UNIVERSITÉ CÔTE D'AZUR

Cédric Richard

Cryptologie

Exercice 1

On rappelle la correspondence entre l'alphabet classique et les entiers $\{0, \ldots, 25\}$:

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	26

On considère le message : $M =$ `LESMAISONSBLANCHES`

1. Soit $K =$ `ULOIDTGKXYCRHBPMZJQVWNFSAE` la clé de chiffrement par substitution telle que l'application induite s'écrit :

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

   Chiffrer le message M. Quelles propriétés du texte clair et du texte chiffré restent inchangées par un chiffrement par substitution ?

2. Trouver le chiffrement de M par transposition avec la clé $K = [3, 5, 2, 6, 1, 4]$, sachant que cette méthode de codage par bloc consiste à changer l'ordre des lettres selon la règle définie par la clé. Quelles propriétés du texte clair et du texte chiffré restent inchangées par un chiffrement par substitution ?

3. Trouver le chiffrement de M par la méthode de Vigenère avec la clé $K =$ `SECURITE`. Que se passe-t-il par rapport aux fréquences des caractères ainsi chiffrés ?

Exercice 2

Alice souhaite envoyer un message $M \in \mathbb{F}_2^n$ à Bob.

1. Alice et Bob partagent une clé secrète $K \in \mathbb{F}_2^n$. Ils suivent le protocole suivant :

   (a) Alice envoie $C_1 = M \oplus K$ à Bob.

   (b) Bob calcule $C_2 = C_1 \oplus K$.

   Montrer que C_2 correspond bien au message M.

2. Alice possède une clé secrète $K \in \mathbb{F}_2^n$ et Bob une clé $L \in \mathbb{F}_2^n$. Ils suivent le protocole suivant :

   (a) Alice envoie $C_1 = M \oplus K$ à Bob.

   (b) Bob envoie $C_2 = C_1 \oplus L$ à Alice.

   (c) Alice envoie $C_3 = C_2 \oplus K$ à Bob.

   Montrer que Bob peut retrouver le message M. Montrer qu'en interceptant tous les messages, un interlocuteur Oscar peut également retrouver M.

Exercice 3

On considère le cryptosystème défini par la Figure 1. Les boites S_1 et S_2 sont données par :

X	$[0,0]$	$[1,0]$	$[0,1]$	$[1,1]$
$S_1(X)$	$[1,1]$	$[1,0]$	$[0,0]$	$[0,1]$
$S_2(X)$	$[1,0]$	$[0,1]$	$[1,1]$	$[0,0]$

Les clefs de ronde se déduisent de la clé de chiffrement $K = [k_1, k_2, k_3, k_4]$ par :

$$K_1 = [k_1 \oplus k_2, k_2, k_3 \oplus k_4, k_3], \quad K_2 = [k_1 \oplus k_2 \oplus k_3, k_2 \oplus k_3, k_3 \oplus k_4, k_4]$$

La permutation P est définie par :

$$P(1) = 3,\ P(4) = 2,\ P(2) = 1,\ P(3) = 4$$

Chiffrer le message $M = [0,1,1,0]$ avec $K = [1,1,1,1]$. Déchiffrer le message $C = [0,1,0,1]$ chiffré avec la même clé.

Exercice 4

On considère un chiffrement de Feistel à 2 rondes défini par :

- La longueur des blocs est 8;
- La clé $K = [k_1, \ldots, k_8]$ est de longueur 8, les deux clés de ronde sont $K_1 = [k_1, \ldots, k_4]$ et $K_2 = [k_5, \ldots, k_8]$, les k_i étant les bits de la clé K;
- La fonction $V = f(U, K)$ est définie par l'expression des bits v_i de $V = [v_1, \ldots, v_4]$ en fonction de ceux de $U = [u_1, \ldots, u_4]$ et $K' = [k'_1, \ldots, k'_4]$ la clé de la ronde selon :

$$\begin{aligned} v_1 &= u_1 k'_4 \oplus u_2 k'_3 \oplus u_4 k'_3 \\ v_2 &= u_1 k'_2 \oplus u_3 k'_1 \\ v_3 &= u_1 k'_4 \oplus u_1 k'_3 \\ v_4 &= u_3 k'_3 \oplus u_1 k'_1 \end{aligned}$$

1. Soit la clé $K = [1,0,1,1,0,0,1,0]$ et le message $M = [0,1,0,0,0,1,1,1]$. Calculer le message chiffré correspondant à M.
2. Déchiffrer le message $C = [0,1,1,1,0,0,1,1]$ obtenu avec la même clé.

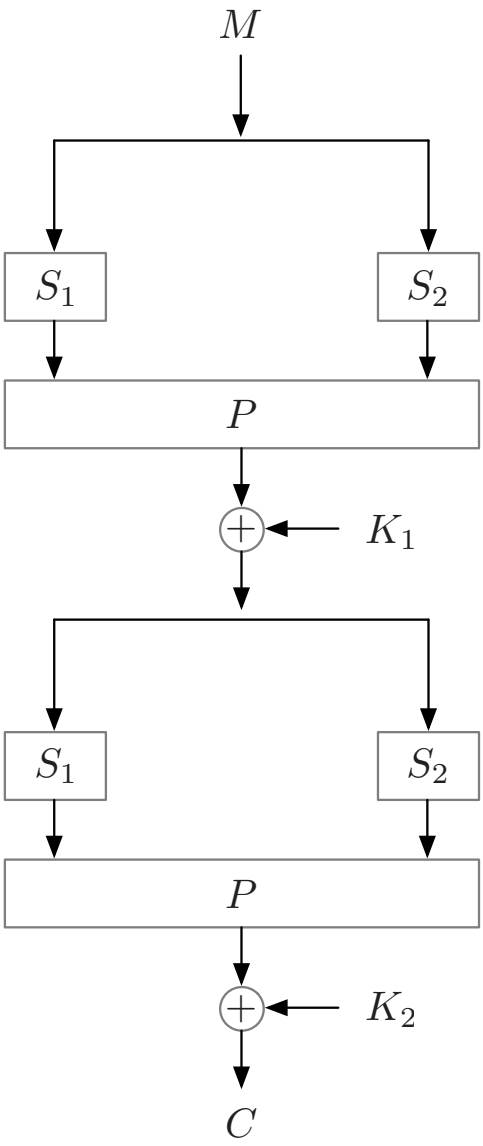

Figure 1: Cryptosystème