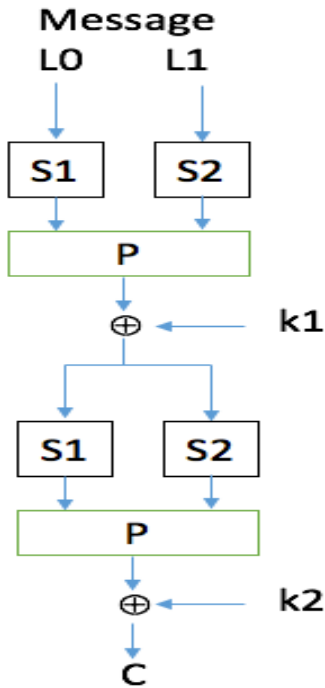


TD de cryptographie Partie I (2h)

- 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) Dans un système de chiffrement par blocs, la clé peut-elle être réutilisée ?
- 4) Quel est l'ordre de grandeur de la taille d'une clé dans un système de chiffrement par blocs ?
- 5) Quels sont les points faibles de DES et 3DES ? Qu'est-ce qui compose l'algorithme DES ?
- 6) Citez quatre primitives de chiffrement par bloc.
- 7) Classez les niveaux d'attaques suivant la puissance de l'attaquant (CPA, CCA, ciphertext only attack, known plaintext attack)
- 8) A quoi sert le mode de chiffrement ? Montrez que ECB n'est pas sémantiquement sûr sous CPA. Citez un mode sûr et parallélisable.
- 9) Un chiffrement déterministe est-il sûr sous CPA ?
- 10) Expliquez pourquoi le mode CBC n'est pas sémantiquement sûr sous CPA si l'IV est prédictible.
- 11) Le mode CBC avec IV aléatoire est-il CCA-sûr ? expliquez pourquoi.
- 12) Qu'est-ce qu'un schéma de Feistel ?
- 13) 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.

Partie II (2h)

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



Les boîtes 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 $K=[k_1, k_2, k_3, k_4]$ par $K_1=[k_1 \oplus k_2, k_2, k_3 \oplus k_4, k_3]$, $K_2=[k_1 \oplus k_2 \oplus k_3, k_2 \oplus k_3, k_3 \oplus k_4, k_4]$

La permutation P est définie par

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

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.

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

La longueur des blocs est 8 ;

La clé $K=[k_1, \dots, k_8]$ est de longueur 8, les deux clés de rondes sont $K_1=[k_1, \dots, k_4]$ et $K_2=[k_5, \dots, k_8]$, le k_i étant les bits de la clé K ;

La fonction $V=f(U, U')$ est définie par l'expression des bits v_i de $V=[v_1, \dots, v_4]$ en fonction de ceux de $U=[u_1, u_2, u_3, u_4]$ et $U'=[u'_1, u'_2, u'_3, u'_4]$,

$$v_1 = u_1 u'_4 \oplus u_2 u'_3 \oplus u_4 u'_3,$$

$$v_2 = u_1 u'_2 \oplus u_3 u'_1,$$

$$v_3 = u_1 u'_4 \oplus u_1 u'_3,$$

$$v_4 = u_3u'_3 \oplus u_1u'_1.$$

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.

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

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

18) 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 ?

