Correction

Exercice 1 :

12. …… signifie que les informations contenues dans un système informatique ne sont accessibles en lecture que par les personnes autorisées.
    a. Authentification
    b. Confidentialité
    c. Intégrité
    d. Disponibilité
13. ……. signifie que les systèmes actifs informatiques ne peuvent être modifiés que par les personnes autorisées.
    a. Authentification
    b. Confidentialité
    c. Intégrité
    d. Disponibilité
14. Parmi les attaques ci-après, lesquelles vise la disponibilité:
    a. Usurpation d'identité
    b. Déni de service
    c. Modification du journal
    d. Bombardement et saturation du réseau
15. Le rôle de la sécurité en entreprise est de :
    a. Réduire les risques à niveau acceptable
    b. Prévenir tout risque
    c. Empêcher les utilisateurs de travailler librement
    d. Surveiller le bon fonctionnement des systèmes
16. L'une des importantes vulnérabilités dans le SI d'entreprises :
    a. L'inexpérience et risque lié aux utilisateurs
    b. La présence de ports USB sur les PCs
    c. L'utilisation des mots de passe au lieu de méthodes plus sures
    d. Les connexions à réseau local
17. Un risque:
    a. est un danger éventuel plus ou moins prévisible.
    b. Il signifie la probabilité qu'une menace exploitera une vulnérabilité du système.
    c. est l'ensemble des actions réalisées en prévention de la menace.
18. Quelle procédé permettant d'assurer l'intégrité des données?
    a. Chiffrement symétrique
    b. Chiffrement asymétrique
    c. Fonction de hachage
    d. Certificat numérique
19. Quelle est la meilleure manière pour protéger l'information confidentielle ?
    a. Un bon anti-virus sur mon ordinateur.
    b. Un bon système de chiffrement du disque dur de mon ordinateur.
    c. Un pare-feu (firewall) efficace et surtout bien configuré sur mon ordinateur.
    d. Aucune des techniques ci-dessus ne répond totalement au besoin.
20. Parmi les propositions suivantes, laquelle ne concerne pas par les aspects techniques de la sécurité:
    a. Vol de matériel informatique
    b. Détection de l'intrusion
    c. Plan de sauvegarde
    d. Licence de logiciel
21. La sécurité de l'exploitation traite les points suivants:
    e. Conception du code source de l'application
    f. Gestion des incidents et leur résolution
    g. Plan de sauvegarde
    h. Plan de secours
22. Quelle dimension ne fait pas partie de l'architecture de sécurité informatique?
    e. Dimension technique
    f. Dimension monétaire
    g. Dimension organisationnelle
    h. Dimension juridique

Exercice 2:

1. ***Donner la différence entre l'identification et l'authentification.***
   Identification = connaitre d'identité d'une entité (qui je suis).
   Authentification = prouver d'identité d'une entité (prouver que je suis celui que je prétends être)

2. ***Quelle est la relation entre : l'authentification, l'intégrité et non-répudiation ?***
   La relation est d'inclusion: intégrité $\subset$ authentification $\subset$ Non-repudiation

3. ***Donner des exemples sur les attaquants dans le monde réel.***
   - Un gouvernement

- Un criminel ou un terroriste
- Espion industriel ou commercial (concurrent) Howawi Samsung
- Employé interne

4. ***Pourquoi les pirates s'intéressent-ils aux SI des entreprises?***
   - Gains financiers: accès à de l'information, puis monétisation et revente (fichiers clients, utilisateur, emails, mots de passe, …)
   - Utilisation de ressource: bande passante et espace de stockage, Zombies (botnets).
   - Chantage: empêcher l'accès aux ressources
   - Récupérer des informations sur le système: espionnage industriel/concurrentiel, étatique.

5. ***Quelle est la différence entre la sécurité informatique et la cybersécurité ?***
   - la sécurité informatique concerne l'ensemble des systèmes informatisés liés ou non à internet ou à des réseaux.
   - la cybersécurité concerne par les systèmes informatisés liés à internet ou en réseau.

Université de M'sila
Faculté de MI
Département d'informatique
Niveau: 3ème Licence – SI **Module :** ***Sécurité Informatique***

TD N°02

Cryptographie Classique

Exercice N° 01:

1. Trouver les coefficients *u*, *v* et le *PGCD* des nombres entiers suivants:
   - (a, b)= (60, 19)

     60 = 19* 3 + 3 ➔ 3=60-19*3

     19 = 3*6 + 1 ➔ 1=19-3*6 = 19- (60-19*3)*6

     1= 19*19 – 60*6

     u=-1, v=19, PGCD=1
   - (a, b)= (280,11)

     u=-2, v=51, PGCD=1
   - (a, b)= (38, 26)

     u=-2, v=3, PGCD=2
2. Calculer l'inverse de :
   - 41^{-1} mod 53.

     Pour calculer l'inverse modulaire de 41 mod 53, on utilise l'algorithme Eclude étendu afin de trouver le PGCD(53,41) et le coefficient v. La condition est PGCD=1

$$\underbrace{(53)}_{A} \times \underbrace{-17}_{u} + \underbrace{(41)}_{B} \times \underbrace{22}_{v} = \underbrace{1}_{\mathrm{PGCD}(A,B)}$$

     v=22, alors 41^{-1} mod 53 = 22

   - 317^{-1} mod 521

$$\underbrace{(521)}_{A} \times \underbrace{-101}_{u} + \underbrace{(317)}_{B} \times \underbrace{166}_{v} = \underbrace{1}_{\mathrm{PGCD}(A,B)}$$

     v=166, alors 317^{-1} mod 521=166
   - 24^{-1} mod 512

$$\underbrace{(512)}_{A} \times \underbrace{1}_{u} + \underbrace{(24)}_{B} \times \underbrace{-21}_{v} = \underbrace{8}_{\mathrm{PGCD}(A,B)}$$

     PGCD(512,24)=8 ≠1. Alors, il n'existe pas
3. Résoudre les équations suivantes:
   - 19x ≡10 mod 60

     19x ≡10 mod 60

     x=10*19^{-1} mod 60

     On calcule tout d'abords 19^{-1} mod 60 = 19 (voir la première question)

     x=10*19 mod 60 = 10

Exercice N° 02: (*Chiffrement par décalage*)

1. Ecrire un pseudo-code de chiffrement/déchiffrement d'un texte avec César.

Chiffrement:

```
char indtolettre (int ind)
int j=0;
while j<26
{ if j== ind
     return alph[j] j
   else j++
}
```

Déchiffrement:

```
l = length(p);
k1=chartoindex (k)
for (i:=0; i< l; i=i+1 )
p[i]= indtolettre (lettretoind (p[i]) – k1 + 26 % 26  )
```

```
char p[], c[], k
char alph[] = {'A','B','C', …., 'Z'}   % tableau de l'alphabet
int l, I, k1
l = length(p);
k1=chartoindex (k)
for (i:=0; i< l; i=i+1 )
c[i]= indtolettre (lettretoind (p[i]) + k1 % 26)

int  lettretoind (char lettre)
int j=0;
while j<26
{ if t[j]== lettre
     return j
   else j++
}
```

2. Prouver que $D_k(E_k(m))=m$.

   Soient $c=E_k(m)= m + k \bmod 26$ et $m=D_k(c)= c – k \bmod 26$

   $D_k(E_k(m))= D_k(m + k \bmod 26)= (m + \cancel{k} \bmod 26) – \cancel{k} \bmod 26$

   $= m$

3. Chiffrer le texte «CRYPTOGRAPHIE» avec la clé **K**.

   On applique la fonction de chiffrement $E_k(m)= m + k \bmod 26$ où k= 10

Texte clair	C	R	Y	P	T	O
Indice. Clair	2	17	24	15	19	14
Clé	K	K	K	K	K	K
Indice. Clé	10	10	10	10	10	10
Ind. Chiff	12	1	8	25	3	24

Texte chiffré	M	B	I	Z	D	Y

E_k(CRYPTOGRAPHIE)= MBIZDYQBKZRSO

4. Déchiffrer le texte « JOPMMYLTLUAZFTLAYPXBLJSHZZPXBL » avec la clé **H**.

On applique la fonction de déchiffrement $D_k(c)= c – k \bmod 26$ où k= 7
(Dans le tableau, chiffrer seulement le mot "CHIFFREMENT")
D_k(JOPMMYLTLUAZFTLAYPXBLJSHZZPXBL)= CHIFFREMENTSYMETRIQUECLASSIQUE

Exercice N° 04: (*Chiffrement Vigenère*)

1. Ecrire un pseudo-code de chiffrement/déchiffrement d'un texte avec Vigenère.

```
Input: char p[], chair k[]
Output: chair c[]

l= length(cle)
For i=0 to length(p)-1
    c[i]= indtolettre(lettretoind(p[i]) + lettretoind(k[i%lc]) % 26)
```

2. Chiffrer le texte «CRYPTOGRAPHIE » avec la clé « SECRET ».
   On applique la fonction de chiffrement $\mathbf{E_k(x_1,x_2,\ldots, x_n) = (x_1 + k_1, x_2 + k_2, \ldots, x_n + k_n)}$
   $\mathbf{E_k}$(CRYPTOGRAPHIE)= UVAGXHYVCGLBW
3. Déchiffrer le texte «ORABCNDIBDIVD» avec la clé « KEY»:
   On applique la fonction de déchiffrement $\mathbf{D_k(y_1,y_2,\ldots,y_n) = (y_1 – k_1, y_2 – k_2 ,\ldots, y_n – k_n)}$
   $\mathbf{D_k}$(ORABCNDIBDIVD)= ENCRYPTEDTEXT

Exercice N°05: (*Chiffrement affine*)

Soit K= (5,11)

1. Prouver que $D_k(E_k(m))=m$

- $E_k(x) = a.x + b \bmod 26$
- $D_k(y) = a^{-1}. (y-b) \bmod 26$

$D_k(y) = a^{-1}. (y-b) \bmod 26 = a^{-1}. (a.x + b -b) \bmod 26$
$= a^{-1}. a.x \bmod 26$
$= x$

2. Calculer les fonctions de chiffrement et de déchiffrement,

Soit K=(5,11)

$E_k(x) = 5x + 11 \bmod 26$
On calcule $5^{-1} \bmod 26$
$26 = 5 * 5 + 1 \Rightarrow 1 = 26 – 5*5$
$5^{-1} \bmod 26 = -5 = -5 + 26 = 21$
Alors $D_k(y) = 21(y-11) \bmod 26 = 21y – 21*11 \bmod 26 = 21y – 23 \bmod 26 = (21y + 3 \bmod 26)$

3. Chiffrer le mot suivant: "AFFINE"

Utilise un tableau comme l'exercice 2 et en appliquant la fonction $E_k(x) = 5x + 11 \bmod 26$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Université de M'sila
Faculté des MI
Département d'informatique
Niveau: 3ème Licence – SI **Module :** ***Sécurité Informatique***

TD N°03

Chiffrement symétrique moderne

Exercice N° 01: *schéma de Feistel*

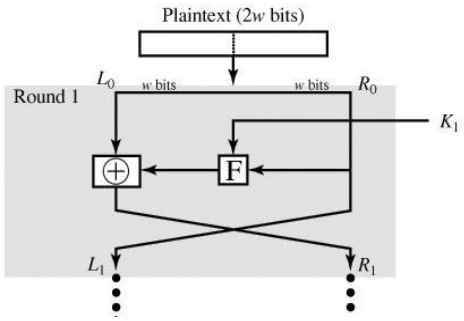
1. Ecrire les formules de chiffrement avec le schéma de Feistel selon l'itération i,

   $L_i = R_{i-1}$,
   $R_i = L_{i-1} \oplus F_K(R_{i-1})$

2. Ecrire les formules de déchiffrement avec ce schéma selon l'itération i,

   $R_{i-1} = L_i$
   $L_{i-1} = R_i \oplus F(R_i, K_i)$

3. Dessiner ce schéma pour le chiffrement



4. Appliquer ce schéma sur:
   - Le bloc: 11010110
   - La clé: 1010
   - F(x,k)= x or k
   - $K_i = k_{i-1}$ xor 1011
   - Nombre d'itérations: 3.

i	1	2	3
L	0110	1111	1101
R	1111	1101	0110
K	1010	1011	1011

Le bloc chiffré est: 11010110

Exercice N° 02: *AES*

1. Définir les quatre transformations de l'AES

   SubByte: substitution d'octets dans le tableau d'état

   ShiftRow: décalage de rangées dans le tableau d'état

   MixColumn: déplacement de colonnes dans le tableau d'état (sauf à la dernière ronde)

   AddRoundKey: addition d'une "clé de ronde " qui varie à chaque ronde.

2. Appliquer SubBytes à l'octet (01001001).

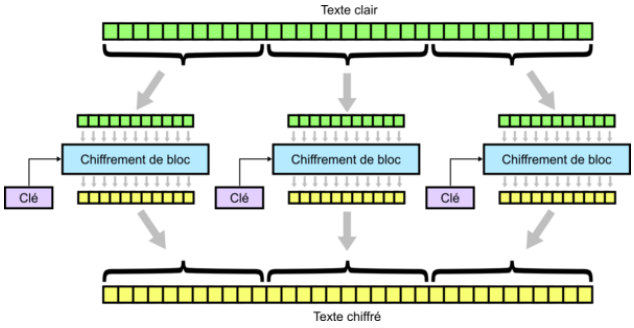
0100 1001

4 9 ➔ on utilise la matrice S-box pour trouver la valeur de ligne 4 et la colonne 9

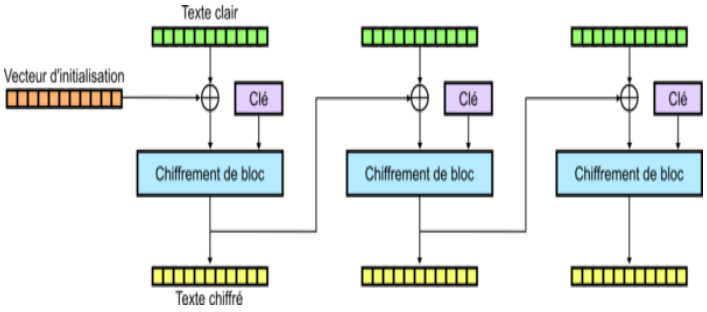
Le résultat est **3b**, alors le nouveau octet est: **00111011**

Exercice N° 03: *Modes d'opération*

Soient les schémas des modes d'opération de chiffrement symétrique :



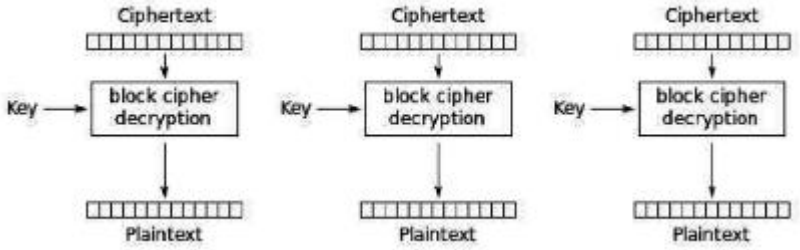
(1) ECB



(2) CBC

1. Le mode **ECB** :

- Dessiner le schéma de déchiffrement.



- Déduire les fonctions de chiffrement / déchiffrement.

  Chiffrement: Ci = EK(Pi)

  Déchiffrement: Pi = DK(Ci)

- Quel est le problème de ce mode ?

  Le problème de reconnaitre du message en clair dans celui chiffré.

- Calculer le texte chiffré:

M = 101100011011101

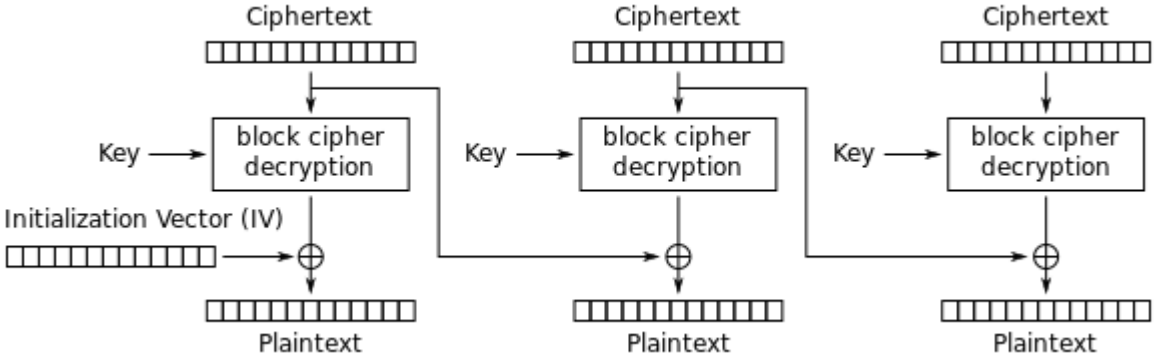
On découpe le texte clair en blocs. Nous avons une clé de taille 4 bits, alors la taille du bloc est 4 bits.

B1=1011, B2=0001, B3=1011, B4=101**0** (ajouter un bit dans le bit de poids faible (LSB) de valeur 0)

Le texte chiffré est: 0111001001110101

2. Le mode **CBC** :

- Dessiner le schéma de déchiffrement.



- Déduire les fonctions de chiffrement / déchiffrement.

  Chiffrement: C1 = EK(P1 $\oplus$ VI) Ci = EK(Pi $\oplus$Ci-1)

  Déchiffrement: C0 =VI Pi = DK(Ci) $\oplus$Ci-1

- Calculer le texte chiffré:

  On applique la fonction de chiffrement après découper le message en blocks.

  0010011010110010

Université de M'sila
Faculté de MI
Département d'informatique
Niveau: 3ème Année Licence – SI **Module :** ***Sécurité Informatique***

TD N°04

Exercice N° 01: *(Chiffrement RSA)*

Soit p = 7 et q= 19

1. Décrire le schéma de génération de clés, schéma de chiffrement, et schéma de déchiffrement.

   Voir le cours

2. Montrer que D(E(m)) = m.

   $D(E(m))= D(m^e \bmod n)= (m^e)^d \bmod n= m^{ed} \bmod n$

   sachant que $ed= 1 \bmod \Phi(n) = k\Phi(n)+1$

   alors $D(E(m))= m^{k\Phi(n)+1} \bmod n = m$

3. Calculer N et Φ (n).

   $N = pq = 133$ et $\Phi(n) = (p-1)(q-1) = 108$

4. On propose e = 5. Calculer la clé privée d.

   $d.e = 1 \bmod \Phi(n)$ _ $d = e^{-1} \bmod \Phi(n)$

   $d=5^{-1} \bmod 108 = 65$

5. Chiffrer le message clair m =6.

   $C = m^e \bmod n = 6^5 \bmod 133 = 62$

6. Déchiffrer le message chiffré c= 62.

   $M = c^d \bmod n = 62^{65} \bmod 133 = 6$

Exercice N°02: *(Protocole Diffie-Hellman)*

1. Quel est le but du protocole Diffie-Hellman ?

   Echange de clés

2. Déterminer la clé de session Diffie-Hellman, si Alice communique à Bob les nombres g = 3 et p = 23.

   Sachant qu'Alice tire le nombre aléatoire a = 5 et Bob le nombre b = 7 ?

   La clé de session calculée dans le protocole Diffie-Hellman est $K = g^{xy} \bmod p$

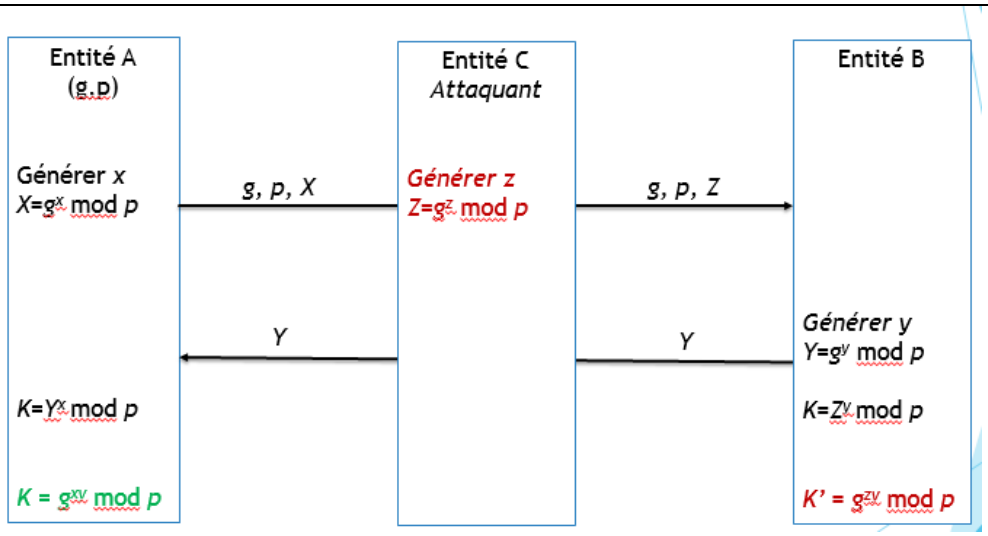
   $K=3^{5*7} \bmod 23 = 9$

3. Expliquez les faiblesses de protocole Diffie-Hellman.

Le protocole de Diffie-Hellman est vulnérable aux attaques de milieu (*man-in-the-middle*)

4. Proposer un scenario d'attaque de type MITM.

Vous pouvez faire une application numérique en utilisant les valeurs prédéfinies.


Entité A
(g,p)
Générer x
X=g^x mod p
g, p, X
Entité C
Attaquant
Générer z
Z=g^z mod p
g, p, Z
Entité B
Y
Y
Générer y
Y=g^y mod p
K=Y^x mod p
K=Z^y mod p
K = g^xy mod p
K' = g^zy mod p