Université Mohammed V-Agdal
Faculté des Sciences de Rabat

Département d'Informatique

Année Universitaire 2020-2021
2ième année du Master
(Sécurité & Cryptographie)

Série 3
(Les cryptosystème DES et IDEA)

Problème 1

Notation : on désigne par C_i le côté gauche de la ième sous clé dérivée K_i et par D_i son côté droit

1) Montrer que les chaînes C_{16} et D_{16} du DES sont obtenues à partir de C_1 et D_1 par un décalage en permutation circulaire de 1 cran vers la droite.

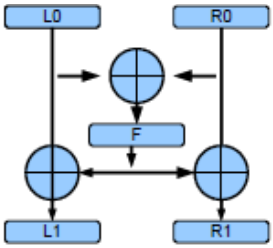
2) On suppose que $K_1 = K_2 = \ldots = K_{16}$. Montrer que les bits de C_1 sont égaux de même que tous les bits de D_1.

3) En déduire qu'il existe exactement 4 clés du DES qui donnent des clés des tournées toutes égales ; on les appelle les clés faibles du DES.

4) Déterminer les clés faibles du DES.

Problème 2

Une version originale de l'algorithme IDEA est basée sur un mécanisme de Feistel (dit Feistel modifié), schématisée ci-dessous :



1) Que pensez-vous de la taille des blocs et des clés d'IDEA comparés à DES et dans l'absolu du point de vue sécurité ?
2) Ecrire les équations donnant l'expression du chiffré (L1, R1) en fonction du clair(L0, R0)
3) Montrer que ce schéma est inversible quelque soit F et donner les formules décrivant le déchiffrement.

4) Décrivez un schéma de Feistel 3 tours équivalent au schéma utilisé par IDEA. On prendra le schéma ci-dessous pour le 3ième tour (Feistel modifié).