

Révision BAC 2023 n°06

Mai 2023

Algorithmique & Programmation**Principe de chiffrement :**

L'idée est d'utiliser comme fonction de chiffrement une fonction affine du type $y = a \cdot x + b$, où a et b sont des constantes, x est le numéro d'ordre de la lettre du message à crypter et y est le numéro d'ordre de la lettre du message chiffrée.

Evidemment, pour que la lettre chiffrée (y) soit aussi un nombre entre 0 et 25, on travaillera avec le modulo 26. La vraie formule sera donc $y = (a \cdot x + b) \bmod 26$.

N.B. : les numéros d'ordres (x et y) sont selon le tableau ci-dessous :

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

Exemple : Soient le message « BRAVO », $a = 3$ et $b = 7$

Message	B	R	A	V	O
x	1	17	0	21	14
y	10	6	7	18	23
Message chiffré	K	G	H	S	X

Principe de Déchiffrement :

Pour déchiffrer une lettre d'ordre y du message chiffré, on calcul l'ordre x de la lettre du message déchiffré par la formule suivante :

$$\begin{cases} x = k * (y - b) \bmod 26 & \text{Si } y \geq b \\ y = 26 + k * (y - b) & \text{Si } y < b \end{cases} \quad \text{Avec } k \text{ est un entier tel que } (a \cdot k) \bmod 26 = 1$$

Exemple :

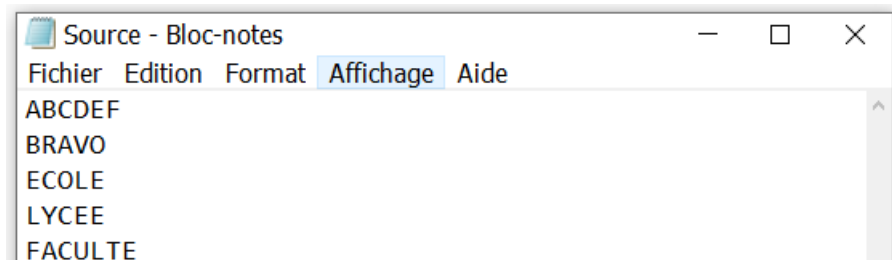
Soient le message « KGHSX », $a = 3$ et $b = 7$

Selon le calcul k vaut 9

Message chiffré	K	G	H	S	X
y	10	6	7	18	23
x	1	17	0	21	14
Message déchiffré	B	R	A	V	O

On se propose de réaliser un programme qui permet :

* **De saisir** à l'aide de l'éditeur de texte disponible le fichier "**Sources.txt**" suivant :



N.B. : Chaque ligne du fichier "**Source.txt**" est formée uniquement par des lettres majuscules.

* De crypter le contenu d'un fichier texte nommé "**Source.txt**" dans un fichier texte nommé "**Crypter.txt**" puis de le décrypter dans le fichier "**Décrypter.txt**".

On se propose de concevoir une interface graphique, comme indiqué dans les figures suivantes, contenant les éléments :

- * Un label contenant le texte : "**Cryptage / Décryptage avec la fonction affine** " comme titre.
- * Trois labels contenant les textes : "Clé : ", "A= " et "B =" suivies de :
 - Une liste déroulante contenant, automatiquement, les valeurs possibles de **A** qui sont 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25
 - Une liste déroulante contenant, automatiquement, les valeurs possibles de **B** qui sont de 0 à 25
- * Un label contenant le texte : "**Opération :**" suivi de 2 boutons Radios intitulés "**Chiffrer**" et "**Déchiffrer** "
- * 3 labels pour les étiquettes "**Fichier source**", "**Fichier chiffré**" et "**Fichier déchiffré**" des 3 ListWidget qui serviront à l'affichage des 3 fichiers "**Source.txt**", "**Crypter.txt**" et "**Décrypter.txt**".
- * Un bouton intitulé "**Appliquer**" qui permet de réaliser l'opération sélectionnée à l'aide des boutons Radios et l'affichage des 3 fichiers.
- * Un bouton intitulé "**Effacer**" qui permet d'effacer les zones d'affichage des fichiers (à programmer).
- * Un bouton intitulé "**Quitter**" qui permet de sortie de l'interface graphique (à programmer).

The diagram shows a GUI window titled "Codage & Décodage par une fonction affine". It features a header bar with a title label and three buttons: "Quitter" (pink), "Effacer" (cyan), and "Appliquer" (yellow). Below the header, there are three sections: "Clé :", "Opération :", and three file display areas labeled "Fichier source", "Fichier chiffré", and "Fichier déchiffré". The "Clé :" section contains labels "A=" and "B=" followed by dropdown menus. The "Opération :" section contains two radio buttons labeled "Chiffrer" and "Déchiffrer".

This screenshot shows the GUI with a callout bubble pointing to the "Clé :" section, containing the text "Message d'erreur si A=1 et B=0". The "Clé :" section shows "A=" with a dropdown menu set to "1" and "B=" with a dropdown menu set to "0". The "Opération :" section shows the "Chiffrer" radio button selected. An error dialog box titled "Erreur" is displayed, with the message "Vous devez choisir la clé avec A et B" and an "OK" button.

This screenshot shows the GUI with the "Clé :" section showing "A=" with a dropdown menu set to "2" and "B=" with a dropdown menu set to "2". The "Opération :" section shows the "Déchiffrer" radio button selected. An error dialog box titled "Erreur" is displayed, with the message "Vous devez choisir une opération Chiffrer ou Déchiffrer" and an "OK" button.

MainWindow

Codage & Décodage par une fonction affine

Quitter

Effacer

Appliquer

Clé :

A=3

B=7

Opération :

☒ Chiffrer

☐ Déchiffrer

Fichier source

Fichier chiffré

Fichier déchiffré

ABCDEF
BRAVO
ECOLE
LYCEE
FACULTE

HKNQTW
KGHSX
TNXOT
OBNTT
WHNPOMT

