

Faculté de Technologie
Département Ingénierie des Systèmes Electrique
Cryptographie et Sécurité Réseaux
Série TDN°1

Exercice 1 :

En utilisant la transposition périodique, chiffrer le message suivant : « mastertélécommunications ». On donne la clé : 12345 vers 45213.

Exercice 2 :

1. Chiffrer le message « transpositionrectangulaire » en utilisant la transposition rectangulaire avec la clé : rouge.
2. Décrypter le message « psoxeeulroapmiaensrcophenxeixa » sachant que la méthode appliquée est la transposition rectangulaire en utilisant la clé michel.

Exercice 3 :

Crypter la séquence 110111 en utilisant deux tours de Feistel.

On donne F1 1 2 3 vers 2 3 1.

F2 NOT

Exercice 4 :

1. Quel est le résultat de chiffrement du texte « TELE » en utilisant trois tours de l'algorithme de Feistel :

On donne F1 : Rotation à gauche

F2 : 5A XOR

F3 : rotation à droite

2. Déchiffrer la séquence 11101000 sachant que le chiffrement utilisé est Feistel à deux tours.

On donne F1 : A XOR

F2 : complément à 2.

Exercice 5 :

1. Donner la permutation initiale de DES pour la séquence 0111111000001111.
2. Appliquer la duplication pour les bits 4, 12, 13, 16.
3. Générer toutes les sous clés (12bits) possibles à partir de la séquence 010111100101110 en adoptant un décalage de 3 bits.

Exercice 6 :

1. Réaliser la permutation expansive pour la séquence 110111011111110 prenant une table de 4x6.
2. Appliquer le xor en utilisant la sous clé 111100001101010111001101
3. Donner le résultat de permutation p de la séquence résultats.

Exercice 7 :

Donner la permutation finale de la séquence 10111101 00011111 11011111 10101000 000000000 1111011 10000001 11110111

Exercice 8 :

Réaliser les étapes suivantes sur la séquence : 1111001100011110.

1. Donner la permutation initiale
2. Diviser en deux blocs G1 et D1

3. En appliquant l'algorithme de Feistel, calculer G2.

4. Calculer D2 sachant que la fonction est

-permutation expansive 2x6.

-la clé utilisée est 1110111110001101

-appliquer la permutation compressive en éliminant les bits répétitifs.

5. donner la permutation finale.