**Exercice 7** (Chiffrement de Polybe)

On considère l’alphabet privé de W, soit 25 lettre Polybe (200-125 av J.C). Il a proposé le mécanisme suivant : On range les lettres dans un tableau 5\*5, en commençant par le mot clé et on supprimant les doublons, puis on continue avec les lettres restantes de l’alphabet, dans l’ordre. Par exemple avec le mot clé MYSTERE, on construit le tableau suivant :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 |
| 1 | M | Y | S | T | E |
| 2 | R | A | B | C | D |
| 3 | F | G | H | I | J |
| 4 | K | L | N | O | P |
| 5 | Q | U | V | X | Z |

Le chiffrement s’effectue alors en remplaçant la lettre par les deux chiffres: ligne + colonne qui indique sa position dans la grille. Par exemple F est chiffré par 31

1. Expliquez comment on peut cryptanalyser un tel système.
2. Raoul a envoyé un message à Anna pour fixer un rendez-vous. Le cryptogramme est le suivant :

123222 512215 424215 512242 242255 534352 111524 225254 322252

512211 515222 532251 142251 154352 21

Décrypter ce message

**Solution**

1. Les dernières lettres du tableau sont rangées dans l’ordre alphabétique, la reconstruction est très rapide. Il faut se baser sur la fréquence d’apparition des lettres (savoir la langue) le chiffrement étant une substitution mono-alphabétique.
2. Pour décrypter ce message nous avons :

chere anna rendez vous a deux heures rue ver 14e raoul

* 1. La présence de 55 supposé **z.**
  2. La fréquence d’apparition de 22 supposé **e**.
  3. La présence des mots comme raoul et anna (mot symétrique)

On obtient te message claire :

« CHERE ANNA RENDEZ VOUS A DEUX HEURES RUE VERTE RAOUL »

**Exercice 8 : (**Chiffrement affine)

Le chiffrement affine consiste à chiffrer toute lettre claire m en une lettre c égale à :

c = (am + b) (mod 26); f(x)=ax+b

où a et b sont deux entiers compris entre 0 et 25 fixés. Le couple (a; b) est la clé de chiffrement. Pour le choix de la clé tous les couples (a; b) ne conviennent pas. Il est nécessaire que a soit inversible modulo 26, ce qui est le cas si a et 26 sont premiers entre eux.  
Pour déchiffrer, on calcule la lettre claire m par l'équation m = a-1(c - b) (mod 26);où a-1 est l'inverse de a modulo 26, c'est à dire l'unique entier x compris entre 0 et 25 tel que ax (mod 26) = 1.

1. Combien y a-t-il de clés ? 26x26

2. Le cryptogramme qui suit a été chiffré avec la clé (a; b) = (11; 17). Déchiffrez-le.

YREHI HRDEJ QJDWJ YRUUI DJENJ  
DESVA JYREH IJHOB EFSHB KREHN  
QRAJR DTPDR OJNNP WYPEW JTAIR  
NRESI JWDCR ENPDS WPAIP EFNPT  
TJHBP EIDBR ORBSS BWJYJ HHDHI  
JHFJE HYJHN JEYJE SIJSV AJJEL  
DJHSB PEHBW WBSJN PESWJ DEOPB  
HBEBI IDBWJ AWPNQ JYJIJ CPDHN  
DIJWN QRLDJ UPBHL DBIAR HHJLD  
JILDD ESPEA IJDWE BNQRW YLDBH  
JOJDS TJNQR ES

3. Retrouvez la clé utilisée pour obtenir le cryptogramme ci-dessous.  
UJWXN WMJCJ GGPGP MVMPU PCPZS

JWFGP XPUPM GJZJW SGPGR WFUNW   
PGVFW PUCRV SPNWA RBRVU PJMCP   
XPWSJ WSNWP ZJGRS SPXMA PCVHN   
PPWSR NCPPU PUPNY XVWNX RVUPX   
JNUPX XNXUN WPMJC SVPZT GVWUC   
VHNPU PGRWF NPNCX NMPCV PNCPJ

WMCPX PWSPN WMRVW SUPZR WSJZS   
JIPZN WARBR VUPSC VIVJG EUPBR   
WSCPC HNPZP MRVWS UPZRW SJZSP   
XSNWM RVWSU PCPEC RNXXP BPWS

**Solution :**

1. Nous avons **c = (am + b) (mod 26).** Cette équation est équivalente à **am=c-b (mod 26)**

donc **m=a-1 (c-b) (mod 26)**, où a-1 est l'inverse de a modulo 26, c'est à dire l'unique entier x compris entre 0 et 25 tel que : ax (mod 26)= 1.

Etant donné que a doit être inversible modulo 26, ce qui est le cas si a et 26 sont premiers entre eux. Il faut donc trouver les a *∈* {0.1.2………25} qui sont premiers avec 26. Il est facile de vérifier que les éléments 1*;* 3*;* 5*;* 7*;* 9*;* 11*;* 15*;* 17*;* 19*;* 21*;* 23 et 25 sont premiers avec 26. En effet ce sont les seuls éléments qui ne sont divisibles ni par 2 ni par 13.

Le nombre de clef possible est le nombre de *a* premiers avec 26 multiplié par 26 (le nombre de *b*). Donc nous avons 12 choix possibles pour *a* et 26 pour *b*, au total =12 x 26 = 312 clés possibles.

1. Etant donné que la clé de chiffrement est (a; b) = (11; 17). Rappelons que :

**11−1 (mod26)=19** (19×11=1(mod26)).

La fonction de chiffrement est : **c = (11 m *+* 17) (mod 26)**

et celle de déchiffrement est : **m =19 (c-17) (mod 26) = 19c - 11 (mod 26)**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |

La fonction de déchiffrement est : **m = 19 c - 11 (mod 26)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| c | Y | R | E | H | I |
| calcul | 19.24 - 11 =3 | 19.17 - 11 =0 | 19.4 - 11 = 13 | 19.7 - 11 =18 | 19.8 - 11 = 11 |
| m | D | A | N | S | L |

En suivant l’exemple précédent à partir du cryptogramme suivant :

YREHI HRDEJ QJDWJ YRUUI DJENJ  
DESVA JYREH IJHOB EFSHB KREHN  
QRAJR DTPDR OJNNP WYPEW JTAIR  
NRESI JWDCR ENPDS WPAIP EFNPT  
TJHBP EIDBR ORBSS BWJYJ HHDHI  
JHFJE HYJHN JEYJE SIJSV AJJEL  
DJHSB PEHBW WBSJN PESWJ DEOPB  
HBEBI IDBWJ AWPNQ JYJIJ CPDHN  
DIJWN QRLDJ UPBHL DBIAR HHJLD  
JILDD ESPEA IJDWE BNQRW YLDBH  
JOJDS TJNQR ES

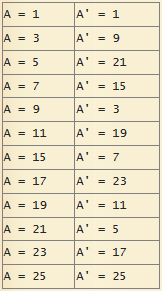
On obtient le message clair suivant :

DANS LSA UNE HEURE DAFFLUENCE UN TYPE DANS LES VINGT SIX ANS CHAPEAU MOU AVEC CORDON REMPLACANT LE RUBAN COU TROP LONG COMMESION LUI AVAIT TIRE DESSUS LES GENS DESCENDENT LE TYPE EN QUESTION SIRRITE CONTRE UN VOISIN IL LUI REPROCHE DE LE BOUSCULER CHAQUE FOIS QUIL PASSE QUELQUUN TON PLEURNICHARD QUI SE VEUT MECHANT

3. Pour retrouver la clé, il y a deux techniques possibles :

* La première technique consiste à tester toutes les valeurs possibles pour les coefficients a et b. Alors le coefficient a peut prendre 12 valeurs et le coefficient b peut prendre 26 valeurs soit seulement 312 tentatives à réaliser.

Les tests peuvent se faire en utilisant la fonction de déchiffrement suivante: **m = a’ (c – b’) (mod 26).** Tels queb' a la même valeur que b et la valeur de a' dépend de a puisque a’=a-1. Donc, les valeurs possibles de a' sont les suivantes :



Après les tests le message le plus significatif que nous pouvons obtenir est le suivant:

DANSUNPARALLELEPIPEDERECTANGLESEDEPLACANTLELONGDUNELIGNEDROITEUNHOMOIDEAPRESENTANTUNECALOTTESPHERIQUEENTOUREEDEDEUXSINUSOIDESAUDESSUSDUNEPARTIECYLINDRIQUEDELONGUEURSUPERIEUREANPRESENTEUNPOINTDECONTACTAVECUNHOMOIDETRIVIALBDEMONTRERQUECEPOINTDECONTACTESTUNPOINTDEREBROUSSEMENT

Donc la clé qui a été utilisée pour chiffrer ce message est bien: **(a,b) = (21,9)**

* La deuxième technique est basée sur l’analyse des fréquences d’occurrence des lettres dans un texte écrit dans une langue donnée (par exemple, l’anglais ou le français). Dans le cas présent, on effectue une hypothèse simplificatrice : on suppose que le texte clair est **un message rédigé en français.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Les fréquences pour la langue française** | |  | **Les fréquences pour le cryptogramme donné** | |
| Lettre | Pourcentage |  | Lettre | Nombre d’occurrence |
| E | 17.76 |  | P | 50 |
| S | 8.23 |  | W | 28 |
| A | 7.68 |  |  |  |
| N | 7.61 |  |  |  |

A partir de ces deux tableaux et de la formule de chiffrement **(a m *+* b) = c (mod 26),** on peut faire les suppositions suivantes:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| c | p | w | w | w |
| calcul | a.4+b =15 mod 26 | a0+b=22 mod 26 | a18+b=22 mod 26 | a13+b=22 mod 26 |
| m | e | a | s | n |
| Le système d’équations à résoudre |  | 4a+b=15 mod 26  0a+b=22 mod 26 | 4a+b=15 mod 26  18a+b=22 mod 26 | 4a+b=15 mod 26  13a+b=22 mod 26 |
|  |  | Pas de solution  Donc w ne correspond pas à la lettre claire a | **Pas de solution**  Donc w ne correspond pas à la lettre claire s | **a=21 ; b=9**  Donc w correspond à la lettre claire n |

Donc la clé qui a été utilisée pour chiffrer ce message est bien : **(a,b) = (21,9)**