

ch 2 : Chiffrement symétrique

I] Modélisation

II] DES (Data Encryption Standard)

① Historique

② Description

Schéma de Feistel

$$\text{Tour } n^{\circ} i \quad : \begin{cases} L_i = R_{i-1} \\ R_i = L_{i-1} \oplus F(R_{i-1}, K_i) \end{cases}$$

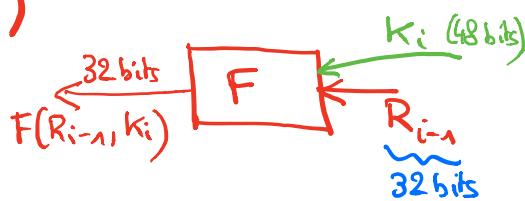
$$\text{Tour } n^{\circ} 16 : \begin{cases} L_{16} = L_{15} \oplus F(R_{15}, K_{16}) \\ R_{16} = R_{15} \end{cases}$$

⇒ Le schéma de chiffrement est inversible

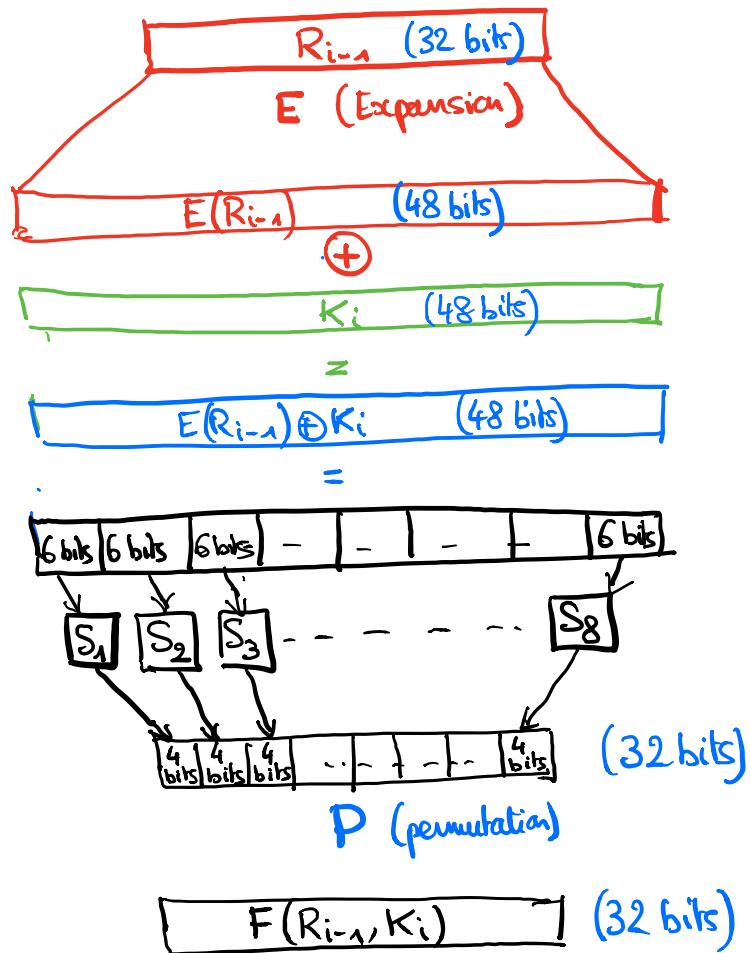
$$\text{Tour } n^{\circ} i : \begin{cases} L_{i-1} = R_i \oplus F(L_i, K_i) \\ R_{i-1} = L_i \end{cases}$$

$$\text{Tour } n^{\circ} 16 : \begin{cases} L_{15} = L_{16} \oplus F(R_{16}, K_{16}) \\ R_{15} = R_{16} \end{cases}$$

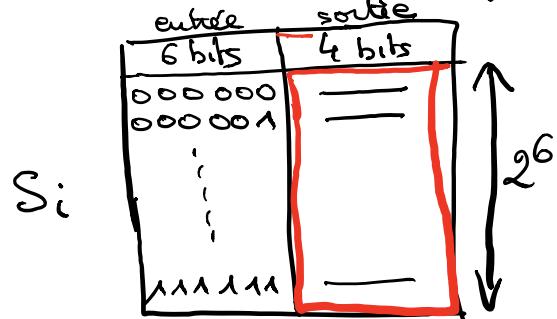
Remarque: Que ce soit pour le chiffrement ou pour le déchiffrement, c'est la fonction F qui est utilisée (pas F^{-1})



Description de F :



S_1, \dots, S_8 : boîtes-S , données sous forme de tables



$$2^6 \times \frac{1}{2} \text{ octet} = 132 \text{ octets}$$

Pour les 8 tables : $8 \times 32 = 256 \text{ octets}$

Remarque : Dans les opérations qui constituent le DES, toutes sont linéaires sauf les boîtes S

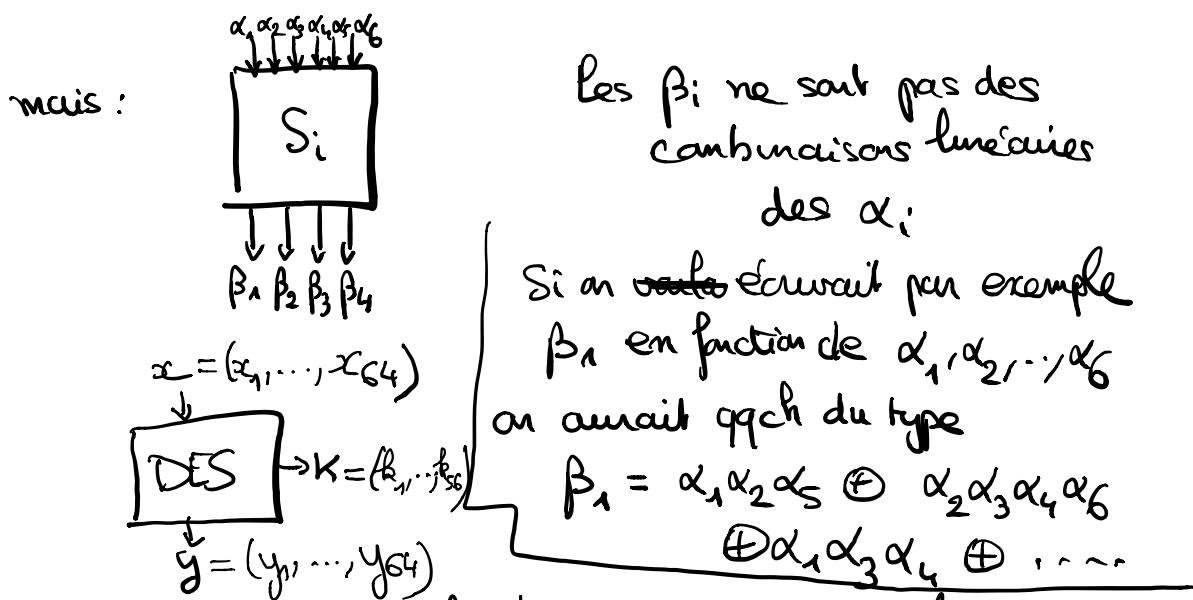
ex: $a \oplus b = c$

$\begin{matrix} \uparrow & \uparrow & \uparrow \\ \text{octet} & \text{octet} & \text{octet} \end{matrix}$

$a = (a_1, \dots, a_8)$
 $b = (b_1, \dots, b_8)$
 $c = (c_1, \dots, c_8)$

bit de sortie combinatoire linéaire des bits d'entrée

$\left\{ \begin{matrix} c_1 = a_1 \oplus b_1 \\ \vdots \\ c_8 = a_8 \oplus b_8 \end{matrix} \right.$



Héritement que les boîtes S ne sont pas linéaires
 Si un le DES serait lui-même une transformation linéaire

et on aurait un système d'équations du type

64 équations

56 inconnues

$$\left\{ \begin{matrix} y_1 = x_3 \oplus x_7 \oplus x_8 \oplus x_{21} \oplus x_{37} \oplus x_{39} \oplus x_{44} \\ \quad \oplus k_3 \oplus k_4 \oplus k_{23} \oplus k_{37} \oplus k_{52} \\ \vdots \\ y_{64} = x_2 \oplus x_7 \oplus x_{12} \oplus x_{26} \oplus x_{51} \oplus x_{63} \\ \quad \oplus k_7 \oplus k_{17} \oplus k_{23} \oplus k_{49} \oplus k_{52} \end{matrix} \right.$$

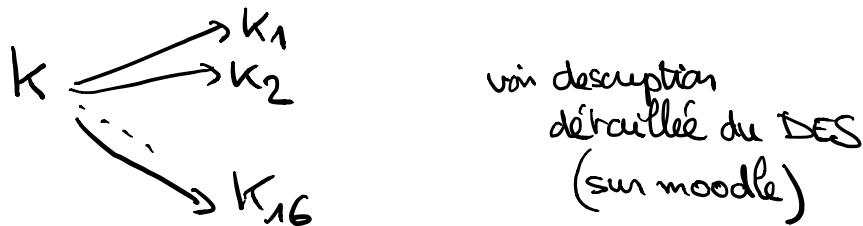
qu'on pourrait résoudre grâce au pivot de Gauss.

Remarque : - Les boîtes-S initiales (de LUCIFER) ont été modifiées en 1975-76 par la NSA

- En 1989, un type d'attaque de cryptanalyse appelé "cryptanalyse différentielle" a été inventé par Biham et Shamir

$\left\{ \begin{array}{l} \rightarrow \text{casse}^{\text{avec}} \text{les boîtes-S de LUCIFER} \\ \rightarrow \text{ne casse pas } \notin \text{ avec les boîtes-S modifiées} \\ \quad (= \text{les vraies boîtes-S du DES}) \end{array} \right.$

Méthode pour obtenir les sous-clés K_1, K_2, \dots, K_{16}
(48 bits) (48 bits) (48 bits)
à partir de la clé K (56 bits)



= Méthode de "key scheduling" (cadencement de clé)

③ Sécurité du DES (si l'attaquant cherche à retrouver la clé)

- Recherche exhaustive : $O(2^{56})$
(attaque par force brute)
à partir de x et y tels que $y = \text{DES}_K(x)$
On résout l'équation $y = \text{DES}_K(x)$

en essayant toutes les possibilités pour la clé K .

Remarque : En 1976, on savait faire $\approx 2^{40}$ calculs
(dans le monde civil) $\Leftrightarrow 2^{56}$ calculs en 2000

En 2001, l'EFF (Electronic Frontier Foundation) a construit un circuit spécialisé (coût: 250000\$) capable de faire une recherche exhaustive de la clé DES en $\approx 2,5$ jours (en moyenne)

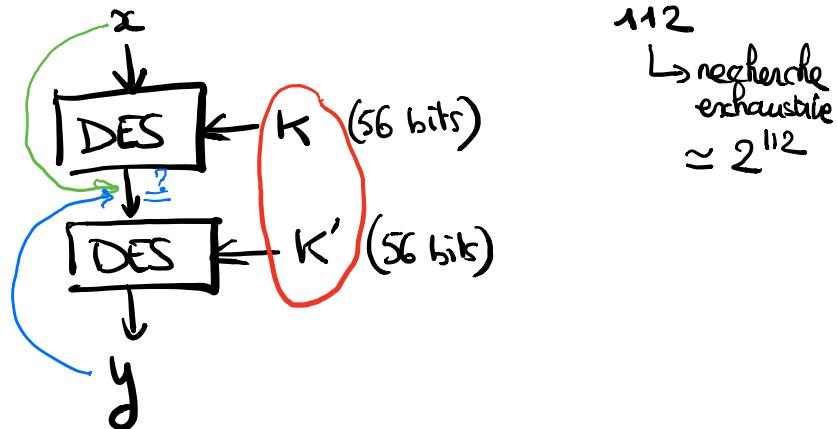
- Cryptanalyse différentielle (Biham, Shamir, 1989)

complexité de l'attaque: $\approx 2^{47}$ opérations élémentaires
en supposant qu'on dispose de $\approx 2^{47}$ couples clair/chiffré

- Cryptanalyse linéaire (Matsui, 1993)

complexité de l'attaque: $\approx 2^{43}$ opérations élémentaires
en supposant qu'on dispose de $\approx 2^{43}$ couples clair/chiffré

- Double-DES avec une clé de 2×56 bits

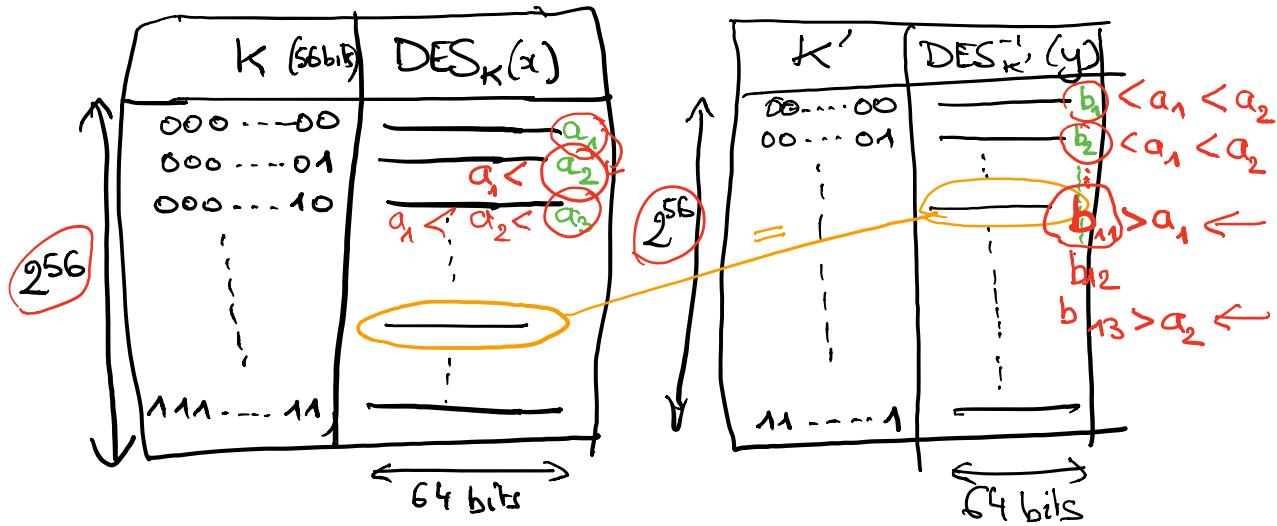


pb: attaque "meet in the middle" (rencontre au milieu)

$$y = \text{DES}_{K'}(\text{DES}_K(x))$$

$$\Leftrightarrow \text{DES}_K(x) = \text{DES}_{K'}^{-1}(y)$$

uncertain



Méthode "naïve" : on prend a_1 (1^{re} valeur de la Table 1)
et on cherche si elle est aussi dans
la 2^e table

puis on recommence avec a_2 (2^e valeur
de la
1^{re} table)
etc

\rightarrow complexité = n^2 où n est la taille
de chaque table
 $\boxed{n = 2^{56}} \rightarrow \boxed{2^{112}}$ (pas intéressant)

Idee qui fonctionne : commencer par trier les tables

\rightarrow complexité, une fois ces tables triées, est
 ~~$\simeq 2^{56} \times 2$~~

\rightarrow complexité du tri (d'un tableau de n valeurs)

$$\boxed{\mathcal{O}(n \ln n)}$$

\Rightarrow pour nos 2 tables : $\boxed{\mathcal{O}(2^{56} \ln 2^{56})}$

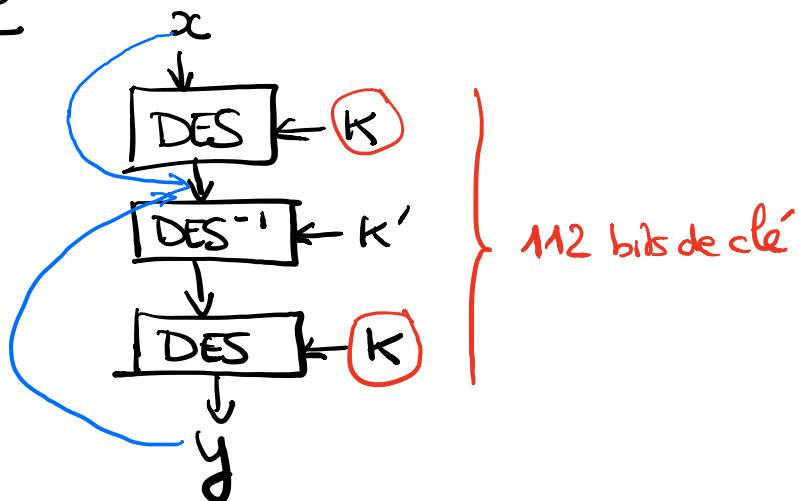
Au total, pour retrouver la clé (K, K') du double DES

- Construction des tables : $\approx 2^{56} \times 2$
- Tri : $\approx 2^{56} \ln 2^{56} \times 2$
- Recherche de la valeur commune : $\approx 2^{56} \times 2$

$$\text{Complexité} \approx 2 \times 2^{56} \ln \underbrace{2^{56}}_{56 \ln 2} \approx 30$$

$$\approx 60 \times \underline{\underline{2^{56}}}$$

Triple-DES



Remarque: si $K = K'$, on retrouve le DES simple

Intérêt du Triple DES : ~~la~~ l'attaque meet-in-the-middle

