**Exercice 5.** (affine)

1. On représente l’alphabet latin par les entiers entre 0 et 25 avec la convention

A = 0;B =1;C = 2; … ; Z=25

Un chiffrement affine x 🡺 ax+b mod 26 transforme le message CRYPTO en le cryptogramme ROXEYZ. Trouver la clé (a; b) correspondante.

2. Le message clair CRYPTO a cette fois été chiffré deux fois de suite par un chiffre affine de clé (a’; b’) (c’est-à-dire qu’on a chiffré le chiffré) pour donner en sortie NGBAMX.

(a) Montrer que NGBAMX est le chiffré de CRYPTO par un chiffre affine de clé (a’’; b’’),

(b) Trouver (a’’; b’’).

**Solution :**

1. Un chiffrement affine x 🡺 ax+b mod 26 transforme le message CRYPTO en le cryptogramme ROXEYZ.

Etant donné que :

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Alors :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| C | R | Y | P | T | O |
| a.2+b=17 | a.17+b=14 | a.24+b=23 | a.15+b=4 | a.19+b=24 | a.14+b=25 |
| R | O | X | E | Y | Z |

Les valeurs de a et b peuvent être déduites à partir des équations le la deuxième ligne du tableau précédent. Donc : (a,b) = ( ?, ?)

1. a)

Si on chiffre une fois un caractère par un chiffre affine de clé (a’; b’) on obtient :

(a’x+b’)

Si on chiffre pour la deuxième fois le caractère obtenu de l’étape précédente (a’x+b’) par un chiffre affine de clé (a’; b’) on obtient :

(a’ (a’x+b’) + b’) = a’2 x + (a’ b’ + b’)= a’’ x+b’’

On a remplacé a’2 par a’’ et (a’ b’ + b’) par b’’ on obtient donc un chiffre affine de clé (a’’; b’’).

b) pour calculer (a’’,b’’) on procède de la même manière que la question N°1 :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| C | R | Y | P | T | O |
| a’’.2+b’’=13 | a’’.17+b’’=6 | a’’.24+b’’=1 | a’’.15+b’’=0 | a’’.19+b’’=12 | a’’.14+b’’=23 |
| N | G | B | A | M | X |

Les valeurs de a’’ et b’’ peuvent être déduites à partir des équations le la deuxième ligne du tableau précédent. Donc : (a’’,b’’) = ( ?, ?)

**Exercice 6**: ( permutation)

1. Définir le chiffrement par permutation.

2. Coder le message “la rencontre est prévue à la cafétéria” à l’aide de cette méthode et de la clé suivante :

 1 2 3 4

 K =

 2 4 1 3

3. Décoder le message « MELSEGESEADESCTPTREY » sachant qu’il a été créé avec la clé suivante :

 1 2 3 4 5

 K =

 3 4 1 5 2

**Solution :**

1. Définir le chiffrement par permutation.

Le chiffrement par **transposition** consiste à écrire le texte clair dans un tableau/une grille, puis à arranger les colonnes de ce tableau selon une **permutation** définie. S'il existe des cases vides, les remplir avec une lettre neutre (comme X).

La clé de permutation est une série de nombres (qui peut être générée à partir d'un mot) qui indique dans quel ordre arranger les colonnes.

Exemple : Le mot KEY permet de générer la permutation 2,1,3 :

|  |  |  |
| --- | --- | --- |
|  | Avant le tri alphabétique | Après le tri alphabétique |
| Mot clé | K,E,Y | E,K,Y |
| Ordre des colonnes | 1,2,3 | 2,1,3 |

Exemple : Chiffrer DCODE avec la clé KEY (permutation 2,1,3).

|  |  |  |  |
| --- | --- | --- | --- |
| Colonnes | 1,2,3 | Colonnes triées | 2,1,3 |
| Texte clair | D,C,O | Texte chiffré | C,D,O |
|  | D,E,X |  | E,D,X |

Le message chiffré est constitué du tableau après permutation des colonnes selon l'ordre de la clé. Le texte chiffré est : CDOEDX.

Le déchiffrement par **transposition** est identique au chiffrement, sauf que l'ordre des colonnes est changé.

Exemple : Une permutation 2,1,3 a permis d'obtenir le message CDOEDX (lecture par lignes):

|  |  |  |  |
| --- | --- | --- | --- |
| Colonnes | 2,1,3 | Colonnes triées | 1,2,3 |
| Texte chiffré | C,D,O | Texte clair | D,C,O |
|  | E,D,X |  | D,E,X |

Exemple : Le texte clair est DCODEX.

2. Coder le message “la rencontre est prévue à la cafétéria” à l’aide de cette méthode et de la clé suivante :

 1 2 3 4

 K =

 2 4 1 3

|  |  |  |  |
| --- | --- | --- | --- |
| Colonnes | 1 2 3 4 | Colonnes triées | 2 4 1 3 |
| Texte clair | l,a,r,e | Texte chiffré | a,e,l,r |
|  | n,c,o,n |  | c,n,n,o |
|  | t,r,e,e |  |  |
|  | s,t,p,r |  |  |
|  | e,v,u,e  |  |  |
|  | a,l,a,c |  |  |
|  | a,f,é,t |  |  |
|  | e,r,i,a |  |  |

Le message chiffré est :………………………..

3.Décoder le message « MELSEGESEADESCTPTREY » sachant qu’il a été créé avec la clé suivante :

 1 2 3 4 5

 K =

 3 4 1 5 2

|  |  |  |  |
| --- | --- | --- | --- |
| Colonnes | 3 4 1 5 2 | Colonnes triées | 1 2 3 4 5 |
| Texte chiffré | M,E,L,S,E | Texte clair | L,E,M,E,S |
|  | G,E,S,E,A |  | S,A,G,E,E |
|  | D,E,S,C,T |  |  |
|  | P,T,R,E,Y |  |  |

Le message clair est :………………