# TP1 Graphique : Cryptage / Décryptage avec le chiffre affine

Le chiffre affine est un chiffre de substitution simple.

**Principe de chiffrement :**

L'idée est d'utiliser comme fonction de chiffrage une fonction affine du type **y = a*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 modulo 26. La vraie formule sera donc **y = (a*x + b) mod 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 :

$$\begin{cases} \mathbf{x = k * (y - b) \bmod 26} & \textbf{Si } \mathbf{y \geq b} \\ \mathbf{x = 26 + k * (y - b)} & \textbf{Si } \mathbf{y < b} \end{cases}$$

Avec **k** est un entier tel que (**a*k) mod 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 crypter le contenu d'un fichier texte nommé " **messBrut.txt** " dans un fichier texte nommé "**messCrypt.txt**".
  **N.B. :** Chaque ligne du fichier "**messBrut.txt**" est formée uniquement par des lettres majuscules.
- ✓ De décrypter le contenu d'un fichier nommé "**messCrypt.txt**" dans un fichier texte nommé "**messBrut.txt**".
  **N.B. :** Chaque ligne du fichier "**messCrypt.txt**" est formée uniquement par des lettres majuscules.

On se propose de concevoir une interface graphique contenant les éléments suivants :

- ✓ Un label contenant le texte : "***Cryptage / Décryptage avec le chiffre affine*** " comme titre.
- ✓ Un label contenant le texte : "***Texte clair*** "
- ✓ Un texte Edit qui contiendra le texte clair à crypter importer à partir du fichier "**messBrut.txt**".
- ✓ Trois labels contenant les textes : "***Clé*** ", "***A*** ", "***B*** "
- ✓ Une liste déroulante contenant les valeurs possibles de **A** qui sont 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25
- ✓ Une liste déroulante contenant les valeurs possibles de **B** qui sont de 0 à 25
- ✓ Un label contenant le texte : "***Texte chiffré*** "
- ✓ Un texte Edit contiendra le texte crypté
- ✓ Deux boutons Radios intitulés "***Chiffrer***" et "***Déchiffrer*** "
- ✓ Un bouton intitulé "***Calculer***" permet de réaliser l'opération sélectionner à l'aide des boutons Radios.
- ✓ Un bouton intitulé "***Effacer***" permet de réinitialiser à vide les zones de textes et les listes déroulantes.

**Travail demandé :**

**1)** A l'aide de logiciel "**QT Designer**", réaliser l'interface graphique "**Interface**" qui contient les éléments présentés précédemment comme illustrée dans la figure suivante :


**2)** Créer le fichier nommé " **crypt_decrypt.py**" dans votre dossier de travail dans lequel vous :

- ✓ Développer le module " ***messBrut*** ", qui s'exécute suite à un clic sur le bouton Radio "**Chiffrer**", et permettant d'importer le contenu du fichier " **messBrut.txt** " dans la zone texte Edit correspond au texte clair

  **N.B. :** Si le fichier n'existe pas il sera créé.

- ✓ Développer le module " ***messCrypt*** ", qui s'exécute suite à un clic sur le bouton Radio " **Déchiffrer**", et permettant d'importer le contenu du fichier " **messCrypt.txt** " dans la zone texte Edit correspond au texte chiffré.

  **N.B. :** Si le fichier n'existe pas il sera créé.

- ✓ Développer le module " ***crypt_decrypt*** ", qui s'exécute suite à un clic sur le bouton "**Calculer**".

  **N.B. :**

  - Si le bouton Radio "**Chiffrer**" est sélectionné, la fonction "***crypt_decrypt*** " réalise le cryptage du contenu du texte Edit correspond au message clair.
  - Si le bouton Radio "**Déchiffrer**" est sélectionné, la fonction "***crypt_decrypt*** " réalise le décryptage du contenu du texte Edit correspond au message chiffré.
  - Si aucun de bouton Radio n'est sélectionné, un message d'alerte sera affiché via "**QMessagebox**".
  - Si l'une des listes déroulantes est vide un message d'alerte sera affiché via "**QMessagebox**".
  - Dans l'opération de cryptage, si le fichier " **messBrut.txt** " est vide un message d'alerte indiquant que le fichier est vide sera affiché via "**QMessagebox**".
  - Dans l'opération de décryptage, si le fichier « **messCrypt.txt »** est vide un message d'alerte indiquant que le fichier est vide sera affiché via "**QMessagebox**".

- ✓ Compléter les instructions de la partie exploitation de l'interface graphique par les informations nécessaires à l'appel de l'interface "**Interface** " et aux différents modules développés.

Ci-dessous quelques captures d'écran montrant des exemples d'exécutions :