Partie QCM et questions

---

1) Quel est l'avantage principal du chiffrement symétrique par rapport à l'asymétrique ?

- a) Il est plus rapide et efficace pour le chiffrement de gros volumes
  Réponse : a

---

2) Hamid et Ali s'échangent des données. Leur échange est intercepté et modifié par un attaquant. Quels concepts de sécurité sont menacés ?

- a) La confidentialité
- b) L'intégrité
- c) La disponibilité
  Réponse : b (L'intégrité)
  Car le contenu est modifié, donc l'intégrité est compromise.

---

3) Ali veut envoyer un message confidentiel à Hamid via chiffrement asymétrique. Quelle assertion est correcte ?

- a) Ali chiffre avec la clé publique de Hamid, et Hamid déchiffre avec la clé publique d'Ali
- b) Ali chiffre avec la clé publique de Hamid, Hamid déchiffre avec sa propre clé privée
- c) Ali chiffre avec sa clé privée, Hamid déchiffre avec la clé publique d'Ali
  Réponse : b

---

4) Hamid veut prouver à Ali qu'il est bien l'expéditeur (signature). Quelle assertion est correcte ?

- a) Hamid chiffre le message avec la clé publique d'Ali puis envoie un message chiffré avec sa clé privée (signature)
- b) Hamid chiffre le message avec sa propre clé privée puis l'envoie. Ali déchiffre avec la clé publique de Hamid
- c) Hamid chiffre avec sa clé publique puis envoie, Ali déchiffre avec clé privée de Hamid
  Réponse : b

---

5) Quel est le principal inconvénient du chiffrement symétrique ?

- c) Il nécessite un canal sécurisé pour l’échange de la clé
  Réponse : c

---

6) Dans un système RSA, que garantit la difficulté de factorisation des grands nombres premiers ?

- b) La sécurité de la clé privée
  Réponse : b

---

7) Dans l’échange Diffie-Hellman, pourquoi une attaque "man-in-the-middle" est-elle possible ?

- d) Parce qu’il n’y a pas d’authentification des parties communicantes
  Réponse : d

---

8) Lequel des algorithmes suivants est le plus rapide ?

- b) AES
  Réponse : b

---

9) Ali a téléchargé un logiciel. Pour vérifier l’intégrité, il utilise :

- c) Une fonction de hachage
  Réponse : c

---

10) Les systèmes à signature numérique assurent :

- a) L’authentification, l’intégrité, et la confidentialité
  Réponse : a

---

11) Dans un système à signature asymétrique, le digest est calculé puis :

- b) Chiffré avec la clé privée de l’émetteur
  Réponse : b

---

12) Dans un système à signature symétrique, le digest est calculé sur :

- a) La concaténation de la clé secrète et le message à envoyer
  Réponse : a

---

29) La carte accélératrice HSM protège la clé privée contre :

- a) Toute vulnérabilité logicielle ou humaine
  Réponse : a

---

30) Inconvénient majeur de l'authentification SSO :

- b) Si le système SSO est rendu inopérant, c'est la totalité de l'entreprise qui est paralysée
  Réponse : b

---

31) Kleopatra de GPG4Win est utilisé pour :

- c) Génération de certificats numériques garantissant l'authenticité des clés publiques
  Réponse : c

---

32) Attaque par Force Brute consiste à :

- b) Tester successivement toutes les combinaisons possibles
  Réponse : b

---

33) Pour empêcher XSS, clickjacking, injection de code, entêtes HTTP à utiliser :

- a) Content Security Policy (CSP)
- b) X-Frame-Options
- c) HSTS
  Réponses : a, b, c (selon la question)

---

34) Entête HTTP pour forcer HTTPS :

- b) Strict-Transport-Security
  Réponse : b

---

35) Entête pour définir les sources autorisées (script, img, etc.) :

- c) Content-Security-Policy
  Réponse : c

---

36) Directive correcte pour désactiver complètement l'affichage dans les frames :

- b) X-Frame-Options : DENY
  Réponse : b

Partie exercices pratiques (page 4)

---

1) Message chiffré par César :

```
"HWOACIAJPWPEKJZAONAOAWQTEJBKNIWPEMQAOWQEILWYPZENAYPOQNHWOAYQNEPA"
```

- Il faut appliquer un décalage (clé de César) pour retrouver le message clair.
- Méthode : tester les décalages de 1 à 25 jusqu'à trouver un texte clair.

(Le texte est long, une méthode automatisée est préférable. Je peux vous aider à le déchiffrer si besoin.)

---

2) Cryptogramme avec clé secrète "82463175" :

```
"OFOEEANTOAOAVDTNMAFMTNNCPNOETCLUXINSOETETINUEEUVSUIUECNATEESEINCITMSDPUNIFESU
ACYSHATR"
```

- Clé utilisée probablement dans un algorithme de substitution ou transposition.
- Nécessite un algorithme précis ou outil pour déchiffrer.

---

3) Calcul RSA avec p=5, q=17 :

- $n = p * q = 5 * 17 = 85$
- $\varphi(n) = (p-1)(q-1) = 4 * 16 = 64$
- Choisir e tel que $1 < e < 64$ et e premier avec 64, par exemple e=5
- Calculer d tel que $(d * e) \bmod 64 = 1$ (d est l'inverse modulaire de e mod 64)
- $d = 13$ (car $5*13=65 \equiv 1 \bmod 64$)
- Clé publique = (e=5, n=85)
- Clé privée = (d=13, n=85)