

Congruences - 2 : Applications, Cryptographie, etc.

NOM et PRENOM : *Il faut tout justifier et expliquer!*

1. Vigenère - modèle mathématique.

Chiffrez le message JOYEUX NOEL avec le vers littéral FETES à l'aide du modèle mathématique de Vigenère.

2. Hill.

On donne la matrice

$$A = \begin{pmatrix} 3 & 1 & 2 \\ 4 & 7 & 5 \\ 5 & 3 & 11 \end{pmatrix}$$

- Vérifiez que cette matrice peut bien être utilisée comme une matrice de Hill d'ordre 3.
- Un texte, chiffré avec cette matrice, a donné le message EOKCYQZRQ .
Déchiffrez ce message!

3. RSA.

Anémone possède la clé publique $(E_A; n_A) = (103; 143)$. Bernadette possède la clé publique $(E_B; n_B) = (11; 187)$.

- Vérifiez que ces deux clés remplissent bien les conditions des clés publiques (détails!).
- Anémone veut envoyer le texte 4 signé-chiffré à Bernadette. Que recevra Bernadette?