Chapitre 2 Initiation à la Cryptographie

May 14, 2021

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.
- La cryptographie est une science mathématique qui comporte deux branches : la cryptographie et la cryptanalyse.

Définitions

cryptographie

la cryptographie étudie l'ensemble des techniques qui permettent de coder un message.

cryptanalyse

l'étude des procédés cryptographiques dans le but de trouver des faiblesses, en particulier, de pouvoir décrypter des messages chiffrés. Le décryptement est l'action consistant à trouver le message en clair sans connaitre la clef de déchiffrement.

L'usage de la cryptographie

- La cryptographie est traditionnellement utilisée pour dissimuler des messages aux yeux de certains utilisateurs.
- la cryptographie sert non seulement à préserver la confidentialité des données mais aussi à garantir leur intégrité et leur authenticité.

L'usage de la cryptographie

pour chiffrer un message clair deux processus sont utilisés:

- la substitution qui consiste à remplacer, les symboles d'un message clair par d'autres symboles sans en modifier l'ordre.
- la transposition qui repose sur le bouleversement de l'ordre des symboles.

Propriétés d'un cryptosystème

Les Propriétés demandées à un système cryptographique sont résumées par les mots clefs suivants:

- **Confidentialité** : Protection d'une donnée contre son écoute par des individus non autorisés.
- **authenticité**: Pouvoir vérifier que la donnée provient bien de la bonne source.
- **Intégrité**: Garantir que les données sont toujours tels qu'elles , sans altération.

CHIFFREMENT PAR SUBSTITUTION MONO-ALPHABÉTIQUE

- le chiffrement par substitution mono-alphabétique qui consiste à remplacer chaque symbole individuel du message par un autre symbole de l'alphabet.
- le chiffrement par substitution mono-alphabétique dépend La fréquence d'apparition des lettres varie bien évidemment en fonction de la langue et du type de texte considérés.

La cryptographie classique

Le chiffrement de César :

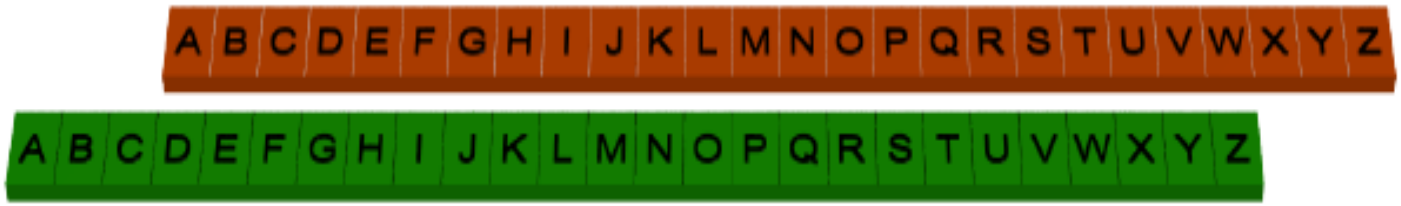
- Le chiffrement par substitution mono-alphabétique le plus simple est le chiffrement par décalage, aussi connu sous le nom de **chiffrement de César**.
- Il consiste simplement à décaler les lettres de l'alphabet d'un nombre de positions constant vers la droite ou la gauche.

Le chiffrement de César

En fait César, pour ses communications importantes à son armée, cryptait ses messages. Ce que l'on appelle le chiffrement de César est un décalage des lettres : pour crypter un message, A devient D, B devient E, C devient F,...

$$A \longmapsto D \quad B \longmapsto E \quad C \longmapsto F \quad \ldots \quad W \longmapsto Z \quad X \longmapsto A \quad Y \longmapsto B \quad Z \longmapsto C$$

Voici une figure avec l'alphabet d'origine en haut et en rouge, en correspondance avec l'alphabet pour le chiffrement en-dessous et en vert.



Le chiffrement de César

Pour déchiffrer le message de César, il suffit de décaler les lettres dans l'autre sens, D se déchiffre en A, E en B,...

Le chiffrement de César

Il est plus facile de manipuler des nombres que des lettres, aussi nous passons à une formulation arithmétique. Nous associons à chacune des 26 lettres de A à Z un nombre de 0 à 25. En termes mathématiques, nous définissons une bijection :

$$f : \{A, B, C, \ldots, Z\} \longrightarrow \{0, 1, 2, \ldots, 25\}$$

par

$$A \longmapsto 0 \quad B \longmapsto 1 \quad C \longmapsto 2 \quad \ldots \quad Z \longmapsto 25$$

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Chiffrer et déchiffrer

Le chiffrement de César est simplement une addition dans en fixons un entier k qui est le décalage (par exemple k = 3 dans l'exemple de César ci-dessus) et définissons la fonction de chiffrement de César de décalage k.

$$C_k : \begin{cases} \mathbb{Z}/26\mathbb{Z} & \longrightarrow & \mathbb{Z}/26\mathbb{Z} \\ x & \longmapsto & x+k \end{cases}$$

Par exemple, pour k = 3 : C3(0) = 3, C3(1) = 4. . .

Chiffrer et déchiffrer

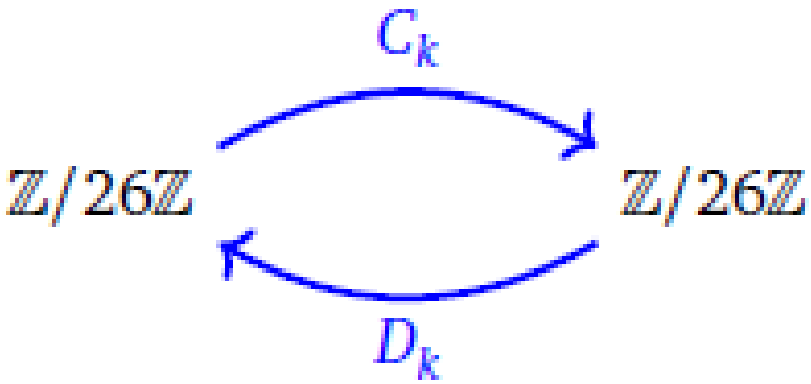
Pour déchiffrer, rien de plus simple ! Il suffit d'aller dans l'autre sens, c'est-à-dire ici de soustraire. La fonction de déchiffrement de César de décalage k est

$$D_k : \begin{cases} \mathbb{Z}/26\mathbb{Z} & \longrightarrow & \mathbb{Z}/26\mathbb{Z} \\ x & \longmapsto & x-k \end{cases}$$

En effet, si 1 a été chiffré en 4, par la fonction C3 alors D3(4) = 4 - 3 = 1. On retrouve le nombre original..

Chiffrer et déchiffrer

En d'autres termes, si x est un nombre, on applique la fonction de chiffrement pour obtenir le nombre crypté y = Ck(x) ; ensuite la fonction de déchiffrement fait bien ce que l'on attend d'elle Dk(y) = x, on retrouve



le nombre original x.

Chiffrer et déchiffrer

Voici le principe du chiffrement : Alice veut envoyer des messages secrets à Bruno. Ils se sont d'abord mis d'accord sur une clé secrète k, par exemple $k = 11$. Alice veut envoyer le message "COUCOU" à Bruno. Elle transforme "COUCOU" en "2 14 20 2 14 20". Elle applique la fonction de chiffrement $C_{11}(x) = x + 11$ à chacun des nombres : "13 25 5 13 25 5" ce qui correspond au mot crypté "NZFNZF". Elle transmet le mot crypté à Bruno, qui selon le même principe applique la fonction de déchiffrement $D_{11}(x) = x - 11$.

Chiffrer et déchiffrer

Il n'y a que 26 façons différentes de crypter un message avec le code de César. Cela en fait donc un code très peu sûr, puisqu'il est très facile de tester de façon exhaustive toutes les possibilités.
Exemple: La clé = 7.

- SALUT
- BONJOUR

Chiffrer et déchiffrer

Solution:

La clé = 7.

- SALUT $\Rightarrow$ ZHSBA
- BONJOUR $\Rightarrow$ IVUQVBY

Analyse des fréquences (Attaque statistique)

- Le pricipe des techniques d'analyse des fréquences reposent sur l'analyse des fréquences des symboles utilisés dans le texte chiffré et utilisent le fait que, dans chaque langue, certains symboles ou combinaisons de symboles apparaissent plus fréquemment que d'autres.
- La principale faiblesse du chiffrement mono-alphabétique est qu'une même lettre est toujours chiffrée de la même façon. Par exemple, ici E devient X. Dans les textes longs, les lettres n'apparaissent pas avec la même fréquence.
- Ces fréquences varient suivant la langue utilisée. En français, les lettres les plus rencontrées sont dans l'ordre et les fréquences suivantes:

E	S	A	I	N	T	R	U	L	O	D
14.69%	8.01%	7.54%	7.18%	6.89%	6.88%	6.49%	6.12%	5.63%	5.29%	3.66%

Analyse des fréquences (Attaque statistique)

Voici la méthode d'attaque : dans le texte crypté, on cherche la lettre qui apparaît le plus, et si le texte est assez long cela devrait être le chiffrement du E, la lettre qui apparaît ensuite dans l'étude des fréquences devrait être le chiffrement du S, puis le chiffrement du A... On obtient des morceaux de texte clair sous la forme d'une texte à trous et il faut ensuite deviner les lettres manquantes.

Analyse des fréquences (Attaque statistique)

Par exemple, déchiffrons la phrase :

LHLZ HFQ BC HFFPZ WH YOUPFH MUPZH

On compte les apparitions des lettres :

H : 6 F : 4 P : 3 Z : 3

On suppose donc que le H crypte la lettre E, le F la lettre S, ce qui donne

*E** ES* ** ESS** *E ***SE ****E

D'après les statistiques P et Z devraient se décrypter en A et I (ou I et A). Le quatrième mot "HFFPZ", pour l'instant décrypté en "ESS**", se complète donc en "ESSAI" ou "ESSIA". La première solution semble correcte ! Ainsi P crypte A, et Z crypte I. La phrase est maintenant :

*E*I ES* ** ESSAI *E ***ASE **AIE

Analyse des fréquences (Attaque statistique)

En réfléchissant un petit peu, on décrypte le message :

CECI EST UN ESSAI DE PHRASE VRAIE

Analyse des fréquences (Attaque statistique)

Exemple

QJ HMNKKWJRJSY IJ HJXFW JXY YWJX UJZ XJHZWNXJ

Chiffrement Affine

le chiffrement affine son principe repose sur l'utilisation de la fonction dite affine pour crypter le message en clair, cette dernière à la forme suivante:
$C = (ax + b) \bmod 26$

- C : la lettres de l'alphabet crypté.
- a,b : sont des constantes représentant la clé de chiffrement.
- x :la lettres de l'alphabet à crypter.

Chiffrement Affine

la formule utilisée pour déchiffrement est la suivante:
$x = a^{-1}(c - b) mod 26$

Exemple

Soit $(a, b) = (7, 2)$ la clé de chiffrement, donné le texte chiffré des mots en clair *ISIL* et *KHENCHELA* en utilisant le chiffrement affine.

Exemple

Solution :

ISIL $\Rightarrow$ GYGB

KHENCHELA $\Rightarrow$ UZEPQZEBC

Le chiffrement de Vigenère

L'espace des clés du chiffrement mono-alphabétique est immense, mais le fait qu'une lettre soit toujours cryptée de la même façon représente une trop grande faiblesse. Un autre algorithme célèbre est le chiffrement de Vigenère. basé sur le principe de substitution, mais en variant la distance de décalage au cours du chiffrement en utilisant un mot ou une phrase comme clé. Chaque lettre de la clé correspond à sa position dans l'alphabet. Pour chiffrer un message, on écrit le texte clair et on écrit la clé en dessous, en répétant la clé autant de fois que nécessaire pour couvrir l'ensemble du message.

- le chiffrement consiste à additionner chaque lettre du message avec la lettre de la clé en dessous, modulo 26 .
- le déchiffrement consiste à soustraire chaque lettre du message chiffré avec la lettre de la clé en dessous, modulo 26.

	Lettre en clair																									
	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**
Lettre de la clé	Lettres chiffrées (au croisement de la colonne *Lettre en clair* et de la ligne *Lettre de la clé*)																									
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

Le chiffrement de Vigenère

Par exemple, avec la clé "RABELAIS" et le message clair suivant on obtient le texte chiffré :
SCIENCE SANS CONSCIENCE N EST QUE RUINE DE L AME
+ RABELAIS RABELAIS RABELAIS RABELAIS RABELAIS
= JCJIYCM KRNT GZNAUZEOGP N MKK QVI CUQFV DF P LMM

Avantage

Contrairement au chiffrement par substitution, chaque lettre peut être substituée par une lettre différente selon sa position dans le message, et donc la lettre de la clé avec laquelle elle est associée.

son principe consiste à bouleverser l'ordre des données à chiffrer de façon à les rendre incompréhensibles.

La technique assyrienne:

Son principe consiste à enrouler une bande de papyrus ou de cuir sur un cylindre appelé scytale,ce dernier est considérée comme le plus ancien dispositif de cryptographie, de cette façon le message à transmettre deviens plus compréhensible.

Pour le déchiffrer, le destinataire devait posséder un cylindre d'un diamètre identique à celui utilisé pour l'opération de chiffrement. Il lui suffit d'enrouler la message autour de ce bâton pour retrouver le texte clair.

La technique assyrienne

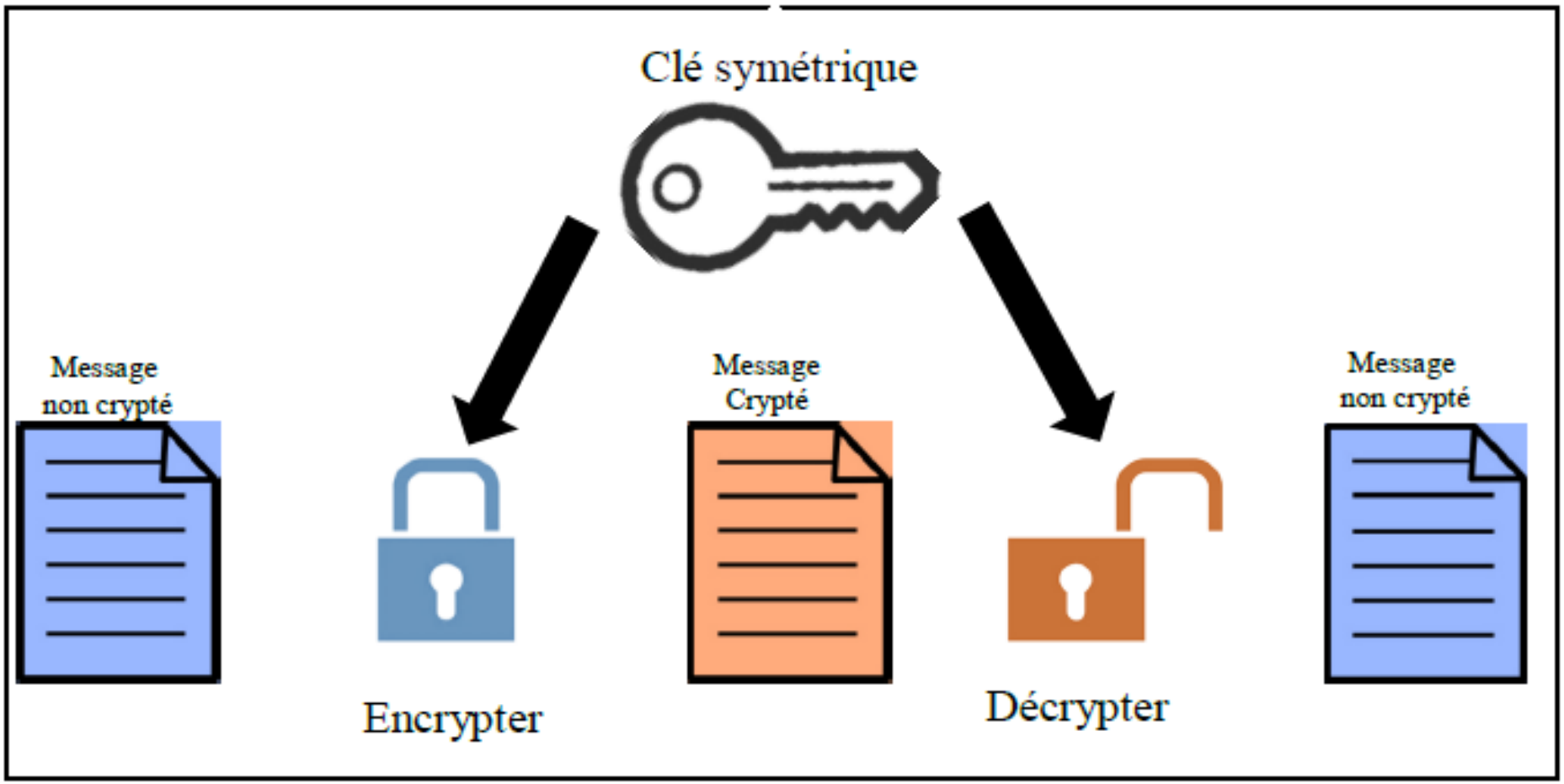
La cryptographie moderne

La Cryptographie symétrique

La cryptographie symétriques également appelée cryptage de clé secrète utilise la même clé pour le processus de cryptage et de décryptage. le chiffrement consiste à appliquer une opération (algorithme) sur les données à chiffrer à l'aide de la clé privée, afin de les rendre inintelligibles.

Dans la majorité des systèmes de cryptages symétrique la clé de chiffrement et la clé de déchiffrement sont identiques.

La Cryptographie symétrique



La Cryptographie symétrique

Les principaux algorithmes à clé privée sont : Blowfish, DES,3DES IDEA.

Avantages:

- chiffrement de grandes quantités de données.
- chiffrement rapide.
- la simplicité d'implémentation

Inconvénients:

- La clé secrète à partager est un point faible.

La Cryptographie symétrique

Les algorithmes symétriques sont de deux types:

- **Les algorithmes de chiffrement en flot (Stream cipher)**: est un chiffrement a clé symétrique permet de crypter et décrypter le texte en prenant un octet (8 bit) du texte à la fois.
  Un des algorithmes de chiffrement par flot le plus rependu est RC4.
- **Les algorithmes de chiffrement en bloc** : chiffre et déchiffre un bloc du texte à la fois (64 bit ou plus)

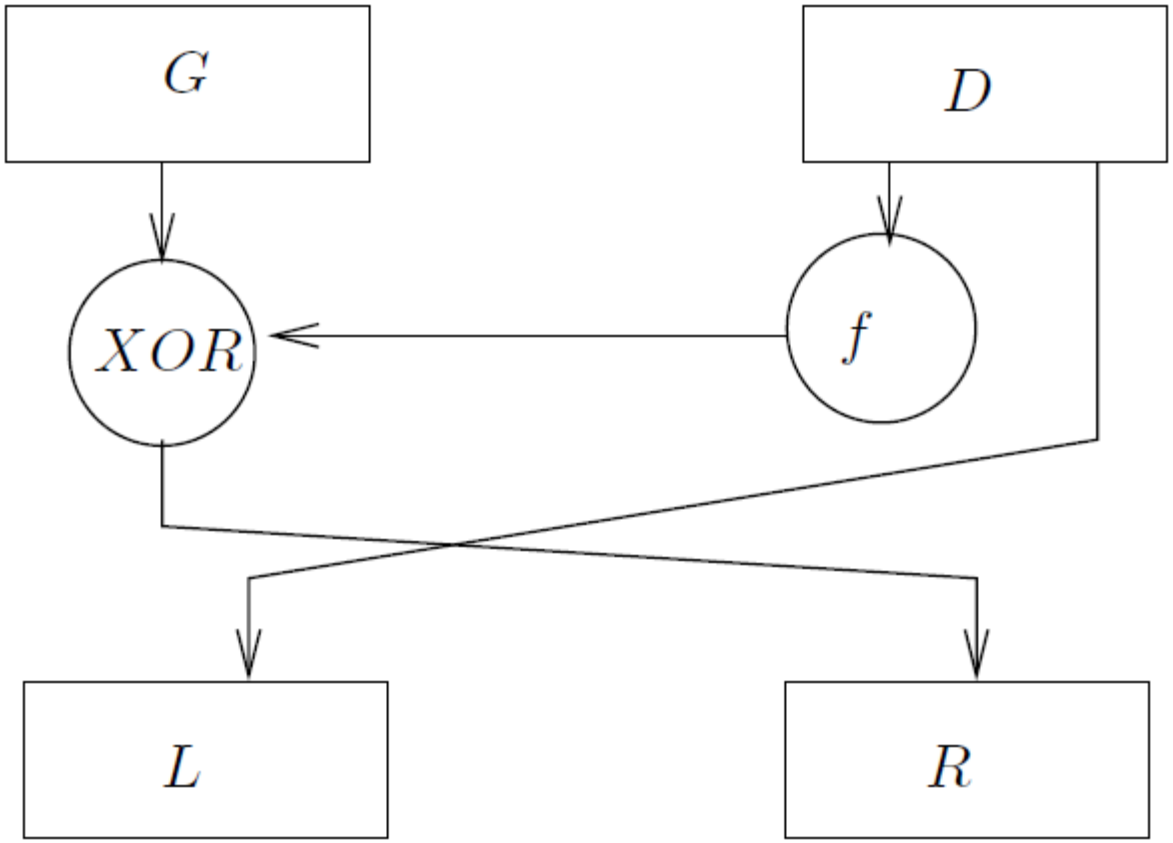
Le chiffrement DES

- le chiffrement DES connu sous le nom de **Data Encryption Algorithm** apparu en 1977, ce dernier utilise des clés de 56 bits pour chiffrer des blocs de 64 bits.
- **Le chiffrement DES** basé sur le schémas de Feistel, en effet il effectue un ensemble d'opérations itératives. Il répète 16 fois un algorithme appelé la fonction d'étage qui dépend de la valeur de la clé d'étage.
- l'exécution en plusieurs tours permet de mélanger les bits du message en clair en respectant les principes de C. Shannon:**confusion et diffusion**. La confusion vise à cacher toute structure algébrique du système et la diffusion doit permettre à chaque bit de texte clair d'avoir une influence sur une grande partie du texte chiffré.

Le chiffrement DES

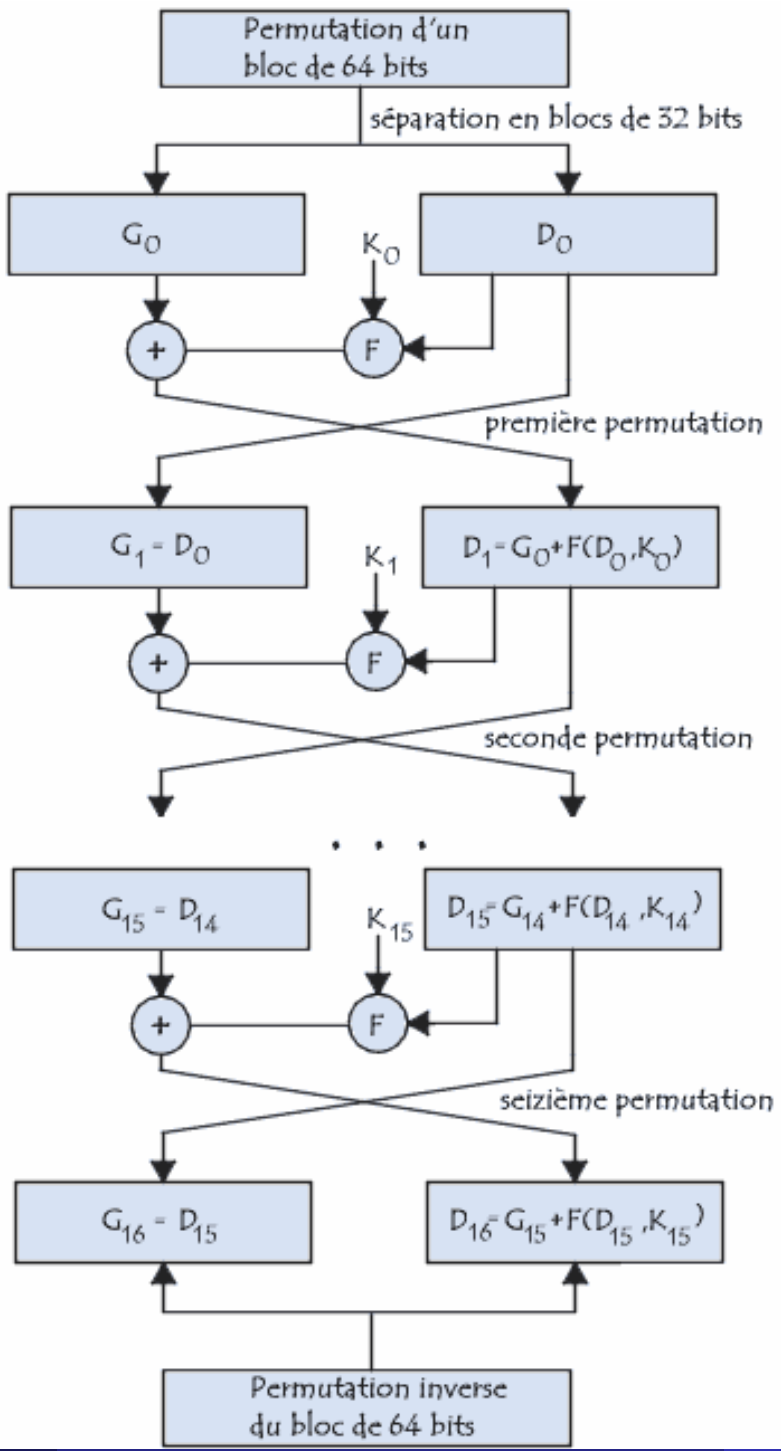
systèmes de chiffrement DES par bloc sont basés sur le schémas de Feistel

Schéma de Feistel



Le chiffrement DES

principe :
1. Dans la première étape, le message en clair converti en binaire est découpé en blocs B_i de 64 bits puis transféré à une fonction de permutation (IP) initiale, ainsi à partir de la clé initiale K, une suite de clés intermédiaires K^i sont crées (prises dans un certain ordre).
2. La permutation initiale effectuée sur le texte en clair B_i.
3. Découpage des blocs en deux parties: gauche et droite, nommées G_0 et D_0 .
4.une étape de permutation et de substitution répétées 16 fois.
5.la permutation inverse de la permutation initiale est effectuée.
Le résultat de ce processus produit un texte chiffré de 64 bits.


Permutation d'un bloc de 64 bits
séparation en blocs de 32 bits
G_0
K_0
D_0
+
F
première permutation
$G_1 = D_0$
K_1
$D_1 = G_0 + F(D_0, K_0)$
+
F
seconde permutation
. . .
$G_{15} = D_{14}$
K_{15}
$D_{15} = G_{14} + F(D_{14}, K_{14})$
+
F
seizième permutation
$G_{16} = D_{15}$
$D_{16} = G_{15} + F(D_{15}, K_{15})$
Permutation inverse du bloc de 64 bits

Le chiffrement DES

après une première étape qui consiste à convertir en binaire est découpé en blocs B_i de 64 bits le message en clair **étape 2**: une étape de permutation initiale (IP) qui consiste à mélanger la position des 64 bits du bloc d'entrée.
cette étape est représentée par la matrice de permutation initiale :

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	33	45	37	29	21	13	5	63	55	47	39	31	23	15	7

étape 3 Le message B_i est découpé en deux parties, une partie gauche de 32 bits et une partie droite de 32 bits.

L

58	50	42	34	26	18	10	2
62	54	46	38	30	22	14	6
57	49	41	33	25	17	9	1
61	33	45	37	29	21	13	5

R

60	52	44	36	28	20	12	4
64	56	48	40	32	24	16	8
59	51	43	35	27	19	11	3
63	55	47	39	31	23	15	7

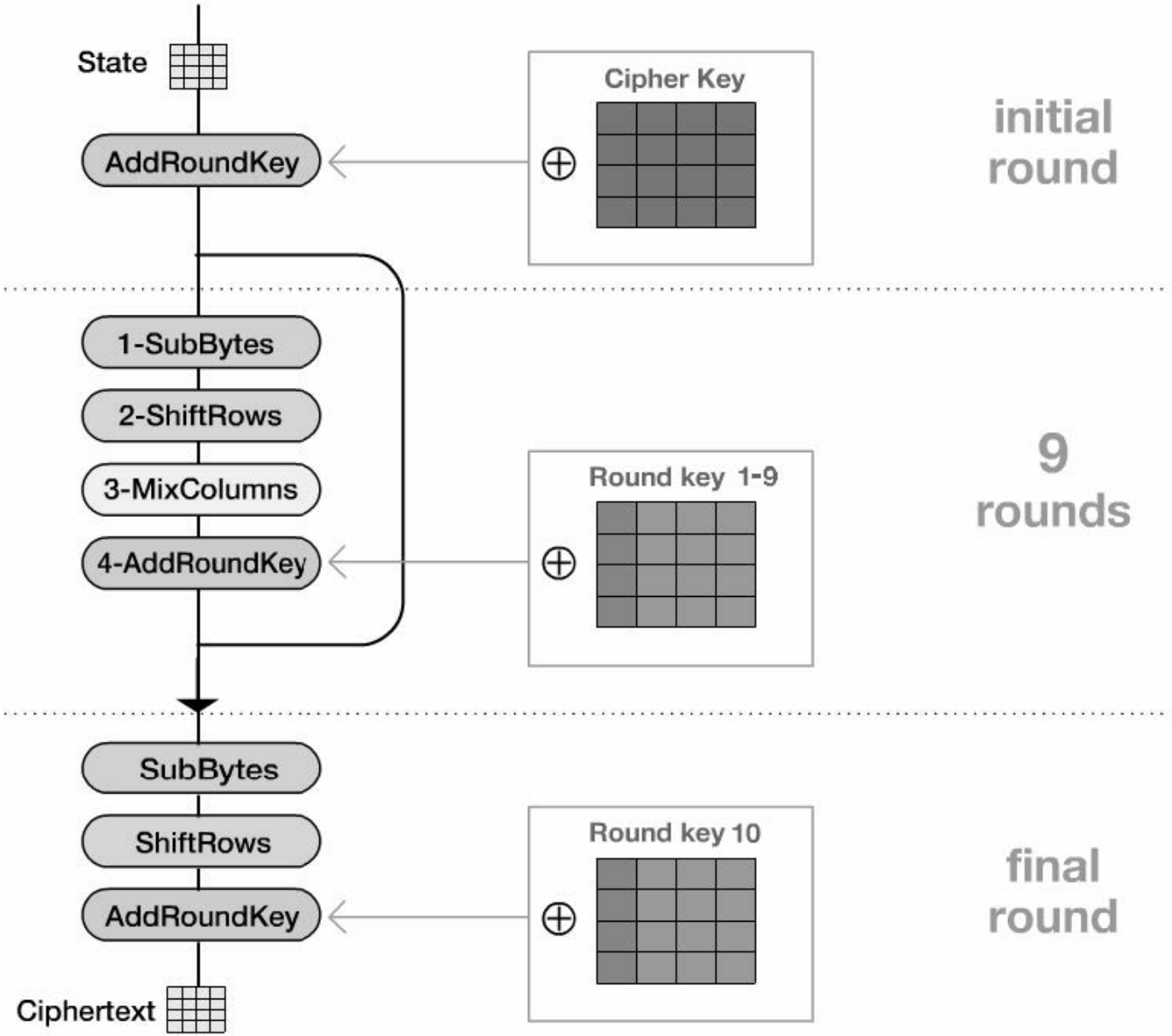
Le chiffrement DES

l'étape de permutation et de substitution répètent 16 fois les opérations suivantes:
$G_i = D_{i-1}$
$D_i = G_{i-1}\ XOR\ f(D_{i-1}, k_i)$
- Le décodage se fait en utilisant la même clé K mais en déroulant l'algorithme dans le sens inverse.

Le chiffrement AES

L'algorithme AES est un algorithme de chiffrement itératif par blocs, la taille du blocs est de 128 bit, La clé secrète possible a une longueur : 128, 192 ou 256 bits.

Le chiffrement AES



Le chiffrement AES

étape 1: Les blocs de messages (128 bits) sont découpés en 16 octets, placés dans une matrice 4*4.

$$\begin{pmatrix} M_{1,1} & M_{1,2} & M_{1,3} & M_{1,4} \\ M_{2,1} & M_{2,2} & M_{2,3} & M_{2,4} \\ M_{3,1} & M_{3,2} & M_{3,3} & M_{3,4} \\ M_{4,1} & M_{4,2} & M_{4,3} & M_{4,4} \end{pmatrix}$$

après la diversification de la clé initiale k^i clés générées sont toutes de 128 bits ces dernières sont également représentées par une matrice 4x4.

$$\begin{pmatrix} K^i_{1,1} & K^i_{1,2} & K^i_{1,3} & K^i_{1,4} \\ K^i_{2,1} & K^i_{2,2} & K^i_{2,3} & K^i_{2,4} \\ K^i_{3,1} & K^i_{3,2} & K^i_{3,3} & K^i_{3,4} \\ K^i_{4,1} & K^i_{4,2} & K^i_{4,3} & K^i_{4,4} \end{pmatrix}$$

Le chiffrement AES

étape 2: la matrice subit 4 transformations par tour

- AddRoundKey: XOR avec la matrice sous-clé.
- SubBytes: passage dans une S-box.
- ShiftRows: décalage des ligne (rotation).
- MixColumns: mélange des colonnes.

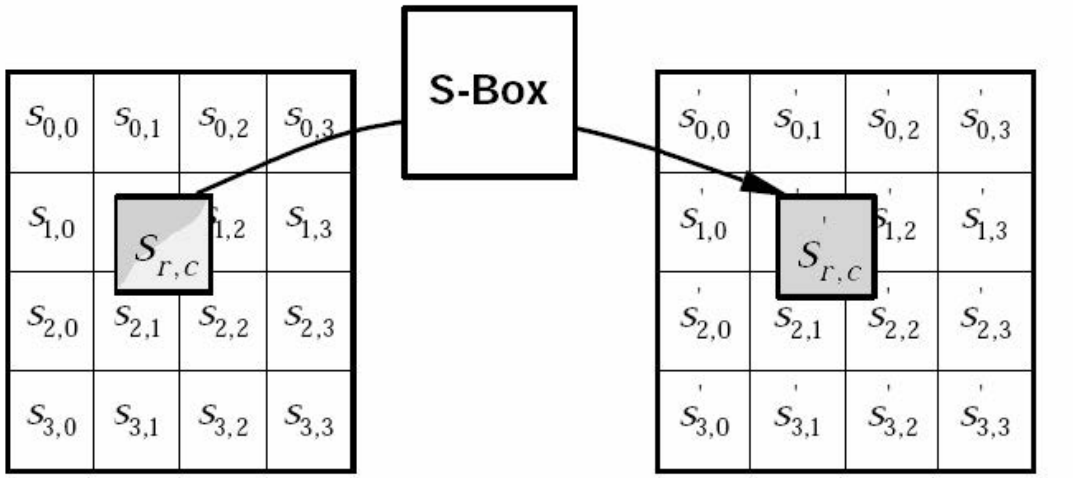
Le chiffrement AES

AddRound Key :cette opération consiste à combiner la matrice du message en clair dite matrice stat avec des bits de la clé en faisant le XOR de chaque élément de la matrice avec l'élément correspondant de la matrice de la clé k^i, comme indiqué sur le schéma suivant.

$$\begin{pmatrix} E_{1,1} & E_{1,2} & E_{1,3} & E_{1,4} \\ E_{2,1} & E_{2,2} & E_{2,3} & E_{2,4} \\ E_{3,1} & E_{3,2} & E_{3,3} & E_{3,4} \\ E_{4,1} & E_{4,2} & E_{4,3} & E_{4,4} \end{pmatrix} \Rightarrow \begin{pmatrix} E_{1,1} \oplus K^i_{1,1} & E_{1,2} \oplus K^i_{1,2} & E_{1,3} \oplus K^i_{1,3} & E_{1,4} \oplus K^i_{1,4} \\ E_{2,1} \oplus K^i_{2,1} & E_{2,2} \oplus K^i_{2,2} & E_{2,3} \oplus K^i_{2,3} & E_{2,4} \oplus K^i_{2,4} \\ E_{3,1} \oplus K^i_{3,1} & E_{3,2} \oplus K^i_{3,2} & E_{3,3} \oplus K^i_{3,3} & E_{3,4} \oplus K^i_{3,4} \\ E_{4,1} \oplus K^i_{4,1} & E_{4,2} \oplus K^i_{4,2} & E_{4,3} \oplus K^i_{4,3} & E_{4,4} \oplus K^i_{4,4} \end{pmatrix}$$

Le chiffrement AES

SubBytes: chaque élément de la matrice State est permuté selon une table de substitution inversible notée S-Box.

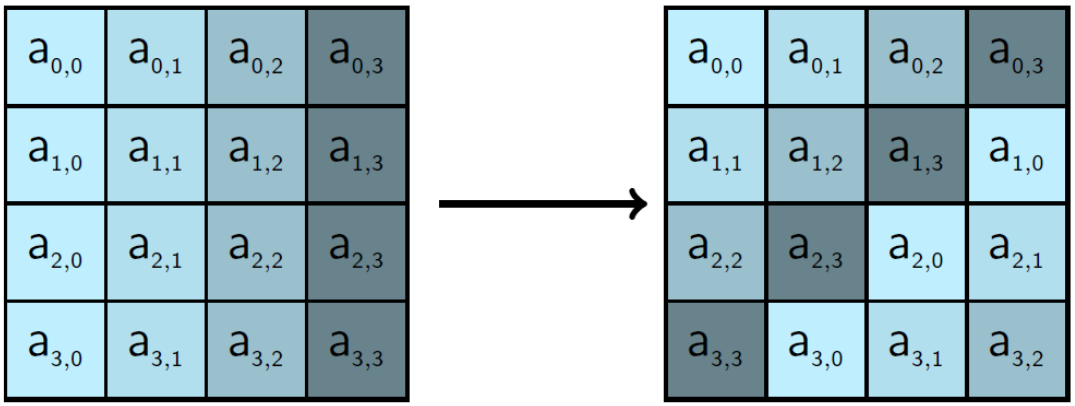


pour s1,1 = 53 s'1,1 = SubBytes(s1,1) = ed

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

Le chiffrement AES

ShiftRows : consiste à effectuer une transformation linaire, en effet le bute de cette opération est d'effectuer un décalage vers la gauche pour chaque ligne sauf la première.



Le chiffrement AES

MixColumns :cette opération est une transformation linéaire Les colonnes sont traitées comme des polynômes dans GF(2^8) et multipliées modulo $x^4 + 1$.
Le but de l'étape précédente est de mélanger les lignes. cette étape a pour pour objectif modifier les colonnes.

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

Le chiffrement AES

AddRoundKey :Une opération XOR est appliqué entre chacun des octets de l'état et de la clé (octet par octet).

Le chiffrement AES

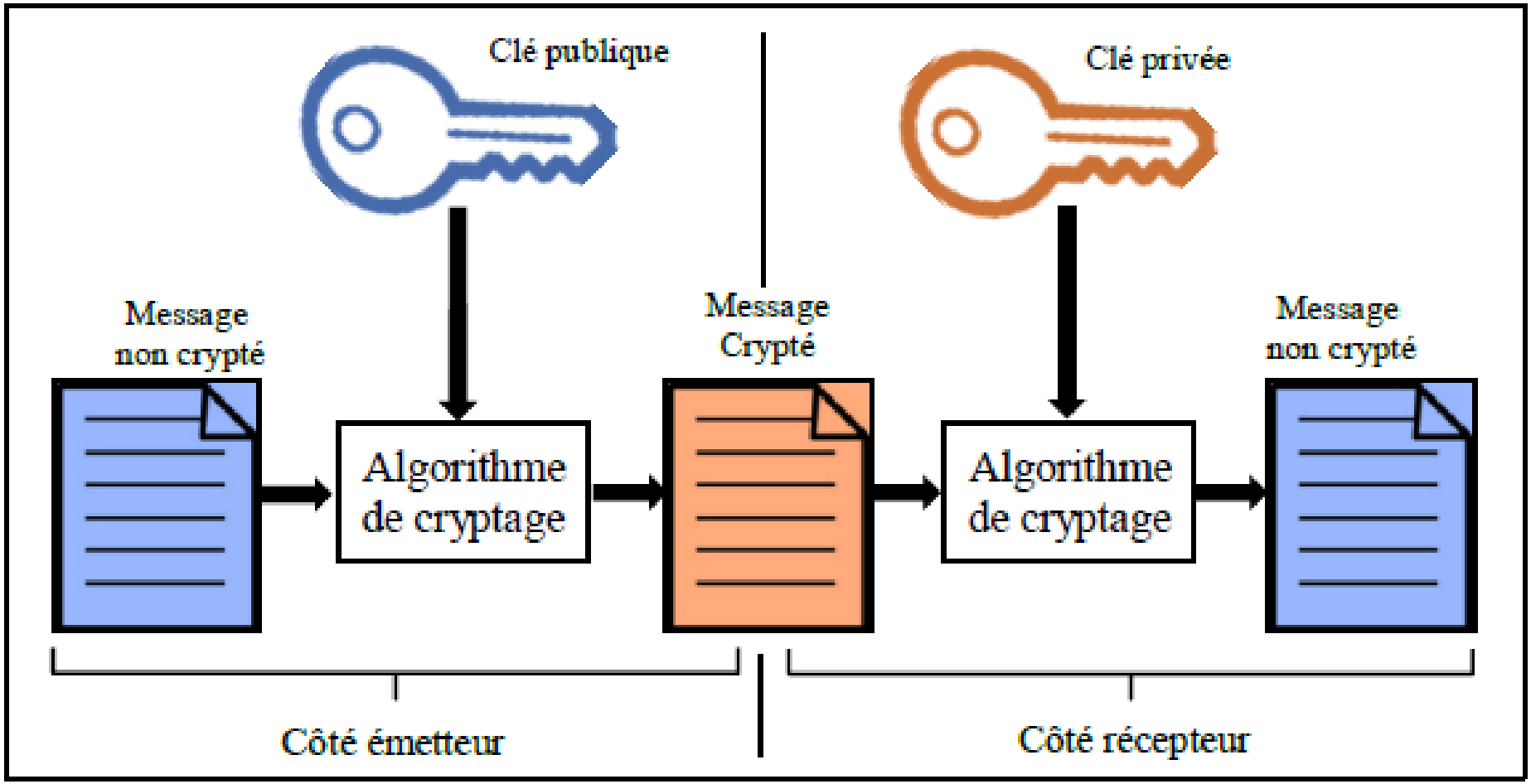
Fonctionnement :
A partir de l'état initial qui est le message clair, et à partir des clés K^i , les étapes de l'algorithme sont les suivantes :
- 9 rondes formées des 4 transformations suivantes :
  - SubBytes
  - ShiftRows
  - MixColumns
  - AddRoundKey
- Une dernière ronde où sont appliquées les transformations suivantes :
  - SubBytes
  - ShiftRows
  - AddRoundKey

La Cryptographie asymétriques

La cryptographie asymétrique à clé publique
son principe consiste à utiliser deux paires de clés, qui sont la clé privée et la clé publique. Seule la clé privée du récepteur est capable de décoder le message, ce qui minimise les risques liés à l'échange de clés. La clé publique est uniquement utilisée lors de la phase de chiffrement du message.

Il doit être impossible de déduire la clé privée de la clé publique.

La Cryptographie asymétriques



La Cryptographie asymétriques

Avantages:

- l'élimination de la problématique de la transmission de clé. on peut chiffrer pour quelqu'un sans partager de secret préalable.
- Seul le destinataire peut déchiffrer.

Inconvénients:

- plus lente que la cryptographie symétrique.

le chiffrement RSA

le chiffremnt RSA apparu en 1978 proposé par L. **R**IVEST, A. **S**HAMIR et L. **A**DLEMAN, ce dernier est un système de chiffrement asymétrique ou chiffrement à clé publique et permis les plus utilisés actuellement, son principe repose sur l'utilisation de deux clés publique et privé préparées par le destinataire l'expéditeur utilise la clé publique du destinataire pour chiffrer son message tandis que pour déchiffrer le message transmis le destinataire utilise sa clé privée.

Le chiffrement RSA

Génération de la clé :

- On choisit donc deux nombres premiers p et q qui serviront à former les clés publiques et privées.
- On calcul N = p*q.
- caluler $\varphi = (p-1) * (q-1)$ (la fonction indicatrice d'Euler)
- choisir un exposant e tel que $PGCD(e, \varphi)$.

le chiffrement RSA

la formule de chiffrement RSA est la suivante :
$C = x^e Mod$ N

le déchiffrement RSA

la formule de déchiffrement RSA est la suivante :
$X = c^d \, modulo \;\; \mathrm{N}$ où :
$e * d = 1 modulo \, [(p-1) * (q-1)]$
la clé publique envoyée à l'expéditeur : (n , e)
la clé privé utilisée pour le déchiffrement est d.

Fonctions de Hachage

Les fonctions de hachage cryptographiques sont des fonctions qui associent à un message de longueur quelconque une valeur de longueur fixe appelée empreinte du message.

- Différentes données en entrée donneront des empreintes différentes.
- l'empreinte ne permet pas la reconstitution du texte original.

En binaire	En hexadécimal
01011010 01100101 01110011 01110100 01100101 00100000 01100100 01100101 00100000 01110011 01100001 01110110 01101111 01101001 01110010	5a 65 73 74 65 20 64 65 20 73 61 76 6f 69 72
01011010 01100101 01110011 01110100 01100101 00100000 01100100 01100101	5a 65 73 74 65 20 64 65

Fonctions de Hachage

Les fonctions de hachage cryptographique doivent assurer les propriétés suivantes :

- résistance à la pré-image : étant donnée une empreinte h, il doit être calculatoirement difficile de trouver un message m tel que $H(m) = h$ (H: la fonction de hachage).
- résistance à la seconde pré-image: étant donné un message m, il doit être calculatoirement difficile de trouver un message $m' \neq m$ tel que $H(m') = H(m)$.
- résistance aux collisions : Il est impossible d'avoir deux messages m et m' différents avec la même valeur de hachage tels que $H(m') = H(m)$.

Exemple : MD5, SHA-1, SHA-2.

Algorithme MD5

L'algorithme MD5 a été inventé par Ronald Rivest en 1991, l'algorithme MD5 produisant en sortie un hash de 128 bits (32 caractères de type Hexadécimal en sortie).

Fonctions de Hachage

fonctionnement MD5:
- Étape 1 : Ajout de bits de padding. Durant cette étape, le message d'origine, par un 1, et de 0 pour que le message étendu ait une longueur congruente à 448 modulo 512,c.a.d ajouter un simple bit "1" suivi par plusieursbit de "0", cela signifie qu'il y aura toujours entre 1 et 512 bits ajoutés dans cette étape.
- Étape 2 : ajouter une représentation de 64 bit au résultat de l'étape présidente.

Fonctions de Hachage

- Étape 3 : initialisation des buffers. Quatre buffers de 32 bits (A, B, C, D) sont utilisés pour un total de 128 bits pour les Valeurs d'initialisation (IV). ainsi 4 fonctions F,G,H et I, qui prennent des arguments codés sur 32 bits, et renvoie une valeur sur 32 bits, les opérations se faisant bit à bit.

$$
\begin{aligned}
F_1(B,C,D) &= (B \wedge C) \vee (\neg B \wedge D) \\
F_2(B,C,D) &= B \wedge D \vee (C \wedge \neg D) \\
F_3(B,C,D) &= B \oplus C \oplus D \\
F_4(B,C,D) &= C \oplus (B \vee \neg D)
\end{aligned}
$$

Fonctions de Hachage