| | | |
|---|---|---|
| **Université de M'sila**<br>**Faculté des MI**<br>**Département d'informatique** | **Interrogation**<br>**Année Universitaire: 2021/2022** | **Niveau: 3ème année Licence**<br>**Module: Sécurité Informatique** |

**QCM: (0.5 * 7 =3.5)**

1. L'aspect technique de sécurité informatique s'articule sur:
   a. Sécurité logique
   b. Sécurité applicative
   c. Sécurité physique
   d. Sécurité  optimisation
2. De quel type d'algorithme est le chiffre de Vigenère?
   a. Substitution mono-alphabétique.
   b. Substitution poly-alphabétique.
   c. Substitution polygraphique.
3. Nombre de clés possibles du chiffrement Affine est:
   a. 26
   b. 52
   c. 312
   d. 676
4. En parlant de la cryptographie symétrique, lesquelles des phrases suivantes sont fausses ?
   a. Elle assure l'intégrité
   b. La gestion des clés est plus simple
   c. Ces algorithmes sont plus rapides que ceux de la cryptographie asymétrique.
   d. Les clés utilisées pour chiffrement et déchiffrement sont différentes.
5. L'algorithme AES ne résiste pas les attaques suivantes:
   a. Recherche exhaustive.
   b. Attaque différentielle.
   c. Attaque linéaire.
   d. Pas de réponse correcte.
6. Le protocole Diffie-Hellman basé sur le problème;
   a. Factorisation
   b. Logarithme discret
   c. Chiffrement symétrique
   d. Courbes elliptiques
7. Parmi les fonctions de hachage ci-dessous, lesquelles ne sont pas sûres:
   a. MD-5
   b. SHA-3
   c. SHA-1
   d. SHA-512

**Exercice: (3.5 points)**

1. Soient a= 7 et b=2, calculer les fonctions de chiffrement de déchiffrement de l'algorithme Affine.

C=E(m) = am + b mod 26
M = D(c) = $a^{-1}$. (y-b) mod 26 **(0.5 pt)**

E(m)= 7m + 2 mod 26 **(0.5 pt)**
D(c) = $7^{-1}$(c-2) mod 26
On utilise l'algorithme d'Euclide étendu pour calculer l'inverse modulaire de $7^{-1}$ mod 26
On trouve $7^{-1}$ mod 26= 15
Alors :
M = D(c) = 15(y-2) mod 26 **(0.5 pt)**

2. En utilisant (7, 2), déchiffrer le texte chiffré " **QRODFCSE** " en utilisant l'algorithme Affine:

   Texte en clair: CRYPTAGE **(1 pt)**
3. Dessiner le schéma de Feistel et quel algorithme utilise ce schéma? **(1 pt)**