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

Année universitaire : 2017/2018
Mardi 15/05/2018, 10h – 11:30h

Corrigé type de l'examen du Semestre

Exercice N°01 : ***(Questions de cours)***

1. Définir les concepts suivants:
   a. Authentification:

0,5 *L'authentification est un mécanisme permettant d'identifier des personnes ou des entités et de certifier leur identité.*

   b. Spyware:

0,5 *Le spyware est un programme indésirable qui s'installe en général sur un poste de travail. Sa fonction est récupérer des informations sur une personne ou une société de façon transparente pour l'utilisateur.*

   c. Attaque XSS:

0,5 *L'attaque XSS est une attaque par injection de code qui permet à un attaquant d'exécuter du code JavaScript malveillant dans le navigateur d'un autre utilisateur.*

   d. Attaque par usurpation (*spoofing*):

0,5 *L'attaque par usurpation est une technique utilisée par des entités malveillantes pour accéder à un réseau en créent une fausse identité d'un dispositif ou d'un utilisateur.*

2. Quelle est la différence entre le chiffrement classique et le chiffrement moderne?

1 **Classique :** lettres, symétrique, militaire et diplomatique
Moderne: binaire, symétrique et asymétrique, tous les domaines

3. Comment protéger les applications Web contre les attaques par injection SQL?

0,5 *On utilise le filtrage de l'input $_GET['id'] par conserver la partie entière de sa valeur et filtrer tous les caractères spéciaux*

.

4. Citer les quatre catégories de classification des techniques d'authentification:

1 1) authentification faible 2) authentification basée sur les méthodes cryptographiques ;
3) authentification forte basée sur des dispositifs matériels 4) authentification biométrique

5. Expliquer les différents rôles des fonctions de hachage:

0,5 MDC: mots de passe, signature numérique, PRNG
HMAC: authentification

Tourner la page →

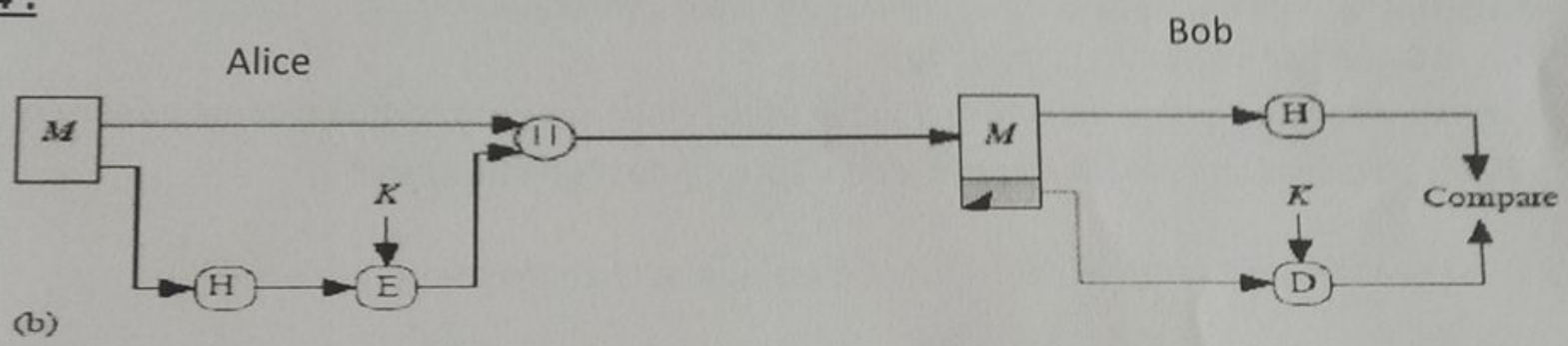
Exercice N°02 : ***(Chiffrement classique)***

1) Expliquer le chiffrement de Vigenère. ***Voir Cours***
2) Ecrire un pseudo-code de la fonction de chiffrement (cryptage) ***Voir TD N°01***
3) Chiffrer le message «**COMPUTER**» avec le chiffrement par décalage, la clé est **K.** → ***MYWZEDOB***
4) Déchiffrer le texte chiffré «**TRKPWVCEKJUOTB**» avec le chiffrement de Vigenère, la clé est **CRYPTO.** → ***RAMADHAN MUBAR***

Exercice N°03 (Signature RSA):

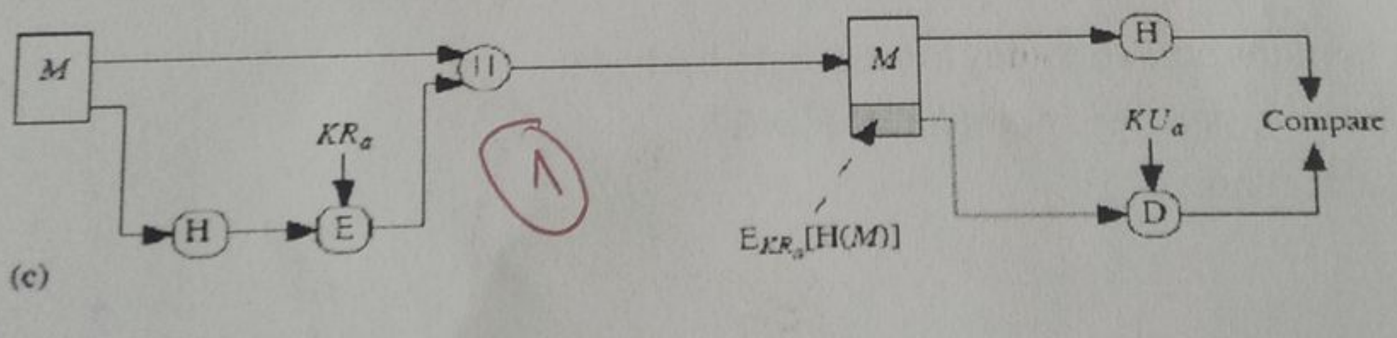
1) Décrire le schéma de génération de clés, schéma de signature, et schéma de vérification. → ***Voir cours***
2) Quelles sont les propriétés de sécurité validées par ce schéma ? → ***intégrité, authentification, non-repudiation***
3) Montrer que $D_{RSA}(E_{RSA}(h(m))) = h(m)$. → ***Voir TD***
4) On pose p=11 et q=7, calculer N et Φ(n). → ***N= 77, Φ(n)= 60***
5) Si la clé de vérification égal à 17, calculer la clé de la signature. → ***d=53***
6) Ecrire la formule de calcul de la signature de h(m) = 10 ? ***Sig = 10^{53} mod 77***

Exercice N°04 :



(b)

1) Expliquer brièvement le processus exécuté par Bob
2) Quelles sont propriétés validées par ce schéma? → ***intégrité et authentification***
3) Quelles sont les primitives utilisées par Alice? → ***fonction de hachage et chiffrement symétrique***
4) Quel est l'algorithme de chiffrement moderne symétrique qui vous proposer? Et pourquoi ? → ***AES, il est très rapide et sécurisé.***
5) Quel est le type de la fonction de hachage utilisée? → ***MDC***
6) Est-ce que la fonction SHA-1 est sûre ? et pourquoi ? → ***Non, SHA-1 a été cassée en 2017.***
7) Pour appliquer la signature numérique, redessiner le schéma.



(c)

Exo N°1 : 5 pts **Exo N°2 : 4 pts** **Exo N°3 : 5 pts** **Exo N°4 : 6 pts**