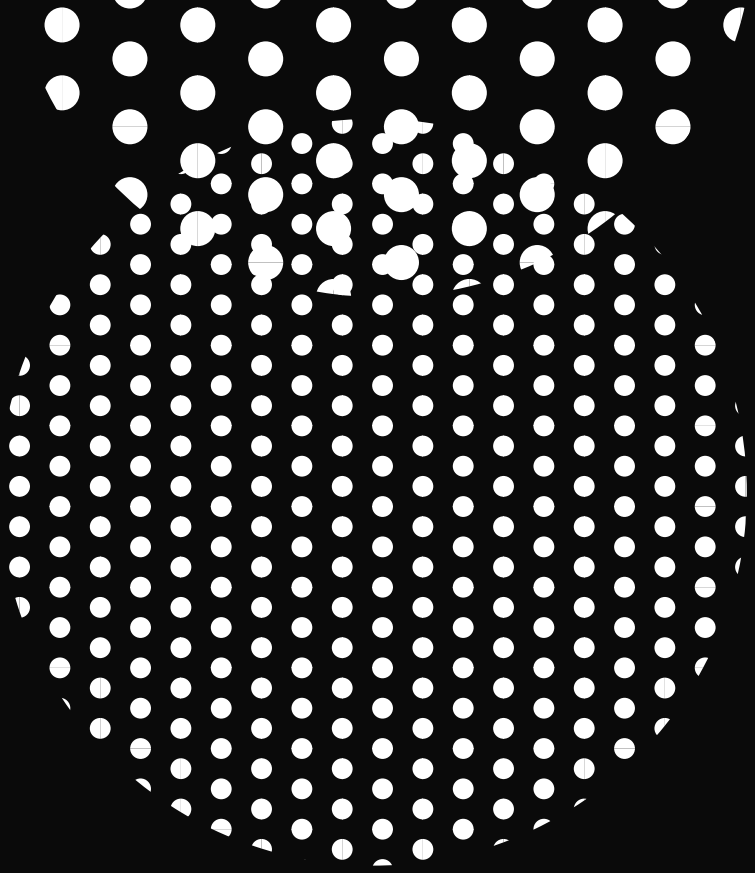


$K_1 = 0111 = 7$

$K_2 = 1100$

$(L_0, R_0) = \underbrace{1010}_{L_0} : \underbrace{0011}_{=R_0}$

| 0 | 0 | 1 | 1 |
|---|---|---|---|
| 0 | 1 | 0 | 1 |
| 0 | 1 | 1 | 0 |

$K_1 \oplus R_0 = 0111 \oplus 0011$

$= 0100$

$4 = x$

$S(4) = 3$

$P(3) = P(0011)$

$= 1100$

$1010 \oplus 1100$

$= 0110$

$L_1 = 0011 \qquad R_1 = 0110 = L_2$

$K_2 \oplus R_1 = 1100 \oplus 0110$

$= \underbrace{1010}_{=10}$

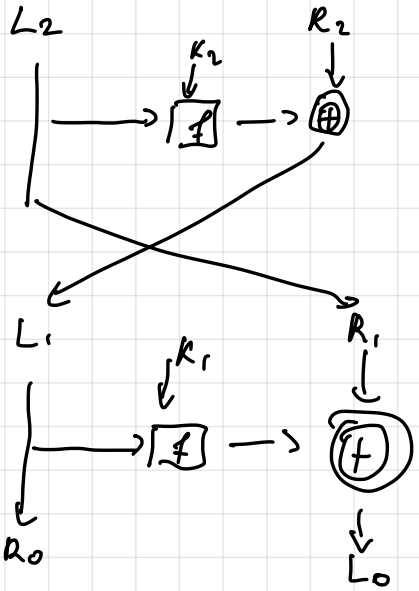
$S(10) = 14 = 1110$

$P(1110) = 0111$

$L_1 \oplus f = 0011 \oplus 0111 = \underbrace{0100}_{=R_2}$

**0100 0110 = chiffré**

2)



Exo 2

1. $f(\overline{K_1}, \overline{R_0}) = P(S(\overline{K_1} \oplus \overline{R_0})) = P(S(K_1 \oplus R_0))$ car $\overline{x \oplus y} = x \oplus y$

2. $L_1' = \overline{R_0} = \overline{L_1}$

$R_1' = \overline{L_0} \oplus P(S(\overline{K_1} \oplus \overline{R_0}))$

$= \overline{L_0} \oplus f(\overline{K_1}, \overline{R_0})$

$= \overline{L_0} \oplus f(K_1, R_0)$

$= \overline{L_0 \oplus f(K_1, R_0)}$ car $\overline{x} \oplus y = \overline{x \oplus y}$

$= \overline{R_1}$

Donc on obtient $\overline{C} = (\overline{L_1} \| \overline{R_1})$

$\overline{DES_K(m)} = DES_{\overline{K}}(\overline{m})$

3. On connaît $m$ $DES_K(m)$ et $DES_K(\overline{m})$
↳ on veut retrouver $K$ (56 bits)

Pour trouver les clés $K$ possibles "candidates" :

$m \xrightarrow{DES_K} DES_K(m) \stackrel{?}{=} DES_K(m)$

1 chiffrement $C = DES_K(m)$

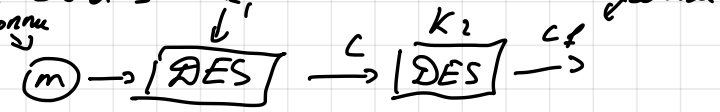
2 tests

1. Si $C = DES_K(m)$ → on renvoie $K$
2. Si $C = DES_K(\overline{m}) \stackrel{?}{=} \overline{DES_K(m)}$
→ on renvoie $\overline{K}$

car $\overline{DES_K(\overline{m})} = DES_{\overline{K}}(m)$

↳ 1 seul chiffrement permet de tester 2 clés d'un coup → attaque exhaustive en $2^{55}$

4] $K = 56$ bits




↳ retrouver $(K_1, K_2)$ en $2^{57}$ essais ? (ou bien des $2^{112}$ possibilités)

Attaque meet-in-the-middle

① $\forall K_1$ possible $= C_{K_1} = DES_{K_1}(m)$ → $2^{56}$ valeurs

② $\forall K_2$ —— $= C_{K_2} = DES^{-1}_{K_2}(c_f)$ → $2^{56}$ valeurs

↳ on regarde quand $C_{K_1} = C_{K_2}$ on obtient des couples $(K_1, K_2)$ candidats

$2^{56} + 2^{56} = 2^{57}$ exemples et $2^{56}$ en mémoire

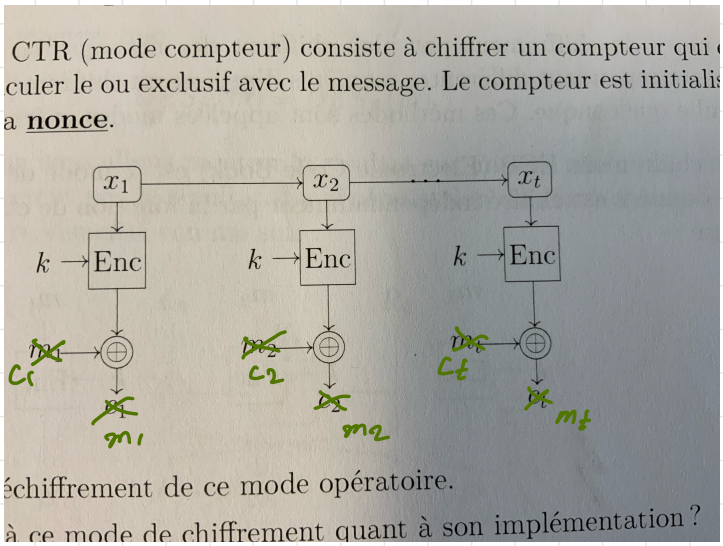
Exo 3

## Exercice 5

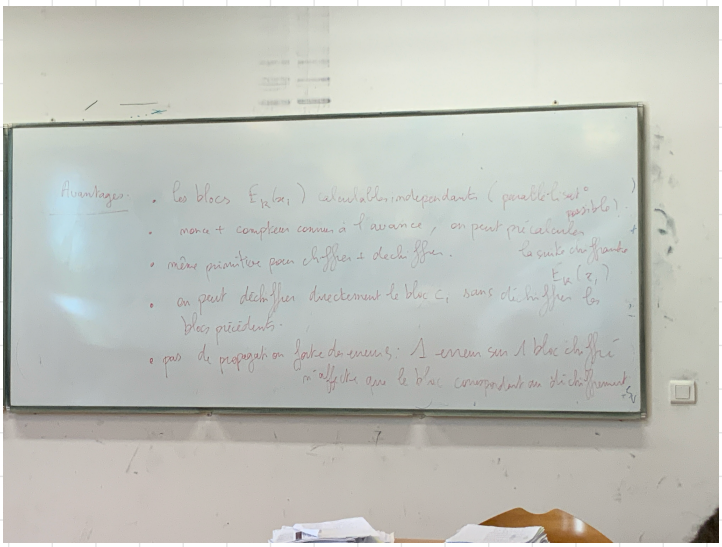
On a $c_j = m_j \oplus E_k(x_j)$

On sait que $a = b \oplus c \Leftrightarrow b = a \oplus c$

Donc $m_j = c_j \oplus E_k(x_j)$, donc le schema devient.




Avantages :




Si la nonce n'est pas changé : $x_i$ fixe

- k est fixe : $E_k(x_i)$ fixe

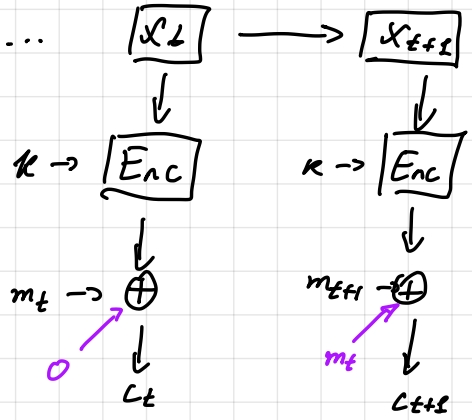
$$c_i = E_k(x_i) \oplus m_i$$

$$c_i' = E_k(x_i) \oplus m_i'$$

$\Rightarrow c_i \oplus c_i' = m_i \oplus m_i'$ ⚠

↳ la nonce sert à initialiser le compteur de manière unique à chaque chiffrement → change la suite chiffrante $E_k(x_i)$

4. On utilise 2 fois la récurrence :




Peut-on retrouver $m_t$ et $m_{t+1}$ ?

$$c_t = m_t \oplus E_k(x_t)$$

$$c_{t+1} = m_{t+1} \oplus E_k(x_{t+1})$$

---

$$c_t = 0 \oplus E_k(x_t)$$

$$c_{t+1} = m_t \oplus E_k(x_{t+1})$$