Cryptographie et Sécurité - TD2

guillaume.postic@universite-paris-saclay.fr

Exercice 1 : sécurité sémantique

Soit (E, D) un chiffrement sémantiquement sécurisé où l'espace des messages clairs et l'espace des chiffré est $\{0, 1\}^n$. Quels sont les chiffrements sémantiquement sécurisés parmi les suivants ?
Pour un chiffrement non sécurisé, détailler l'échange des messages entre l'adversaire et le *challenger*, puis calculer l'avantage de l'adversaire sur le protocole.

1. $E'((k, k'), m) = E(k, m) \| E(k', m)$
2. $E'(k, m) = 0 \| E(k, m)$
3. $E'(k, m) = E(k, m) \| MSB(m)$
4. $E'(k, m) = E(0^n, m)$

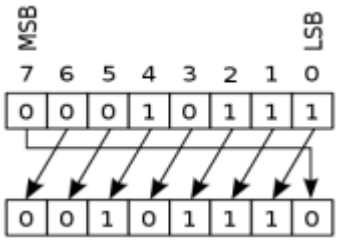
Exercice 2 : réseau de Feistel

En utilisant un réseau de Feistel à deux rondes, chiffrer le texte clair suivant :
`01100010 01100101`

avec les clés de ronde
k_1 : `10101011`
k_2 : `11001101`

et la fonction de ronde
$f(k, \mathrm{R}) = k \oplus$ **[décalage circulaire à gauche sur 4 bits de R]**

Illustration d'un décalage circulaire à gauche sur 1 bit :



Exercice 3 : Mode d'opération

Soit un chiffrement par bloc de 3 bits défini dans la table ci-dessous et soit un message clair m = `011011011`

1. Produire le chiffré de m en utilisant le chiffrement par bloc avec le mode ECB.
2. Supposons que Trudy intercepte le chiffré. Supposons aussi qu'elle sache que le texte a été chiffré avec un chiffrement par bloc de 3 bits en mode ECB, mais sans connaître le chiffrement spécifique. Que peut-elle trouver à propos du message clair ?
3. Produire le chiffré de m en utilisant le chiffrement par bloc avec le mode CBC, en utilisant le vecteur d'initialisation `010`.

Entrée	Sortie	Entrée	Sortie
`000`	`001`	`100`	`010`
`001`	`100`	`101`	`110`
`010`	`111`	`110`	`011`
`011`	`000`	`111`	`101`

Exercice 4 : réseau S-P

Calculer une ronde du réseau S-P suivant.
La taille de bloc est de **1 octet**, avec une S-box de **4 bits** pour chaque moitié du bloc.
La P-box est décrite par une permutation sous la forme $(a, b, c, \ldots, p)$, où le bit a de l'entrée devient le bit b de la sortie, le bit b en entrée devient le bit c en sortie et ainsi de suite, jusqu'à ce que le bit p en entrée devienne le bit a en sortie.

S-Box :

in	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
out	9	3	7	E	C	A	1	8	4	0	F	6	B	2	D	5

P-Box : **(0, 3, 1, 6, 2, 4, 5, 7)**, les positions étant numérotées de gauche à droite

Si l'entrée est `0B`, quelle est la valeur de l'octet de sortie après une seule ronde ?