

### Devoir Surveillé 1

**Exercice 1** – Expliquer pourquoi 257 est inversible modulo 2357 et déterminer son inverse.

**Exercice 2** –

1) Définir le chiffrement de Vigenère.

2) Le message suivant :

Longtemps je me suis couché de bonne heure  
a été chiffré par la méthode de Vigenère et on a obtenu le message

CCZGGVABSWVAQSHZGOOHTVQDRSCZNRYSGRR

Déterminer la clef qui a été utilisée.

**Exercice 3** –

1) Expliquer pourquoi l'équation suivante n'a pas de solutions dans  $\mathbb{Z}/26\mathbb{Z}$  :

$$2x + 3 \equiv 4 \pmod{26}.$$

2) Montrer que l'équation suivante a exactement 2 solutions dans  $\mathbb{Z}/26\mathbb{Z}$  et les déterminer :

$$2x + 3 \equiv 7 \pmod{26}.$$

3) Montrer que pour tout  $a \in \mathbb{Z}/26\mathbb{Z}$ , l'équation suivante a exactement une seule solution dans  $\mathbb{Z}/26\mathbb{Z}$  et déterminer cette solution en fonction de  $a$  :

$$3x + 2 \equiv a \pmod{26}.$$

4) Un message a été chiffré à l'aide du chiffrement affine, avec la clé  $(3, 2)$ . Donner le message original, si le cryptogramme est

JODSKOKBLOIXOIE