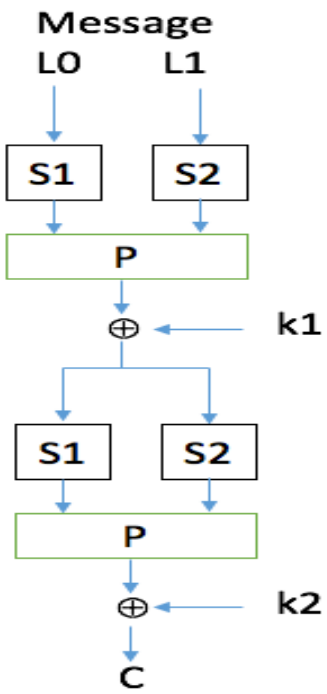
INFO3 Polytech Marseille

TD de cryptographie
Partie I (2h)

1) Dans un stream-cipher, la clé peut-elle être réutilisée ? pourquoi ?
2) Alice et Bob veulent chiffrer des messages à l'aide d'un stream-cipher basé sur un LFSR.
   a) Comment vont-ils procéder ?
   b) Leur stream-cipher sera-t-il sûr ? pourquoi ?
   c) Comment faire pour que leur stream-cipher soit sûr ?
3) Classez les niveaux d'attaques suivant la puissance de l'attaquant (CPA, CCA, ciphertext only attack, known plaitext attack)
4) Un chiffrement déterministe est-il sûr sous CPA ?
5) Dans un système de chiffrement par blocs, la clé peut-elle être réutilisée ?
6) Quel est l'ordre de grandeur de la taille d'une clé dans un système de chiffrement par blocs ?
7) Citez quatre primitives de chiffrement par bloc.
8) Quels sont les points faibles de DES et 3DES ? Qu'est-ce qui compose l'algorithme DES ?
9) Qu'est-ce qu'un schéma de Feistel ?
10) Schéma de Feistel :
   a) Dessiner un schéma de Feistel à 2 tours.
   b) Montrer, en considérant 2 messages distincts ayant une partie droite identique, qu'un schéma de Feistel à 2 tours peut être distingué d'une fonction aléatoire.
11) 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.

Partie II (2h)

12) 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.

13) Dans DES, qu'est-ce-qui permet la confusion, qu'est-ce-qui permet la diffusion ?
14) Quelles sont les longueurs de blocs et de clés dans l'AES ?
15) A quoi sert le mode de chiffrement ? Montrez que ECB n'est pas sémantiquement sûr sous CPA. Citez un mode sûr et parallélisable.
16) Expliquez pourquoi le mode CBC n'est pas sémantiquement sûr sous CPA si l'IV est prédictible.
17) Le mode CBC avec IV aléatoire est-il CCA-sûr ? expliquez pourquoi.
18) 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 ?