

Principe du chiffrement affine :

On numérote de 0 à 25 les vingt-six lettres de l'alphabet français.

On code un nombre x en lui associant le reste de la division euclidienne de $ax + b$ par 26.

Le couple $(a; b)$ est la clé du codage : c'est une clé secrète connue seulement du chiffreur et du déchiffreur.

►1. En utilisant la clé (3; 4), coder le mot « NEPER ». Retrouver le mot codé par « OUCPDQ ».

►2. En utilisant la clé (13; 7), coder les mot « GALOIS » et « MOBIUS ». Que peut-on en dire ?

►3 a) Sur un tableur, en utilisant la clé (11; 4), coder la citation “L'essence des mathématiques, c'est la liberté” de Georg Cantor.

b) Déterminer un nombre entier a entre 0 et 25 tel que $11 \times a \equiv 1 [26]$. En déduire la fonction de décodage.

c) Décoder alors le message suivant, codé avec la clé (11; 4), :

V W U A D E Q U U Q J W U U C R F Q R O R U F J Q G W R F N C Q J G E J A D
W J V W U G E F D W G E F O Y Q W U U C R F Q R O R U F J Q G W R F N C Q J
N W R U W J C R N W Q F G E J A D W J U E R U A D E Q U U Q J W U G E O U C
R B E G C O R U V C O R
Z W E R G E J O W U C Q J O E Q

►4. On intercepte le message français ci-dessous, codé par un chiffrement affine dont **la clé est inconnue** :

N V L L X Q U P X C D R U R G F Z X G X P L D U M X L D U R F Z X P F Z R P
V Q U Z Q A K V S Z R U S X G D A X Q P X X M Z L D R Q X R Q S X A X Q S D
Q U S X G X O A X K R X Q N X P V R X Q U P R D S L R K D I G X L X Q U D S
D A U X X P D Z O V I W X U P S X G D K X D G R U X