****

**Travail pratique #1**

# But du travail pratique

Le but de ce travail pratique est de vous familiariser avec

* Les algorithmes de chiffrement symétriques
* Les algorithmes de chiffrement asymétriques
* La comparaison des algorithmes
* Les signatures numériques

**Instructions**

* Répondez à toutes les questions le mieux possible.
* Montrez toutes les étapes et calculs.
* Écrivez vos réponses de manière claire.

Prénom et nom étudiant 1 : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Prénom et nom étudiant 2 : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Partie 1 – Évaluation de l'Encryption AES**

**Ronde initiale**

1. Opération SubBytes
2. Opération ShiftRows
3. Opération MixColumns



1. Opération AddRoundKey

5. Réflexion

**Partie 2 – Algorithme RSA**

1. Expliquez les principes de base de la cryptographie RSA. Incluez les rôles de la clé publique et de la clé privée, ainsi que la manière dont elles sont générées.
2. Alice veut envoyer un message confidentiel à Bob en utilisant RSA. La clé publique de Bob est (e, N) = (17, 3233), où N est le modulo. Alice chiffre son message M en utilisant la clé publique de Bob. Si son message M est 123, calculez le texte chiffré C.
3. Bob reçoit le texte chiffré C = 2753 d'Alice. En utilisant sa clé privée (d, N) = (2753, 3233), déchiffrez le message pour obtenir le texte en clair d'origine.
4. Alice génère sa paire de clés RSA. Elle choisit deux nombres premiers, p = 61 et q = 53. Calculez les valeurs de N, φ(N) et l'exposant public (e) pour sa paire de clés.
5. Décrivez une application du monde réel ou un cas d'utilisation où la cryptographie RSA est couramment utilisée. Discutez des avantages spécifiques en termes de sécurité fournis par RSA dans ce contexte.

**Partie 3 – Analyse et application des signatures numériques**

# Imaginez une entreprise de développement de logiciels qui crée et distribue un programme antivirus populaire. L'entreprise publie régulièrement des mises à jour logicielles pour faire face aux menaces émergentes et améliorer les capacités du programme. Les utilisateurs peuvent télécharger ces mises à jour depuis le site officiel de l'entreprise.

1. Décrivez comment les signatures numériques peuvent être appliquées pour garantir l'intégrité et l'authenticité des mises à jour logicielles.
2. Discutez du rôle des clés publiques et privées dans ce scénario.
3. Analysez les risques potentiels et les conséquences si les signatures numériques n'étaient pas utilisées pour vérifier l'authenticité et l'intégrité des mises à jour logicielles.

*Considérez l'impact sur la confiance des utilisateurs, la réputation de l'entreprise et la sécurité globale du programme antivirus.*