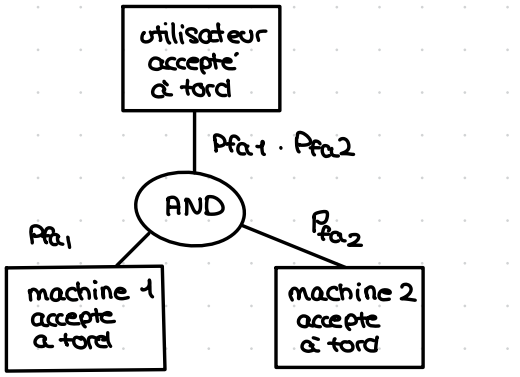
TD 1 05/02/2025

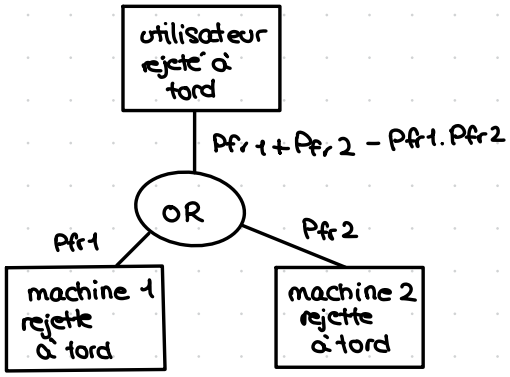
Pf_{a1} P_{fr1}
Pf_{a2} Pf_{r2}

politiques: 2 machines acceptent
au moins une des deux machines accepte

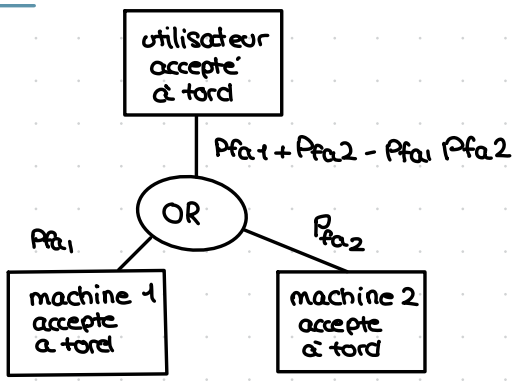
1)

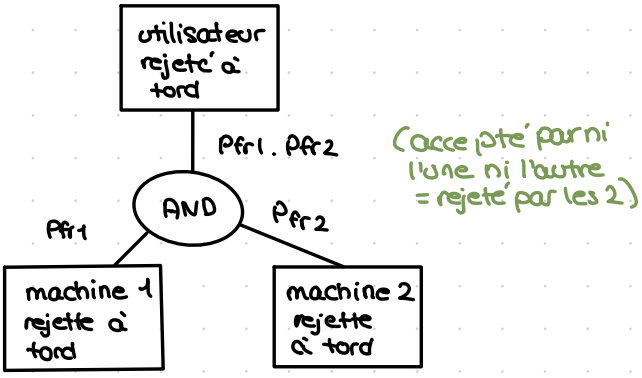
politique 1:





politique 2:





(Accepté par ni l'une ni l'autre = rejeté par les 2)

2) Appli numérique

$Pf_{a1} = 0.1$ $Pf_{r1} = 0.2$ $Pf_{a2} = 0.3$ $Pf_{r2} = 0.4$

politique 1: acceptation à tord: $0.1 \times 0.3 = \boxed{0.03}$
rejet à tord: $0.2 + 0.4 - 0.2 \times 0.4 = 0.6 - 0.16 = \boxed{0.44}$

politique 2: acceptation à tord: $0.1 + 0.3 - 0.1 \times 0.3 = 0.4 - 0.03 = \boxed{0.37}$
rejet à tord: $0.2 \times 0.4 = \boxed{0.16}$

3) Quelle politique conseiller?

politique 1: pour une zone très sensible (base militaire)
politique 2: améliore le confort d'accès (moins de refus): bibliothèque universitaire
(impact d'un faux rejet est plus critique)

Exo2 :

1) nb de combinaisons par une attaque brute force

- 8 caractères minuscules : 26^8
- 8 caractères minuscules, sans repetition: $26 \times 25 \times 24 \times 23 \times 22 \times 21 \times 20 \times 19 = A_{26}^{8} = \frac{26!}{(26-8)!}$
- minuscules ou majuscules S 1er, chiffres 3 derniers $(26.2)^5 . 10^3 = 52^5 . 10^3$
- 7 caractères minuscules ou majuscules, 2 caractères spéciaux (1S): $C_9^2 \, 52^7 . 15^2$

↳ l'ordre compte
9 places où mettre les 2 caractères spéciaux

- 6 à 10 caractères composés uniquement de minuscules, majuscules, ou caractères spéciaux :

$52+15=67$

$67^6+67^7+67^8+67^9+62^{10}$

$= \sum_{i=6}^{10} 67^i$

- 8 caractères minuscules, majuscules ou caractères spéciaux, au plus 2

$52^8 + 52^7 \cdot 15 \cdot C_8^1 + 52^6 \cdot 15^2 \cdot C_8^2$

↑ pour l'ordre des caractères spéciaux

$= \left(\sum_{s=0}^{2} C_8^s \cdot 52^{8-s} \cdot 15^s \right)$

2) longueur $n \leq K$, pour $K=4, 6, 8$

- sans distinction majuscules / minuscules

$K=4$: $\sum_{n=1}^{4} 26^n = 475\,254$

$K=6$: $\sum_{n=1}^{6} 26^n = 308\,915\,775$

$K=8$: $\sum_{n=1}^{8} 26^n = 217\,180\,147\,158$

avec distinction majuscules / minuscules

$K=4$: $\sum_{n=1}^{4} 52^n = 7{,}48$ million

$K=6$: $\sum_{n=1}^{6} 52^n \approx 20$ milliards

$K=8$: $\sum_{n=1}^{8} 52^n \approx$

Formule générale : $\sum_{n=1}^{K} 26^n = \frac{26(26^K-1)}{26-}$

3) $n=6$, estimer le temps nécessaire si un essai prend 0.1s, 1 microseconde

52^6 possibilité

0.1 s : $52^6 \times 0.1 \approx 1977 \cdot 10^9$ secondes $\simeq$ 2 milliards de secondes, $\frac{1.977 \times 10^9}{3.156 \times 10^7} \approx 62.6$ ans

↑ nb de secondes

1 ms : $T = 52^6 \times 10^{-6} \approx 1977 \times 10^4$

$\approx 5{,}5$ heures

4) système sensible à la casse, système sensible à la casse

↳ bruteforce : 26^n → 52^n

soleil → SoLEil

trouver le mdp : $26^n + \underbrace{2^n}_{\text{trouver maj/min}}$ (soleil) m n m n

borne : (attaque en 2 étapes) : $26^n + 2^n$

5) intérêt + limites d'un gestionnaire de mots de passe

mdp unique et long par service

Inconvenients : mdp maître est un point de défaillance

Exo3 : ---

niveaux de sécurité : NC, C, S, TS

Catégories : OPINT, NUCL, R&D

$L = \{NC, C, S, TS\}$ $P(\text{Catégories}) = P(\{OPINT, NUCL, R\&D\})$

$(N,K) \sqsubseteq (N',K') \Leftrightarrow N \leq N',\ K \leq K'$ ((N',K') domine (N,K) $\ell_1 \sqsubseteq \ell_2$ ℓ_2 ↑ ℓ_1

* écrire vers le haut, lire vers le bas

labels: $\ell_1 = (C, \{OPINT\})$

$\ell_2 = (S, \{OPINT, NUCL\})$

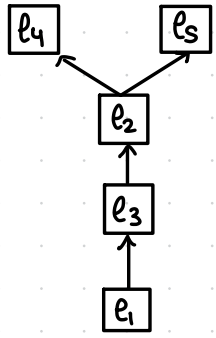
$\ell_3 = (S, \{OPINT\})$

$\ell_4 = (TS, \{OPINT, NUCL\})$,

$\ell_5 = (S, \{OPINT, NUCL, R\&D\})$

$NC \subseteq C \subseteq S \subseteq TS$

1) ordre partiel:



$\ell_1 \sqsubseteq \ell_3$

$\ell_3 \sqsubseteq \ell_2$

$\ell_2 \sqsubseteq \ell_5$

$\ell_2 \sqsubseteq \ell_4$

Un **treillis** est un ensemble partiellement ordonné $(L, \leq)$ tel que, pour toute paire $(a, b) \in L \times L$, il existe :

- une **borne supérieure** (plus petit majorant), notée $a \oplus b$;
- une **borne inférieure** (plus grand minorant), notée $a \otimes b$.
- Un treillis possède un **plus grand élément** (majorant de tous), et un **plus petit élément** (minorant de tous), quand L est fini.

2) a) $\inf(\ell_1, \ell_2) = \ell_1$

b) $\sup(\ell_3, \ell_5) = \ell_5$

c) $\sup(\ell_2, \ell_5) = \ell_5$

3) Mq L x PC Catégories est un treillis fini

$(TS, \{OPINT, R\&D, NUCL\}) \longrightarrow$ max

$(NC, \{\}) \longrightarrow$ min

Ce treillis est 1 produit de 2 treillis fini donc c'est un treilli fini

$L \times P(C)$

↑ {OPINT, R&D, NUCL} → 3 elts

4.2^3 noeuds au total

↑ nb sous ensembles d'un ensemble à 3 éléments.

formule: $4.2^{\text{nb catégories}}$

PARTIE B: No read up , No write Down

identifiant	Nom	Label de sécurité
U_1	Capitaine Thomas	$(\{S, \{OPINT, NUCL\})$
U_2	Colonel Nguyen	$(TS, \{OPINT\})$
U_3	Ingénieur Moreau	$(C, \{OPINT, NUCL, R\&D\})$

identifiant	Label de sécurité
D_1	$(\{C, OPINT\})$
D_2	$(S, \{OPINT, NUCL, R\&D\})$
D_3	$(TS, \{OPINT\})$
D_4	$(S, \{OPINT\})$

pas sa catégorie: ni lire ni écrire

	D_1	D_2	D_3	D_4
U_1	L	E	-	L
U_2	L	-	L,E	L
U_3	L	E	-	-

(si $L_O \subseteq L_U$, $S \leq TC$, $\{NUCL\} \subseteq \{NUCL, Asx\}$)

read down
write UP

TD 2 12/02/2025

Exo 1:

lunlaes satsaduea tebamtmeuiaalfsq ieonun crooaht

1) diamètre ?

n = 45. d = {1, 3, 5, 9, 15, 45}

lunlaes satsaduea tebamtmeuiaalfsq ieonun crooaht

l e s a m i s n o
u s a t t a q u o
n s d e m a i n a
e a u b e l e c h
a t e a u f o r t

diamètre = 5 (nb de lignes)

2) message: les amis nous attaquons demain à l'aube le chateau fort

Chiffrer en utilisant le même diamètre le message: Repas pour demain

n = 15. d = 5 ⇒ 3 colonnes

r e p
o s p
o u r ⇒ roodaesueipprmn
d e m
a i n

Exo 2,

substitution mono alphabetique: 1) chiffrement par décalage
2) chiffrement par substitution

(note: une substitution mono alphabétique est un chiffrement où chaque lettre est remplacée par une autre lettre, et ce remplacement est toujours le même dans tout le message)

Ce nouveau procédé ne renforce pas réellement la sécurité.
Si D est un décalage et S une substitution mono-alphabétique, alors S o D est encore une substitution mono-alphabétique.

Exo 2:

Tableau:

	A	D	F	G	V	X
A	c	l	o	f	w	j
D	y	m	t	s	b	4
F	i	7	a	2	8	s
G	p	3	o	q	h	x
V	k	e	u	e	6	d
X	v	r	g	z	n	9

ex: attaque

① FF | DF | DF | FF | GG | VF | VD

② permutation: $n=4$, $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$ ↓ échange de colonnes

F F D F
D F F F
G G V F
V D X X

⇒

F D F F
F F D F
G V G F
D X V X

⇒ FFGD | DFVX | FDGV | FFFX

③ lecture des caractères de haut en bas de gauche vers la droite

1) Chiffrer le texte:
attaquesurparis le 12 janvier
avec $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 3 & 6 & 4 \end{pmatrix}$

① FF DF DF FF GG VF VD FX VF XD VG VD ADFG AX FF XU XA FA VD XD

② n=6:

F	F	D	F	D	F
F	F	G	G	V	F
V	D	F	X	V	F
X	D	V	G	V	D
A	D	F	G	A	X
F	F	X	U	X	A
F	A	V	O	X	D

⇒

F	F	F	F	D	D
F	F	G	F	G	V
D	V	X	F	F	V
D	X	G	D	V	V
D	A	G	X	F	A
F	F	U	A	X	X
A	F	O	D	V	X

③ message chiffré: FF DD DF AF FV XA FF FG XG GV DF FF DX AD DG FV FX VD VV VA XX

2) Déchiffrer: GFFV FFDFF DDFXG FUDVV XFVVF GXGAD AXDGV FGVFX FFVAF FVV
$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 6 & 2 & 5 & 4 \end{pmatrix}$

① n=6, mettre en colonne: ($9 \times 5 + 3 = 48$, $48 \div 6 = 8$ lignes)

G	F	V	F	D	F
F	F	D	G	G	F
F	D	V	X	V	V
F	D	V	G	F	A
V	F	X	A	G	F
F	X	F	D	V	F
F	G	V	A	F	V
D	F	V	X	X	V

⇒ π^{-1}

V	G	F	F	D	F
D	F	F	F	G	G
V	F	V	D	V	X
V	F	A	D	F	G
X	V	F	F	G	A
F	F	F	X	V	D
V	F	V	G	F	A
V	D	V	F	X	X

⇒ l'attaque du 12 n'a pas eu lieu

Exo4:

1) ligne C, colonne 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
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

mot clé: 'citron'. Chiffrer:

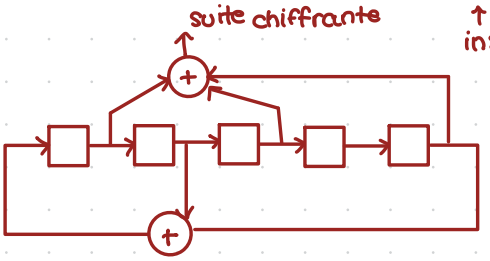
A	t	t	a	q	u	o	n	s	v	e	r	s	a	i	l	l	e	s	
C	I	T	R	O	N	C	I	T	R	O	N	C	I	T	R	O	N	C	
C	B	U	R	E	H	Q	V	L	U	S	E	U	I	B	C	Z	R	U	

TD 3 19/02/2026

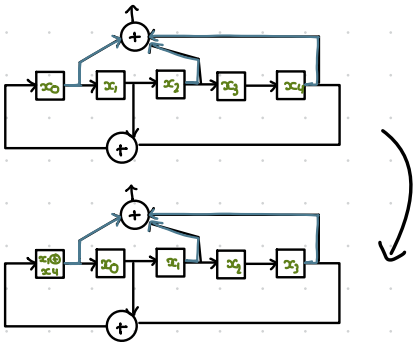
$0 \oplus 0 = 0$
$0 \oplus 1 = 1$
$1 \oplus 0 = 1$
$1 \oplus 1 = 0$

Exo 2 :

Etat interne de 5 bits : 11101 (↑ instant 0)



comment retrouver l'état initial $x_0\, x_1\, x_2\, x_3\, x_4$ (graine) du générateur



$X^{(0)} = (x_0, x_1, x_2, x_3, x_4)$
$\rightarrow z_0 = x_0 \oplus x_2 \oplus x_4 = 1$

$X^{(1)} = (x_1 \oplus x_4,\ x_0,\ x_1,\ x_2,\ x_3)$
$\rightarrow z_1 = (x_1 \oplus x_4) \oplus x_1 \oplus x_3 = x_4 \oplus x_3 = 1$

$X^{(2)} = (x_0 \oplus x_3,\ x_1 \oplus x_4,\ x_0,\ x_1,\ x_2)$
$\rightarrow z_2 = (x_0 \oplus x_3) \oplus x_0 \oplus x_2 = x_3 \oplus x_2 = 1$

$X^{(3)} = (x_2 \oplus (x_1 \oplus x_4),\ x_0 \oplus x_3,\ x_1 \oplus x_4,\ x_0,\ x_1)$
$\rightarrow z_3 = ((x_2 \oplus (x_1 \oplus x_4)) \oplus (x_1 \oplus x_4) \oplus x_1) = x_1 \oplus x_2 = 0$

$X^{(4)} = ((x_0 \oplus x_3) \oplus x_1,\ x_2 \oplus (x_1 \oplus x_4),\ x_0 \oplus x_3,\ x_1 \oplus x_4,\ x_0)$
$\rightarrow z_4 = ((x_0 \oplus x_3) \oplus x_1) \oplus ((x_0 \oplus x_3) \oplus x_0) = x_1 \oplus x_0 = 1$

résolution du système :

On a : $x_0 \oplus x_2 \oplus x_4 = 1$
$x_4 \oplus x_3 = 1$
$x_3 \oplus x_2 = 1$
$x_1 \oplus x_2 = 0$
$x_1 \oplus x_0 = 1$

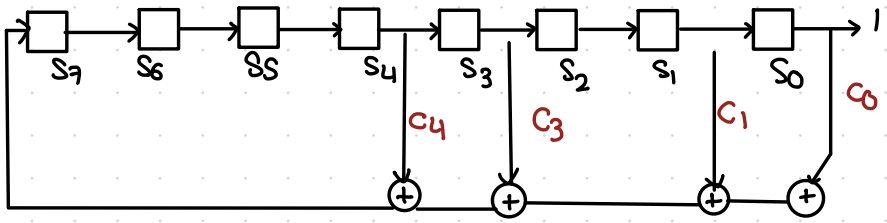
$x_1 \oplus x_2 = 0 \Rightarrow x_2 = x_1$
$x_3 \oplus x_2 = 1 \Rightarrow x_3 = x_2 \oplus 1 = x_1 \oplus 1$
$x_4 \oplus x_3 = 1 \Rightarrow x_4 = x_3 \oplus 1 \Rightarrow (x_1 \oplus 1) \oplus 1 = x_4$
$\Rightarrow x_4 = x_1$
$x_1 \oplus x_0 = 1 \Rightarrow x_0 = x_1 \oplus 1$

$\Rightarrow \begin{cases} x_0 = x_1 \oplus 1 \\ x_1 = x_1 \\ x_2 = x_1 \\ x_3 = x_1 \oplus 1 \\ x_4 = x_1 \end{cases}$

$\Rightarrow X^{(0)} = (x_1 \oplus 1, x_1, x_1, x_1 \oplus 1, x_1)$
$z_0 = (x_1 \oplus 1) \oplus x_1 \oplus x_1 = 1$
$\Rightarrow x_1 \oplus 1 = 1$
$\Rightarrow x_1 = 0$
donc $X^{(0)} = (1, 0, 0, 1, 0)$

Exo 4:

LFSR, m=8 coefs: $(c_0, c_1, c_2, c_3, c_4, c_5, c_6, c_7) = (1,1,0,1,1,0,0,0)$ init par 0xff



donner les 8 premiers octets:

Etat initial: $S_0 = S_1 = \_\_\_\_\_ = S_7 = 1$ (car 0xff)

def d'un LSFR: $s_{n+8} = c_0 s_n \oplus c_1 s_{n+1} \oplus \_\_\_\_\_ \oplus c_7 s_{n+7}$

$= S_n \oplus S_{n+1} \oplus S_{n+3} \oplus S_{n+4}$ en remplaçant les coefficients

$S_8 = S_0 \oplus S_1 \oplus S_3 \oplus S_4 = 1 \oplus 1 \oplus 1 \oplus 1 = 0$

$S_9 = S_1 \oplus S_2 \oplus S_4 \oplus S_5 = \_\_ = 0$

$S_{10} = S_2 \oplus S_3 \oplus S_5 \oplus S_6 = \_\_\_\_\_ = 0$

$S_{11} = S_3 \oplus S_4 \oplus S_6 \oplus S_7 = \_\_\_\_\_ = 0$

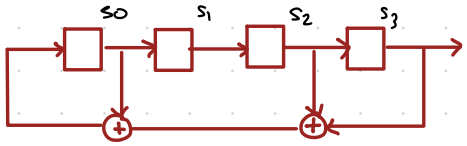
$S_{12} = S_4 \oplus S_5 \oplus S_7 \oplus S_8 = \_\_\_\_\_ = 1$

$S_{13} = S_5 \oplus S_6 \oplus S_8 \oplus S_9 = 1 \oplus 1 \oplus 0 \oplus 0 = 0$

$S_{14} = S_6 \oplus S_7 \oplus S_9 \oplus S_{10} = 1 \oplus 1 \oplus 0 \oplus 0 = 0$

$S_{15} = S_7 \oplus S_8 \oplus S_{10} \oplus S_{11} = 1 \oplus 0 \oplus 0 \oplus 0 = 1$

Exo 5:



1) $(S_0, S_1, S_2, S_3) = (0, 1, 1, 0)$

décalage: $(S_0, S_1, S_2, S_3) \rightarrow (S_1, S_2, S_3, S_4)$

fil de retour: $S_4 = S_0 \oplus S_1 \oplus S_3$

$S_5 = S_1 \oplus S_2 \oplus S_4 = 1$

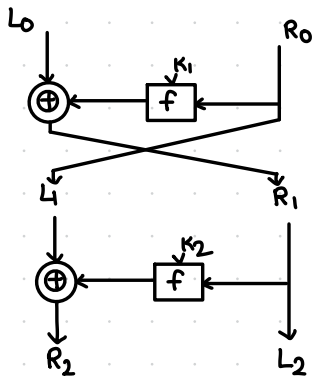
$S_6 = S_2 \oplus S_3 \oplus S_5 = 0$

$S_7 = S_3 \oplus S_4 \oplus S_6 = 1$

$S_8 = S_4 \oplus S_5 \oplus S_7 = 1$

TD 4 19/03/2026

Exo 1 : Réseau de Feistel



$f : \{0,1\}^4 \times \{0,1\}^4 \longrightarrow \{0,1\}^4$

$f(K_{i+1}, R_i) = P(S(K_{i+1} \oplus R_i))$

$P : \{0,1\}^4 \longrightarrow \{0,1\}^4$ $P = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \end{pmatrix}$ ↓ positions des bits (pos0 → pos3)

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

1) Chiffrer $m = 163_{10} = 1010\ 0011_2$ $K_1 = 7$ $K_2 = 12$, $c = (L_2 \| R_2)$

Tour 1 :

$f(K_1, R_0) =$

$K_1 \oplus R_0 = 0111 \oplus 0011 = 0100$

$S(0100) = S(4) = 0011$

$P(0011) = 1100$

m.à.s. $L_1 = R_0 = 0011$

$R_1 = L_0 \oplus f_1(K_1, R_0)$

$= 1010 \oplus 1100 = 0110$

$(L_1, R_1) = (0011, 0110)$

$L_1 = R_0 = 0011$

$R_1 = P(S(K_1 \oplus R_0)) \oplus L_0$

$0111 \oplus 0011$

$0100 = (4)_{10}$

$(3)_{10} = 0011$

$= 1100 \oplus L_0 = 1100 \oplus 1010$

$= 0110$

Tour 2 :

$f(K_2, R_1)$

$K_2 \oplus R_1 = 1100 \oplus 1100 = 1010$

$S(1010) = S(10) = 1110$

$P(1110) = 0111$

m.à.s. $L_2 = R_1 = 0110$

$R_2 = L_1 \oplus f(K_2, R_1) = 0011 \oplus 0111 = 0100$

$L_2 \| R_2 = 0110\ 0100$

$L_2 = R_1$

$R_2 = P(S(K_2 \oplus R_1)) \oplus L_1$

$(10)_{10}$

$(14)_{10}$

$P(1110) = 0111$

$= 0111 \oplus 0011 = 0100$

$(L_2 \| R_2) = (0110\ 0100)$

$= 2^2 + 2^5 + 2^6 = 4 + 32 + 64 = (100)_{10}$

2)

$L_2 = R_1$

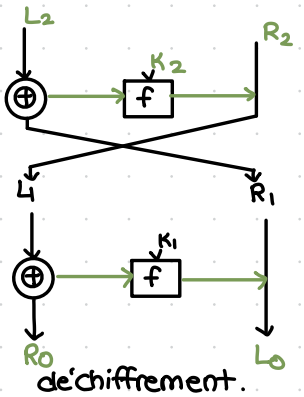
$R_2 = f(K_2, R_1) \oplus L_1$

$\oplus f(K_2, R_1)$

$R_1 = L_2$

$L_1 = R_2 \oplus f(K_2, R_1)$

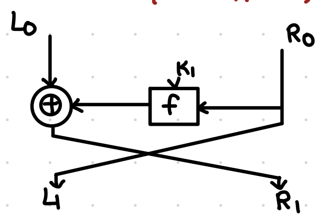
$= R_2 \oplus f(K_2, L_2)$



f n'a pas besoin d'être inversible pour le déchiffrement.

Exo2 :

On veut mq $\overline{DES_K(m)} = DES_{\bar{K}}(\bar{m})$



$m = (L_0 \| R_0)$, $c = (L_1 \| R_1)$

1) Mq $f(\bar{K_1}, \bar{R_0}) = f(K_1, R_0)$ (astuce : $\bar{x} \oplus \bar{y} = x \oplus y$)

$f(\bar{K}, \bar{R_0}) = P(S(\bar{K} \oplus \bar{R_0}))$
$= P(S(K \oplus R))$ $(x \oplus y = \bar{x} \oplus \bar{y})$
$= f(K, R)$

2) Mq lorsqu'on chiffre $m = (\bar{L_0} \| \bar{R_0})$ avec la clé $\bar{K}$ pendant 1 tour on obtient : $(\bar{L_1} \| \bar{R_1}) = \bar{c}$
(Astuce : $\bar{x} \oplus y = \overline{x \oplus y}$)

$\bar{L_1} = \bar{R_0}$
$\bar{R_1} = \bar{L_0} \oplus f(\bar{K_1}, \bar{R_0})$
$= \bar{L_0} \oplus f(K_1, R_0)$ Q1
$= \overline{L_0 \oplus f(K_1, R_0)}$ $(\bar{x} \oplus y = \overline{x \oplus y})$
$= \bar{R_1}$

donc $(\bar{L_1}, \bar{R_1}) = (\bar{R_0}, \bar{R_1}) = \overline{(L_1, R_1)}$

On peut généraliser pour 16 tours de DES

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

3) Déduire une attaque par brute force contre DES avec une complexité en temps dans le pire cas 2^{55} chiffrements.
(Astuce : supposer que l'adversaire qui cherche la clé K possède un bloc de message m et les valeurs $c = DES_K(m)$ et $c' = DES_{\bar{K}}(\bar{m})$)

On connait m, $DES_K(m)$ et $DES_{\bar{K}}(\bar{m})$
↳ on veut retrouver K (56 bits) — attaque force brute : 2^{56}

Pour toutes les clés possibles "candidates"

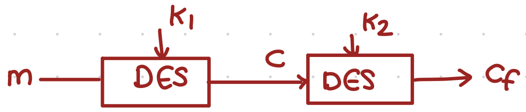
$m \xrightarrow{DES_0(m)} DES_K(m) \stackrel{?}{=} DES_{\boxed{K}}(m)$

$c = DES_{\textcircled{K}}(m)$ <u>1 chiffrement</u>

- si $c = DES_{\boxed{K}}(m)$ <u>2 tests</u>
  → on renvoie $K = \boxed{K}$
- si $c = DES_K(\bar{m})$
  $\textcircled{=}$ $DES_{\bar{K}}(m)$
  ↳ on renvoie $\bar{K}$
  car $DES_K(\bar{m}) = DES_{\bar{K}}(m)$

→ un seul chiffrement permet de tester 2 clés candidats

4)



$(K_1 \| K_2) \rightarrow 112$ bits

Attaque : meet in the middle

① $\forall K_1$ possible : $C_{K_1} = DES_{K_1}(m) \rightarrow 2^{56}$ valeurs
② $\forall K_2$ possible : $C_{K_2} = DES_{K_2}(cf) \rightarrow 2^{56}$ valeurs

$2^{56} + 2^{56} = 2^{57}$

→ on obtient des couples (K_1, K_2) candidats.

③ leve des faux positifs : pour eviter les collisions accidentelles, on utilise un 2ᵉ couple :

\+ <u>Exo3</u> : 500 000 €

mise enforme (caractères commun, mise enforme)

JACK-- 10 5000
①2DFPVXC9IO

JANE-- 500000
②9AXFPC9IOIO

TD 5 02/04/2026 (cours de révisions)