1. Définir la cryptographie, la cryptanalyse et la cryptologie.

Exercice 1

Le chiffrement de données constitue l'une des solutions adoptées pour renforcer la sécurité logique. En utilisant le code de césar codez le message suivant avec une clé k=9 ;

M=Travaux dirigés du module SSI

Soit le message chifré suivant C=VOC PSXC XO TECDSPSOXD ZKC VOC WYIOXC

Trouvez le message clair M tel que k_e=10.

Exercice 2

Un professeur envoie ses notes au secrétariat de l'École par mail. La clef publique du professeur est (3,55); celle du secrétariat est (3,33).

1. Vérifier que la clef privée du professeur (supposée connue de lui seul) est 27; et que celle du secrétariat est 7.
2. Pour assurer la confidentialité de ses messages, le professeur chiffre les notes avec la clef RSA du secrétariat. Quel message chiffré correspond à la note 12 ?
3. Pour assurer l'authenticité des messages contenant les notes, le professeur signe ses messages pour le secrétariat aprés les avoir chiffrés. Le secrétariat reçoit le message 23.

Quelle est la note correspondante ?

Exercice 3

Soit un système de chiffrement où p = 11 et q = 23. Trouvez n, e et d.

- Calculer les clés (privée et publique).
- Chiffrez le message m = 165
- Mêmes questions pour : p = 29, q = 37 et p=5, q=11

2. Soit un système de chiffrement où p=131 q=151 et e=11143
   - Calculer d, quel entier positif inferieur à p.q sera le message en clair si le message codé est c=141 ?

Exercice 4

II-On veut assurer la confidentialité d'un document en chiffrant son contenu par le code de Vigenère.

1. Le chiffrement de Vigenere fait partie de quelle famille de code ?
2. Chiffrer avec le chiffre de Vigenère le texte suivant M= **BONNE CHANCE** tel que la taille du bloc est m = 4, n_1 = 5, n_2 = 14, n_3 = 7, n_4 = 25

– Pour le même texte en clair on obtient le texte chiffré suivant **GSRLRGYUESNSQSWGQSL**.

3. Quels sont les clés utilisées telle que m=4?

Exercice 5

Alice publie les données suivantes

n = pq = 221 et e = 13.

- Bob reçoit le message C = 65 et la signature digitale correspondante S = 182.
- Vérifier la signature.