Bloc 3 - Cybersécurité - TP Cyber

CHIFFREMENT SYMÉTRIQUE ET ASYMÉTRIQUE : CONFIDENTIALITÉ ET SIGNATURE

Terminal Debian, Dolphin et OpenSSL.

Nom : ..... **Date :** .....

1. Chiffrement symétrique

1. Lorsque vous ouvrez `ordonnance.7z` ou que vous tapez `cat ordonnance.enc`, que s'affiche-t-il ? Pourquoi ?

.....

.....

2. Pour déchiffrer `ordonnance.enc`, la commande est `openssl enc -d -aes-256-cbc -in ordonnance.enc -out ordonnance_claire.txt`. Quel mot de passe le système demande-t-il ?

.....

.....

3. Rappelez la différence fondamentale entre le chiffrement et le hachage SHA-256.

.....

.....

2. Échange de clés et chiffrement asymétrique

4. Le Dr Valois envoie le fichier chiffré par email au chirurgien. Quel problème majeur se pose s'il veut transmettre le mot de passe ?

.....

.....

.....

5. Lequel des deux fichiers (`cle_privee_chirurgien.pem` ou `cle_publique_chirurgien.pem`) le chirurgien doit-il envoyer au Dr Valois ?

.....

.....

6. Un pirate intercepte `secret.enc` et possède la clé publique. Peut-il déchiffrer ? Justifiez avec la règle d'or.

.....

.....

3. Signature électronique

7. Le Dr Valois chiffre une ordonnance avec sa clé privée. Qui peut la déchiffrer et la lire ?

8. Quel est alors l'intérêt de chiffrer avec sa clé privée ? Que prouve-t-on à la pharmacie ?

9. Quelle opération mathématique rapide réduit un document de 200 pages en une chaîne de taille fixe ?

10. Déduisez la méthode complète : que doit chiffrer le Dr Valois pour prouver son identité rapidement tout en garantissant l'intégrité ?

4. Bilan Référentiel BTS SIO & Carnet de bord

Bilan du TP adossé au Référentiel Officiel BTS SIO

Compétences & Savoirs mobilisés :

- **C-3.2.1** : Protéger l'identité numérique d'une organisation.
- **C-3.2.2** : Déployer les moyens appropriés de preuve électronique.
- **S-3.2.1** : Chiffrement, authentification et preuve : principes et techniques
- **S-3.1.2** : Principes de la sécurité : disponibilité, intégrité, confidentialité, preuve

Preuves à insérer dans votre carnet de bord :

- Capture terminal : cat ordonnance.enc illisible, puis déchiffrement réussi avec openssl enc -d.
- Capture terminal : génération de la paire RSA, chiffrement avec la clé publique et déchiffrement avec la clé privée.
- Note de synthèse : confidentialité, authenticité, intégrité et non-répudiation.