Faculté de Technologie

Département Ingénierie des Systèmes Electrique

Cryptographie et sécurité réseaux

Série de TDN°2

Exercice 1 :

1. Réaliser la substitution en utilisant la S-Box de la matrice

00	47	A5	27
38	5F	24	FD
AE	05	69	BF
65	BA	FF	04

2. Appliquer le XOR pour les deux premiers et derniers octets en utilisant la clé

65	41	27	A5
38	50	FD	24
A1	79	BF	69
95	B2	04	F

Exercice 2 :

Dans le cas de l'AES à clé 192 bits.

65	38	A1	95	8F	5B
41	50	79	B2	5B	A2
27	FD	BF	04	28	59
A5	24	69	FF	4A	23

1. On désire chiffrer un bloc de 128bits, donner les deux premières sous clés.
2. Ayant le message suivant donner le résultat du premier octet avec chaque sous clés.

00	47	A5	27
38	5F	24	FD
A2	D5	69	BF
65	BA	FF	04

Exercice 3 :

Donner le résultat en appliquant le shift row sur le bloc

4A	47	A5	27
AE	05	69	BF
A2	D5	60	1F
65	BA	FF	04

Exercice 4 :

Donner la suite chiffrante et la complexité linéaire du LFSR. Le polynôme de rétroaction est : $p(x) = 1 + x + x^4$

L'état initial est 0110.