Département d'informatique **13/03/2020**

3ème année Licence

Module : Cryptographie

Série 4 (Cryptographie moderne)

Exercice 1 : *(Chiffrement DES)*

Soit le message clair: **0123456789ABCDEF** et la clé : **133457799BBCDFF1**.
Calculez :

- Appliquer *PI* sur le message clair.
- Déterminer L_0 et R_0.
- Calculer K_1
- Calculer $E(R_0) \oplus K_1$
- Le message crypté après le round 1 (étape 1)

Exercice 2 : *(RSA)*

Soit p = 7 et q= 19

- Calculer N et Φ (n).
- On propose e = 5. Calculer la clé privée d.
- Chiffrer le message clair m =6.
- Déchiffrer le message chiffré c= 62.

Exercice 3 : *(RSA)*

- Déchiffrer le message reçu 18 chiffré avec la clé publique (35;11).
- Chiffrer le message M = 10 avec la clé publique (55;7). Calculer p; q et d. Déchiffrer C = 35.

Exercice 4 : *(EL GAMAL)*

Prenons p = 2357 et g = 2 qui est d'ordre maximal 2356.

- Bob choisit a = 1751; calculer la valeur de b.
- Déduire la clé publique et la clé privée.
- Si Alice choisit k = 1520, chiffrer le message m = 2035.