FSBM
2024-2025
Master DSBD
Sécurité de données & Blockchain

TD2- Introduction à la sécurité de données
Cryptographie

Exercice 1

On souhaite générer une paire de clés RSA à partir de n=221 et φ(n)=192.

1. Déterminer les valeurs de p et q.
2. Calculer la clé privée correspondante à e=5
3. Chiffrer le message M=42, puis déchiffrer le résultat.

Exercice 2

Bob choisit comme nombre premier p = 17 et q = 19, comme exposant e = 5. Alice et lui se fixent un protocole RSA dans lequel les messages sont des nombres en base 10 que l'on code par bloc de 2 chiffres. Alice veut envoyer le message 462739.

1. Donnez la clé publique de Bob.
2. Donnez la clé secrète d de Bob.
3. Ecrivez le message chi re que Alice envoie a Bob.
4. Déchiffrez le message qua reçu Bob et vérifiez que c'est bien celui qu'a envoyé Alice.

Exercice 3 : Factoring Attack (Factorisation de N)

On vous donne une clé publique :

- N=143, e=7

Message chiffré : C=80

1. Retrouvez p et q en factorisant N.
2. Calculez φ (N).
3. Trouvez d (inverse modulaire de e modulo ϕ(N)).
4. Déchiffrez C pour retrouver M.

Exercice 4 : Attaque par facteur commun

Deux utilisateurs ont les clés publiques suivantes :

- **Alice** : n_A=18721, e_A=5
- **Bob** : n_B=27641, e_B=3

L'attaquant découvre que les deux partagent un facteur premier.

1. Trouvez ce facteur commun en calculant le PGCD de n_A et n_B.
2. Factorisez n_A et n_B grâce à ce facteur.
3. Calculez les clés privées de chaque utilisateur.

Exercice 5 : Utilisation de *PyCryptodome*

1. Générer une paire de clés RSA avec une taille de 2048 bits.
2. Exporter la clé publique et la clé privée en format PEM.
3. Chiffrer le message "RSA avec PyCryptodome" avec la clé publique.
4. Déchiffrer ce message avec la clé privée.
5. Signer le message avec la clé privée.
6. Vérifier la signature avec la clé publique