# *CHIFFREMENT DÉCHIFFREMENT*

Quel que soit le mode de chiffrement, la première étape consiste à associer un nombre à chaque lettre de l'alphabet, après avoir supprimé les accents et les espaces entre mots.

On utilisera la table suivante :

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

## *I) Chiffrement par décalage*

- Le principe consiste à ajouter au nombre *n*, correspondant à chaque lettre, un entier naturel *a* appelé « clé de déchiffrement » et à garder son reste modulo 26.
- Le nombre *m* obtenu est tel que $m \equiv n + a\ [26]$ et $0 \leq m < 26$. On code alors le nombre *m* par la lettre correspondante.

**E1 :** Expliquer alors le principe de décodage.

- Ce codage se développa à l'époque romaine, sous Jules César. Elle perdura longtemps, notamment grâce à la faible alphabétisation des populations.
- Si, pendant la seconde guerre mondiale, les Alliés avaient utilisé ce codage, ils auraient, par exemple, utilisé le mot GHEDUTXHPHQW.
- La fréquence d'apparition des lettres dans la langue française étant très régulière, la lettre E apparait au moins deux fois plus souvent que les autres lettres les plus utilisées.
- En supposant cette propriété respectée dans ce message, déterminer la clé de chiffrement et déchiffrer le message.

## *II) Chiffrement affine*

### 1) Chiffrement

- Il nécessite une clé de chiffrement constituée de deux entiers *a* et *b* avec $0 < a \leq 25$ et $0 \leq b \leq 25$.
- Le principe consiste à associer au nombre *n*, le nombre *m* tel que $m \equiv an + b[26]$ et $0 \leq m \leq 25$.

**E2 :** a) Que peut-on dire de *m* ?
b) Si la clé du chiffrement est le couple (3 ; 11), déterminer le chiffrement de la lettre M.
c) À l'aide la calculatrice, chiffrer le mot MATHS.

- À l'aide d'un tableur : en informatique, **le code ASCII** consiste à associer à chaque caractère (lettre de l'alphabet (majuscule et minuscule), chiffre, signe de ponctuation, …) un code numérique *n* tel que $0 \leq n \leq 255$.
- Dans la plupart des tableurs, le code ASCII est donné par la fonction CODE.
- La fonction réciproque est habituellement CAR.
- Exemple : « = CODE(A) » renvoie le nombre 65 et « = CAR(65) » renvoie la lettre A.
- Pour simplifier, nous ne nous intéresserons ici, qu'au codage ASCII des lettres majuscules pour coder le mot : « MATHEMATIQUES »

**E3 :** a) Entrer le message dans la première ligne.
b) Chiffrer le message en code ASCII en ligne 2.
c) Chiffrer le message en ligne 3 par la fonction *C* qui à tout *n* entier appartenant à [65 ; 91] associe le reste de la division de $3(n - 65) + 11$ par 26.
d) Reproduire et compléter le tableau sur un tableur :

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | | | message | M | A | T | H | E | M | A | T | I | Q | U | E | S |
| 2 | | | | n (code ASCII) | 77 | 65 | 84 | 72 | | | | | | | | | |
| 3 | | | | N=n-65 | 12 | 0 | 19 | 7 | | | | | | | | | |
| 4 | a= | 3 | | aN+b(modulo26)+65 | 86 | 76 | 81 | 71 | | | | | | | | | |
| 5 | b= | 11 | | message codé | V | L | Q | G | | | | | | | | | |

Dans la cellule E2, on entre ……. ,
Dans E3 ……..,
Dans E4 ……
Dans E5……...

**Deux problèmes se posent :**

**E4 :** a) Un code est exploitable lorsque deux lettres distinctes sont codées par deux lettres distinctes. Est-ce toujours le cas pour un chiffrement affine ?
b) Peut-on trouver une clé permettant de déchiffrer un message codé ?

### 2) Conditions pour qu'un chiffrement affine soit exploitable

**E5 :** a) On suppose $a = 3$.
Montrer que deux lettres distinctes sont chiffrées par deux lettres distinctes
b) On suppose que $a = 2$ et $b = 7$.
Déterminer deux lettres distinctes chiffrées par la même lettre.
c) **Généralisation** : Montrer que si *a* est premier avec 26, deux lettres distinctes sont toujours chiffrées par deux lettres distinctes et que si *a* et 26 ne sont pas premiers entre eux, alors les lettres chiffrées par *n* et $n + \frac{26}{g}[26]$, où *g* est le PGCD de *a* et 26, sont chiffrées par la même lettre.

### 3) Déchiffrement

- Pour tout chiffrage affine de clé (*a* ; *b*) tel que *a* est premier avec 26, on se propose de trouver une clé (*a'* ; *b'*) permettant de déchiffrer un message codé en utilisant le même procédé.

**E6 :** a) Montrer que si $aa' \equiv 1\,[26]$ et $a'b + b' \equiv 0\,[26]$, alors le couple (*a'* ; *b'*) convient.
b) Justifier qu'il existe deux entiers *u* et *v* tels que $au + 26v = 1$.
c) En déduire l'existence d'un nombre *a'* tel que $aa' \equiv 1\,[26]$.
d) On suppose que $a = 5$ et $b = 9$. Déterminer un couple (*u* ; *v*) tel que $au + 26v = 1$.
En déduire une valeur de *a'* puis de *b'*. Déchiffrer alors à l'aide du tableur : KXKDMJVGDRJAS
e) Même chose avec $a = 5$ et $b = 17$ et SFBIJFYL.

### 4) Déchiffrement sans clé de chiffrement

Pierre intercepte le message suivant :

TU SATUMT NHMTTU.

Il n'a pas la clé de chiffrement mais il pense la retrouver à l'aide du premier mot car il espère que celui-ci est LE.

**E7 :** a) Montrer que la clé ($a$ ; $b$) vérifierait alors le système : $\begin{cases} 11a+b \equiv 19[26] \\ 4a+b \equiv 20[26] \end{cases}$.

b) En déduire que $7a \equiv -1[26]$

c) Déterminer un couple ($u$ ; $v$) tel que $7u + 26v = 1$ et en déduire une valeur de $a$ qui convient.

d) Déterminer $b$ et déchiffrer le message à l'aide du tableur.

## *III) Chiffrement de Vigenère*

**1) Principe :** Avec le chiffrement de Vigenère, une lettre n'est pas toujours codée par la même lettre dans un message, ce qui rend l'analyse des fréquences d'apparition des lettres inutilisable.

**Règle** : on choisit une clé qui déterminera le décalage pour chaque lettre du message :

| message | B | O | N | J | O | U | R | M | O | N | A | M | I |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *n* | 1 | 14 | 13 | 9 | 14 | 20 | 17 | 12 | 14 | 13 | 0 | 12 | 8 |
| clé | C | E | S | A | R | C | E | S | A | R | C | E | S |
| décalage | 2 | 4 | 18 | 0 | 17 | 2 | 4 | 18 | 0 | 17 | 2 | 4 | 18 |
| *m* | 3 | 18 | 5 | 9 | 5 | 22 | 21 | 4 | 14 | 4 | 2 | 16 | 0 |
| message codé | D | S | F | J | F | W | V | E | O | E | C | Q | A |

**E8 :** 1) À l'aide d'un tableur, chiffrer le message suivant :

| | A | B | C | D | E | F | G | H | I | J |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Vigénère | | clé : CESAR | | | | | | | |
| 2 | | | | | | | | | | |
| 3 | | message | V | A | C | A | N | C | E | S |
| 4 | | n | 21 | 0 | | | | | | |
| 5 | | clé | C | E | S | A | R | C | E | S |
| 6 | | décalage | 2 | 4 | | | | | | |
| 7 | | m | 23 | 4 | | | | | | |
| 8 | | message codé | X | E | | | | | | |
| 9 | | | | | | | | | | |

- Pour déchiffrer, il suffit, si on connait la clé, de la soustraire au texte chiffré.

### 2) Déchiffrement sans clé

- On suppose que la longueur de la clé est de trois lettres.
- On donne un texte chiffré avec cette clé dont le début est donné ci-dessous.
- Les lettres ont été regroupées par paquets de trois.

NEK UVG DST CIC VWW SYP BVD SIR FVE IIV FRV JXG OWQ OFG DYP GVK NEI F…

- En étudiant les fréquences d'apparitions des lettres sur l'ensemble du texte, on a les résultats suivants :
  - La première lettre de chaque « paquet » la plus fréquente est le F
  - La lettre centrale la plus fréquente de chaque « paquet » est le I
  - La dernière la plus fréquente de chaque « paquet » est la lettre G.

**E9 :** En admettant que la lettre le plus fréquente d'un groupe de lettres assez grand soit un E, déterminer la clé de chiffrement.

| | F | I | G |
|---|---|---|---|
| *m* (message codé chiffré) | 5 | 8 | 6 |
| codage | E | E | E |
| *n* (lettre initiale chiffrée) | 4 | 4 | 4 |
| décalage | | | |
| clé | | | |

Déchiffrer alors le début du message

## *IV) Chiffrement de Hill*

**1) Principe :** Le chiffrement de Hill transforme des chaînes de caractères de longueur donnée, chaque lettre étant alors transformée en fonction de sa valeur et de sa place dans la chaîne de caractères.

- On se donne un entier $n$ supérieur ou égal à 2. Le texte à chiffrer est découpé en blocs successifs de $n$ lettres.
- S'il y a un reste, on peut compléter arbitrairement le texte ou l'amputer du bloc incomplet.
  Les lettres de chaque bloc sont remplacées par des nombres.
- À chaque bloc de lettres est associée une matrice colonne $B_i$ à $n$ lignes.
- On se donne une matrice carrée $M$ d'ordre $n$, appelée *matrice de chiffrement*, connue de l'expéditeur et du destinataire du message, à coefficients entiers naturels.
- Le produit $C_i = M \times B_i$ est une matrice-colonne qui peut à son tour être transformée en une suite de $n$ lettres, chacun de ses éléments étant ramené à son **reste modulo 26** puis transformé en la lettre correspondante de l'alphabet.
- Pour décoder, il faudra faire le chemin inverse. Si toutefois la suite des deux opérations (produit de la colonne par la matrice suivie de détermination du reste modulo 26) définit une matrice inversible.

**E10 :** ***Un exemple de chiffrage lorsque n = 2***

On utilise la matrice $M = \begin{pmatrix} 2 & 5 \\ 3 & 4 \end{pmatrix}$ comme matrice de codage. On cherche à coder le mot SOLEIL c'est-à-dire : 18 – 14 – 11 – 4 – 8 – 11.

a) Déterminer le découpage en blocs $B_i$ de deux lettres et leur transformation en matrices-colonnes.

b) Déterminer les matrices-colonnes $C_i = M \times B_i$ obtenues par l'action de $M$ sur les matrices colonnes précédentes

c) Déterminer les matrices-colonnes $D_i$, transformées de $C_i$ modulo 26.

d) Déterminer alors le texte chiffré.

## 2) Conditions pour que le chiffrement de Hill soit exploitable

On cherche une condition sur la matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ pour que deux matrices colonnes distinctes $\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$ et $\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}$ soient codées par deux matrices colonnes distinctes $\begin{pmatrix} x_1' \\ y_1' \end{pmatrix}$ et $\begin{pmatrix} x_2' \\ y_2' \end{pmatrix}$

On suppose par exemple que $x_1$ et $x_2$ sont différents.

**E11 :** Montrer que, du système $\begin{cases} x_1' \equiv x_2' [26] \\ y_1' \equiv y_2' [26] \end{cases}$, on peut déduire que $(ad-bc)(x_1 - x_2) \equiv 0 [26]$, et que $ad - bc$ et 26 ne sont pas premiers entre eux.

- Une condition **nécessaire** pour que deux blocs différents de lettres soient chiffrés différemment est donc que ***ad – bc* et 26 soient des entiers premiers entre eux**.
- On admet qu'elle est suffisante pour assurer le déchiffrage de tout message.

**E12 :** ***Un exemple de déchiffrage***

1) Justifier que la matrice $M = \begin{pmatrix} 2 & 5 \\ 3 & 4 \end{pmatrix}$ est inversible et déterminer sa matrice inverse.

2) Cette matrice ne répond pas au problème posé, puisque ses coefficients ne sont pas entiers, mais ses coefficients vont permettre de répondre au problème. Pour assurer le déchiffrage, il suffit de déterminer une matrice $N$ à coefficients entiers telle que les coefficients des matrices $M \times N$, $N \times M$ et $I_2$ soient congrus modulo 26.
Calculer $\begin{pmatrix} 2 & 5 \\ 3 & 4 \end{pmatrix} \times \begin{pmatrix} -4 & 5 \\ 3 & -2 \end{pmatrix}$ et $\begin{pmatrix} -4 & 5 \\ 3 & -2 \end{pmatrix} \times \begin{pmatrix} 2 & 5 \\ 3 & 4 \end{pmatrix}$.

3) Soit un entier $u$ tel que $7u \equiv 1 [26]$, justifier que la matrice $N = 7u \times M^{-1}$ convient.

4) Il ne reste donc plus qu'à déterminer un entier $u$ vérifiant la condition précédente (c'est-à-dire un inverse de 7 modulo 26) : Justifier qu'il existe des entiers $u$ et $v$ tels que $7u + 26v = 1$ et ensuite qu'il existe un unique entier $u$ compris entre 0 et 25 tels que $7u \equiv 1 [26]$.

5) Soit $M' = 15 \times \begin{pmatrix} -4 & 5 \\ 3 & -2 \end{pmatrix}$. Calculer alors $M \times M'$.

6) Calculer sa congruence modulo 26, notée $P$. On dit que $P$ est la matrice inverse de $M$ modulo 26. Elle sert à déchiffrer un message.

7) Déchiffrer alors le message :

WK – GJ – GI – AZ – CB – ZZ

**E13** : *Clé de validation de numéro de carte bancaire*

Un numéro de carte bancaire est de la forme :
$a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9 a_{10} a_{11} a_{12} a_{13} a_{14} a_{15} c$ où $a_1$, $a_2$,…, $a_{15}$ et $c$ sont des chiffres compris entre 0 et 9.

Les quinze premiers chiffres contiennent des informations sur le type de carte, la banque et le numéro de compte bancaire.

Le chiffre $c$ est la clé de validation du numéro.

Ce chiffre est calculé à partir des quinze autres.

L'algorithme suivant permet de valider la conformité d'un numéro de carte donné.

| | |
|---|---|
| Initialisation | *I* prend la valeur 0 |
| | *P* prend la valeur 0 |
| | *R* prend la valeur 0 |
| Traitement | Pour *k* allant de 0 à 7 |
| | *R* prend la valeur du reste de la division euclidienne de $2a_{2k+1}$ par 9 |
| | *I* prend la valeur *I* + *R* |
| | Fin Pour |
| | Pour *k* allant de 1 à 7 |
| | *P* prend la valeur $P + a_{2k}$ |
| | Fin Pour |
| | *S* prend la valeur *I* + *P* + *c* |
| Sortie | Si *S* est un multiple de 10 alors |
| | Afficher « *Le numéro de la carte est correct.* » |
| | Sinon |
| | Afficher « *Le numéro de la carte n'est pas correct.* » |
| | Fin Si |

1) On considère le numéro de carte suivant : 5635 4002 9561 3411.

a) Compléter le tableau en annexe permettant d'obtenir la valeur finale de la variable *I*

b) Justifier que le numéro de la carte : 5635 4002 9561 3411 est correct.

c) On modifie le numéro de cette carte en changeant les deux premiers chiffres. Le premier chiffre (initialement 5) est changé en 6. Quel doit être le deuxième chiffre *a* pour que le numéro de carte obtenu 6*a*35 4002 9561 3411 reste correct ?

2) On connaît les quinze premiers chiffres du numéro d'une carte bancaire. Montrer qu'il existe une clé *c* rendant ce numéro de carte correct et que cette clé est unique.

3) Un numéro de carte dont les chiffres sont tous égaux peut-il être correct ? Si oui, donner tous les numéros de carte possibles de ce type.

4) On effectue le test suivant : on intervertit deux chiffres consécutifs distincts dans un numéro de carte correct et on vérifie si le numéro obtenu reste correct.
On a trouvé une situation où ce n'est pas le cas, l'un des deux chiffres permutés valant 1. Peut-on déterminer l'autre chiffre permuté ?