un ensemble de composants physiques (ordinateurs, équipements cryptographiques, cartes à puces), de procédures humaines (vérifications, validation) et de logiciels (système et application) en vue de gérer le cycle de vie des certificats électroniques).

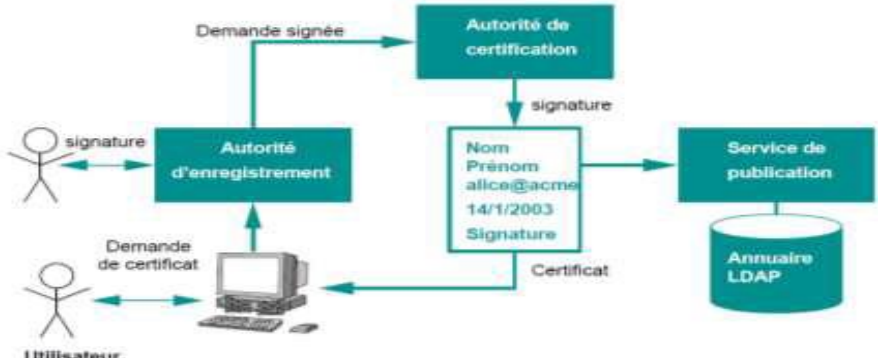


Schéma d'Infrastructure de Gestion de Clés (PKI)

8. Autorités de certification et PKI

Une PKI délivre un ensemble de services pour le compte de ses utilisateurs. Parmi eux :

- Enregistrement des utilisateurs (ou équipement informatique)
- Génération de certificats
- Renouvellement de certificats
- Révocation de certificats
- Publication des certificats
- Publication des listes de révocation (CLR)
- Identification et authentification des archivage, séquestre et recouvrement des certificats