Programme du module sécurité I

Chapitre I : Introduction à la sécurité des données

- Vocabulaire de base
- Objectifs de la sécurité

Chapitre II : Un outil de base pour la sécurité ''La Cryptographie''

II-1)Concepts de base

- Principe de la cryptographie

II-2)Cryptographie classique

- Chiffrement par transposition
- Chiffrement par substitution
- Cryptanalyse de la cryptographie classique

II-3)Cryptographie moderne

- A clé secrète
- A clé publique

Chapitre III : Signature numérique et Fonctions de hachage

Chapitre IV : La Gestion des

Chapitre V : Stéganographie et Tatouage numérique

Références bibliographiques :

005.8/01 ----------005.8/30

Chapitre I : Introduction à la sécurité

I-1) Introduction

De nos jours, la sécurité informatique est devenue un problème majeur dans la gestion des systèmes informatiques, en effet, ces derniers connaissent une grande évolution sur les plans d'échange d'informations et ouverture sur le monde extérieur. Les systèmes informatiques sont donc de plus en plus accessibles depuis des machines de moins en moins contrôlées.

La sécurité à pour objectifs la protection des données et des ressources en mettant en place des mécanismes de contrôle permettant d'assurer le bon fonctionnement du système informatique.

I-2) Vocabulaire de base

a) **sûreté :** protection contre les actions non intentionnelles
b) **sécurité** : protection contre les actions intentionnelles malveillantes

c) **Menace :** Événement, d'origine accidentelle ou délibérée, capable s'il se réalise de causer un dommage à un système donné.

d) **Vulnérabilité** : Une vulnérabilité est une faiblesse dans le système qui peut être exploitée par une menace.

e) **Risque** : Association d'une menace aux vulnérabilités qui permettent sa réalisation.

f) **Attaques** : elles représentent les moyens d'exploiter une vulnérabilité. Il peut y avoir plusieurs attaques pour une même vulnérabilités.

g) **Politiques de sécurité**
- Définition des autorités et des ressources
- Organisation, règles d'usage
- Spécification des droits

h) **Mécanismes de sécurité**
- Moyens pour la mise en œuvre d'une politique
- Exemple : protection physique, authentification par mot de passe, chiffrement, listes d'accès.

Exemple

I-3) Objectifs de la sécurité

La sécurité d'un système informatique à pour mission la protection des informations contre toutes divulgation, altération ou destruction. L'accès à ces informations doit être également protégé par un accès protégé.

a. **Intimité et Confidentialité** : empêcher la divulgation d'informations à des entités(sites, organisations, personnes, etc.) non habilitées à les connaître.

b. **Authentification :**
   D'une information : prouver qu'une information provient de la source annoncée (auteur, émetteur).
   D'une personne (ou groupe ou organisation) : prouver que l'identité est bien celle annoncée.

c. **Intégrité des informations :** Assurer que les informations n'ont pas été altérées par des personnes non autorisées ou inconnues.

d. **Signature :** Le moyen de lier l'information à une entité.

e. **Validation :** Les moyens de fournir l'autorisation d'utiliser ou de manipuler des informations.

f. **Contrôle d'accès :** Limiter l'accès des ressources aux personnes privilégiées.

g. **Certification :** L'approbations de l'information par une entité de confiance.

h. **Réception :** Approuver la réception de l'information.

i. **Anonymat :** Cacher l'identité d'une entité impliquée dans un processus.

j. **Non-répudiation :** Empêcher le démenti(nier) d'engagements ou d'actions précédentes.

I-4) Menaces sur les systèmes informatiques

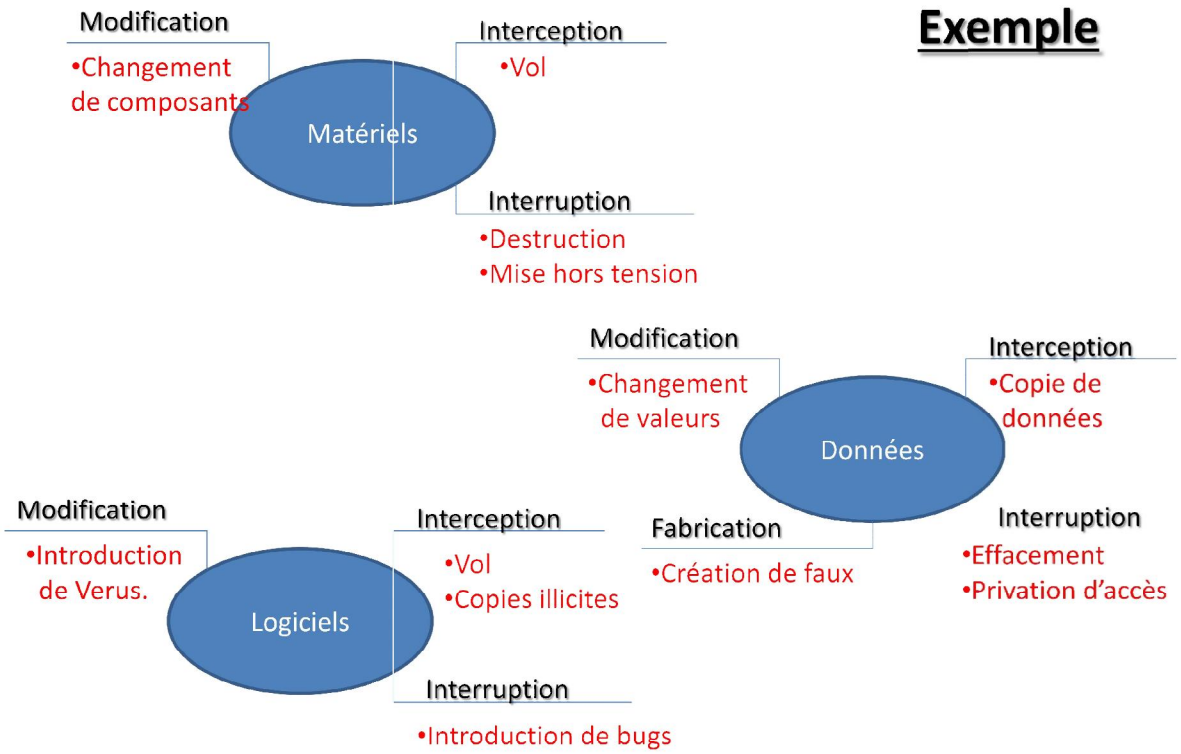
Dans un système informatique les menaces peuvent toucher les composants matériels, logiciels ou informationnels. Il existe principalement deux types de menaces :

1. Les menaces non intentionnelles (accidentelles)
2. Les menaces intentionnelles :
   - passives
   - actives

Les menaces accidentelles ne supposent aucune préméditation. Dans cette catégorie, sont repris les bugs logiciels, les pannes matérielles, et autres défaillances "incontrôlables".

Les menaces intentionnelles quant à elles, reposent sur l'action d'un tiers désirant s'introduire et relever des informations.
Dans le cas d'une ***attaque passive***, l'intrus va tenter de dérober les informations par audit ou intrusion, ce qui rend sa détection relativement difficile. En effet, ses actions ne modifient pas les fichiers, ni n'altère le système.
Dans le cas d'une ***attaque active***, la détection est facilitée, mais il peut être déjà trop tard lorsque celle-ci a eu lieu. Ici, l'intrus aura volontairement modifié les fichiers ou le système pour s'en emparer.

Les menaces actives peuvent être des interceptions, des interruptions, fabrication ou des modifications.



Menaces liées aux échanges d'informations

Les entreprises informatisées nécessitent un réseau sécurisé pour le transfert de leurs données, que ce soit entre les machines de cette entreprise, ou avec des machines externes, distantes de plusieurs milliers de kilomètres.

A l'origine, c'est Shannon qui, en 1948 puis en 1949 avec Weaver, a défini les bases d'une transmission de données entre deux parties. Son idée est illustrée à la **figure 1.1**.

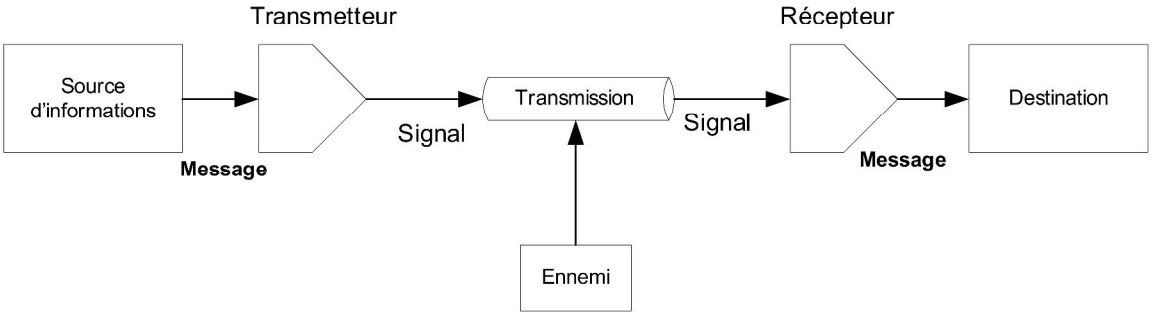


Figure 1.1 : Schéma de transmission de données de shannon

Dans une communication on trouve quatre catégories de menaces intentionnelles :
(illustrées à la figure I.2 dans le cas d'une communication entre deux entités **A** et **B**) :

– Interruption = problème lié à la disponibilité des données
– Interception = problème lié à la confidentialité des données
– Modification = problème lié à l'intégrité des données
– Fabrication = problème lié à l'authenticité des données

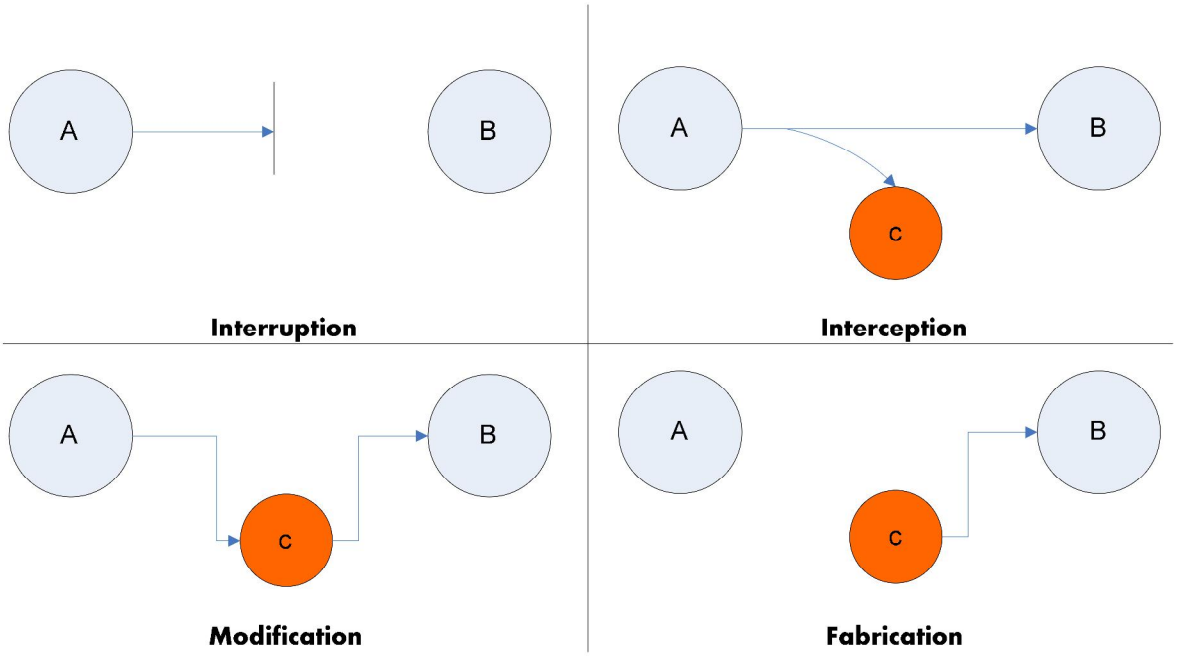


Figure 1-2 : Menaces intentionnelles

Chapitre II

Un outil de base pour la sécurité des données ''La Cryptographie''

II-1) Concepts de base

A) Définition

La *cryptographie* est la science qui utilise les mathématiques pour chiffrer et déchiffrer des données. La cryptographie permet la protection des données stockées ou transmises, à travers des réseaux non sûrs (comme Internet), de telle sorte qu'elles ne puissent être lues par personne à l'exception des destinataires convenus.

« « (cryptographie = "écriture cachée")» »

Le but fondamental de la cryptographie est de respecter adéquatement les quatre objectifs majeurs de la sécurité suivants:

la confidentialité,
l'intégrité des données,
l'authentification,
la non-répudiation.

B) Terminologie

- **communication :** la communication est l'action d'échanger quelque chose entre deux ou plusieurs personnes.
- **Message** : texte en claire compréhensible par l'expéditeur et le destinataire.
- **Chiffrement :**(encryption) : le processus de transformation d'un message de telle manière à le rendre incompréhensible.
- **Texte chiffré :** (cryptogramme) : résultat de l'opération de chiffrement.
- **Déchiffrement** :(décryptage) : processus de reconstruction du texte en clair à partir du texte chiffré.

- **cryptographie :** L'art et la science de garder le secret des messages, pratiquée par des ***Cryptographes***.

- **Cryptanalyse :** L'art de décrypter des messages chiffrés, pratiquée par des ***Cryptanalystes***.

- **Cryptologie :** La branche des mathématiques qui traite de la Cryptographie et de la cryptanalyse, ses pratiquants sont appelés ***cryptologues***.

- **Cryptosystème :** Un algorithme cryptographique, plus toutes les clés possibles et tous les protocoles qui le font fonctionner.

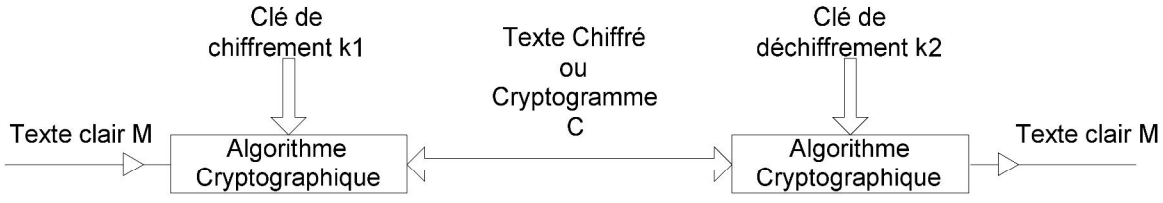
C- Principe de la cryptographie

Transformation des messages à l'aide d'informations gardées secrètes (les clés de chiffrement).

Modèle mathématique :

Un cryptosystème est un 5-uple $\{\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}\}$ ayant les propriétés suivantes :

1- $\mathcal{P}$ ensemble appelé l'espace des messages en clair. Un élément de $\mathcal{P}$ s'appelle un message en clair.
2- $\mathcal{C}$ est un ensemble appelé espace des messages chiffrés. Un élément de $\mathcal{C}$ s'appelle un message chiffré ou bien encore un cryptogramme.
3- $\mathcal{K}$ est un ensemble appelé espace des clés ; ses éléments sont les clés de chiffrement.
4- $\mathcal{E} = \{ E_K : k \in \mathcal{K} \}$ est une famille de fonctions $E_K : \mathcal{P} \rightarrow \mathcal{C}$;ses éléments sont les fonctions de chiffrement.
5- $\mathcal{D} = \{ D_K : k \in \mathcal{K} \}$ est une famille de fonctions $D_K : \mathcal{C} \rightarrow \mathcal{P}$;ses éléments sont les fonctions de déchiffrement.
6- A chaque clé k1 $\in \mathcal{K}$ est associé une clé k2 $\in \mathcal{K}$ telle que $D_{k2}(E_{k1}(M))=M$ pour tout message M $\in \mathcal{P}$.



Exemple

Déchiffer le message suivant :
« CPOKPVS MF NPOEF »
Indice n°1 : les espaces restent des espaces
Indice n°2 : l'alphabet a été décalé
Clé : chaque lettre a été décalée d'un rang

Modèle mathématique

Nous identifions les lettres par des chiffres pour permettre le calcul.

II-2)La cryptographie classique

II-2-1) Chiffrement par transposition

Lors d'un chiffrement par transposition, seul l'ordre des lettres du texte en clair est modifié, les lettres elles-mêmes n'étant pas remplacées par d'autres lettres ou d'autres symboles.

Le système de **transposition le plus simple** consiste à écrire le message en sens inverse.

Ainsi, le message MASTER devient RETSAM .
Naturellement, ce système échoue dès que l'on chercher à chiffrer un palindrome ''RADAR'' .

a) Transposition par blocs

On écrit le message en clair dans un tableau de dimension prédéfinie, avant de relever le texte chiffré en le lisant selon un procédé convenu

Exemple: écriture du texte dans des blocs de 3*3 en ligne.

JE SUIS INFORMATICIEN

J	E		N	F	O	I	E	N
S	U	I	R	M	A			
S		I	T	I	C			

Lecture par colonne pour avoir le texte chiffré.

Déchiffrement :

Cheminement inverse pour reconstruire le message clair

b) Transposition avec clé simple

Un mot clé est utilisé pour définir une clé numérique.

Cette clé est obtenue en numérotant les lettres du mot clé selon l'ordre de leur apparition dans l'alphabet.

Le message est alors chiffré en l'écrivant dans un tableau dont le nombre de colonnes coïncide avec le nombre de lettres du mot clé et en recopiant ses colonnes dans l'ordre de la clé numérique.

Clé= MASTER

Texte : JE SUIS INFORMATICIEN

M	A	S	T	E	R
3	1	5	6	2	4
J	E		S	U	I
S		I	N	F	O
R	M	A	T	I	C
I	E	N			

Résultat :

Déchiffrement :

Cheminement inverse pour reconstruire le message clair

II-2-2) Chiffrement par substitution

a) chiffrement de César

Chiffrement : chaque lettre du texte en clair est remplacée par la lettre située **n** rangs plus loin dans l'alphabet.

Déchiffrement : s'effectue en remplaçant les lettres du texte crypté par celles situées **n** rangs avant dans l'alphabet.

Pour un code décalé de ***trois positions***, le chiffrement est donc le suivant :

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
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

Le même tableau sert au chiffrement et au déchiffrement.

b) Masque Jetable (one-time pad)

L'algorithme est simple: on ajoute le rang de la lettre à chiffrer au rang de la lettre correspondante du masque, le résultat mod 26 donne le rang de la lettre chiffrée. Le destinataire dispose d'un bloc identique et utilise le masque de la même manière pour déchiffrer chaque lettre du message chiffré. Le masque est utilisé une seule fois, pour un seul message.

M a s q u e j e t a b l e Texte

T b f r g f a r f m i l k Masque

Chiffré

Pour le déchiffrement : On soustrait le rang de la lettre à déchiffrer au rang de la lettre correspondante du masque, le résultat mod 26.

c) Le chiffre de Hill (Lester S. Hill, 1891-1961)

Ce cryptosystème, proposé en 1929, est un chiffre polygraphique : le texte n'est pas chiffré lettre par lettre, mais par groupes de lettres. On désigne par 2-chiffre de Hill, le chiffre obtenu en codant les lettres par blocs de deux, par 3-chiffre de Hill celui obtenu en codant les lettres par blocs de trois, et ainsi de suite.

Dans une première phase, chaque lettre du texte à chiffrer est remplacée par une valeur numérique, celle de son rang dans l'alphabet :

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
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	0

Les valeurs numériques des lettres du texte en clair sont ensuite codées par blocs de deux, en leur substituant les valeurs obtenues par le procédé suivant :

• On choisit une matrice A **, régulière**, de format 2x2 et à **coefficients dans Z_{26}** .

Cette matrice va constituer la clé de chiffrement.

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

• On code chaque paire de lettres du texte en clair *p1p2* à l'aide du produit

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \end{pmatrix} = \begin{pmatrix} ap_1 + bp_2 \\ cp_1 + dp_2 \end{pmatrix}$$ (on travaille modulo 26)

(Si le nombre de lettres du texte en clair est impair, on ajoute une lettre supplémentaire choisie arbitrairement, la lettre x par exemple)

• On convertit les résultats obtenus en caractères alphabétiques.

- Pour déchiffrer un message codé, il suffit d'appliquer la même méthode, en utilisant la matrice inverse A^{-1} de A.

II-3) Cryptanalyse de la cryptographie classique

Objectif : Attaquer un système cryptographique, cassable (**vulnérable**).

Un cryptosystème est dit **vulnérable** s'il est possible de :

- Décrypter des messages sans connaître la clé.
- Encrypter des messages sans connaître la clé.
- Trouver la clé.

Remarque : L'étude de la sécurité des cryptosystèmes suppose l'existence de cryptanalystes ayant :

1. Suffisamment d'intelligence pour trouver les failles dans les cryptosystèmes lorsqu'elles existent.
2. Les ordinateurs les plus puissants pour monter leurs attaques.

✓ En d'autres termes, on raisonne toujours par rapport au pire cas.

II-3-1) Classification des attaques

Elles peuvent être classifiées selon les informations disponibles aux cryptanalystes.

Attaque à texte chiffré: l'analyste dispose de textes chiffrés *c1, …, cn* et cherche à trouver leurs correspondants en clair ;

Attaque à texte clair: l'analyste dispose de textes en clair *m1, ..., mn* et de leurs chiffrements *c1, ..., cn* respectifs et essaye de trouver la clé du cryptage ou de décrypter d'autres textes.

Attaque à texte clair choisi: L'analyste peut choisir des textes clairs et obtenir leurs textes chiffrés correspondants. En ayant ces connaissances, il essaye de trouver la clé du cryptage ou de décrypter d'autres textes.

Attaque à texte chiffré choisi : L'analyste peut choisir des textes chiffrés et obtenir leurs textes clairs correspondants. L'objectif est d'arriver à déchiffrer avec ses propres moyens.

II-3-2) Quelques techniques de cryptanalyse

a) Recherche exhaustive de la clé (Brute force attack)

Un système cryptographique manipule un ensemble fini de clés (espace de clés), Si l'espace de clés est petit alors un adversaire peut les essayer une par une jusqu'à ce qu'il trouve la bonne clé.

Limites

1-Temps de calcul

Question : Peut-on appliquer cette technique, par exemple, sur le chiffrement par substitution arbitraire ?

***Réponse* :**

C'est peut être trop pour un humain, mais est ce que c'est trop pour un ordinateur qui peut faire 3 milliard d'opérations par seconde 3ghz= $3x10^9$ ops ?

2-Choix de la clé

Supposons qu'on a des capacités infinies (des ordinateurs ultra puissants et que nous sommes éternel !)
Question: La recherche exhaustive nous permet-elle de casser n'importe quel cryptosystème qui utilise un nombre fini de clés.
Réponse: Pas du tout ! En effet, cette technique repose sur le fait que seule la bonne clé puisse déchiffrer un message crypté en un message qui a un sens.
Question: Qu'adviendra t-il si toutes les clés ou une grande partie d'entre elles donnent des textes qui ont un sens? Laquelle de ces clés est la bonne clé ?

Exemple : Le message crypté avec le chiffrement par décalage est C = WNAJW.
K=5 DK(C)=
K=22 DK(C)=

b) Attaque par dictionnaire

L'attaque par dictionnaire est une méthode utilisée en cryptanalyse pour trouver un mot de passe ou une clé. Elle consiste à tester une série de mots de passe potentiels, les uns à la suite des autres, en espérant que le mot de passe utilisé pour le chiffrement soit contenu dans le dictionnaire. Si ce n'est pas le cas, l'attaque échouera.

Cette méthode repose sur le fait que de nombreuses personnes utilisent des mots de passe courants (par ex : un prénom, une couleur, le nom d'un animal…).

L'attaque par dictionnaire est une méthode souvent utilisée en complément de l'attaque par force brute.

c) Cryptanalyse par analyse des fréquences

Un des moyens les plus simples pour chiffrer un message est de remplacer chaque lettre par une autre (ou un autre symbole). Par sa simplicité et par sa force, ce système a dominé la technique des écritures secrètes pendant tout le premier millénaire. Il a résisté aux cryptanalystes jusqu'à ce que le savant arabe ***Abu Yusuf Ya'qub ibn Is-haq ibn as-Sabbah Oòmran ibn Ismaïl al-Kindi*** mette au point, au IXème siècle, une technique appelée analyse des fréquences.

Principe

- Établir la fréquence de chaque lettre de l'alphabet. En français la lettre la plus fréquente est «e» suivie par «a» puis par «i», etc
- Examiner les fréquences des caractères dans le texte chiffré.
- Remplacer les caractères les plus fréquents du texte chiffré par les caractères les plus fréquents du langage.
- Si par exemple la lettre la plus fréquente du texte chiffré est «j», suivie par «m», suivi par «k», alors on fait un premier essai en remplaçant «j» par «e», «m» par «a» et «k» par «i».

	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
Fran	9,	1,	2,	3,	15,	0,	1,0	0,7	8,4	0,8	0,0	5,3	3,2	7,1	5,1	2,8	1,0	6,4	7,9	7,2	6,2	2,1	0,0	0,3	0,2	0,3

çais	42	02	64	39	87	95	4	7	1	9	0	4	4	5	4	6	6	6	0	6	4	5	0	0	4	2
Anglais	8.08	1.67	3.18	3.99	12.56	2.17	1.80	5.27	7.24	0.14	0.63	4.04	2.60	7.38	7.47	1.91	0.09	6.42	6.59	9.15	2.79	1.00	1,89	0,21	1,65	0,07

Ce qui nous donne l'ordre suivant.

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

On peut aussi analyser la fréquence des ***bigrammes*** dans un texte, c'est-à-dire la fréquence des groupes de deux lettres. Cela amènera des indices importants pour décrypter un texte chiffré car on sait que l'on ne pourra pas trouver des ***bigrammes*** tels que *XK* ou *WX* dans le texte clair.

Les 20 bigrammes les plus fréquents en français																			
Bigrammes	ES	DE	LE	EN	RE	NT	ON	ER	TE	EL	AN	SE	ET	LA	AI	IT	ME	OU	EM	IE

On peut aussi analyser la fréquence des ***trigrammes*** dans un texte, c'est-à-dire la fréquence des groupes de trois lettres.

Les 20 trigrammes les plus fréquents en français																			
Trigrammes	ENT	LES	EDE	DES	QUE	AIT	LLE	SDE	ION	EME	ELA	RES	MEN	ESE	DEL	ANT	TIO	PAR	ESD	TDE

Limites

1. Cette technique ne fonctionne bien que si le cryptogramme est suffisamment long pour avoir des moyennes significatives.
2. Cependant, il existe également des cas où cette analyse ne fonctionne pas, comme le montre l'exemple ci-dessous.

De Zanzibar à la Zambie et au Zaïre, des zones d'ozone font courir les zèbres en zigzags zinzins.

Exemple :

Déchiffrer le texte suivant, sachant qu'il est chiffré par décalage.

WMZSX VIGSI YVIWX YRIVS WIZSX VIFSY GLIHM VEHIW QSXWT EVJYQ IW

II-4) Cryptographie moderne

La cryptographie s'est littéralement transformée avec l'émergence des ordinateurs. L'automatisation des calculs de plus en plus complexe a permis à la cryptologie de jouer un rôle très important à partir de la seconde guerre mondiale. La cryptographie moderne manipule des informations numériques (Bits) qui peuvent être : des Fichiers, voix numérique, vidéo numérique…etc .

On distingue deux grands types d'algorithmes de chiffrement moderne, les algorithmes à **clé secrète** et les algorithmes **à clé publique**. Chacune de ces deux classes possède ses propres avantages et inconvénients.

Les systèmes à clé secrète nécessitent le partage d'un secret entre les interlocuteurs.

La découverte en 1976 des systèmes à clé publique a permis de s'affranchir de cette contrainte, mais elle n'a pas pour-autant apporté de solution parfaite, dans la mesure où tous les algorithmes de chiffrement à clé publique, de par leur lenteur, ne permettent pas le chiffrement en ligne. Dans la plupart des applications actuelles, la meilleure solution consiste à utiliser un système hybride, qui combine les deux types d'algorithmes.

II-4-1) Chiffrement à clé secrète

Les algorithmes de chiffrement à clef secrète (ou symétriques ou encore conventionnels) sont ceux pour lesquels émetteur et destinataire partagent une même clef secrète (autrement dit, les clefs de chiffrement et de déchiffrement sont identiques. L'emploi d'un algorithme à clef secrète lors d'une communication nécessite donc l'échange préalable d'un secret entre les communicants.

Propriétés :

- Les clés sont identiques : $K_E = K_D = K$,
- La clé doit rester secrète,
- 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.

La cryptographie à clé secrète peut se classer en deux catégories :

1-Système de chiffrement par flot (de flux ou par stream).
2- Système de chiffrement par blocs.

Les schémas de chiffrement par flot, traitent l'information bit(ou caractère) par bit(ou caractère) , et sont très rapides.
Ils peuvent être traités avec une mémoire limitée et la propagation des erreurs de transmission du chiffré au clair est limitée. Ils opèrent sur les symboles du clair par une transformation dépendant de la clé et de la position du symbole dans le flot de données. Le chiffrement par Stream repose sur un générateur de clés qui produit une séquence de clés k1, k2, ..., ki. Ce type de chiffrement est parfaitement adapté aux systèmes disposant de moyens de calcul, de mémoire et de transmission limités (cryptographie en temps réel), comme la cryptographie militaire, ou la cryptographie entre le téléphone portable GSM et son réseau.

Les schémas par blocs sont plus lents et nécessitent plus de moyens informatiques que les schémas par flots. Mais ils sont bien adaptés à la cryptographie civile comme celle des banques.
Dans un système par blocs, chaque clair est découpé en blocs de même longueur et chiffré bloc par bloc.

L'idée générale du chiffrement par blocs est la suivante :

1. Remplacer les caractères par un code binaire.
2. Découper cette chaîne en blocs de longueur donnée.
3. Chiffrer un bloc en ''l'additionnant" bit par bit à une clé.
4. Déplacer certains bits du bloc.
5. Recommencer éventuellement un certain nombre de fois l'opération 3.
6. Passer au bloc suivant et retourner au point 3 jusqu'à ce que tout le message soit chiffré.

RC4, un système de chiffrement par flot

RC4 a été conçu par *Ronald Rivest* de RSA Security en 1987. Officiellement nommé **Rivest Cipher 4**, l'acronyme **RC** est aussi surnommé **R**on's **C**ode comme dans le cas de RC2, RC5 et RC6. Il s'agit probablement du chiffrement par flots le plus utilisé. On le retrouve notamment dans le standard SSL/TLS, dans Oracle Secure SQL, ou encore dans le protocole WEP (Wired Equivalent Privacy, de la norme 802.11). Ce dernier fut remplacé par le WPA (Wi-Fi Protected Access), mais celui-ci utilise toujours le RC4.

Fonctionnement du RC4

Cet algorithme fonctionne sur les octets. Ainsi, la clé (**K**), de longueur variable, peut avoir une taille comprise entre 1 et 256 octets (de 8 à 2048 bits). La clé RC4 permet d'initialiser un tableau (T) de 256 octets en répétant la clé autant de fois que nécessaire pour remplir le tableau. Par la suite, des opérations très simples sont effectuées : les octets sont déplacés dans le tableau, des additions sont effectuées, etc.

Le but est de mélanger autant que possible le tableau.

- **Initialisation**

Initialement, les cellules de **S** reçoivent une valeur égale à leur position (i.e., S[0]=0, S[1]=1, ...) Un vecteur temporaire de longueur T (de longueur égale à S) est également créé destiné à recevoir la clé. Si la longueur de la clé K est égale à 256 octets, K est simplement transféré dans T. Si K est inférieur à 256 octets, il est recopié dans T jusqu'à atteindre la taille de T. La figure 3 illustre cette étape d'initialisation.

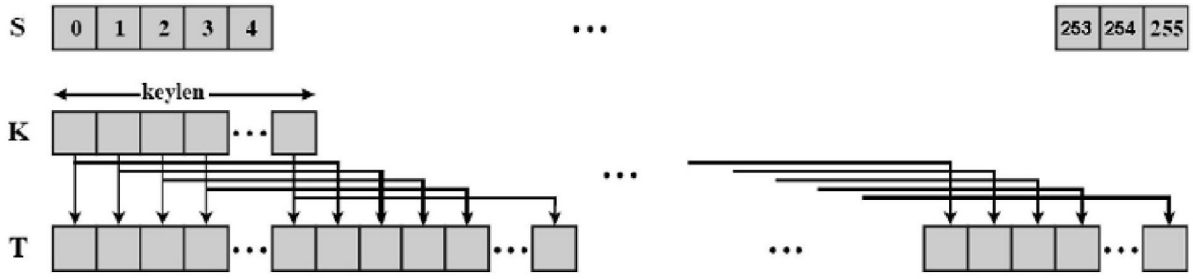


Figure 3 : Initialisation RC4

Le vecteur temporaire T est ensuite utilisé pour produire la permutation initiale de S. Pour chaque cellule S[i] de S, celle-ci sera échangée avec une autre cellule de S selon un calcul basé sur la valeur comprise dans la cellule T[i] correspondante.

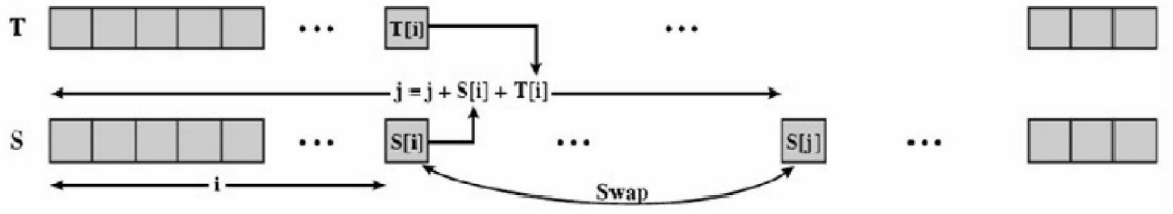


Figure 4 : Permutation Initiale dans RC4

- **Génération du flux de chiffrement**

A partir de cet instant, la clé d'entrée n'est plus utilisée. Pour chaque S[i], on procèdera à un échange avec un autre octet de S, selon un schéma basé sur la configuration courante de S. Une fois arrivé à S[255], le processus redémarre à la cellule S[0] (on parle de PRGA pour Pseudo-Random Generation Algorithm). La figure 5 présente la procédure :

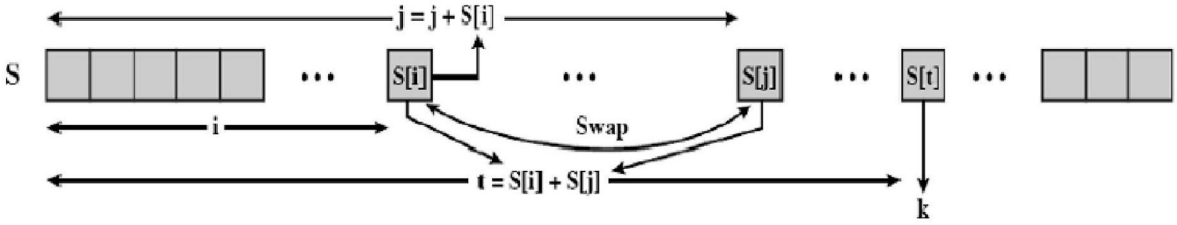


Figure 5 : Flux de chiffrement dans RC4

La valeur de k est alors utilisée pour le chiffrement par une opération XOR avec le prochain octet de texte clair, ou pour le déchiffrement par une opération XOR avec le prochain octet de texte chiffré.

- **Robustesse du RC4**

On peut tout d'abord remarquer que la sécurité repose uniquement sur la clé. En effet, c'est elle, et uniquement elle, qui détermine le flux de sortie du générateur.

En 2001, une découverte affaiblit l'aspect sécuritaire du RC4. Fluhrer, Mantin et Shamir remarquèrent que les **premiers octets** en sortie du RC4 n'étaient pas tout à fait aléatoires. De fait, il semblerait que ces quelques premiers Octets divulgueraient des informations importantes sur la clé d'initialisation. Le protocole WEP a été remplacé par le protocole WPA pour pallier les problèmes rencontrés avec la gestion des clés dans le RC4.

DES (Data Encryption Standard), un système de chiffrement par blocs

Ce système de chiffrement à clé privée par blocs est le plus connu. Il a été adopté comme standard américain en 1977 (standard FIPS 46) pour les communications commerciales, puis par l'ANSI (American National Standards Institute)en 1991.

- **Algorithme général**

Ce système fonctionne par blocs de 64 bits en utilisant une clé de 56 bits(la clé compte 64 bits dont 8 bits pour le contrôle de parité). A partir de la clé initiale on génère 16 sous clés de taille 48 bits chacune.

L'algorithme se déroule en trois étapes :

Entrée : Bloc de 64 bits ; K : clé de 64 bits

1-Soit p un bloc de texte de 64 bits. On lui applique une permutation initiales IP() fixée pour obtenir une chaine initiale notée P_0. On a donc :

$P_0=IP(p)=L_0.R_0$

Où L_0 sont les 32 premiers bits de P_0 et R_0 les 32 bits restants ;

2- Appliquer seize itérations (ou tours) d'une certaine fonction ***f***. On calcule L_i et R_i , $1<=i<=16$ suivant les règles :

$L_i=R_{i-1}$

$R_i=L_{i-1} \oplus f(R_{i-1},K_i)$ // les K_i sont obtenues à partir de la clé initiale K

3- L'inverse de IP (noté IP^{-1}) est appliqué au dernier bloc de la dernière itération (tour) $R_{16}||L_{16}$ pour obtenir le texte chiffré C ;

$\mathbf{C=IP^{-1}(R_{16}L_{16})}$ // noter l'inversement dans l'ordre de L16 et de R16 au dernier tour.

L’algorithme est illustré par le schéma suivant :

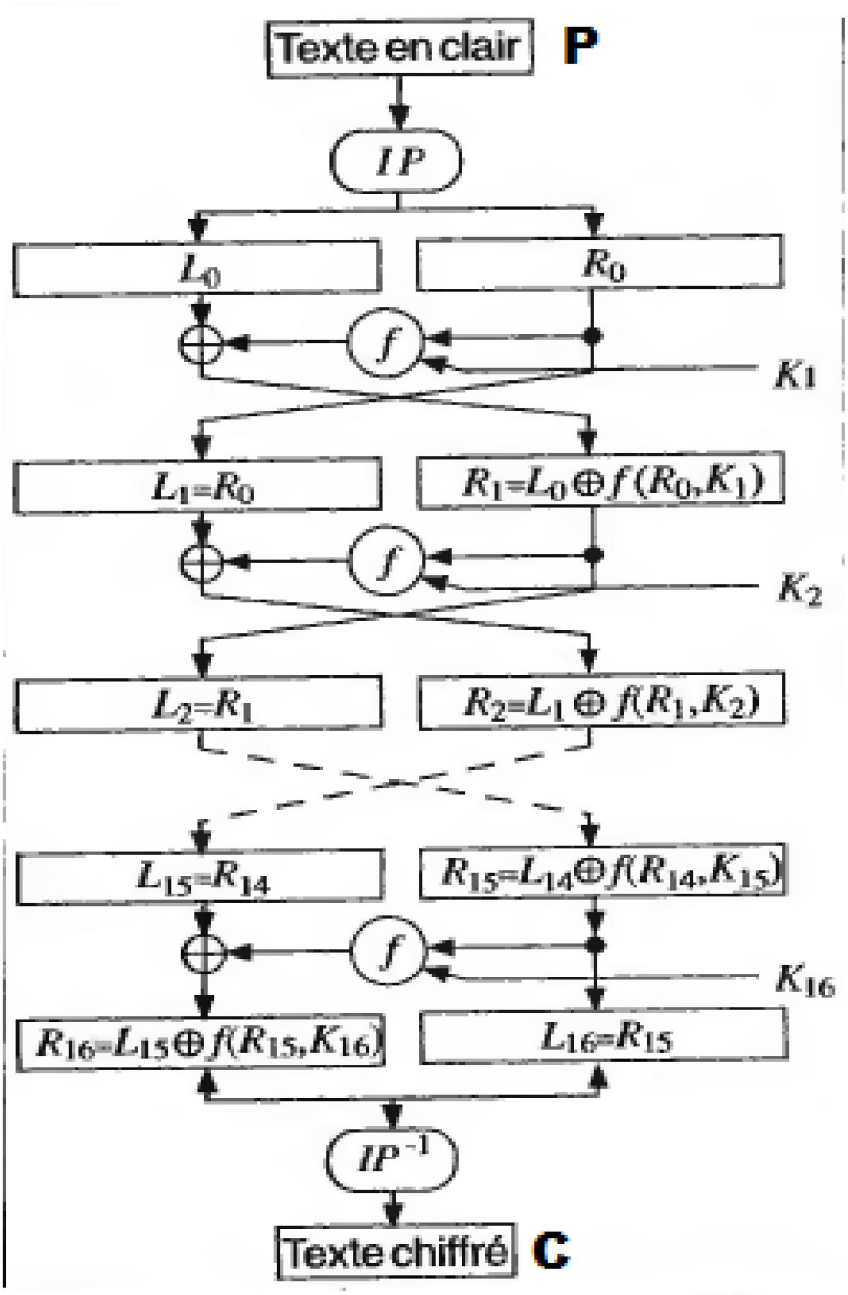


Figure 6 : Chiffrement DES

b)Les permutations IP et IP^{-1}

Elles opèrent sur l'ordre des bits du bloc Comme suite :

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	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Permutation initiale inverse

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

Figure7 : **IP()** **IP^{-1}()**

Les tableaux se lisent de gauche à droite et de haut en bas. Cela signifie que dans le calcul de IP(p), le bit 58 de du bloc p devient le premier, le bit 50 devient le deuxième …etc.
IP^{-1} est la matrice inverse de IP.

c) La fonction *f*

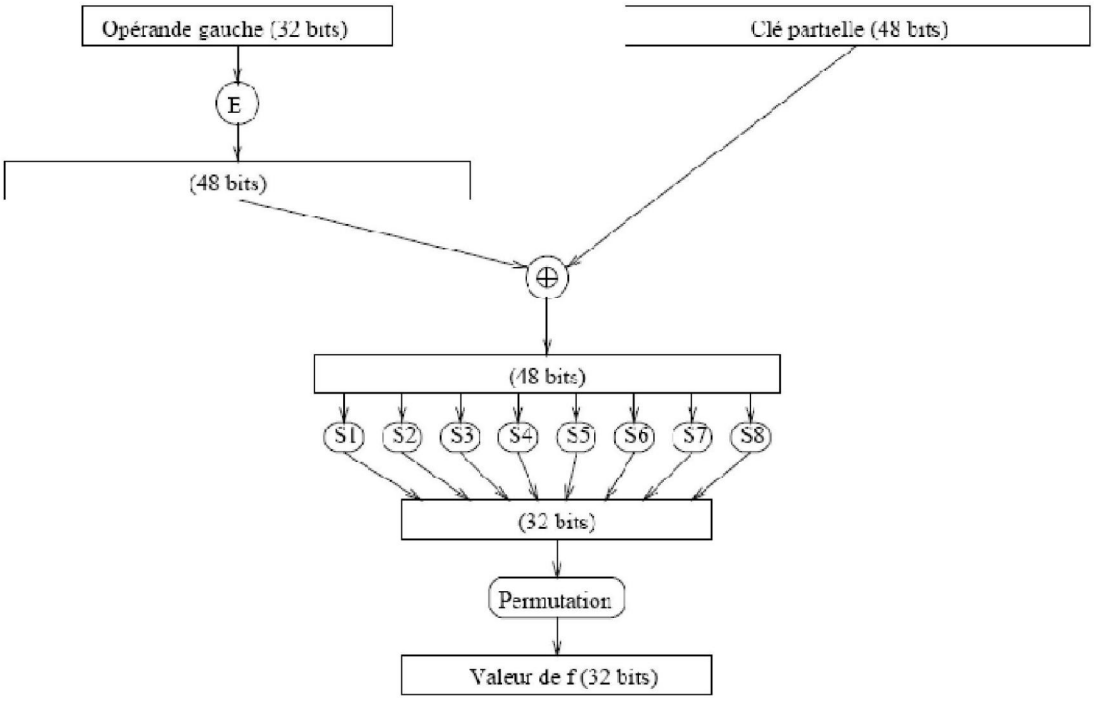


Figure 8 : Fonction *f*

Tout d'abord, l'argument de gauche qui possède 32 bits est expansé en 48 bits en redoublant certains bits (fonction E()). Cette expansion est précisée par la figure 9. Ensuite, on calcule le XOR de cet argument expansé avec le deuxième argument qui est la sous clé K_i (48 bits). Le résultat possède 48=8*6 bits est transformé en une chaine de 32 =8*4 bits en utilisant des dispositifs appelés boîtes-S qui calculent un bloc de 4 bits à partir d'un bloc de 6 bits. Enfin, on applique la permutation décrite par la figure9 à ces 32 bits pour obtenir le résultat final de ***f***

Fonction E d'expansion

32	1	2	3	4	5	4	5	6	7	8	9
8	9	10	11	12	13	12	13	14	15	16	17
16	17	18	19	20	21	20	21	22	23	24	25
24	25	26	27	28	29	28	29	30	31	32	1

Permutation P finale

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Figure 9 : Expansion, Permutation

d) Les Boites-S

DES utilise huit boîtes-S différentes. On les représente par des tableaux à 2 lignes et 16 colonnes. Les premiers et derniers bits de l'entrée déterminent une ligne du tableau, les autres bits déterminent une colonne. La valeur numérique trouvée à cet endroit indique la valeur des quatre bits de sortie.

S_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_5	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Figure 10 : Boites-S

e)Génération des sous clés K_i (diversification)

Le principe de diversification de la clé initiale K est schématisé par la figure 11.

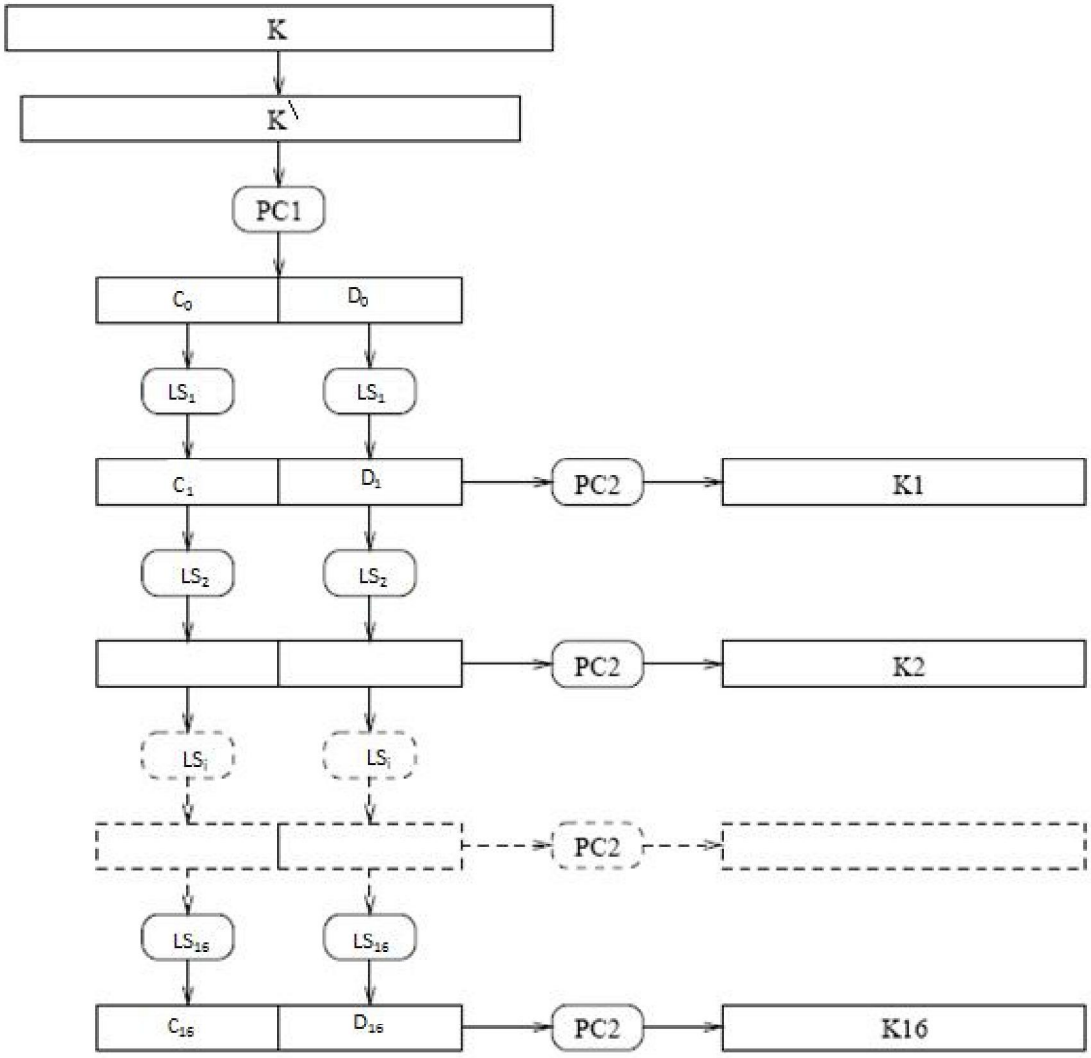


Figure 11 : Diversification de la Clé K

on applique d'abord une permutation PC1 à K. puis, à chacune des 16 étapes, chaque moitié de la chaine de 56 bits obtenue subit une rotation à gauche, d'un cran aux étapes 1,2,9,16 et de deux crans aux autres étapes. A chacune de ces étapes on obtient une clé partielle de 48 bits en appliquant la règle d'extraction PC2. La permutation PC1 et la règle PC2 sont détaillées par la figure 12. Les 56 bits de K y sont numérotés de 1 à 64 en évitant les multiples de 8, puisque dans la pratique, ces positions sont des bits de parité.

Permutation PC_1

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

Règle d'extraction PC_2

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Figure 12 : PC1 et PC2

AES, successeur de DES

Le **DES** opère sur des blocs de 64 bits et utilise une clef secrète de 56 bits. Il est donc désormais vulnérable aux attaques exhaustives. C'est pourquoi la plupart des applications l'utilisent maintenant sous la forme d'un triple DES à deux clefs, constitué de trois chiffrements DES successifs avec deux clefs secrètes. Cette technique permet de doubler la taille de la clef secrète (112 bits). Plus précisément, pour chiffrer avec le triple DES, on effectue d'abord un chiffrement DES paramétré par une première clef de 56 bits, puis un déchiffrement DES paramétré par une seconde clef, et à nouveau un chiffrement DES avec la première clef. Seules deux clefs sont utilisées dans la mesure où l'emploi de trois clefs secrètes différentes ne permet pas d'accroitre la sécurité de l'algorithme. Le triple DES à deux clefs a notamment été adopté dans les standards ANSI X9.17 et ISO 8732. Il est extrêmement utilisé pour les applications bancaires. Il a été remplacé en 2000 par l'AES (Advanced Encryption Standard), car sa clé de 56 bits était trop courte (et de longueur non modifiable!) pour assurer de nos jours une résistance suffisante à l'attaque exhaustive.