Université Kasdi Merbah Ouargla
Département d'Informatique et des Technologies de l'Information

1ère MASTER ASR — Module Sec1

18 Janvier 2022

Contrôle Sec1 corrigé type

(Durée 1 H)

Cocher les réponses correctes :

Critères de sécurité (2 pts)

1. Quels sont les trois principaux objectifs de la sécurité informatique ? a. Confidentialité b. Intégrité **C.** Disponibilité	2. Pour assurer les objectifs de la sécurité informatique un autre critère de sécurité doit être assuré, il s'agit de l': Authentification
3. Quel est le meilleur outil pour assurer la sécurité dans l'entreprise ? a. Un système de détection d'intrusion (IDS) ***X*** b. PowerPoint c. un antivirus ***X*** d. un firewall ***X***	4. Pour assurer l'intégrité de l'information transmise on utilise : a. Une fonction de hachage ***X*** b. Un chiffrement de données c. Une signature numérique e. Un certificat numérique

Cryptologie : Concepts généraux (2.5 pts)

1. L'art de déchiffrer des messages sans connaître la clé de chiffrement est appelé: a. La cryptographie b. La cryptologie c. La cryptanalyse ***X***	2. Un algorithme de chiffrement qui possède une bonne propriété de diffusion est tel que: a. le chiffrement du message s'effectue rapidement b. une petite modification du message en clair se traduit par une modification complète du chiffré ***X*** c. aucune propriété statistique ne peut être déduite du message chiffré ***X***
3. Le chiffrement de César est : a. une substitution poly alphabétique b. une substitution mono alphabétique ***X*** c. un chiffrement par bloc 4. Le chiffrement de Vigénère est : a. une substitution poly alphabétique ***X*** b. une substitution mono alphabétique c. un chiffrement par bloc ***X***	5. Oscar a réussi à intercepter un couple (message chiffré, message en clair correspondant). A l'aide de ce couple, il a réussi à déterminer la clé ***k*** utilisée entre Alice et Bob. C'est une attaque de type: a. Attaque à texte chiffré b. Attaque à texte clair connu c. Attaque à texte clair choisi ***X*** 6. Le résultat de l'attaque est un: a. Cassage partiel b. Cassage local c. Cassage complet ***X***
7. Le principal défaut de l'algorithme de chiffrement One-Time Pad est: a. Il est très facile à casser b. Il est peu pratique à utiliser ***X*** c. Il est lent	8. Les chiffrements alphabétiques sont désormais moins utilisés que les chiffrements par bloc. a. Vrai ***X*** b. Faux c. Les deux sont autant utilisés
9. Le principal défaut de DES était:	10. Après l'abandon de DES, un nouveau standard Américain

a. Sa lenteur ***X*** b. La petite taille de la clé ***X*** c. La complexité de l'algorithme	a été choisi. L'algorithme qui a remplacé DES est: a. TDES b. Blowfish c. AES X

Chiffrements asymétriques, fonctions de hachage et Macs (5.5)

1. Un *MAC* se calcule sur : a. un message b. un secret c. un message et un secret ***X***	2. L'algorithme *SHA1* calcule une empreinte de : a. 128 bits b. 160 bits ***X*** c. 256 bits
3. L'avantage des chiffrements asymétriques par rapport aux chiffrements symétriques est que: a. Ils sont plus rapides que les chiffrements symétriques b. Il n'y a pas besoin de s'échanger de clé secrète ***X*** d. Ils possèdent une meilleure propriété de confusion ***X***	4. Le protocole ***Diffie-Hellman (DH***) est un protocole qui sert principalement à: a. chiffrer/déchiffrer des messages b. signer des messages c. s'échanger une clé secrète (key agreement) ***X***
5. Une opération clé publique peut être : a. Chiffrer une clé de session ***X*** b. Chiffrer un petit message ***X*** c. Déchiffrer une clé de session d. Générer une signature e. Vérifier une signature ***X***	6. Une opération clé privée peut être: a. Déchiffrer une clé de session ***X*** b. Générer une signature ***X*** c. Vérifier une signature d. Déchiffrer un petit message chiffré avec la clé publique correspondante ***X***
7. Alice veut envoyer un message à Bob. Elle décide de chiffrer ce message via l'algorithme RSA. Elle aura besoin de: a. la clé publique de Bob ***X*** b. la clé privée de Bob c. la clé privée et la clé publique de Bob Soit (e_b, n_b) la clé publique de Bob et d_b sa clé privée. Posez le calcul que vont effectuer: Alice lorsqu'elle chiffrera le message m: $\underline{c = m^{e_b} \bmod n_b}$ Bob lorsqu'il déchiffrera le message c : $\underline{m = c^{d_b} \bmod n_b}$	8. Sur quel(s) problème(s) difficile(s) est basé le cryptosystème RSA ? a. Factorisation ***X*** b. LogarithmeDiscret c. Diffie-Hellman d. RacineIemeModulaire 9. Quelle(s) propriété(s) du message permet de garantir la signature ? a. l'intégrité du message b. la confidentialité du message c. l'authenticité du message ***X***
10. Alice veut signer le message qu'elle envoie à Bob. Le message va être signé avec a. la clé publique d'Alice b. la clé privée d'Alice ***X*** c. la clé privée de Bob	11. Alice veut envoyer un message chiffré via RSA à Bob. L'infrastructure à clé publique (ou PKI) lui permet de: a. chiffrer le message de manière plus efficace b. augmenter la confidentialité du message c. s'assurer que la clé publique du destinataire est bien celle de Bob ***X***

Exercice 1 cryptographie Asymétrique – RSA (5 pts) :

Génération des paramètres RSA

On donne : $368^{185} = 23 \bmod 391$ et $(-72 \times 352) + (137 \times 185) = 1$

Soient $p = 23$ *et* $q = 17$ *deux nombres premiers*

1. *Calculer le module RSA (n) :* $\boldsymbol{n = p \times q = 23 \times 17 = 391}$ **(1 pt)**
2. Qui est φ ? Comment ce nombre est-il calculé ?
   φ est la fonction indicatrice d'Euler, $\varphi = |Z_n^*|$ =Le nombre d'éléments inversibles de $\mathbb{Z}_n$,
   $\boldsymbol{\varphi(n) = \varphi(391) = (p-1)(q-1) = (23-1)(17-1) = 22 \times 16 = 352}$ **(1 pt)**
3. Soit $e = 185$ l'exposant publique, Comment est-il choisi ?
   e doit être impair, $0 < e < \varphi(n)$ *et* $pgcd(e, \varphi(n) = 1$ **(1 pt)**
4. Calculer l'exposant privé :
   On doit avoir $e \times d = 1 \bmod \varphi(n)$, *nous avons :* $(-72 \times 352) + (137 \times 185) = 1$ c-a-d
   $185 \times 137 = 1 \bmod 352$ donc $185^{-1} = 137 \bmod 351$, $\boldsymbol{d = 137}$ **(1 pt)**
5. Commente chiffrer le message $x = 368$?, Comment déchiffrer le message $y = 23$?
   $Chiffrer\ x = 368$
   $\boldsymbol{y = e_{kpub}(x) = x^e mod\ n = 368^{185} mod\ 391 = 23}$ **(0.5 pt)**
   $Déchiffrer\ y = 23$
   $\boldsymbol{x = d_{kpriv}(y) = y^d mod\ n = 23^{137} mod\ 391 = 368}$ **(0.5 pt)**

<u>Exercice 3 (QCM) (5 pts)</u> : choisir une seule réponse et justifier

1. Une recherche exhaustive sur les 56 bits d'une clé DES nécessite environ 56 heures. Combien de temps faudrait-il approximativement sur une clé de 64 bits ? 56 heures 64 heures 64 jours plus d'un an
   plus d'un an :
   56 bits en 56 heures implique 57 bits en $56 \times 2 = 112$ heures, 58 bits en 112×2 *heures*. 64 bits en $2^{(64-56)} \times 56 = 2^8 \times 56$ heures soit 256×56 heures soit plus d'un an. (1 pt)
2. Alice a utilisé le chiffrement de Vernam (OTP) pour envoyer un message $m \in \{0,1\}^{100}$ à Bob. Ils partageaient tous les deux une clé aléatoire $k \in \{0,1\}^{100}$ .Charlie intercepte le chiffré $c = m \oplus k$. Quel est le temps nécessaire pour retrouver m ?
   instantané 100 *secondes* 100 *essais* 2^{100} *essais*

   2^{100} essais :
   Une clé aléatoire de 100 bits donc 2^{100} essais. (1 pt)
3. Combien y a-t-il d'éléments dans Z_{28}^*? 0 10 12 20 27 28

   12 :
   $\boldsymbol{\varphi(28)}$ = nombres d'éléments inversibles dans Z_{28}^*; $\boldsymbol{\varphi(28) = \varphi(2^2 \times 7) = \varphi(4) \times \varphi(7) = (2^2 - 2^1) \times (7-1) = 2 \times 6 = 12}$ (1 pt)
4. Que vaut $\varphi(77)$? 0 1 24 60 76 77

   60 :
   $\boldsymbol{77 = 7 \times 11; \varphi(77) = (7-1) \times (11-1) = 6 \times 10 = 60}$ (1 pt)
5. Que vaut pgcd(12345, 17)? 0 1 17 34 12344 12345

   1 :
   12345 et 17 sont premiers entre eux car 17 est premier et 12345 n'est pas un multiple de 17. (1 pt)