**Université Ferhat Abbas – Sétif-1**
**Département d'Informatique**

**L3 Informatique**
**2022-2023**

# Correction examen : SECURITE INFORMATIQUE

01 juin 2023
Durée : 1h30

Prénom : . . . . . Nom : . . . . . Groupe : . . . . Note : . . . .

L'examen est constitué de deux parties : une partie QCM, et une partie exercices.
La réponse aux QCM doit être reportée sur le sujet d'examen.
La réponse aux exercices doit être reportée sur la feuille de réponse.
Prière de rendre cette copie avec la feuille de réponse.

**I- QCM** : Cochez **la** (ou **les**) bonne(s) réponse(s). Une réponse juste (0.5 pts), une réponse fausse (0 pts).

1. Qu'est-ce qu'un fichier de mots de passe à sens unique ?
   - ☐ Un schéma dans lequel le mot de passe est chiffré et stocké
   - ☐ Un schéma dans lequel le mot de passe est mélangé et stocké
   - ☐ Un schéma dans lequel le mot de passe XOR une clé est stocké
   - ☐ Un schéma dans lequel le hachage du mot de passe est stocké

2. Un expéditeur ne doit pas être en mesure de nier l'envoi d'un message qui a été envoyé, c'est ce qu'on appelle :
   - ☐ Authentification des messages
   - ☐ Non-répudiation des messages
   - ☐ Intégrité des messages
   - ☐ Confidentialité des messages

3. Combien d'itérations AES-128 effectue-t-il ?
   - ☐ 16
   - ☐ 10
   - ☐ 12
   - ☐ 14

4. SHA-1 produit un digest de taille :
   - ☐ 128 bits
   - ☐ 256 bits
   - ☐ 160 bits
   - ☐ 180 bits

5. Alice signe numériquement un message et l'envoie à Bob. La vérification de la signature par Bob nécessite :
   - ☐ Clé privée d'Alice.
   - ☐ Clé publique d'Alice.
   - ☐ Clé privée de Bob.
   - ☐ Clé publique de Bob.

6. 10 personnes désirent communiquer de façon confidentielle (chacune avec chaque autre) en utilisant un algorithme de chiffrement asymétrique. Combien de clés privées auront-elles besoin ?
   - ☐ 100
   - ☐ 10
   - ☐ 45
   - ☐ 90

7. Une collision se produit :
   - ☐ Si x = y, alors H(x) ≠ H(y).
   - ☐ Si x = y, alors H(x) = H(y).
   - ☐ Si x ≠ y, alors H(x) = H(y).
   - ☐ Si x ≠ y, alors H(x) ≠ H(y).

8. Parmi ces attaques, quelles sont les attaques de collecte d'informations ?
   - ☐ Spamming
   - ☐ Sniffing
   - ☐ Phishing
   - ☐ Spoofing

9. Parmi ces propriétés, quelles sont les propriétés d'une fonction de hachage :
   - [ ] Résistant à la pré-image
   - [ ] Taille d'entrée variable
   - [ ] Résistant aux collisions
   - [ ] Taille de sortie variable

10. L'attaque qui bloque les services d'une banque à succursales multiples est :
   - [ ] Attaque de site Web
   - [ ] Botnet
   - [ ] DoS
   - [ ] DDoS

11. Dans SHA-1, le message est divisé en blocs, la taille de chaque bloc est :
   - [ ] 128 bits
   - [ ] 1024 bits
   - [ ] 512 bits
   - [ ] 256 bits

12. Dans MD5, si la taille du message est 1144, la taille du Padding est :
   - [ ] 328
   - [ ] 392
   - [ ] 1536
   - [ ] 64

13. Les aspects principaux de la sécurité sont :
   - [ ] Automatization
   - [ ] Réaction
   - [ ] Détection
   - [ ] Prévention

14. Quelle est l'expression juste ?
   - [ ] Menace = Vulnérabilité + Risque
   - [ ] Menace = Vulnérabilité = Risque
   - [ ] Vulnérabilité = Risque + Menace
   - [ ] Risque = Vulnérabilité + Menace

15. Dans chaque itération DES, la taille de la sous-clé est :
   - [ ] 64
   - [ ] 16
   - [ ] 48
   - [ ] 56

16. Dans l'algorithme DES, chaque table S-BOX prend en entrée … bits, et retourne en sortie … bits :
   - [ ] 12 ; 8
   - [ ] 6 ; 4
   - [ ] 4 ; 6
   - [ ] 8 ; 12

17. 10 personnes désirent communiquer de façon confidentielle (chacune avec chaque autre) en utilisant un algorithme de chiffrement symétrique. Combien de clés auront-elles besoin ?
   - [ ] 100
   - [ ] 10
   - [ ] 45
   - [ ] 90

18. Une attaque informatique passe par les phases suivantes :
   - [ ] Installation, contrôle, exploitation
   - [ ] Installation, exploitation, contrôle
   - [ ] Contrôle, installation, exploitation
   - [ ] Exploitation, installation, contrôle

19. La contre mesure à mettre en place pour éliminer une erreur non intentionnelle est :
   - [ ] Utiliser la cryptographie
   - [ ] Sensibiliser et former les employés
   - [ ] Mettre à jour les systèmes
   - [ ] Acquérir de nouveaux matériels

20. Un expéditeur utilise la cryptographie à clé publique pour envoyer un message secret à un destinataire. Lesquels des énoncés suivants sont vrais ?
   - [ ] Le récepteur déchiffre en utilisant sa propre clé privée.
   - [ ] L'expéditeur chiffre à l'aide de la clé publique du destinataire.
   - [ ] L'expéditeur chiffre à l'aide de sa propre clé publique.
   - [ ] Le récepteur déchiffre à l'aide de sa propre clé publique.

**Exercice 1 : (5 pts)**

1. Quel est le nombre de **clés possibles** du chiffre affine pour cet alphabet ?
   Nombre de clé $K_1$ possible (inversible) = 12 (1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20)
   Nombre de clé $K_2$ possible = 21
   Nombre de **clés possibles** du chiffre affine pour cet alphabet = 12 * 21 = 252 (1 pts)
   On enlève la clé de la valeur neutre (1, 0). (12 * 21) -1 = 252-1
   La réponse : 12 * 21 = 252 est acceptée.
2. Chiffrez le texte en clair « **ROMA** » en utilisant le chiffre **affine** avec la **clé (17, 5)**.
   R : (15 * 17 + 5) mod 21 = 8 … I
   O : (12 * 17 + 5) mod 21 = 20 … Z
   M : (10 * 17 + 5) mod 21 = 7 … H
   A : (00 * 17 + 5) mod 21 = 5 … F
   Texte chiffré = IZHF (1 pts)

3. Déchiffrez le texte chiffré « **UVR** » qui a été chiffré avec la même **clé de chiffrement (17, 5)**.
   Il faut d'abord trouver la clé de déchiffrement,
   $K_1^{-1} * K_1 \bmod 21 = 1$
   $K_1^{-1} * 17 \bmod 21 = 1$
   $K_1^{-1} = 5$
   $K_2^{-1} = -5$, ou $K_2^{-1} = 16$
   La clé inverse = (5, -5) ou (5, 16). (0.5 pts)
   U : (18 – 5) * 5) mod 21 = 2 … C
   V : (19 – 5) * 5) mod 21 = 7 … H
   R : (15 – 5) * 5) mod 21 = 8 … I
   Texte en clair = CHI (1 pts)
4. En utilisant la méthode d'analyse de fréquence, trouvez la **clé de chiffrement** utilisée pour chiffrer le texte chiffré suivant sachant qu'il est écrit en italien, puis déchiffrez le mot souligné.
   A → H, 0 → 7, f (0) = 7, 0 * a + b = 7
   E → C, 4 → 2, f (4) = 2, 4 * a + b = 2
   De la première équation on a : b = 7.
   De la deuxième on trouve a = 4.
   Puisque PGCD (4, 21) = 1, 4 est une clé valide.
   Donc la clé de chiffrement est (4, 7). (1 pts)
   Pour déchiffrer on calcule la clé inverse,
   $K_1^{-1} * 4 \bmod 21 = 1$
   $K_1^{-1} = 16$
   $K_2^{-1} = -7$, ou $K_2^{-1} = 14$
   La clé inverse = (16, -7) ou (16, 14). (0.5 pts)
   S : (16 – 7) * 16) mod 21 = 18 … U
   P : (13 – 7) * 16) mod 21 = 12 … O
   Z : (20 – 7) * 16) mod 21 = 19 … V
   H : (7 – 7) * 16) mod 21 = 0 … A
   Texte en clair = UOVA (1 pts)

**Exercice 2 : (5 pts)**

1. Chiffrez le texte en clair « **ALPHA** » en utilisant le chiffre de **Hill** avec la **clé « KEYS »**.

   La fonctio de chiffrement : C = M * K.

   On écrit K et M en matrices, la taille de la clé est (2x2), donc la matrice M doit être de taille (3 x 2), et puisque M contient 5 lettres, on ajoute la lettre Z à la fin du mot, donc M = ALPHAZ

   $K = \begin{pmatrix} 10 & 4 \\ 24 & 18 \end{pmatrix}$, $M = \begin{pmatrix} 0 & 11 \\ 15 & 7 \\ 0 & 25 \end{pmatrix}$

   $C = \begin{pmatrix} 0 & 11 \\ 15 & 7 \\ 0 & 25 \end{pmatrix} * \begin{pmatrix} 10 & 4 \\ 24 & 18 \end{pmatrix} \bmod 26 = \begin{pmatrix} 264 & 198 \\ 318 & 186 \\ 600 & 450 \end{pmatrix} \bmod 26 = \begin{pmatrix} 4 & 16 \\ 6 & 4 \\ 2 & 8 \end{pmatrix}$ = EQGECI (1 pts)

2. Déchiffrez le texte chiffré « **EWGEGK** » qui a été chiffré avec la même **clé de chiffrement « KEYS »**.

   Pour déchiffrer on cherche la clé inverse, on commence par calculer le determinant de K :

   $\text{Det} \begin{pmatrix} 10 & 4 \\ 24 & 18 \end{pmatrix} = 10 * 18 - 24 * 4 = 84 \bmod 26 = 6.$

   Pour trouver la matrice inverse on cherche l'inverse du déterminant, mais PGCD (6, 26) ≠ 1, donc 6 n'est pas inversible, alors on ne peut pas trouver l'inverse de K. (1 pts)

3. Le chiffrement du texte en clair « **LAMB** » donne le texte chiffré « **HACH** », trouvez la clé utilisée pour ce chiffrement, sachant que la taille de la clé est **m = 2.**

   Pour trouver la clé on a : $K = M^{-1} * C$.

   $M = \begin{pmatrix} 11 & 0 \\ 12 & 1 \end{pmatrix}$ , $C = \begin{pmatrix} 7 & 0 \\ 2 & 7 \end{pmatrix}$.

   On cherche $M^{-1}$ :

   $\text{Det} \begin{pmatrix} 11 & 0 \\ 12 & 1 \end{pmatrix} = 11 * 1 - 12 * 0 = 11$. PGCD (11, 26) = 1, donc 11 est inversible,

   Son inverse est 11 * a mod 26 = 1, $\text{Det}^{-1} = 19$.

   On calcule la comatrice de M : $\text{com} \begin{pmatrix} 11 & 0 \\ 12 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -12 & 11 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 0 \\ 14 & 11 \end{pmatrix}$

   $M^{-1} = 19 * \begin{pmatrix} 1 & 0 \\ 14 & 11 \end{pmatrix} \bmod 26 = \begin{pmatrix} 19 & 0 \\ 6 & 1 \end{pmatrix}$. (1 pts)

   $K = \begin{pmatrix} 19 & 0 \\ 6 & 1 \end{pmatrix} * \begin{pmatrix} 7 & 0 \\ 2 & 7 \end{pmatrix} \bmod 26 = \begin{pmatrix} 3 & 0 \\ 18 & 7 \end{pmatrix}$ = DASH (1 pts)