République Algérienne Démocratique et Populaire
الجمهورية الجزائرية الديمقراطية الشعبية
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
وزارة التعليم العالي والبحث العلمي

École Supérieure en Informatique
08 Mai 1945 – Sidi Bel Abbes–

المـدرســـــة العـــلـــيا للإعـــــلام الآلـــي
08 ماي 1945–ســـيـــدي بـــلـــعـــبـــاس

Introduction à la Sécurité Informatique

Examen Correction **Durée : 2h**

Questions de cours : (6pts)

1. Qu'apporte le chiffrement de Vigénère en matière de sécurité par rapport à une simple substitution (e.g., César cipher) ?
   Solution.
   Vigénère cipher apporte un plus car une même lettre peux être chiffre différemment dans le plaintext (texte en clair), ce qui complique l'analyse statistique. (1pts)
2. Sur quel concept cryptographique repose DES et AES cipher algorithms?
   Solution.
   DES repose sur Feistel Network (1pts)
   AES repose sur Substitution et Transposition (Subbytes (0.25pts), ShiftRows (0.25pts), MixColumns (0.25pts), AddRoundKey (0.25pts)) (1pts)
3. Quel est le type de chiffrement pour lequel sont définis les modes de chiffrement ?
   Solution.
   Le chiffrement symétrique par bloc (block ciphers) (1pts)
4. Que signifie les concepts de **confusion** et de **diffusion** en cryptographie ?
   Solution.
   La **confusion** correspond à une volonté de rendre la relation entre la clé de chiffrement et le texte chiffré la plus complexe possible. (1pts)
   La **diffusion** est une propriété où la redondance statistique dans un texte clair (plaintext) est dissipée dans les statistiques du texte chiffré (ciphertext). (1pts)

Exercice 1 : (8pts)

1. Soit le schéma de chiffrement DES illustré dans la **figure 1.**
   1.1 Donner la taille des éléments **P**, **C**, **Li**, **Ri** et **Ki** (i=1..16)
   Solution.
   La taille des éléments : **P**=64bits (0.25pts), **C**=64bits (0.25pts), **Li** =32bits (0.25pts), **Ri** =32bits (0.25pts), **Ki**=48bits (0.25pts). (1.25pts)
   1.2 Dans un chiffrement de DES, si on a l'égalité entre les sous clés comme suit : k1=k16, k2=k15, k3=k14, k4=k13, k5=k12, k6=k11, k7=k10, k8=k9, quel est le problème qu'on va avoir lors des opérations de chiffrement multiples ? ce problème est dû à quoi ?
   Solution.
   Quel est le problème qu'on va avoir lors des opérations de chiffrement multiples ? :
   Le chiffrement d'un résultat de chiffrement nous donnera le texte en clair. (1pts)
   Ce problème est dû à quoi ? :
   Car le processus de déchiffrement consiste à appliquer le même schéma de chiffrement avec l'ordre des clés inversé, et comme l'ordre k1…k16=k16…k1, le fait de chiffrer deux fois un message reproduira le même message en clair $(DES_K(DES_K(m)) = m)$ (1pts)

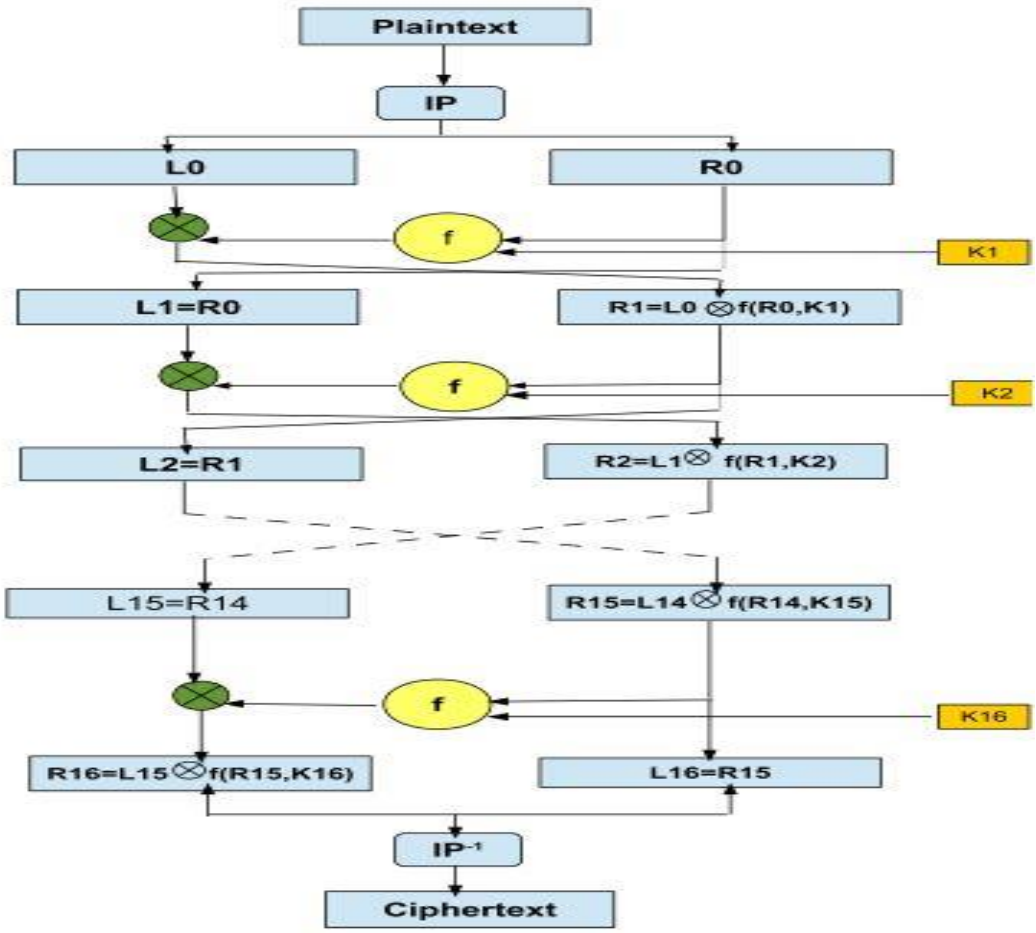

Figure 1. Chiffrement DES

2. Soit le mode de chiffrement CBC de la **figure 2.**

2.1 Donner ses formules de chiffrement et celles de déchiffrement.

Solution.

Formule de chiffrement : $c_i = E_k(m_i \oplus c_{i-1})$, i=1..n (1pts)

Soit $E_k^{-1}()$ la fonction inverse de $E_k()$ (0.5pts). **Le déchiffrement sera :** $m_i = c_{i-1} \oplus E_k^{-1}$ (0.5pts). (1pts)

2.2 Combien de blocs seront mal déchiffrés si un bloc C_i a été altéré durant la transmission ?

Solution.

$i \neq n$ (2blocs) (0.5pts)

$i = n$ (1bloc) (0.25pts)

2.3 Proposer une modification sur le schéma CBC, pour ne pas avoir à définir la fonction inverse de E_K lors du processus de déchiffrement.

Solution.

Le mode CFB (1pts) : **chiffrement :** $c_i = m_i \oplus E_k(c_{i-1})$ (0.5pts); **déchiffrement :** $m_i = c_i \oplus E_k(c_{i-1})$ (0.5pts)

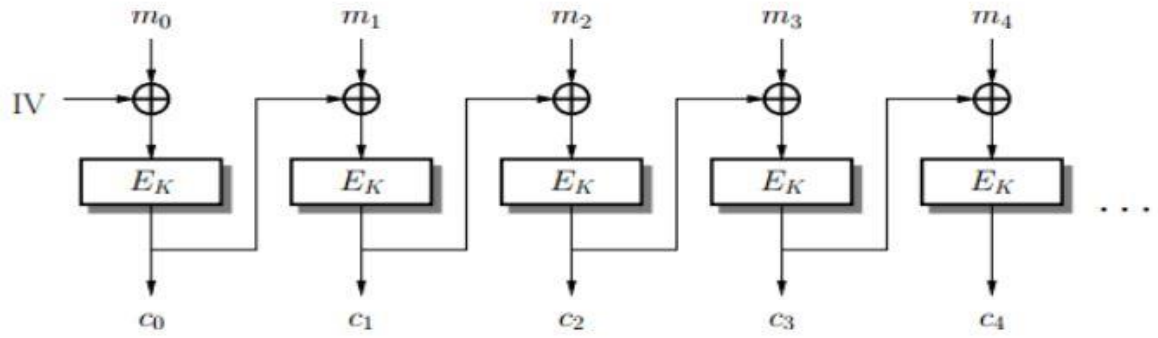

Figure 2. Mode CBC

Exercice 2 : (6pts)

On utilise les notations habituelles du chiffrement RSA : N est un entier et p et q sont deux entiers premiers tels que $N = p.q$. On note φ l'indicatrice d'Euler $\varphi = \varphi(N) = (p-1)(q-1)$ et e et d sont deux éléments de Z/NZ tels que $ed = 1\ mod\ \varphi$.

1. On souhaite utiliser l'algorithme de chiffrement RSA
   a) Comment chiffre-t-on un message m ?
      Solution.
      Chiffrement : on convertit le message en un entier $m \in [1, N]$ (0.5pts) et on calcule le chiffre : $\boldsymbol{c = m^e\ mod\ N}$ (0.5pts)
   b) Et comment déchiffre-t-on un message c ?
      Solution.
      Déchiffrement : on calcule : $\boldsymbol{m = c^d\ mod\ N}$ (1pts)
   c) Parmi les entiers N, p, q, φ, e et d quels sont ceux qui doivent rester secrets ?
      Solution.
      $\boldsymbol{p, q, \varphi}$ et **d** doivent rester secrets. (1pts)

2. On pose $N = 1003$ et $e = 3$
   a) Calculer p, q et φ
      Solution.
      La factorisation de N donne $p = 59$ et $q = 17$ (ou l'inverse). (0.5pts)
      L'entier φ vaut alors $58 \times 16 = 928$ (0.5pts)
   b) Que vaut alors l'entier d associé à e ?
      Solution.
      En utilisant l'algorithme d'Euclide, nous obtenons : $928 = 3 \times 309 + 1$ (1pts)
      Donc $1 = 928 + 3 \times (-309)$ et l'inverse de e=3 mod φ est 619 (=928-309)
   c) Que vaut le message chiffré c associé au message clair $m = 4$?
      Solution.
      Le chiffre c vaut $4^3 = 64$ (0.5pts)
   d) Dans ce cas particulier, est-il possible de retrouver m à partir de c sans connaitre d ?
      Solution.
      Il est facile connaissant cette valeur de retrouver $m = 64^{1/3}$ (0.5pts)