**INFO3 Polytech Marseille**

# TD de cryptographie

1) Quels sont les éléments intervenants dans un système de chiffrement symétrique ?

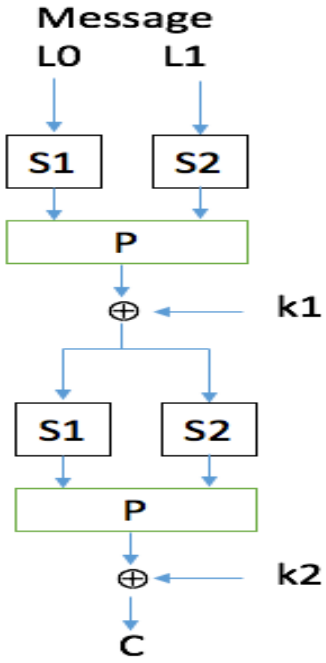
2) Qu'est-ce qu'un algorithme de chiffrement par blocs ?

3) Quels sont les algorithmes principaux utilisé ?

4) Qu'est-ce qu'un schéma de Feistel ?

5) Schéma de Feistel :
Dessiner un schéma de Feistel à 2 tours.
Comment peut-on distinguer un schéma de Feistel à 2 tours d'une fonction aléatoire ?

6) On considère le système de chiffrement par bloc suivant :




Les boites S1 et S2 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 clés de ronde se déduisent de la clé de chiffrement K=[k1,k2,k3,k4] par
K1=[k1⊕k2, k2, k3⊕k4, k3], K2=[k1⊕k2⊕k3, k2⊕k3, k3⊕k4, k4]
La permutation P est définie par
P(1)=3, P(2)=1, P(3)=4, P(4)=2.

Chiffrer le message M=[0,1,1,0] avec K=[1,1,1,1] et déchiffrer C=[0,1,0,1] qui a été chiffré avec la même clé.

7) On considère un chiffrement de Feistel à deux rondes défini par :

La longueur des blocs est 8 ;
La clé K=[k1,…,k8] est de longueur 8, les deux clés de rondes sont K1=[k1,…,k4] et K2=[k5,…,k8], le ki étant les bits de la clé K ;
La fonction V=f(U,U') est définie par l'expression des bits vi de V=[v1,…,v4] en fonction de ceux de U=[u1,u2,u3,u4] et U'=[u'1,u'2,u'3,u'4],

v1 = u1u'4 ⊕ u2u'3⊕u4u'3,
v2 = u1u'2 ⊕ u3u'1,
v3 = u1u'4 ⊕ u1u'3,
v4 = u3u'3 ⊕ u1u'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 chiffré de M à travers ce schéma de Feistel à 2 tours.
Déchiffrer C=[0,1,1,1,0,0,1,1] qui a été chiffré avec la même clé.

8) Qu'est-ce qui compose l'algorithme DES ?

9) Pourquoi DES a-t-il été remplacé ?

10) Dans DES, qu'est-ce-qui permet la confusion, qu'est-ce-qui permet la diffusion ?

11) Comment utilise-t-on généralement un algorithme de chiffrement symétrique ?

12) Quelles sont les longueurs de blocs et de clés dans l'AES ?

13) Quels sont les modes de chiffrement les plus courants ?

14) Mode de chiffrement :
Alice utilise le mode suivant pour chiffrer ses messages. Avec ce mode de chiffrement, la fonction de chiffrement est-elle distinguable d'une fonction choisie aléatoirement ?