University of khenchela
Departement MI

Computer security

Dr.Hichem Rahab

rahab.hichem@univ-khenchela.dz
L3 ISIL

2022 - 2023

Chapitre 3 :La cryptologie

Overview

Introduction (1)

- 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.
- 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.

Introduction (2)

Avec la popularité grandissante des réseaux, des échanges de données, et donc des transmissions entre individus, de nombreuses menaces émergèrent.

1. Interruption : problème lié à la disponibilité des données
2. Interception : problème lié à la confidentialité des données
3. Modification : problème lié à l'intégrité des données
4. Fabrication : problème lié à l'authenticité des données

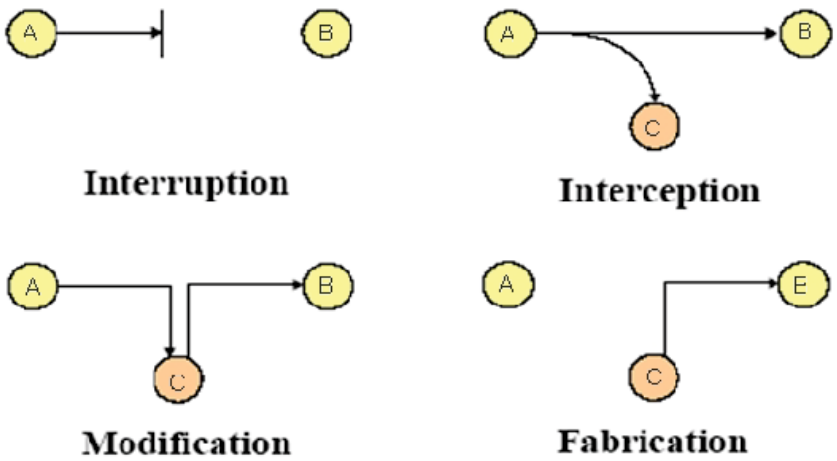


Figure: Les menaces actives

Terminology

- La cryptographie utilise des concepts issus de nombreux domaines (Informatique, Mathématiques, Électronique).
- Toutefois, les techniques évoluent et trouvent aujourd'hui régulièrement des racines dans d'autres branches (Biologie, Physique, etc.)

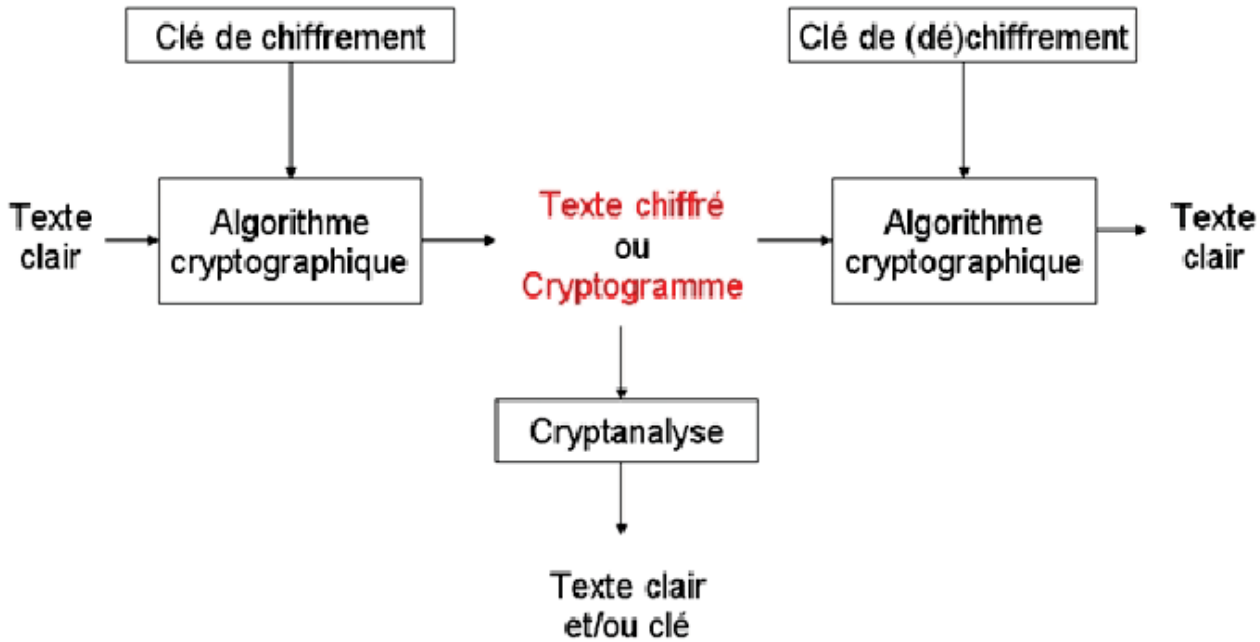


Figure: Protocole de chiffrement

Basic Vocabulary

- **Cryptologie (Cryptology):** Il s'agit d'une science mathématique comportant deux branches : la cryptographie et la cryptanalyse,
  1. **Cryptographie (Cryptography):** La cryptographie est l'étude des méthodes donnant la possibilité d'envoyer des données de manière sécurisée sur un support donné.
  2. **Cryptanalyse (Cryptanalysis):** 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.
- **Chiffrement (Encryption ou enciphering) :** Le chiffrement consiste à transformer une information donnée (texte, message, ...) afin de la rendre incompréhensible par une personne autre que celui qui a créé le message et celui qui en est le destinataire.
- **Déchiffrement (Decryption or deciphering):** La fonction permettant de retrouver le texte clair à partir du texte chiffré utilisant la *clé de déchiffrement* (Decryption key).

Vocabulaire de base (suite)

- **Texte claire (Plaintext):** C'est le texte à échangé entre les entités communicantes, il est le sujet de l'opération de chiffrement afin de le rendre inintelligible qu'aux entités autorisées.
- **Texte chiffré (Ciphertext):** Appelé également **cryptogramme**, le texte chiffré est le résultat de l'application d'un chiffrement à un texte clair.
- **Clef (Key):** Il s'agit du paramètre impliqué et autorisant des opérations de chiffrement et/ou déchiffrement.
  1. Dans le cas d'un algorithme symétrique, la clef est identique lors des deux opérations.
  2. Dans le cas d'algorithmes asymétriques, elle diffère pour les deux opérations.
- **Cryptosystème (Cryptosystem):** Il est défini comme l'ensemble des clés possibles (espace de clés), des textes clairs et chiffrés possibles associés à un algorithme donné.

Notations

En cryptographie, la propriété de base est que:

$$M = D(E(M))$$

Tel que:

$$C = E_{E_k}(M) \qquad et \qquad M = D_{D_k}(C)$$

où:

- M représente le texte clair,
- C est le texte chiffré (cryptogramme),
- E_k et D_k sont les clés de chiffrement et de déchiffrement respectivement. (Dans le cas d'algorithmes symétriques, $E_K \equiv D_k$)
- E(x) est la fonction de chiffrement, et
- D(x) est la fonction de déchiffrement.

Principe de Kerckhoff

Principe de Kerckhoff

La sécurité du chiffrement ne doit pas dépendre de ce qui ne peut pas être facilement changé.

- En d'autres termes, aucun secret ne doit résider dans l'algorithme mais plutôt dans la clé. Sans celle-ci, il doit être impossible de retrouver le texte clair à partir du texte chiffré.
- Par contre, si on connaît K, le déchiffrement est immédiat.
- On parle aussi de la Maxime de Shannon, dérivée du principe de Kerckhoff.

Maxime de Shannon

L'adversaire connait le système.

La publication des algorithmes

Selon l'endroit où réside le secret, on peut parler d'algorithme secret ou d'algorithme publié. Chacun possède ses atouts et inconvénients.

- **Algorithme secret:**
  - La cryptanalyse, souvent basée sur le secret de la clé, doit ici en plus retrouver l'entièreté de l'algorithme (mécanisme de récupération).
  - Souvent, de tels algorithmes sont utilisés par un petit nombre d'utilisateurs. Et comme souvent dans ce cas, moins il y a de monde l'utilisant, moins il y a d'intérêts à le casser.
  - De tels algorithmes sont rarement distribués par delà les frontières, afin de garder un nombre d'utilisateurs restreint.

La publication des algorithmes (2)

Selon l'endroit où réside le secret, on peut parler d'algorithme secret ou d'algorithme publié. Chacun possède ses atouts et inconvénients.

- **Algorithme publié:**
  - Puisque l'algorithme est publié, tout le monde a le droit de l'explorer. Ainsi, les failles (laissées intentionnellement ou non par les concepteurs) peuvent être plus facilement découvertes. La sécurité en est donc améliorée.
  - Comme la publication est autorisée, il n'est pas nécessaire de chercher à protéger le code contre le reverse-engineering.
  - Cette publication permet d'étendre les travaux sur l'algorithme au niveau mondial. Toute une série d'implémentations logicielles peuvent donc être réalisées.
  - Tout le monde utilise la même version publique ce qui permet une standardisation générale.

En conséquence, on préférera les algorithmes publiés, souvent plus sûrs pour les raisons explicitées ci-dessus.

Classical Encryption (La cryptologie classique)

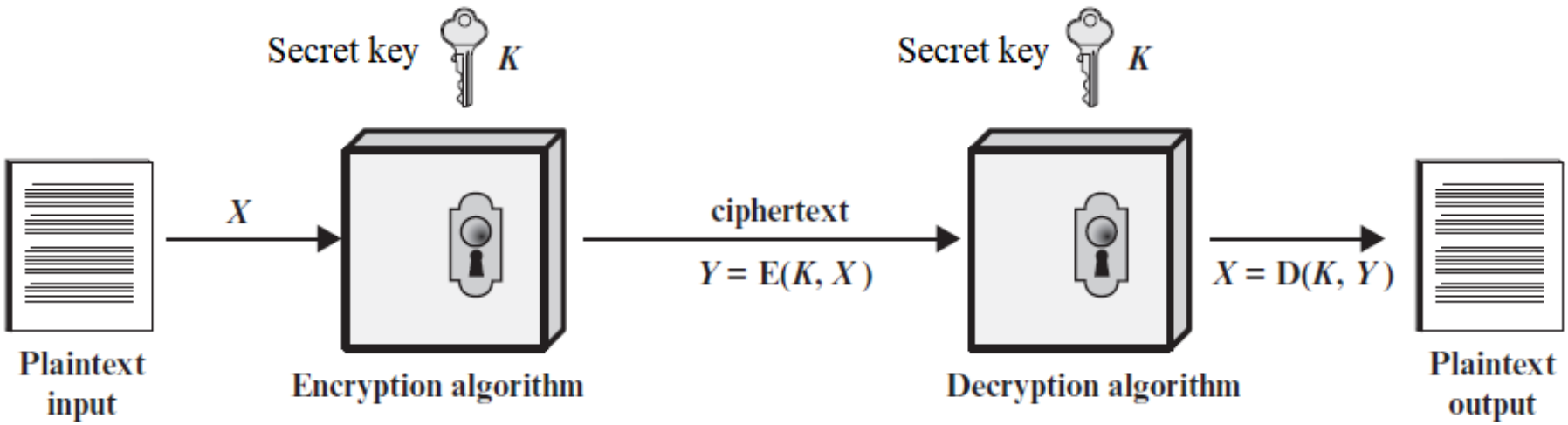
La cryptologie classique

La cryptographie symétrique (Symmetric encryption), connu aussi comme la cryptographie conventionnelle (conventional encryption) ou crypograpie à une seule clé (single-key encryption), est le seul type de chiffrement connu avant le développement des systèmes de chiffrement à clé publique (public-key encryption) dans les années 1970.

La cryptologie classique

Un système de chiffrement symétrique possède cinq ingrédients:

1. Texte claire (Plain text):
2. Algorithme de chiffrement (Encryption algorithm):
3. Clé secrète (Secret key):
4. Teste chiffré (Ciphertext):
5. Algorithme de déchiffrement (Decryption algorithm):



Caesar Cipher (50 av. J-C)

- Il s'agit d'un des plus simples et des chiffres classiques les plus populaires.
- C'est une **substitution monoalphabétique** où chaque lettre est remplacée par une autre lettre ou symbole.
- Dans les formules ci-dessous, p est l'indice de la lettre de l'alphabet, k est le décalage.
- Pour le chiffrement, on aura la formule:

$$c = E(p) = (p + k) mod 26$$

- Pour le déchiffrement, il viendra

$$p = D(c) = (c - k) mod 26$$

Caesar Cipher (50 av. J-C) - (2)

Exemple 1 :

Par exemple, si on a le text suivant: 'A cat'

et on a besoin de chiffrer par une clé: k=2 ,le message devient: C ecv

$$e = \begin{pmatrix} ABCDEFGHIJKLMNOPQRSTUVWXYZ \\ CDEFGHIJKLMNOPQRSTUVWXYZAB \end{pmatrix}.$$

Lorsque on le chiffre avec clé=3, le message devient: D fdw.

$$e = \begin{pmatrix} ABCDEFGHIJKLMNOPQRSTUVWXYZ \\ DEFGHIJKLMNOPQRSTUVWXYZABC \end{pmatrix}.$$

A vous:

Chiffrez vos noms et prénoms avec une clé égale au jour de votre naissance mod 26.

Caesar Cipher (50 av. J-C) -(3)

Exemple 2 :

Avec une clé de 15 (le décalage circulaire fait que le A est remplacé par P, B par Q, C par R ... comme le montre le tableau suivant).

1	2	3	4	5	6	7	8	9	10	11	12	13
A	B	C	D	E	F	G	H	I	J	K	L	M
14	15	16	17	18	19	20	21	22	23	24	25	26
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
•	•	•	•	•	•	•	•	•	•	•	•	•
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

Il devient simple de faire le chiffrement :

VIVE LE MONDE DES RESEAUX

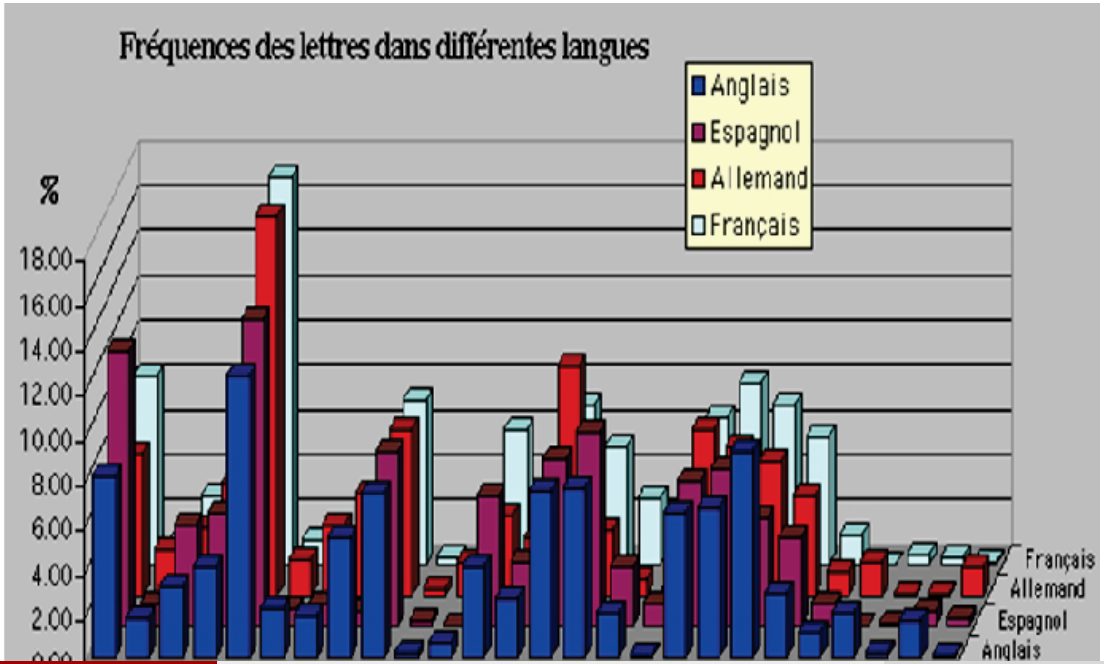
devient :

KXKT AT BDCST STH GTHTPJM

Caesar Cipher (50 av. J-C) -(4)

Exemple 2 : (suite)

- Un tel système ne résiste pas à la cryptanalyse c'est-à-dire au déchiffrement brutal sans la clé.
- La méthode utilisée étant une simple substitution, les fréquences d'apparition des lettres dans la langue utilisée restent respectées : ici il y a six T et au plus deux fois une autre lettre. Il est facile de penser que T code le E . . . et le reste suit.



Caesar Cipher - Cryptanalysis

KEY	
	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kvmot
9	gyyn gy uznyl nby niau julns
10	fxxm fx tymxk max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg iwt idvp epgin
15	assh as othsf hvs hcuo dofhm
16	zrrg zr nsgre gur gbtn cnegl

Caesar Cipher - Cryptanalysis

- Si on connait l'algorithme utilisé (ici César), la cryptanalyse par force brute est très facile.
- En effet, dans le cas du chiffre de César, seules 25 clés sont possibles.
- Trois caractéristiques importantes de ce problème rend l'attaque par force brute très probable:
  1. Les algorithmes de cryptage et de décryptage sont connus.
  2. Il y a seulement 25 clés à essayer.
  3. La langue du texte claire est connue et facilement reconnue.
- Pour ces raison le chiffrement de césar est loin d'être sécurisé.

Vigenère Cipher (1568)

- Le plus connu, et l'un des plus simples chiffrements polyalphabétiques est le chiffrement de Vigenère.
- 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 clef qui définit le décalage pour chaque lettre du message (A : décalage de 0 cran, B : 1 cran, C : 2 crans, ..., Z : 25 crans).

Vigenère Cipher -(2)

	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

Vigenère Cipher -(3)

Exemple 1:

On a à chiffrer le texte *"CHIFFRE DE VIGENERE"* avec la clef *"BACHELIER"* (cette clef 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

Le message chiffrée est alors: *DHKMJCMHVWIILRPZI*

Vigenère Cipher -(4)

Exemple 2: Déchiffrer le Message :"UHZZWJSCKIVWKBVRUZEFR" utilisant la clef:"AURESS".

$$e = \begin{pmatrix} UHZZWJSCKIVWKBVRUZEFR \\ AURESSAURESSAURESSAUR \end{pmatrix}.$$

	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

Vigenère Cipher -(5)

Exemple 2:(Réponse sur la page suivante)

Vigenère Cipher -(5)

Exemple 2:(Réponse)

$$d = \begin{pmatrix} UHZZWJSDKIVWKBVRUZEFR \\ AURESSAURESSAURESSAUR \\ - - - - - -- \\ UNIVERSITEDEKHENCHELA \end{pmatrix}.$$

Vigenère Cipher -(6)

Exemple 3:

Chaque étudiant doit chiffrer son nom et prénom utilisant comme clé; le prénom de son collègue.

Chiffrement par transposition

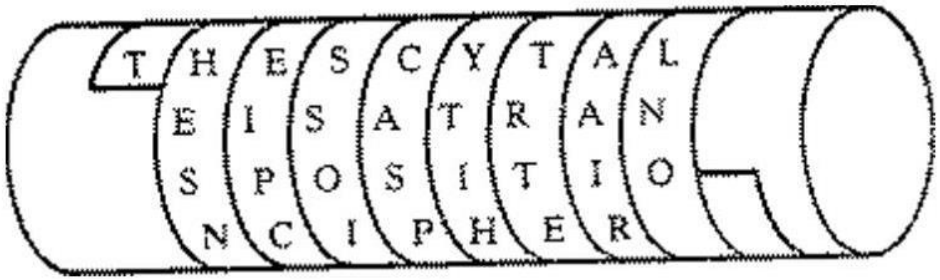
- Les méthodes de chiffrement par transposition consistent à réarranger les données à crypter de telle façon à les rendre incompréhensibles.
- Il s'agit généralement de réarranger géométriquement les données pour les rendre visuellement inexploitables.
- Une forme de transposition utilise le premier dispositif de cryptographie militaire connu, la scytale spartiate, remontant au V^e siècle avant J.-C. La scytale consiste en un bâton de bois autour duquel est entourée une bande de cuir ou de parchemin, comme le montre la figure.

Chiffrement par transposition -(2)

La technique assyrienne:

La technique consistait à:

- Après avoir enroulé la ceinture sur la scytale, le message était écrit en plaçant une lettre sur chaque circonvolution (axe). Question : comment le destinataire déchiffrerait le message sur le scytale ?
- Le message une fois déroulé n'est plus compréhensible "TNSEHCPIEIOSSPSACHITYETRTRIAAONL".
- Il suffit au destinataire d'avoir un cylindre de même rayon pour pouvoir déchiffrer le message "THE SCYTALE IS A TRANSPOSITION CIPHER".



Transposition matricielle (1)

Transposition à base matricielle

- Le message en clair est écrit dans une matrice.
- La clé est le nombre de colonnes de la matrice. La technique de transposition de base consiste à lire la matrice en colonne.

Exemple :

Soit à chiffrer le message "MESSAGE SECRET A TRANSPOSER" avec la matrice M(6).

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"

Transposition matricielle (2)

Exemple 2: Déchiffrer le message suivant chiffré avec une matrice M(8).(Les tirets représentent le espaces)
TITESRTR - AAIIDGNOCEESNI - - P - EMNOMLEESALST

Transposition matricielle avec permutation

- Une alternative plus compliquée consiste à permuter l'ordre des colonnes.
- L'ordre des colonnes devient la clé de l'algorithme.

Exemple 3:

Key:	4	3	1	2	5	6	7
Plaintext:	a	t	t	a	c	k	p
	o	s	t	p	o	n	e
	d	u	n	t	i	l	t
	w	o	a	m	x	y	z

Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

Dans cet exemple, la clé est 4312567. Pour crypter, on commence avec la colonne numéro 1, dans ce cas la colonne 3. On écrit les lettres de ce colonne vers le bas. Ensuite, on va à la colonne 4, numéroté 2, puis la colonne 2, ensuite la colonne 1, et après les colonnes 5, 6, et 7.

Transposition matricielle avec permutation (2)

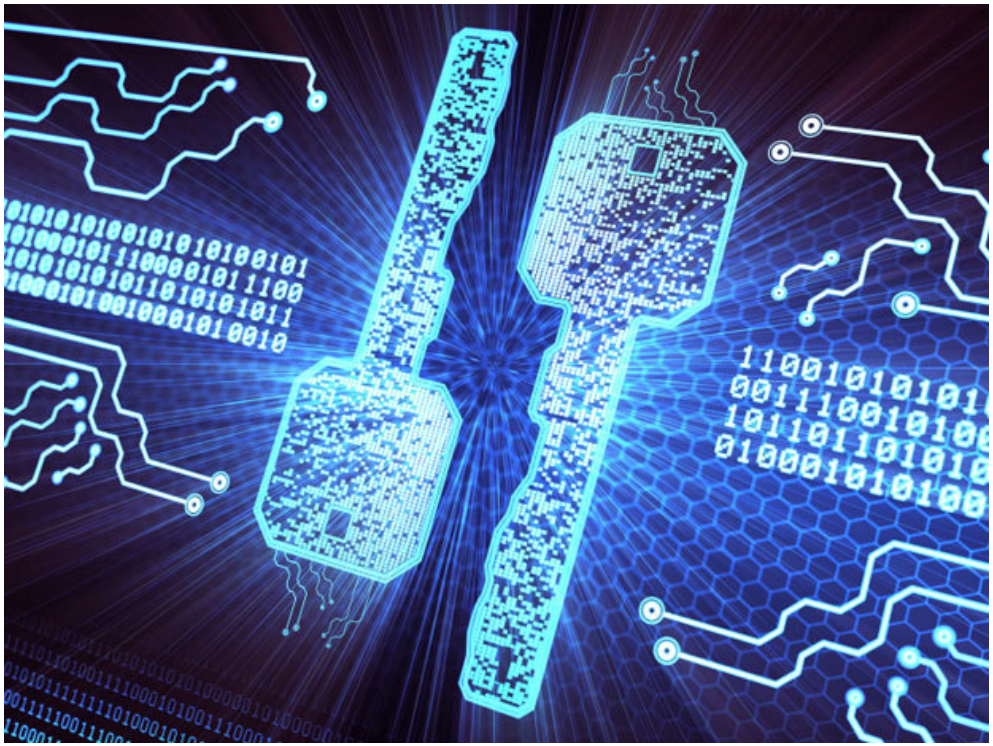
- Un chiffrement par transposition peut être renforcer par ajouter plusieurs stages de transposition.

Exemple 4:

Key:	4	3	1	2	5	6	7
Plaintext:	t	t	n	a	a	p	t
	m	t	s	u	o	a	o
	d	w	c	o	i	x	k
	n	l	y	p	e	t	z

Output: NSCYAUOPTTWLTMDNAOIEPAXTTOKZ

La cryptographie moderne



Cryptographie symétrique

- Depuis l'ère de "Jules César" jusqu'à la fin des années 70 la cryptographie symétrique était la seule méthode de chiffrement pour les domaines: diplomatiques, militaires, et commerciales.
- La *cryptographie symétrique* reste la méthode universelle pour assurer la confidentialité des transmission et de stockage de données à travers des années.
- Les algorithmes de cryptage le plus importants dans cette catégories son: DES (Data Encryption Standard) et AES (Advanced Encryption Standard).
- Un cryprosystème symétrique a cinq ingrédients:
  1. *Plaintext* ou message original,
  2. *Algorithme de chiffrement*,
  3. *Clé secrète*,
  4. *Cryptogramme* ou message chiffré,
  5. *Algorithme de déchiffrement*.

Cryptographie symétrique -(2)

Définition

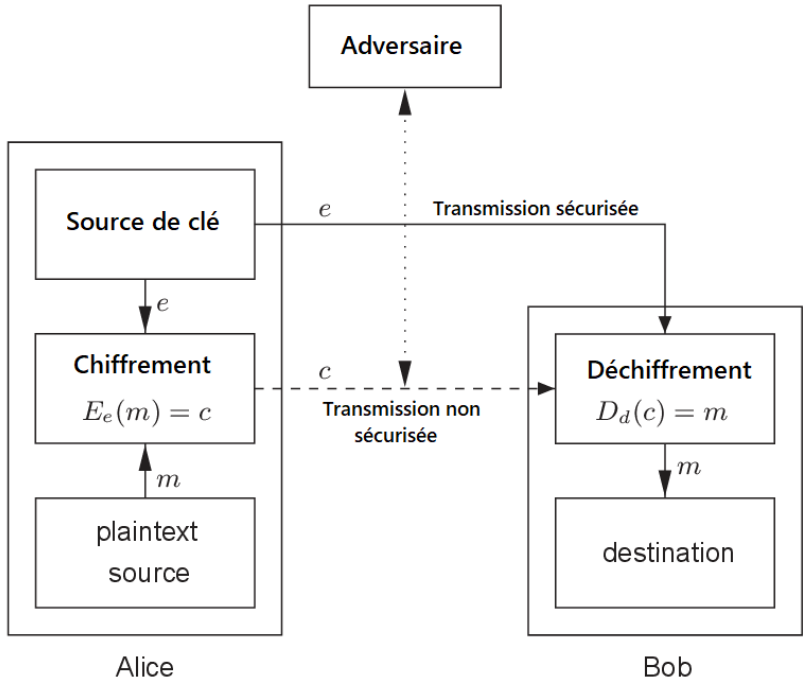
Considérant un cryptosystème consistant sur un ensemble de transformations de chiffrement $E_e : e \in K$ et de déchiffrement $D_d : d \in K$ où K est l'espace des clés.

- Le cryptosystème est à clé symétrique, si pour chaque pair ; clé de chiffrement/clé de déchiffrement (e, d) il est facile de calculer d à partir de e et de déterminer e depuis d.

- Dans la plupart des cryptosystèmes à clé symétrique on a $e = d$, alors les termes; *clé symétrique* ,*une seule clé* et *clé secrète* sont utilisés.
- La cryptographie symétrique aussi appelée; cryptographie conventionnelle ou cryptographie à une seule clé.

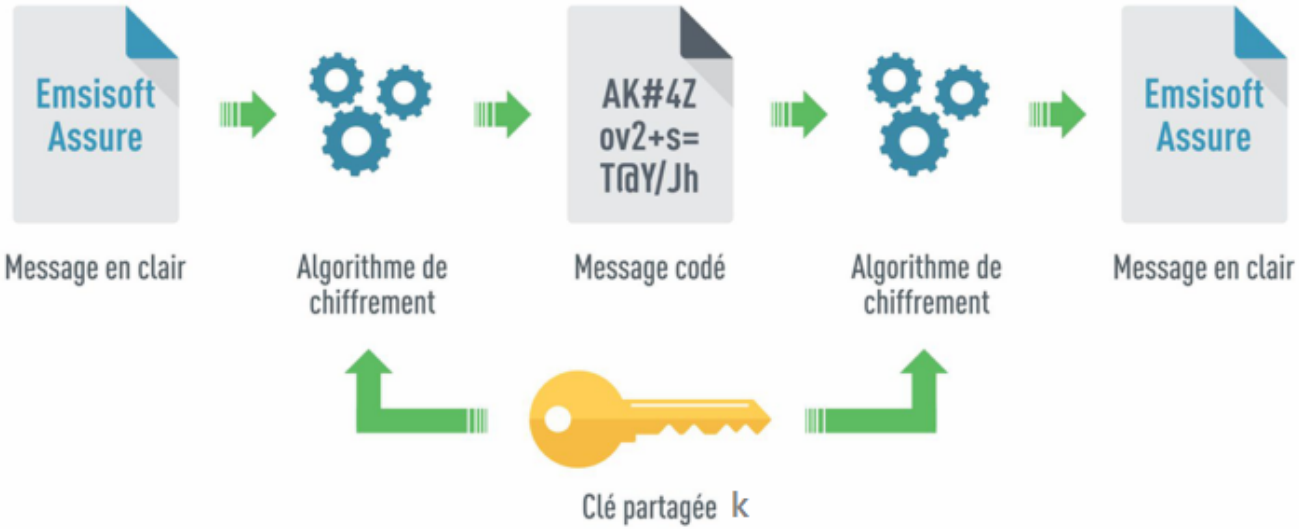
Cryptographie symétrique (3)

- 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 permet une utilisation massive.



Caractéristiques :

- Les clés sont identiques : $K_E = K_D = K$,
- La clé doit rester secrète,
- Les algorithmes les plus répandus sont le DES, AES, 3DES, ...
- La génération des clés est aléatoire dans l'espace des clés,
- Ces algorithmes sont basés sur des opérations de transposition et de substitution des bits du texte clair en fonction de la clé,

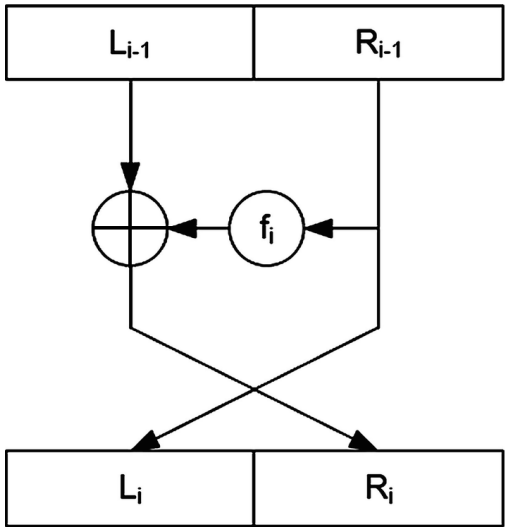


Caractéristiques (suite) :

- La taille des clés est souvent de l'ordre de 128 bits. Le DES en utilise 56, mais l'AES peut aller jusque 256,
- L'avantage principal de ce mode de chiffrement est sa rapidité,
- Le principal désavantage réside dans la distribution des clés.
- Pour une meilleure sécurité, on préfèrera l'échange manuel.
- Malheureusement, pour de grands systèmes, le nombre de clés peut devenir conséquent. C'est pourquoi on utilisera souvent des échanges sécurisés pour transmettre les clés.
- En effet, pour un système à N utilisateurs, il y aura $N(N-1)/2$ paires de clés. Pour trois utilisateurs on a besoin de 3 clés. Pour 4, 6 clés et pour 10 on besoin de 45 clés.

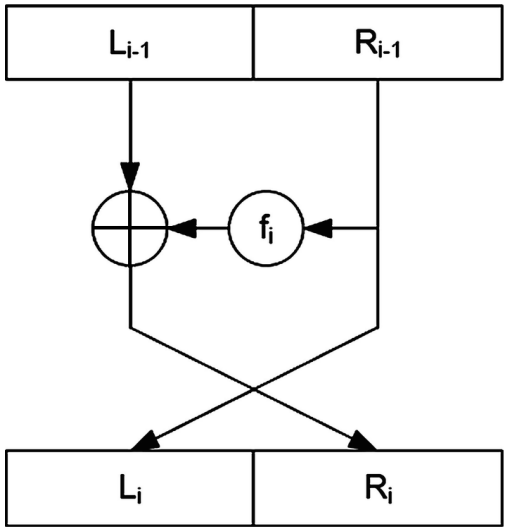
Les structures de Feistel

- Fut décrite en 1973 (par Horst Feistel, employé chez IBM).
- La plupart des chiffrements de la fin du XXè siècle sont basés sur cette structure.
- Le bloc d'entrée d'un round est séparé en deux parties. La fonction de chiffrement est appliquée sur la première partie du bloc et l'opération binaire OU-Exclusif (XOR $\oplus$) est appliquée sur la partie sortante de la fonction et la deuxième partie. Ensuite les deux parties sont permutées et le prochain round commence.

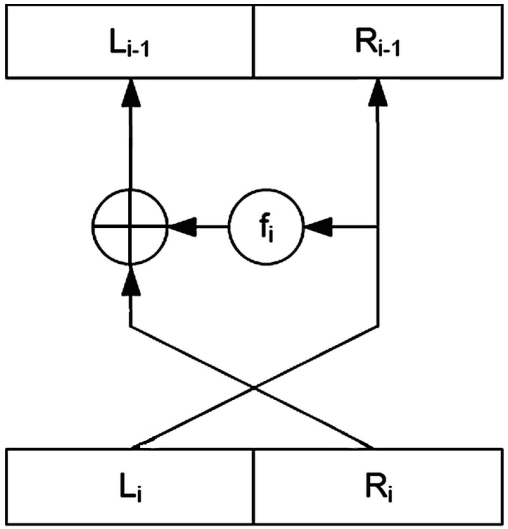


Les structures de Feistel -(2)

- L'avantage est que la fonction de chiffrement et la fonction de déchiffrement sont identiques.
- Elle est inversible ce qui permet de réutiliser le matériel de chiffrement pour déchiffrer un message.



Chiffrement



Déchiffrement

Les structures de Feistel -(3)

Exemple:

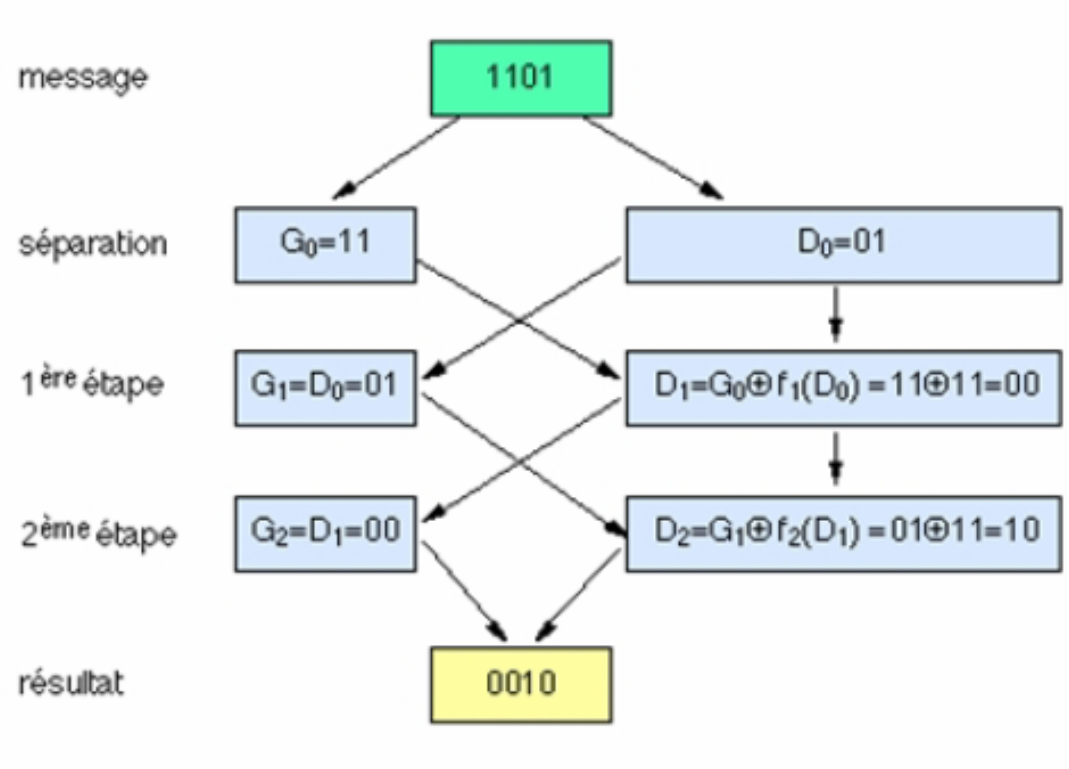
Soient deux fonctions de chiffrement. A partir d'une table de correspondance, on peut déterminer le résultat du chiffrement d'un bloc après passage dans une structure de Feistel.

entrée	f_1	sortie	entrée	f_2	sortie
00	$\rightarrow$	01	00	$\rightarrow$	11
01	$\rightarrow$	11	01	$\rightarrow$	00
10	$\rightarrow$	10	10	$\rightarrow$	00
11	$\rightarrow$	01	11	$\rightarrow$	01

Les structures de Feistel -(4)

Exemple: (suite)

Exécution d'un schéma de Feistel pour chiffrer le message:**1101**.



message	résultat
0000	0100
0001	1100
0010	1010
0011	0111
0100	0011
0101	1001
0110	1111
0111	0000
1000	1101
1001	0101
1010	0001
1011	1110
1100	1000
1101	0010
1110	0110
1111	1011

Les structures de Feistel-(5)

Choix des paramètres:

La réalisation d'un tel réseau dépend des choix effectués pour les paramètres suivants :

- Taille du bloc : Lorsqu'elle augmente, la sécurité augmente également.
- Taille de clé : Lorsqu'elle augmente, la sécurité aussi.
- Nombre de cycle : Plus il y en a, plus la sécurité est renforcée. Un nombre typique est de 16 cycles.
- Algorithme de génération des sous-clés : Plus il est complexe, plus la compréhension est rendue difficile.

Data Encryption Standard (DES)

- Le DES (Data Encryption Standard, Standard de Chiffrement de Données) est un standard mondial depuis la fin des années 1970.
- Au début de cette décennie, le développement des communications entre ordinateurs a nécessité la mise en place d'un standard de chiffrement de données pour limiter la prolifération d'algorithmes différents ne pouvant pas communiquer entre eux.
- Pour résoudre ce problème, l'Agence Nationale de Sécurité américaine (NSA, pour National Security Agency) a lancé des appels d'offres.
- La société I.B.M. a développé alors un algorithme nommé **Lucifer**, relativement complexe et sophistiqué. Après quelques années de discussions et de modifications, cet algorithme, devenu alors un standard, DES, et fut adopté au niveau fédéral le 23 novembre 1976.
- DES fait partie de la famille des chiffrements itératifs par blocs, plus particulièrement il s'agit d'un schéma de Feistel.

DES (2)

Particularités:

Le DES comporte plusieurs avantages qui en ont fait l'algorithme de chiffrement symétrique standard pendant longtemps, jusqu'il y a quelques années. En voici quelques-uns :

- Il possède un haut niveau de sécurité,
- Il est complètement spécifié et facile à comprendre,
- la sécurité est indépendante de l'algorithme lui-même (*principe de Kerckhoff*),
- Il est rendu disponible à tous, par le fait qu'il est public,
- Il est adaptable à diverses applications (logicielles et matérielles),
- Il est rapide et exportable,
- Il repose sur une clé relativement petite, qui sert à la fois au chiffrement et au déchiffrement,
- Il est facile à implémenter.

DES (3)

- Le DES est un cryptosystème agissant par blocs. Il découpe virtuellement le texte clair en blocs de 64 bits qu'ils code séparément, puis qu'il concatène.
- Un bloc de 64 bits du texte clair entre et un bloc de 64 bits de texte chiffré sort de l'autre coté.
- L'algorithme est assez simple puisqu'il ne combine en fait que des permutations et des substitutions.
- La clé a ici une longueur de 64 bits, c'est-à-dire 8 caractères, mais dont seulement 56 bits sont utilisés.
- L'entière sécurité de l'algorithme repose sur les clefs puisque l'algorithme est parfaitement connu de tous. La clé de 64 bits est utilisée pour générer 16 autres clés de 48 bits chacune qu'on utilisera lors de chacune des 16 itérations du DES.
- Ces clés sont les mêmes quel que soit le bloc qu'on code dans un message.

DES (4)

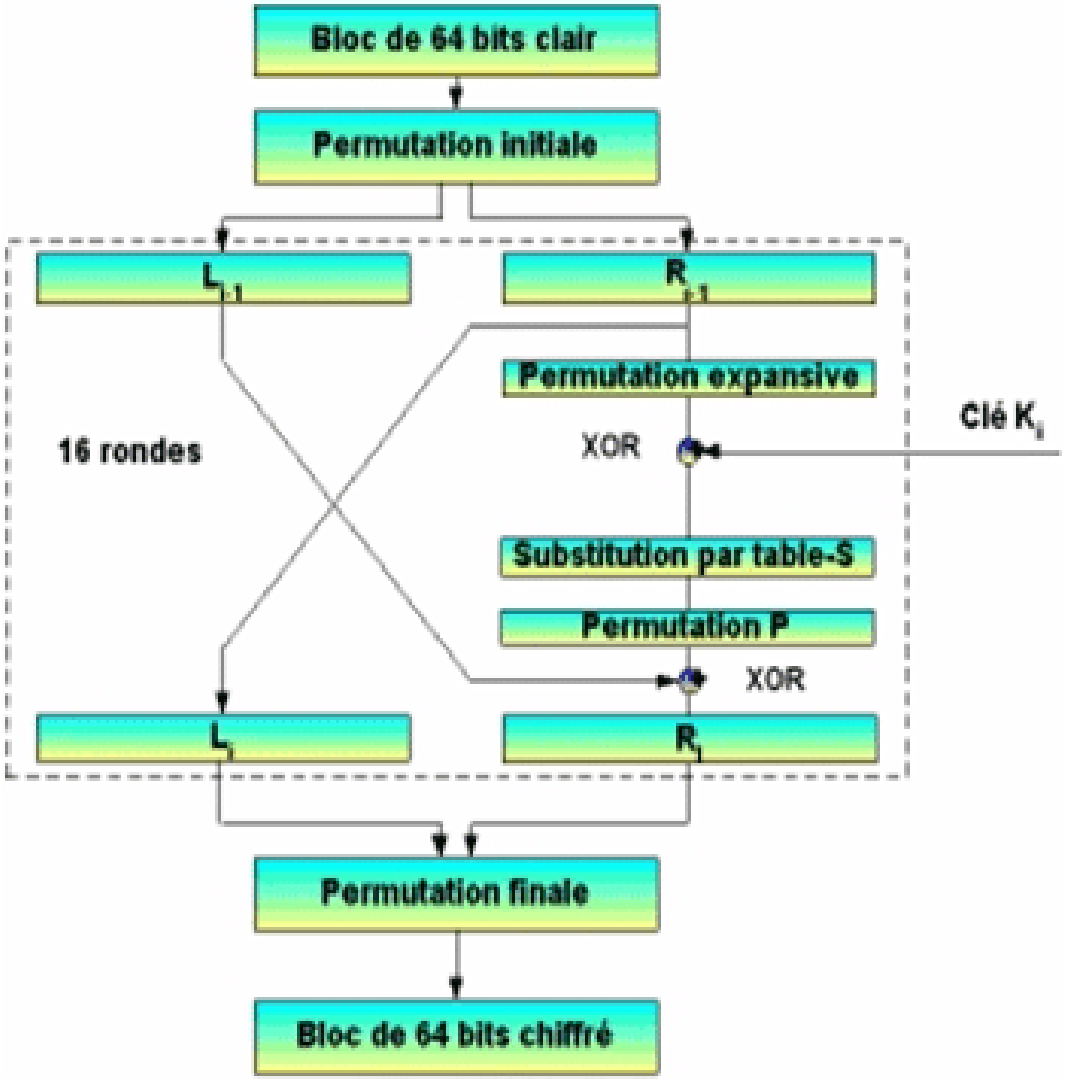
- Cet algorithme est relativement facile à réaliser matériellement et certaines puces chiffrent jusqu'à $1Go$ de données par seconde.
- Pour les industriels, c'est un point important notamment face à des algorithmes asymétriques, plus lents, tels que l'algorithme RSA.

DES (5)

Algorithme de chiffrement

- L'algorithme repose principalement sur 3 étapes, en plus de la gestion spécifique de la clé :
  1. Permutation initiale
  2. Calcul médian (16 fois) : application de l'algorithme en fonction de la clé,
  3. Permutation finale

DES (6)


Bloc de 64 bits clair
Permutation initiale
L_{i-1}
R_{i-1}
Permutation expansive
Clé K_i
16 rondes
XOR
Substitution par table-S
Permutation P
XOR
L_i
R_i
Permutation finale
Bloc de 64 bits chiffré

DES (7)

La permutation initiale:

Les 64 bits du bloc d'entrée subissent la permutation de la figure suivante. Cette "matrice" permet d'effectuer des changements internes au bloc (i.e. il n'y a pas d'apport de données extérieures). Le premier bit sera le bit 58, le second le bit 50, etc.

01	09	17	25	33	41	49	57
02	10	18	26	34	42	50	58
03	11	19	27	35	43	51	59
04	12	20	28	36	44	52	60
05	13	21	29	37	45	53	61
06	14	22	30	38	46	54	62
07	15	23	31	39	47	55	63
08	16	24	32	40	48	56	64

58	50	42	34	26	18	10	02
60	52	44	36	28	20	12	04
62	54	46	38	30	22	14	06
64	56	48	40	32	24	16	08
57	49	41	33	25	17	09	01
59	51	43	35	27	19	11	03
61	53	45	37	29	21	13	05
63	55	47	39	31	23	15	07

DES (8)

Le calcul médian

Les 64 bits initiaux de données sont divisés en 2 blocs (L et R).

Itérations :

- $L_n = R_{n-1}$
- $R_n = L_{n-1} \oplus F(R_{n-1}, K_n)$
- $K_n = G(K, n)$

Avec:

- $T_n = L_n R_n$
- $L_n = t_1 \ldots t_{32}$
- $R_n = t_{33} \ldots t_{64}$

DES (9)

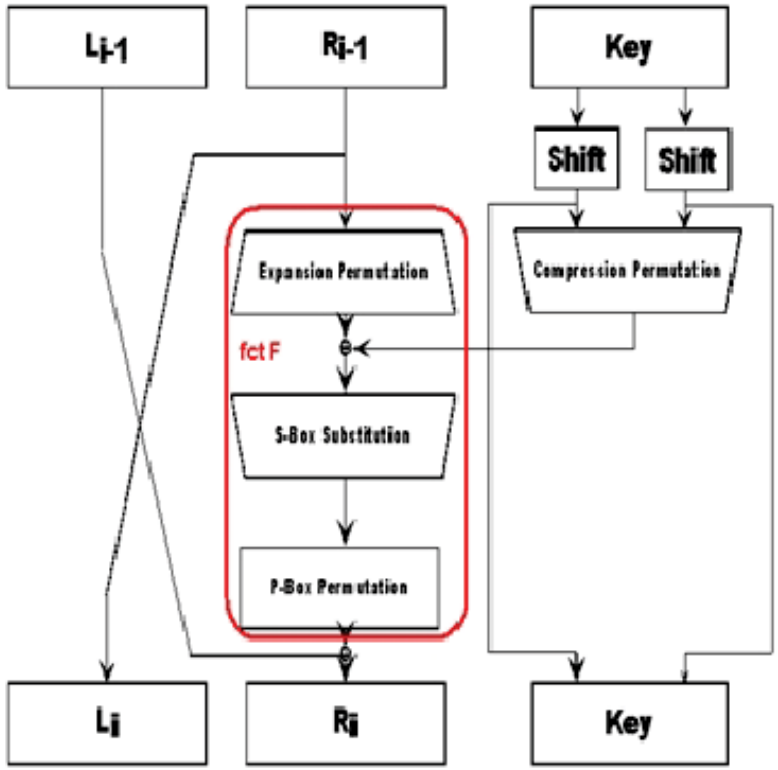


Figure: Etape générale du calcul médian

DES (10)

Permutation finale

- Une fois le calcul médian terminé, on pratique la permutation inverse de la permutation initiale.

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Figure: Permutation finale DES

Déchiffrement:

Il suffit d'appliquer le même algorithme mais inversé en tenant bien compte du fait que chaque itération du déchiffrement traite les mêmes paires de blocs utilisés dans le chiffrement.

Attaques sur DES

Plusieurs attaques existent pour casser le DES. Parmi ces attaques on trouve la recherche exhaustive par force brute où on teste toutes les clés possibles afin de déchiffrer un bloc de données. On a besoin, en moyenne, de 2^{55} essais.

- EFF DES cracker (ou Deep Crack, élaboré par l'Electronic Frontier Foundation). est une machine spécialisée développée pour l'attaque de DES. En juillet 1998, Deep Crack gagne le DES Challenge II-2 en décryptant un message en 56 heures de travail et gagne 10 000 $.
- Le calcul distribué : un regroupement d'ordinateurs par Internet qui partagent leur puissance de calcul. En 1998, Distributed.net a pu décrypter un message en 39 jours. Le 19 janvier 1999, EFF et Distributed.net ont cassé en travaillant conjointement une clé en 22 heures et 15 minutes.
- Depuis 2006, un autre ordinateur dédié, nommé COPACABANA, permet de casser une clé DES en 9 jours.

Attaques sur DES (suite)

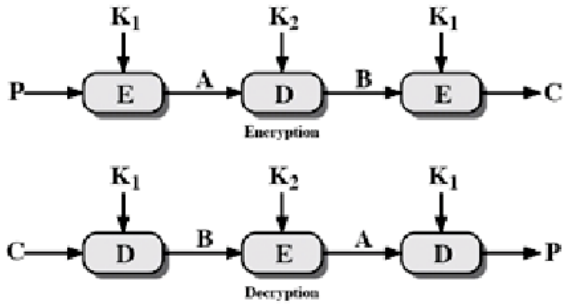
- En 2008, des améliorations logicielles ont même permis de diminuer le temps de recherche à 6,4 jours. Son avantage est son coût : 10.000$. On peut donc facilement en acquérir plusieurs et donc diminuer le temps de recherche en conséquence. Par exemple, pour 4 machines acquises (=40,000$), il faudra compter 1,6 jour de recherche.
- Pour des sociétés importantes ou des gouvernements, construire de telles machines est désormais possible.
- Cela marque la fin du DES.

Triple DES (3DES)

- Grâce à 2 clefs, on pratique 3 opérations :

$$E(k_1, D(k_2, E(k_1, m))).$$

- C'est équivalent au fait de doubler la taille effective de la clé (ce qui est une longueur sûre actuellement).
- Il existe deux versions : la première utilise deux clés, la seconde trois (le dernier chiffrement utilise une troisième clé).
- En comparaison au DES, 3DES est plus robuste contre les attaques faisables connues. Cependant, il est beaucoup plus lent que le DES car on triple les opérations.



AES (Advanced 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.).
- Pour cette tâche, on préfère utiliser l'algorithme connu sous le nom générique d'AES (Advanced Encryption Standard), issu d'un concours créé en raison des faiblesses avérées du DES.
- Cet algorithm est développé par deux cryptographes Belges, John Daemen et Vincent Rijmen.
- Le véritable nom de l'AES est le **Rijndael**, nom résultant de la contraction des noms de ses inventeurs : Rijmen et Deamen.
- Le Triple DES demeure toutefois une norme acceptée pour les documents gouvernementaux aux USA Pour l'instant, il n'y a pas de projet ou d'obligation de rechiffrer les documents existants.

AES (2)

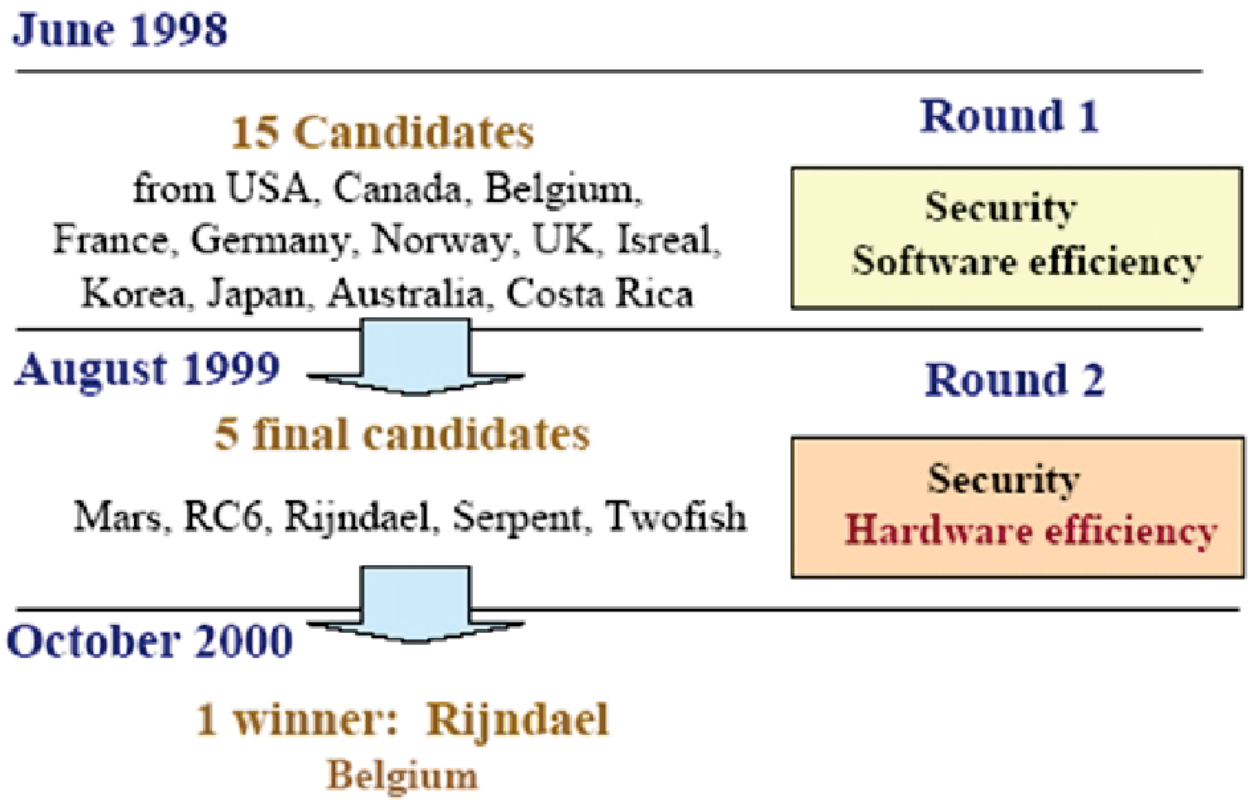


Figure: Concours AES

AES (3)

AES possède les propriétés suivantes :

- Plusieurs longueurs de clé et de bloc sont possibles : 128, 192, ou 256 bits,
- Le nombre de cycles (”rondes”) varie en fonction de la longueur des blocs et des clés (de 10 à 14),
- La structure générale ne comprend qu'une série de transformations/permutations/sélections,
- Il est beaucoup plus performant que le DES ,
- Le parallélisme peut être implémenté

À chaque ronde, quatre transformations sont appliquées :

1. Substitution d'octets dans le tableau d'état,
2. Décalage de rangées dans le tableau d'état,
3. Déplacement de colonnes dans le tableau d'état (sauf à la dernière ronde),
4. addition d'une ”clé de ronde” qui varie à chaque ronde.

AES (4)

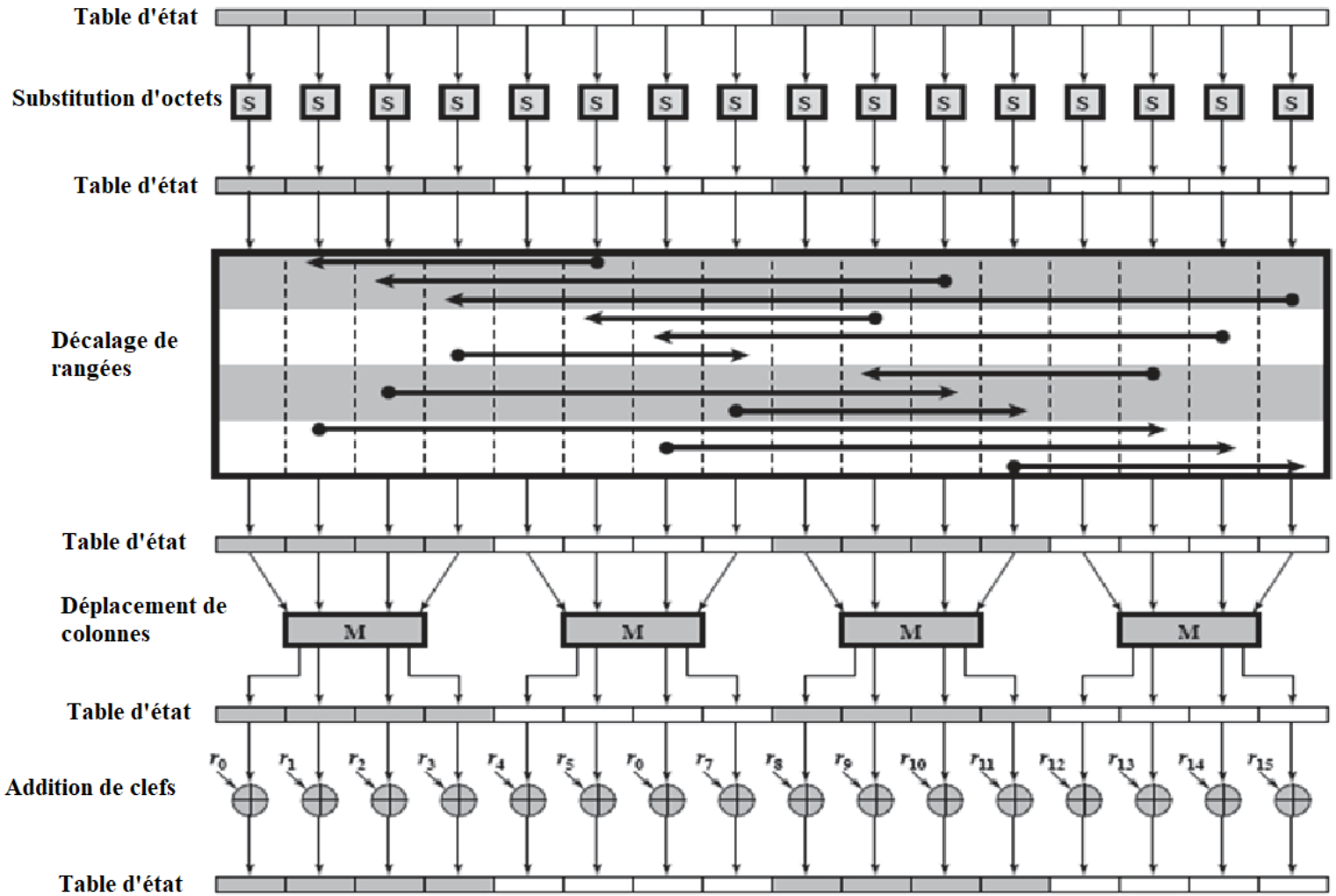


Figure: Schéma général AES

AES (5)

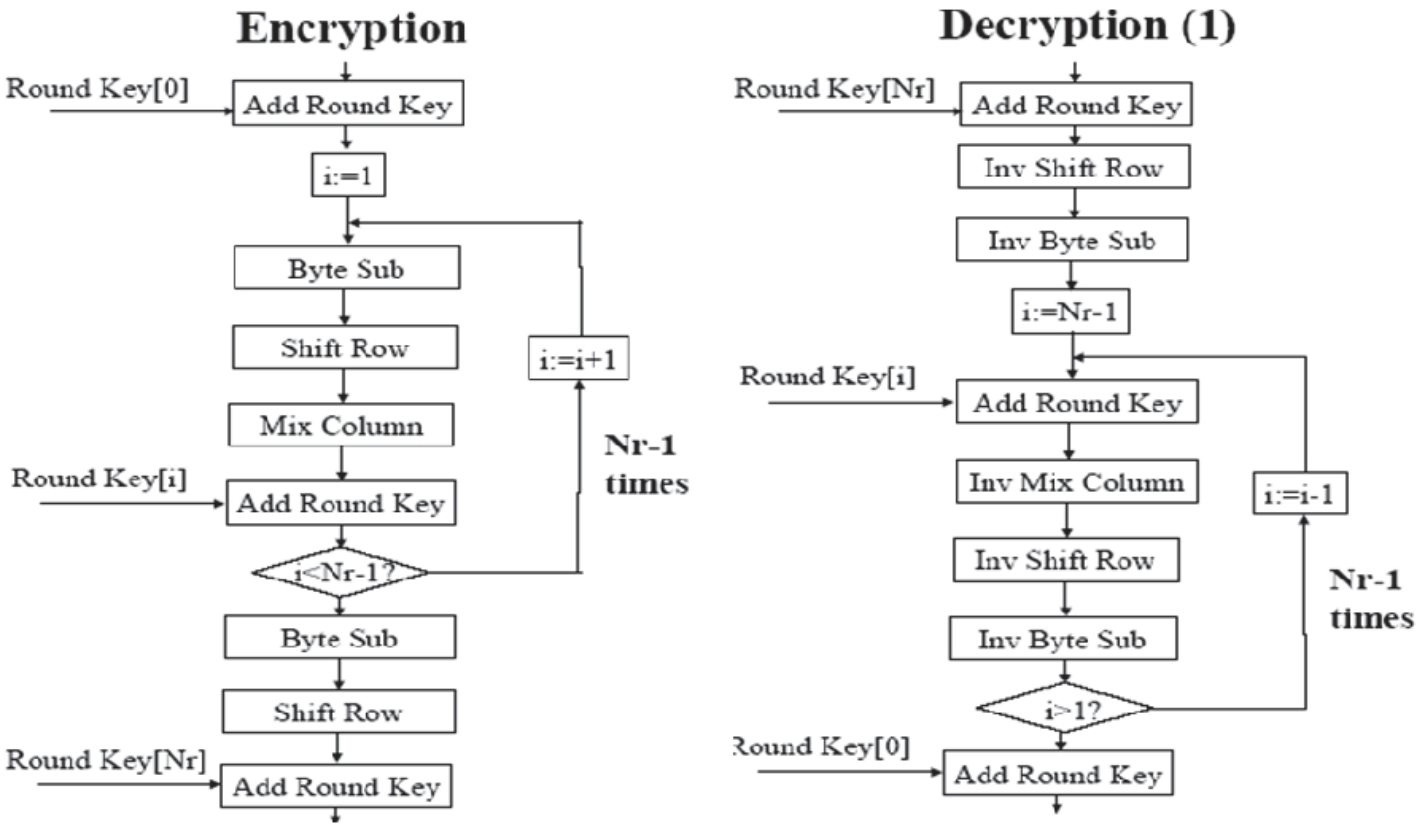


Figure: Chiffrement et Déchiffrement AES

AES (6)

Les principaux avantages sont :

- Des performances très élevées,
- Possibilité de réalisation en "Smart Card" avec peu de code,
- Possibilité de parallélisme,
- Ne comprend pas d'opérations arithmétiques : ce sont uniquement des décalages et des XOR ($\oplus$),
- N'utilise pas de composants d'autres cryptosystèmes,
- Nombre de rondes peut facilement être augmenté si c'est requis,
- Ne possède pas de clés faibles,

AES (7)

Inconvénients et limites :

- Le code et les tables sont différents pour le chiffrement et déchiffrement,
- Le déchiffrement est plus difficile à implanter en "Smart Card",
- Dans une réalisation matérielle, il y a peu de réutilisation des circuits de chiffrement pour effectuer le déchiffrement.

Attaques sur les cryptosystèmes symétriques

Une attaque sur un crypto-système vise à récupérer la clé utilisé plutôt de décrypter seulement un text chiffré. On trouve deux approches principales d'attaques aux cryptosystèmes symétriques

1. **La cryptanalyse :** Ce type d'attaque exploite les caractéristiques de l'algorithme. Elle utilise aussi quelques caractéristique des textes claires et des exemples de paires, "texte claire"-"texte chiffré".
2. **La force-brute:** Cette méthode essaye tous les clés possibles sur une pièce de texte chiffré jusqu'à l'arrivée au text claire correspondant. En moyenne l'attaque, l'attaquant utilisant la moitie de tous les clés possibles pour réussir.

Le résultat de la succès d'une attaque à trouver la clé est catastrophique au système d'information. Dans ce cas de figure, tous les messages chiffrés avec cette clé seront compromis.

Critique des chiffrements symétriques

- L'inconvénient d'un système de chiffrement symétrique aussi sophistiqué soit-il est que la clé K doit être transmise entre l'émetteur et le récepteur. Or si les correspondants ont choisi de faire du chiffrement, c'est en général parce qu'ils considèrent que le réseau n'est pas sûr : comment transmettre alors la clé ? On peut imaginer un transport physique de la clé par des moyens différents (valise diplomatique, par exemple).
- La non-répudiation est importante; Considérons un couple d'utilisateurs A et B qui se partageant une clé K. L'utilisateur B peut fabriquer des messages et faire croire que A les lui a envoyés !
- Le nombre de clé aussi est un problème, pour N utilisateurs on a besoin de $N \times (N-1)$ clés. Pour communiquer avec un nouvel utilisateur, on a besoin, au préalable, de générer, d'échanger la clef K, et de conserver cette clef.