Devoir Surveillé – BTS SIO 1ere année (B3)

Chiffrement, Hachage et Signature Numérique

Durée totale : 2 heures
Partie 1 – Définitions et concepts fondamentaux
Partie 2 – Exercices pratiques de chiffrement

La justification, la rigueur, la rédaction et le soin de la copie entrent dans la notation sur 2 points. Un manquement de ces 4 critères entraîne une perte de 2 points.

Partie 1 – Définitions et concepts (10 points)

1.1 Les piliers de la sécurité (2 points)

Question 1 : Définir les propriétés fondamentales (1 point – 0,25 pt par définition)

Définir chacune des 4 propriétés fondamentales de la sécurité :

a) **Confidentialité**
b) **Intégrité**
c) **Authenticité**
d) **Non-répudiation**

Question 2 : Association technique et propriété (1 point – 0,33 pt par ligne correcte)

Associer chaque technique de sécurité à la propriété qu'elle garantit principalement et justifier votre réponse :

Technique	Propriété garantie	Justification (1 phrase)
Chiffrement		
Hachage		
Signature numérique		

1.2 Terminologie cryptographique (2 points)

Question 1 : Définitions essentielles (1 point – 0,25 pt par définition)

Définir précisément les termes suivants :

a) **Chiffrement (Encryption)**
b) **Déchiffrement (Decryption)**
c) **Décryptage (Cryptanalysis)**
d) **Hachage (Hash)**

Question 2 : Distinction importante (1 point)

Expliquer en détail la différence entre **déchiffrement** et **décryptage**.
Lequel des deux processus est légitime et pourquoi ?

1.3 Chiffrement monoalphabétique vs polyalphabétique (2 points)

Question 1 : Chiffrement monoalphabétique (0,5 point)

a) Définir ce qu'est un **chiffrement monoalphabétique**.
b) Donner un **exemple d'algorithme** de chiffrement monoalphabétique.

Question 2 : Chiffrement polyalphabétique (0,5 point)

a) Définir ce qu'est un **chiffrement polyalphabétique**.
b) Donner un **exemple d'algorithme** de chiffrement polyalphabétique.

Question 3 : Analyse comparative (1 point)

a) Expliquer la **principale faiblesse** du chiffrement monoalphabétique. (0,5 point)
b) Pourquoi le chiffrement polyalphabétique est-il **plus sécurisé** ? (0,5 point)

1.4 Chiffrement symétrique et asymétrique (2 points)

Question 1 : Chiffrement symétrique (0,5 point)

a) Définir le **chiffrement symétrique**.
b) Quel est son **principal avantage** ?

Question 2 : Le problème majeur du chiffrement symétrique (0,5 point)

Expliquer en détail le **problème majeur** du chiffrement symétrique concernant l'échange de clefs.
Pourquoi ce problème est-il critique pour la sécurité ?

Question 3 : Chiffrement asymétrique (0,5 point)

a) Définir le **chiffrement asymétrique**.
b) Quelles sont les **deux clefs** utilisées et à quoi servent-elles ?

Question 4 : Limitation du chiffrement asymétrique (0,5 point)

Quel problème le chiffrement asymétrique **ne résout-il PAS** à lui seul, notamment concernant l'intégrité du message ?

1.5 Hachage et signature numérique (2 points)

Question 1 : Fonction de hachage (0,5 point)

a) Qu'est-ce qu'une **fonction de hachage** ?
b) Citer **3 propriétés essentielles** d'une fonction de hachage.

Question 2 : Signature numérique (0,5 point)

Expliquer le **fonctionnement complet** d'une signature numérique :

a) **Étapes de CRÉATION** de la signature par Alice
b) **Étapes de VÉRIFICATION** de la signature par Bob

Question 3 : Différence chiffrement vs signature (0,5 point)

Quelle est la différence fondamentale entre **chiffrer un message** et **signer un message** ?

Question 4 : Autorité de Certification (0,5 point)

a) Qu'est-ce qu'une **Autorité de Certification (CA)** ?
b) Quel est son **rôle principal** dans la sécurité des communications ?

Partie 2 – Exercices pratiques (8 points)

2.1 Chiffrement de César (2 points)

Expliquer : le fonctionnement du chiffrement César.

Exercice 1 : Chiffrement (1 point)

Chiffrer le message suivant avec un **décalage de 5**, justifier avec les positions de chaque lettre :
Message clair : `SECURITE`

Exercice 2 : Déchiffrement (1 point)

Déchiffrer le message suivant qui a été chiffré avec un **décalage de 5**, justifier avec les positions de chaque lettre :
Message chiffré : `HMFWNKKJRJSY`

2.2 Chiffrement de Vigenère (2 points)

Expliquer : le fonctionnement du chiffrement de Vigenère.

Exercice : Chiffrement complet (2 points)

Chiffrer le message suivant grâce à la clef fournie.
Message à chiffrer : `CRYPTO`
clef : `CLE`

Question supplémentaire (0,5 point) :

Pourquoi les deux lettres "R" dans "CRYPTO" (s'il y en avait deux) seraient-elles chiffrées différemment avec Vigenère alors qu'elles seraient identiques avec César ?

2.4 Attaque Human-in-the-Middle (HITM) (2 points)

Contexte :

Alice souhaite envoyer un message confidentiel à Bob en utilisant le chiffrement asymétrique. Elle doit donc obtenir la clef publique de Bob pour chiffrer son message. Cependant, un attaquant nommé Charlie surveille le réseau et souhaite intercepter et lire le message.

Question 1 : Description de l'attaque (1 point)

Décrire **en étapes détaillées** comment Charlie pourrait réaliser une attaque Human-in-the-Middle (HITM) pour lire le message d'Alice destiné à Bob.

Question 2 : Conséquences de l'attaque (0,5 point)

Quel est le résultat final de cette attaque ? Que peut faire concrètement Charlie avec les messages échangés entre Alice et Bob ?

Question 3 : Solution de protection (0,5 point)

Quelle **solution technique** permet de se protéger efficacement contre cette attaque Human-in-the-Middle ? Expliquer comment cette solution résout le problème.

2.4 Cas pratique : Signature et vérification (2 points)

Contexte :

Alice est chercheuse en biologie et souhaite envoyer un document scientifique important à son collègue Bob. Elle veut garantir que :

1. Bob puisse vérifier que c'est bien elle qui a envoyé le document;
2. Bob puisse vérifier que le document n'a pas été modifié pendant le transfert;
3. Le contenu du document reste confidentiel.

Question 1 : Création de la signature (0,5 point)

Décrire les **étapes précises** qu'Alice doit suivre pour créer une signature numérique de son document.

Question 2 : Vérification de la signature (0,5 point)

Décrire les **étapes précises** que Bob doit suivre pour vérifier la signature numérique reçue d'Alice.

Question 3 : Effet avalanche (0,5 point)

Supposons que Bob modifie **une seule lettre** du document après l'avoir reçu (par exemple, il corrige une faute de frappe).

Que se passera-t-il lors de la vérification de la signature ? Pourquoi ?

Question 4 : Ordre des opérations (0,5 point)

Alice veut maintenant que son message soit à la fois :

- **Authentifié**
- **Confidentiel**

Dans quel **ordre** doit-elle effectuer les opérations suivantes ?

- A) Signer le message
- B) Chiffrer le message