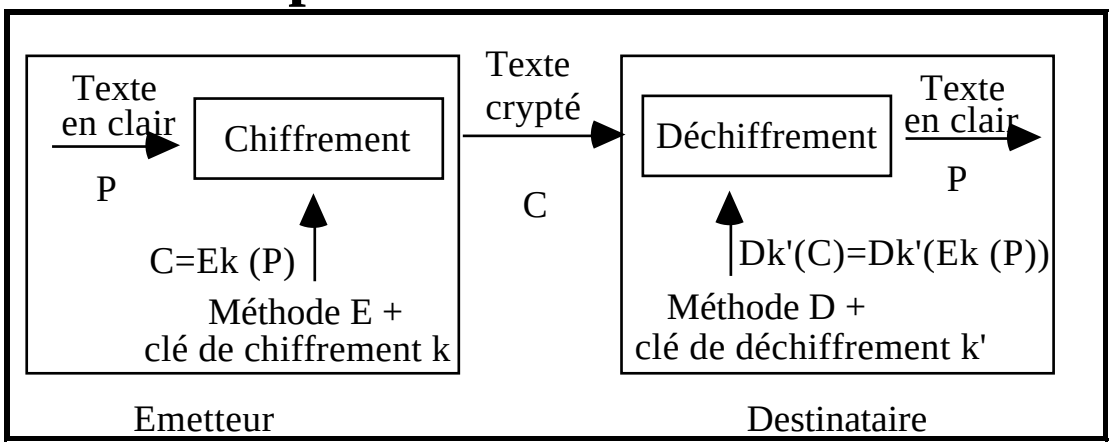
LES TECHNIQUES DE CRYPTOGRAPHIE

G Florin

Introduction

Chiffrement (cryptage) = Transformation d'un texte pour en cacher le sens

L'outil primordial de la sécurité



L'usage ancien du chiffre et l'usage actuel en informatique ont conduit aux contraintes suivantes:

- Réalisation rapide du codage et du décodage.
- La méthode de chiffrement est stable (on ne peut la changer que très rarement) Elle est publiquement connue.
- Elle dépend de paramètres secrets (clés de chiffrement ou de déchiffrement) qui doivent pouvoir être modifiés aisément et si possible fréquemment.

- C'est sur le secret des clés que doit reposer la sécurité de la méthode.

Différentes difficultés d'attaque d'une méthode de cryptage

Crypter ne se justifie que relativement à l'existence d'attaquants ou cryptanalystes dont le travail est plus ou moins difficile.

a) - L'attaque à textes chiffrés

On dispose seulement de textes chiffrés

b) - L'attaque à textes en clair connus

On dispose de quelques morceaux de texte en clair et de leur cryptage

c) - L'attaque à textes en clair choisis

On peut faire crypter ce que l'on veut par la méthode de cryptage et voir ce qu'elle produit

Remarque.

Une bonne méthode doit résister aux attaques de type c.

Plan de l'exposé
Les approches principales

Chapitre I

- Les chiffres à clés privées
  . Systèmes classiques de cryptographie
  . Chiffres symétriques

Chapitre II

- Les chiffres à clés publiques
  . Systèmes modernes de cryptographie
  . Chiffres asymétriques

Chapitre III

- Les signatures numériques
(fonctions de hachage à sens unique).

I
LA CRYPTOGRAPHIE CLASSIQUE (à clés privées)

Principe général

- La connaissance de la méthode et de la clé de chiffrement et celle de la méthode et de la clé de déchiffrement **se déduisent facilement l'une de l'autre**.

- Les deux méthodes et les clés sont connues de l'émetteur et du destinataire
=> **L'émetteur et le destinataire doivent se mettre préalablement d'accord** sur un secret (la clé) pour utiliser le chiffre**.**

Deux problèmes

- L'échange préalable à toute communication sécurisée d'un secret **("la distribution de clés)**

- Dans un réseau de N entités susceptibles de communiquer secrètement il faut distribuer **N*(N-1)/2 clés.**

Les méthodes de chiffrement par substitution

Principe général

A chaque lettre ou groupe de lettres on substitue une autre lettre ou un autre groupe de lettres.

La substitution simple (substitution mono alphabétique)

Pour chaque lettre de l'alphabet de base on se donne une autre lettre utilisée dans le texte chiffré.

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

Exemple historique: Le chiffre de César

On décale les lettres de 3 positions

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

Les techniques d'attaque statistique

- Analyse statistique des textes cryptés.

- Détermination des fréquences d'apparition des symboles

- Comparaison avec les fréquences types caractéristiques des langues

Fréquences d'apparition (en anglais)

Lettres	Digrammes	Trigrammes
E 13,05	TH 3,16	THE 4,72
T9,02	IN 1,54	ING 1,42

Une analyse statistique d'un texte suffisamment long permet de casser un code mono ou même poly-alphabétique

Le problème est de disposer:

- de puissance de calcul

- de suffisamment de texte en regard de la longueur des clés utilisées.

La substitution poly-alphabétique

- Une attaque est facile avec un seul alphabet.

- On utilise une suite de chiffres mono alphabétiques.

- La suite des chiffres mono alphabétiques est réutilisée périodiquement.

Exemple : le chiffre de Vigenere

On prend les 26 chiffres de César.

Les chiffres associés aux 26 décalages possibles sont représentés par une lettre.

Ex : chiffre avec décalage de k associé à la k iéme lettre de 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**
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 B**
C->

- On choisit une clé de répétition comme une suite de lettres: un mot ou une phrase ou un livre

- Cette clé répétée indéfiniment vis à vis de chaque lettre d'un texte à chiffrer sert à déterminer le chiffre à utiliser.

Autres substitutions

Les substitutions homophoniques

Au lieu d'associer un seul caractère crypté à un caractère en clair on dispose d'un ensemble de possibilités de substitution de caractères dans laquelle on choisit aléatoirement.

Les substitutions de polygrammes

Au lieu de substituer des caractères on substitue par exemple des digrammes (groupes de deux caractères)

- Au moyen d'une table
  (système de Playfair)
- Au moyen d'une transformation mathématique (système de Hill).

Les chiffres de substitution à longueur de clé égale à celle du texte (systèmes à clés jetables)

- Pour éviter les attaques statistique il faut utiliser une substitution qui rend le texte crypté non analysable statistiquement.

Exemple de solution:

- Générer une clé qui est **une suite binaire parfaitement aléatoire**
  Phénomène physique aléatoire
    Le bruit électro magnétique

- Pour chiffrer un message **faire le ou exclusif du message et de la clé**.

- **Si chaque clé ne sert qu'une fois le chiffre est incassable**.

Difficultés de la méthode

- **Volume des clés**
  Devant être connu aux deux bouts.

- **Problème de synchronisation**
  Si l'on perd une seule donnée on ne sait plus décrypter.

Les méthodes de chiffrement par transposition

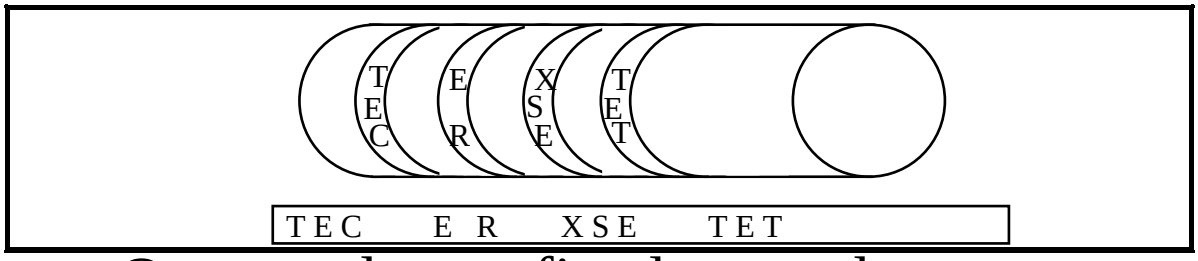
Principe général

On procède à un réarrangement de l'ensemble des caractères (une transposition) qui cache le sens initial.

La technique est très peu résistante aux attaques statistiques.

Exemple

Le plus souvent on utilise deux visions géométriquement différentes du texte.



- On enroule une fine langue de papyrus ou de peau sur un tambour d'un diamètre donné (technique assyrienne 400 av JC).

- On écrit horizontalement un texte sur la lamelle enroulée.

- Quand la lamelle est déroulée les lettres sont incompréhensibles.

- Pour décrypter le message il faut un cylindre du bon diamètre.

Exemple de transposition à base matricielle

- Le message en clair est écrit dans une matrice.

- La clé est la matrice.

- La technique de transposition de base consiste à lire la matrice en colonne.

Exemple (6,5):

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

Le message crypté est donc:

MEERSE TAESS NRSEAS AC P GRTO

Chiffre à transposition avec chiffre à substitution simple.

- On combine la transposition avec une substitution et on réarrange l'ordre des colonnes selon une permutation qui est ajoutée à la matrice pour former la clé.

Exemple d'ordre d'exploration des colonnes 1 6 4 3 2 5, le texte crypté est:

"MEERSGRTO SEAS SN NRE TAEAC P "

- On peut générer et mémoriser simplement des permutations en prenant une clé sous forme d'un mot qui ne comporte pas deux fois la même lettre

On numérote les colonnes dans l'ordre ou apparaissent les lettres du mot dans l'alphabet.

Exemple ESPOIR correspond à la permutation 1 6 4 3 2 5.

Le DES "Data Encryption Standard"

-Dès le début des années 1960 la technologie des circuits intégrés permet de travailler à des circuits combinatoires complexes permettant d'automatiser:

la méthode de substitution.

la méthode de transposition.

=> Idée d'appliquer ces techniques en cascade dans un produit de chiffres.

- Mise au point à partir de 1968 d'une méthode de cryptage basée sur 16 étages de substitutions et transpositions basés sur des clés (IBM)

- Appel d'offre NBS (1973) pour la mise au point d'un système de cryptographie

- Proposition IBM (1975)

- Adoption définitive et normalisation du DES d'IBM (1978) par le NBS ("National Bureau of Standards").

-Normalisation ANSI X3.92 connue sous le nom de DEA ("Data Encryption Algorithm").

Principes Généraux du DES

Choix possibles pour la sécurité

- Méthodes simples de chiffrement et des clés très longues .

Le DES

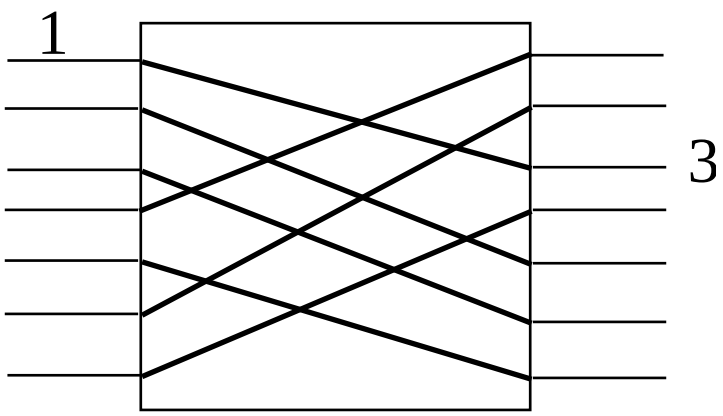
- Produit de transpositions et substitutions nombreuses et compliquées pour une clé relativement courte
  => facilité de transport.

- Les chiffres à substitution et à transposition sont faciles à réaliser en matériel.

Les boîtes de transposition
"P-Box"
Les boites de substitution
"S-Box"

Boîte de transposition (P - box "Permutation box")

Exemple pour 8 bits (solution matérielle)



Le bit 1 remplace le 3

Facile à réaliser par simple câblage
Autre solution (logicielle) par des tables

Exemple de transposition sur 64 bits

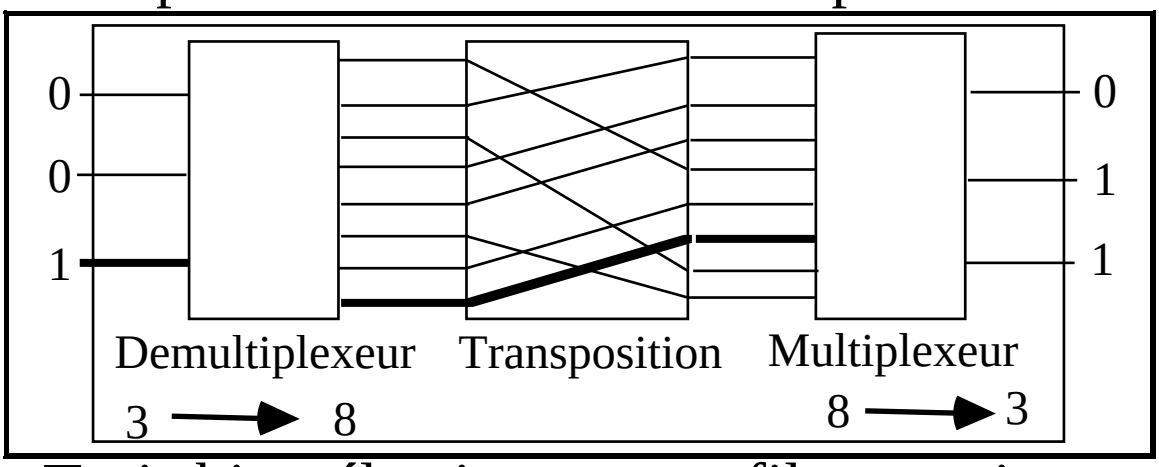
La permutation initiale du DES

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

Le bit 1 remplace le 58

Boîte de substitution (S - box)

Exemple de solution matérielle pour 3 bits



- Trois bits sélectionnent un fil en sortie
- L'ensemble subit une transposition.
- Le résultat est remultiplexé sur 3 bits

Solution par consultation de table

Pour une configuration d'entrée on sélectionne directement au moyen d'une table la configuration de sortie.

Exemple: Table S-1 du DES

Approche particulière on substitue à une valeur sur 6 bits une valeur sur 4 bits.

Les deux bits faible et fort sélectionnent la ligne, les 4 bits intermédiaires la colonne.

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

DES - Caractéristiques

Deux modes

- Mode cryptage par bloc de 64 bits
- Mode cryptage à la volée ("stream") (octets par octets avec des registres à décalage)

Utilisation d'une clé sur 56 bits

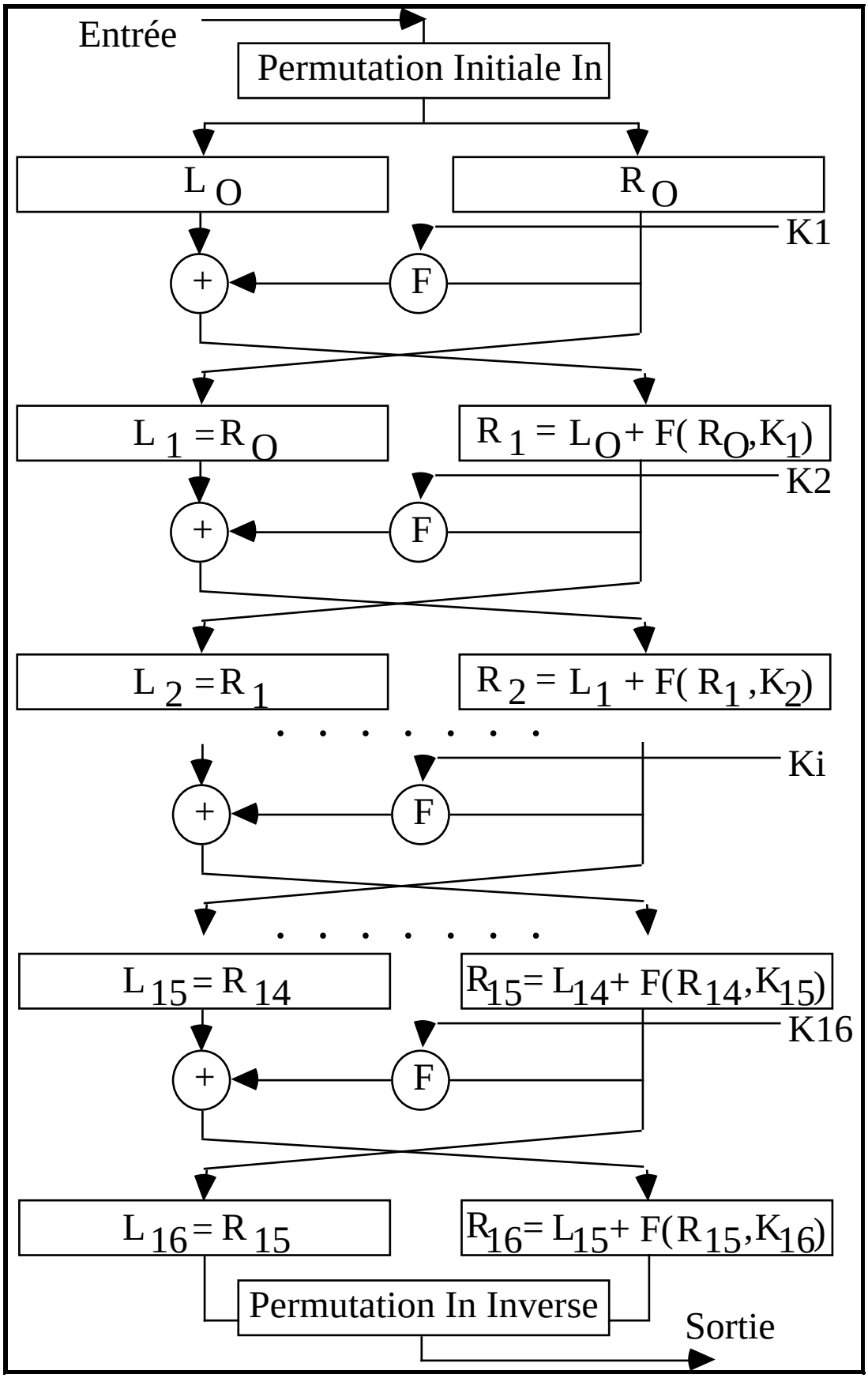
En fait 8 fois 7 bits avec une parité (initialement 128 bits)

19 étages de logique combinatoire

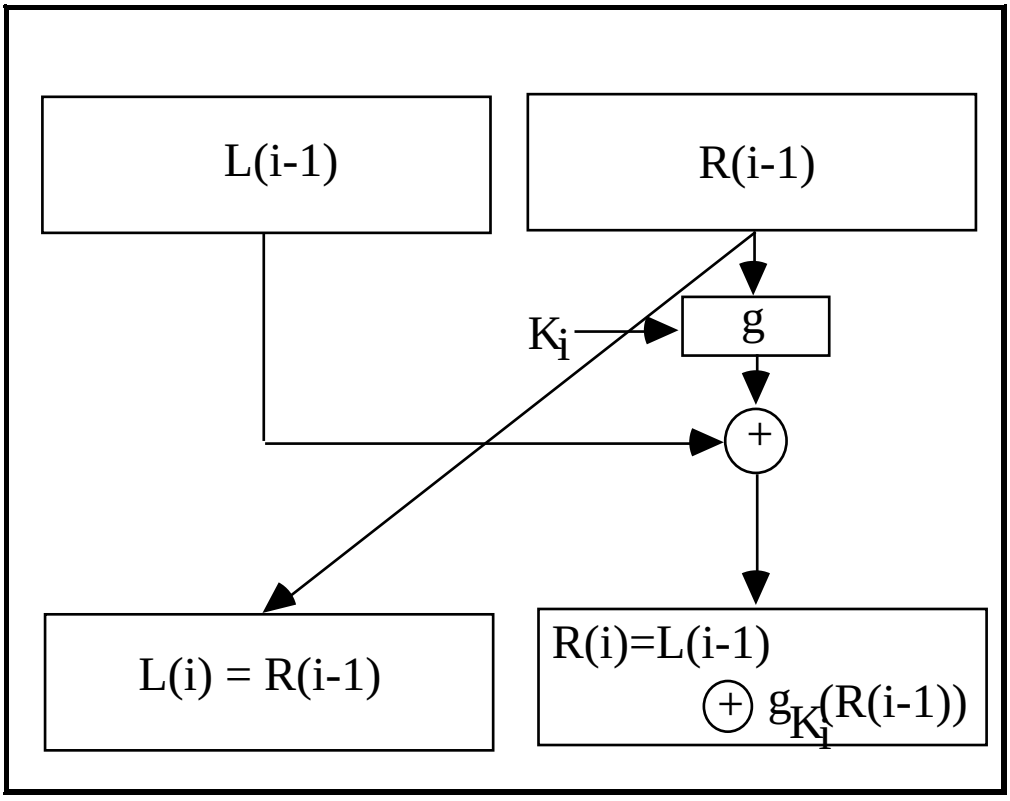
Appliquent des transpositions substitutions sur des blocs de 2 x 32 bits

- 1 étage amont, 2 en aval sont des transpositions simples fixes
- 16 étages intermédiaires dépendent de la clé de façon complexe.

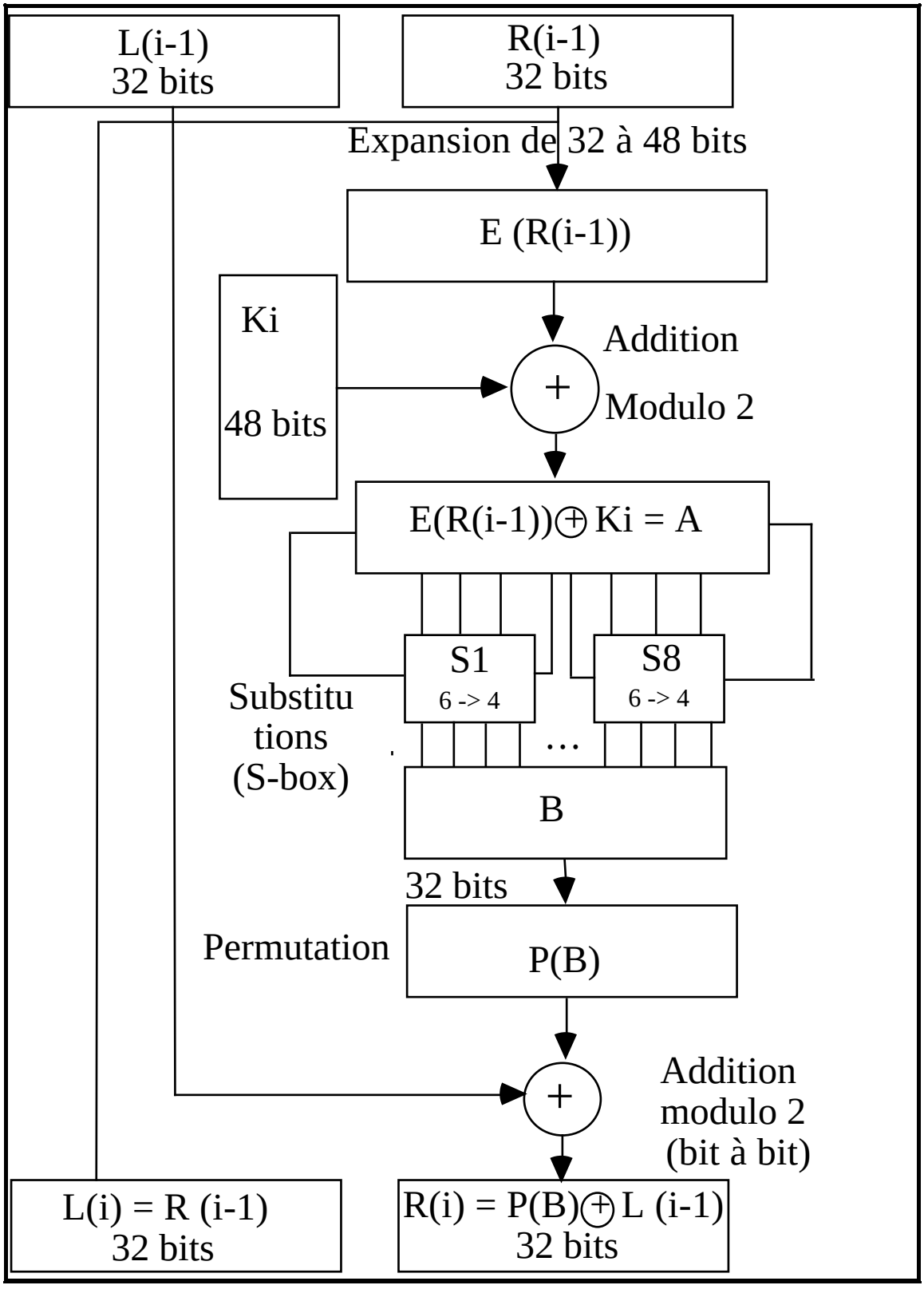
Architecture générale du DES


Entrée
Permutation Initiale In
L O
R O
K1
+
F
L 1 = R O
R 1 = L O + F(R O, K 1)
K2
+
F
L 2 = R 1
R 2 = L 1 + F(R 1, K 2)
. . . . . .
Ki
+
F
. . . . . .
L 15 = R 14
R15 = L14 + F(R14, K15)
K16
+
F
L 16 = R 15
R16 = L15 + F(R15, K16)
Permutation In Inverse
Sortie

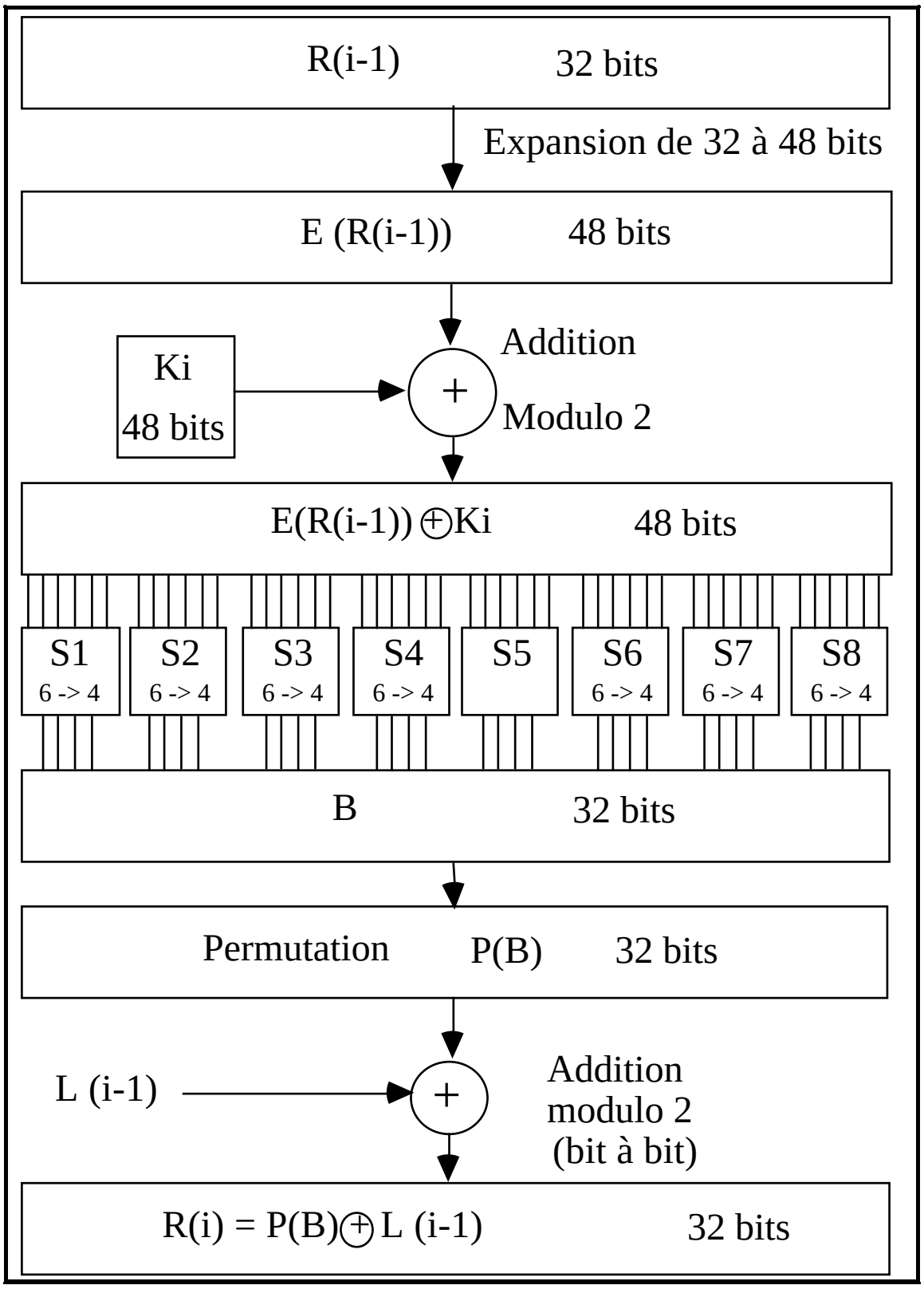
Principe de réalisation d'un étage



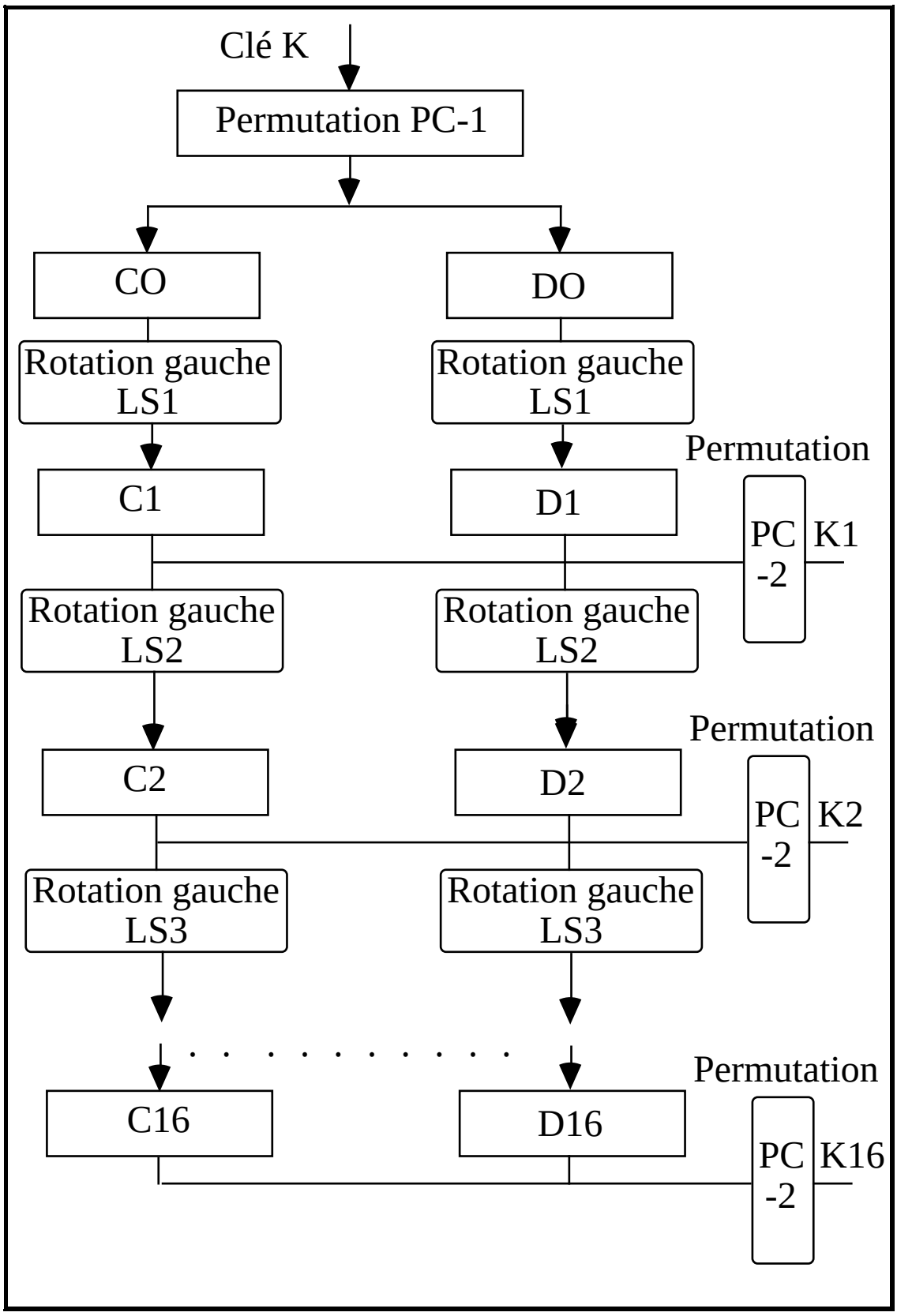
Détails de la fonction principale d'un étage



Détail des boites de substitution



Méthode de calcul des clés



Complément sur le calcul des clés intermédiaires

- La clé initiale K est sur 64 bits.

- La permutation PC-1 enlève les bits de parité et opère sur les 56 bits restants.

- On divise le résultat en deux moitiés C0 et D0 de 28 bits.

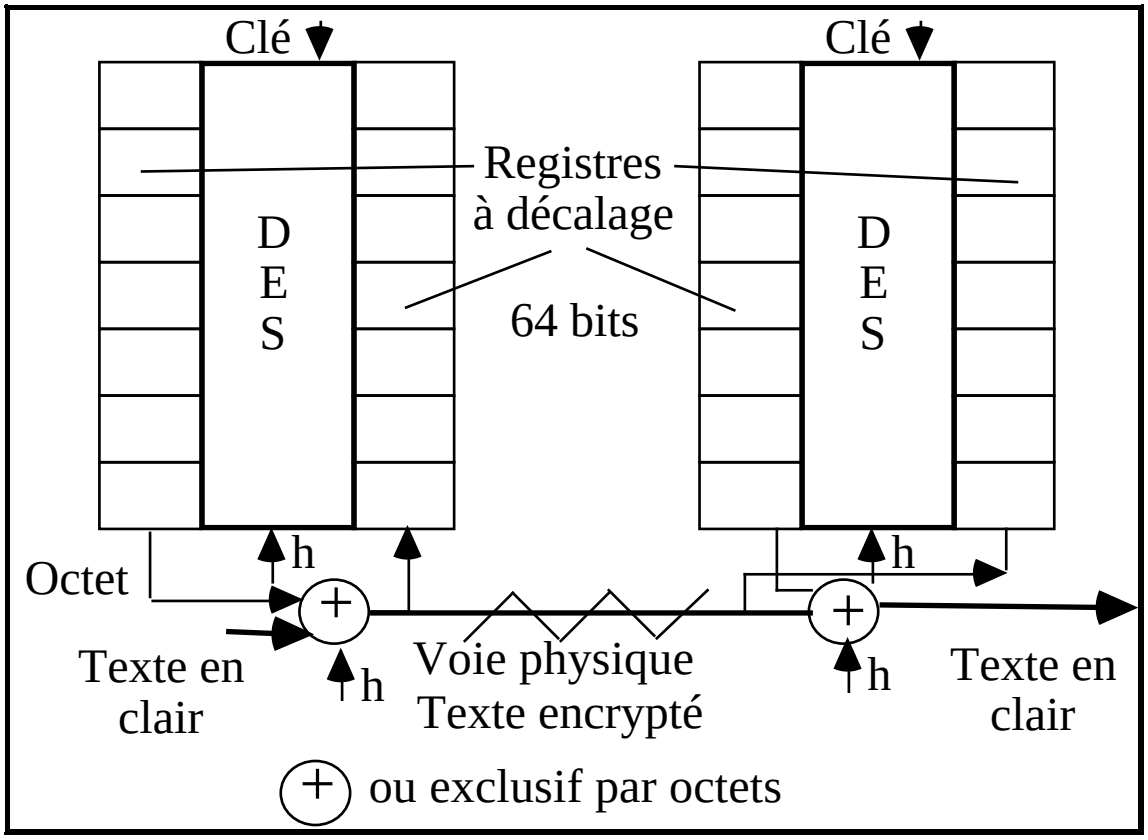
- On génère une suite Ci, Di en opérant des décalages à gauche successifs:

$$Ci = LSi\ (Ci\text{-}1)$$
$$Di = LSi\ (Di\text{-}1)$$

- Pour obtenir la clé Ki on regroupe Ci et Di et l'on opère sur les 56 bits une permutation PC-2

$$Ki = PC\text{-}2(Ci\ Di)$$

DES Utilisation A la Volée



- Un circuit DES de cryptage par blocs de 64 bits est utilisé octets par octets au moyen de registre à décalage (octets) d'entrée et de sortie.

- Performances Excellentes - cryptage à la volée à débits potentiellement très élevés (dizaine/ centaine de Mégabits/seconde).

- Utilisation multiples
Transmission de données informatiques
Cryptage de chaînes de télévision à péage.

Controverse sur la sécurité du DES

Problème de longueur des clés

- Initialement défini avec une clé de 112 bits le DES a été finalement doté par les autorités américaines d'une clé de 56 bits.

=> Le DES 56 est très probablement attaquable par des moyens informatiques plus ou moins lourds à la portée des états.

Des puces spéciales permettant l'essai de 10^6 clés par seconde ont été construites Elles peuvent être organisées en processeurs spéciaux massivement parallèles.

Problème du choix des substitutions

- Les principes de choix des S-box n'ont jamais été rendu public.
Officiellement elles sont conçues pour résister à une attaque particulière
(la cryptanalyse différentielle).

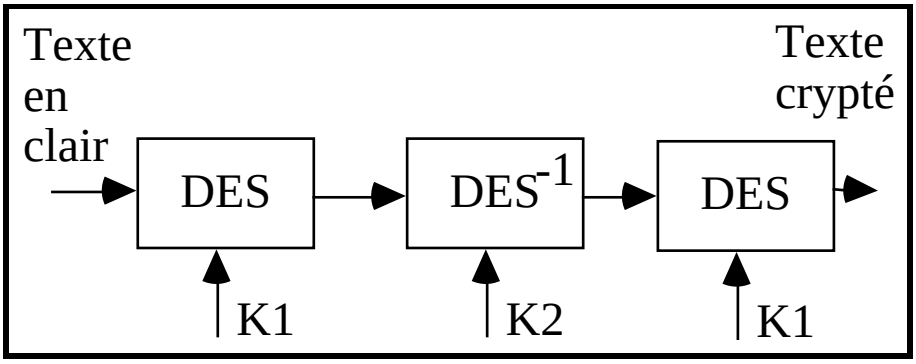
=> Personne n'a jamais rien trouvé concernant d'éventuelles propriétés cachées des boites de substitution.

Amélioration de la sécurité du DES

Utilisation de DES en cascade

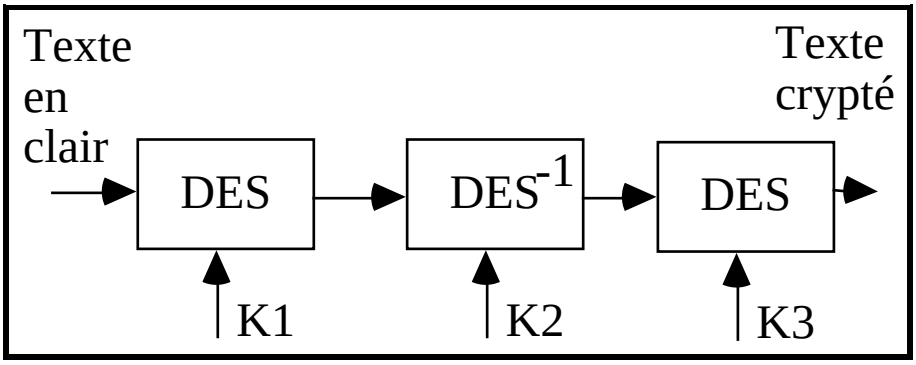
Première proposition

Avec deux clés K1, K2 (128 bits).
Moins bon qu'un DES 128 bits



Seconde proposition

Avec trois clés K1, K2 , K3.



Conclusion
- DES -

- Standard maintenant assez ancien ayant finalement bien tenu.

- Excellentes performances en vitesse de cryptage.
  Un circuit dédié crypte à 1 Gigabit/s
  En logiciel on crypte à 1 Mégabit/s

- Niveau de sécurité pour une solution à clés privées très correct pour des applications ne nécessitant pas une confidentialité de haut niveau (militaire).

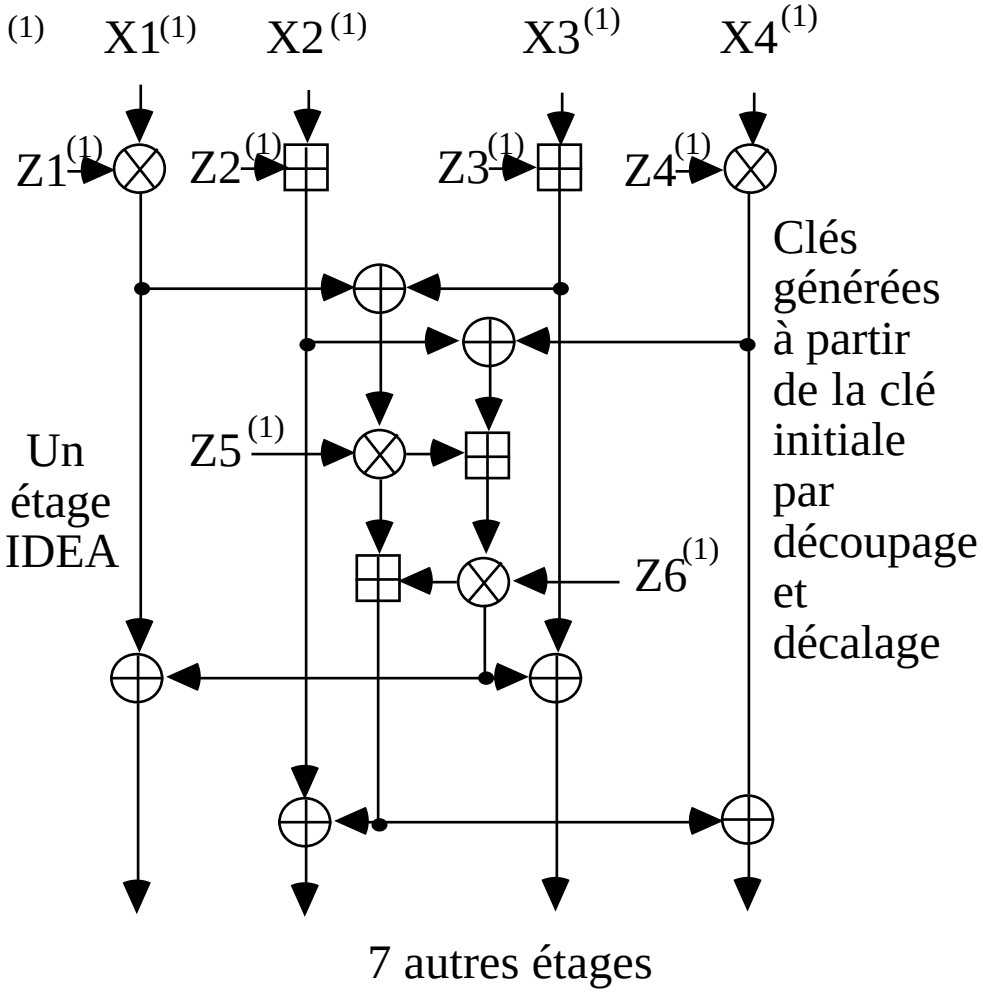
Le DES 56 est probablement peu sûr pour un attaquant ayant de gros moyens mais performant et trop coûteux à casser pour des applications habituelles.

IDEA: International Data Encryption Algorithm

Autre solution de chiffrement par blocs de 64 bits basé sur huit étages facilement réalisable en matériel ou en logiciel.

Les opérations utilisées sont des opérations arithmétiques:

- ou exclusif
- addition modulo 2^{16} $\boxplus$
- multiplication modulo $2^{16}+1$



Conclusion IDEA

- IDEA est considéré par les spécialistes comme l'un des meilleurs cryptosystème à clé privée.

- La longueur de clé est élevée (128 bits).

- La vitesse de chiffrement et de déchiffrement peut-être élevée au moyen de circuits spéciaux.
  Circuits à 55 Mb/s et 177 Mb/s
  En logiciel sur 386 33Mhz: 880 Kb/s

- Les attaques semblent difficile mais le système est assez récent (1990)

Chapitre II

LA CRYPTOGRAPHIE A CLÉS PUBLIQUES

Deux problèmes essentiels limitent les méthodes de cryptographie à clés privées dans les réseaux (utilisées seules):

- **L'échange de clés** entre des sites qui n'ont jamais été en relation
  => Il faut un moyen différent pour échanger des clés.

- Pour communiquer dans un groupe de n participants il faut **n(n-1)/2 clés**.

1976 - Diffie et Hellman définissent les principes d'une nouvelle approche en cryptographie sans proposer de solution au problème qu'ils posent.

La cryptographie à clés publique.

1978 - R. Rivest A. Shamir L. Adelman donnent une première solution:

La méthode RSA.

Cryptographie à clés publiques

L'idée est de supposer que l'on sait trouver deux fonctions E_k et $D_{k'}$ qui dépendent de clés k et k'.

E_k est la méthodes d'encryptage.
$D_{k'}$ est la méthodes de déchiffrage.

Ayant les propriétés suivantes :

1- Définition même de la cryptographie: le déchiffrage est l'inverse de l'encryptage.

$$\mathbf{D_{k'}\,(\,E_k\,(M)\,)\,=\,M}$$

2- Il est très très difficile **de déduire $D_{k'}$ de la connaissance de messages cryptés par E_k ou de E_k complète** car cette fonction est diffusée à tous.

=> Des milliers d'années de calcul seraient nécessaires dans l'état des connaissances.

3- Idéalement $E_k(M)$ et $D_{k'}(M)$ devraient être **faciles à calculer**.

Les clés publiques: une révolution dans l'approche cryptographique

Un utilisateur a un couple (E_k, $D_{k'}$)

- L'idée essentielle est que E_k (en fait k) peut-être **rendue publique** par exemple dans un **annuaire** (le nom vient de là).

- $D_{k'}$ est **privée** (en fait k' est privée et nécessairement différente de k).

- **Tout le monde peut connaître E_k** et envoyer des messages secrets qu'**un seul destinataire** (celui qui connaît $D_{k'}$) **peut comprendre**.

- D'où l'hypothèse fondamentale d'un tel système.

=> **On ne doit pas pouvoir trouver $D_{k'}$ quand on connaît E_k.**

Comme un attaquant connaît E_k et des messages cryptés par E_k il ne doit pas pouvoir casser E_k

=> Décrypter des messages cryptés par E_k en essayant des messages connus.

L'Algorithme RSA

Fonction E Encodage (publique)

- La clé publique est un couple d'entiers:

$$k = (e, n)$$

- L'encodage se fait au moyen de l'élévation à la puissance e modulo n:

$$E_k(M) = M^e \pmod n$$

Fonction D Décodage (secrète)

- La clé secrète est un couple d'entiers:

$$k' = (d, n)$$

- Le décodage se fait au moyen de l'élévation à la puissance d modulo n:

$$D_{k'}(M) = M^d \pmod n$$

Remarque: Les entiers n, e, d doivent être choisis selon des règles précise.

Méthode de choix des clés

1. Détermination de n

Trouver **deux entiers premiers** p et q très grands:

Calculez n = p q

De préférence détruisez p et q.

La sécurité du système repose sur la difficulté de factoriser un grand entier n en deux entiers premiers p et q (taille de n : 320 bits, 512 bits, 1024 bits conditionne également la lenteur des algorithmes).

2. Détermination de d

Calculez z = (p-1) (q-1)

Choisir un entier **e premier avec z.**

La clé publique est (e , n)

3. Détermination de d

Choisir un entier d tel que :

$$e\ d \equiv 1 \pmod{z}$$

(d inverse de e dans l'arithmétique mod z)

La clé privée est (d , n)

Réversibilité de RSA

Fonction d'Euler

Pour n entier z = $\varphi(n)$ est le nombre d'entiers premiers avec n.

- si n est premier $\varphi(n) = n-1$
- si n = pq avec p et q premiers

$$\varphi(n) = (p-1)(q-1)$$

Théorème d'Euler

Si a et n sont premiers entre eux

$$a^{\varphi(n)} \pmod n = 1$$

Pourquoi RSA marche

$$D(E(M)) = ((M)^e \pmod n)^d \pmod n$$
$$= (M^e)^d \pmod n = M^{e.d} \pmod n$$

Mais on a choisi $e.d \equiv 1 \pmod z$

Soit en fait $e.d = j\,z + 1$

$$M^{e.d} \equiv M^{j.z}\, M \pmod n \equiv M \pmod n$$

Parceque théorème d'Euler:

$$M^{j\,z} \pmod n = (M^z)^j \pmod n = (1)^j = 1$$

Remarques

1. Le RSA doit toujours être appliqué à des blocs de chiffres d'amplitude inférieure à n pour faire des calculs modulo n.
   =>Décomposition des messages en blocs

2. On voit ici que l'on a aussi:

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

Exemple

1 Soient deux entiers premiers p =47,q =71
n = pq = 3337

2 z= (p-1)(q-1)= 46 . 70 = 3220
Choisissons e = 79 (premier avec n)

3 Calcul de l'inverse de e modulo z
Une solution possible: le théorème d'Euler
$e^{\varphi(n)} = 1 = e\ e^{-1} = e\ e^{\varphi(n)-1} \pmod z$
Donc $d = e^{-1} = e^{\varphi(n)-1} \pmod z$
Numériquement $79^{78} \pmod{3220} = 1019$
Une autre solution plus simple:
L'algorithme d'Euclide

4 Crypter M = 688232687966683
Décomposition en blocs de taille inférieure à n= 3337 => Des blocs de 3 chiffres
M= 688 232 687 966 668 3
Crypter 688:
$688^{79} \pmod{3337} = 1570$
E(M) = 1570 2756 2091 2276 2423 158
Décrypter 1570:
$1570^{1019} \pmod{3337} = 688$

Tiré de "Cryptographie appliquée"
B. Schneier

Intuitions relatives au RSA

Crypter = bousculer les informations pour rendre le sens inaccessible.
RSA = l'utilisation de l'élévation à la puissance puis d'une congruence.

- L'élévation a une puissance permet de changer le registre des entiers choisis

Exemple très simple e = 3 et n = 41:
Pour M = 27, M' = 28 peu différents.
$E(M) = 27^3 = 19683$
$E(M') = 28^3 = 21952$

- Les congruences introduisent des discontinuités => il est très difficile de trouver le logarithme d'un nombre dans un ensemble d'entiers modulo n.

$E(M) = 27^3 \bmod (41) = 19683 \bmod (41)$
$E(M) = 480 \times 41 + 3 \bmod (41)$
$E(M) = 3$
$E(M') = 28^3 \bmod (41) = 21952 \bmod (41)$
$E(M') = 535 \times 41 + 17 \bmod (41)$
$E(M') = 17$

Attaque du RSA

Solution de base

- n étant public le cryptanalyste cherche à trouver p et q pour calculer z.

=> Il doit factoriser un grand nombre en deux facteurs premiers.

Ce problème est **complexe**

Meilleurs algorithmes connus

- En 1989 avec 400 Vax pendant 3 semaines factorisation d'un nombre de 106 chiffres (352 bits)
- Actuellement factorisation possible de nombres de 110 à 120 chiffres (350 à 400 bits)

- Si on a trouvé p et q alors utiliser l'algorithme d'Euclide pour trouver e, d premiers avec (p-1) (q-1) = z

D'autres attaques sont à découvrir...

Sécurité et performances du RSA

Utiliser des longueurs de clés de plus en plus importantes

Valeurs envisagées

512 bits, 640 bits

1024 bits (considéré comme assez sûr pour plusieurs années)

2048 bits

Utiliser des circuits intégrés de cryptage de plus en plus performants

Actuellement une dizaine de circuits disponibles.

Vitesse de cryptage de base pour 512 bits:

de 10 à 30 Kb/s

Évolution en cours

de l'ordre de 64 Kb/s

A venir

de l'ordre de 1 Mb/s

Remarque: Compte tenu de la complexité des traitements le DES doit être environ toujours 100 fois plus rapide que le RSA.

Problèmes du RSA

- Trouver de grands nombres premiers (on prend en fait des nombres premiers en probabilité).

- Choisir des clés secrètes et publiques assez longues.

- Réaliser les opérations modulo n rapidement.

RSA carte bancaire

limitation des calculs du fait de la puissance de calcul disponible.

n sur 320 bits (de l'ordre de 95 chiffres)

clé publique 3 pour tout le monde

Conclusion RSA

- Problème principal

Complexité algorithmique de la méthode.

Solution assez générale.

Utiliser le RSA brièvement au début d'un échange pour échanger des clés secrètes de session d'un algorithme efficace à clés privées.

- Efficacité en sécurité

La méthode est officiellement sûre si l'on respecte certaines contraintes de longueur de clés et d'usage.

Personne depuis 2500 ans n'a trouvé de solution rapide au problème de la factorisation ...

III
Les fonctions de hachage à sens unique

Notion de fonction à sens unique ("one way function")

C'est une fonction f(M) facile à calculer mais telle qu'il est extrêmement difficile de déduire M de f(M).

Exemple:

Calcul modulo n (dans un corps fini)

M^2 est facile à calculer modulo n (M^e).

$\sqrt{M}$ est difficile à calculer (log M).

Les fonctions à sens unique sont utiles pour garder sous forme inaccessible des mots de passe.

Par contre pour la cryptographie elles sont peu utiles car une fois M chiffré on ne sait pas déchiffrer M.

Notion de fonction à sens unique à brèche secrète

C'est une fonction f(M) facile à calculer telle qu'il est extrêmement difficile de déduire M sauf si l'on connaît un secret K.

Notion de fonction de hachage

Une fonction de hachage est une fonction mathématique qui a partir d'un message (d'une donnée) génère une autre chaîne (généralement plus courte).

Terminologie: fonction de contraction, digest, empreinte digitale, ...

Exemples: Calcul de parité verticale
On fait le ou exclusif de tous les octets d'une chaîne de caractères.

Calcul de code polynomial.

Notion de fonction de hachage à sens unique sans clé

C'est une fonction de hachage à sens unique qui peut être calculée par n'importe qui (MD5).

Notion de fonction de hachage à sens unique avec clé

C'est une fonction de hachage à sens unique qui ne peut être calculée que par une seule entité détentrice de la clé.

Nombreux exemples de fonctions de hachage à sens unique avec clé.

Signatures numériques

Une signature manuscrite idéale est réputée posséder les propriétés suivantes:

- La signature **ne peut-être imitée.**
Elle prouve que le signataire a délibérément signé le document.

- La signature **authentifie** le signataire.
Seul le signataire peut avoir signé.

- La signature appartient à un seul document (elle **n'est pas réutilisable**).

- Le document signé ne peut être partiellement ou totalement **modifié**.

- La signature ne peut-être **reniée**.

Base de la signature numérique:
L'existence d'une fonction de hachage à sens unique avec clé.
Une solution possible: une fonctions de hachage à sens unique et une technique classique de cryptographie (exemple le RSA)

MD5 Message Digest version 5

Une fonction de hachage à sens unique.

On génère une signature sur 128 bits.

Le message est décomposé en blocs de 512 bits soient 16 sous-blocs Mj de 32 bits.

Pour chaque bloc de 512 bits on réalise 4 séries de 16 applications successives des fonctions de base FF, GG , HH, II qui dépendent des sous-blocs Mj et de constantes a, b, c, d, ti:

$FF(a,b,c,d,Mj,s,ti) \rightarrow a = b + ((a = F(b,c,d) + Mj + ti) \lhd s)$

$GG(a,b,c,d,Mj,s,ti) \rightarrow a = b + ((a = G(b,c,d) + Mj + ti) \lhd s)$

$HH(a,b,c,d,Mj,s,ti) \rightarrow a = b + ((a = H(b,c,d) + Mj + ti) \lhd s)$

$II(a,b,c,d,Mj,s,ti) \rightarrow a = b + ((a = I(b,c,d) + Mj + ti) \lhd s)$

Dans les formules précédentes $\lhd s$ désigne un décalage à gauche de s positions les fonctions F,G, H,I sont données par:

$F(X,Y,Z) = (X \quad Y) \quad (\neg X \quad Z)$

$G(X,Y,Z) = (X \quad Z) \quad (Y \quad \neg Z)$

$H(X,Y,Z) = (X \quad Y \quad Z)$

$I(X,Y,Z) = Y \quad (X \quad \neg Z)$

Bibliographie

A.S. Tannenbaum - Computer Networks Prentice Hall

B. Schneier - Cryptographie appliquée Thomson Publishing International France

D.E. Denning - Cryptography and data security Addison Wesley 1982