

# Cryptographie

Léa MENERET, Fathima SAHADATTALY, Ulrike KULZER

22 décembre 2017

## Table des matières

<b>1 Guide utilisateur</b>	<b>2</b>
1.1 Introduction . . . . .	2
1.1.1 En général . . . . .	2
1.1.2 Méthodes de cryptage . . . . .	2
1.2 Fonctionnement du programme . . . . .	4
1.2.1 Accueil et choix de la langue . . . . .	4
1.2.2 Crypter/Décrypter . . . . .	5
1.2.3 Choix du principe . . . . .	6
<b>2 Guide de maintenance</b>	<b>10</b>
2.1 Fonctionnalité . . . . .	10
2.1.1 En général . . . . .	10
2.1.2 Différents états du programme . . . . .	10
2.1.3 En détail et coupé en modules . . . . .	11
2.1.4 Structure du programme . . . . .	12
2.1.5 Explications des modules, constantes et fonctions . . . . .	12
<b>3 Annexe : Code du programme</b>	<b>18</b>

# 1 Guide utilisateur

## 1.1 Introduction

### 1.1.1 En général

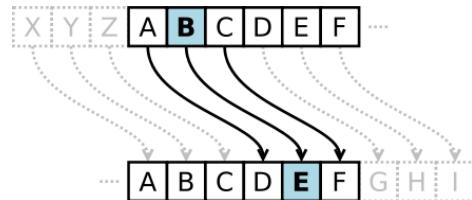
La cryptographie est une technique utilisée pour rendre incompréhensible à autrui un message entre un expéditeur et un destinataire. Ce procédé a notamment été utilisé en période de guerre pour permettre des attaques surprises. Le principe est le suivant : L'expéditeur à partir d'une clé crypte son message et l'envoie au destinataire. Celui-ci possède aussi la clé qui va lui permettre ainsi de décrypter le message.

### 1.1.2 Méthodes de cryptage

La cryptographie est utilisée depuis l'Antiquité mais certaines de ces méthodes les plus abouies datent du 20e siècle. Il existe différents principes de cryptage plus ou moins compliqués tels que

#### — le chiffre de César :

Ce procédé a été inventé lors de l'époque romaine par Jules César pour ses communications secrètes. En décalant l'alphabet par un entier donné chaque lettre est associée à une nouvelle lettre, ainsi on peut crypter le message initiale en remplaçant chaque lettre par la nouvelle lettre attribuée.



#### — le chiffre de Vigenère :

Il a été inventé au 16e siècle par Blaise de Vigenère et est basé sur le tableau à droite. Une clé (un mot) est répétée et mis sous le message et de cette manière on peut trouver les lettres correspondantes à partir du tableau.

Exemple :

	Lettre en clair																										
	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	
A	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	
B	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	A	
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	
I	I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	
M	M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	
Z	Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	

clé : musique

Texte : J'adore écouter la radio toute la journée.  
Texte en claire et en dessous la clé répétée:

j'adore écouter la radio toute la journée.  
M USIQU EMUSIQU EM USIQU EMUSI QU EMUSIQU  
^ ^ ^ ^

|| Colonne 0, ligne I : on obtient la lettre W.  
|| Colonne D, ligne S : on obtient la lettre V.  
Colonne A, ligne U : on obtient la lettre U.  
Colonne J, ligne M : on obtient la lettre V.

— *celui de la machine Enigma :*

L'Enigma est une machine de cryptographie inventée par Arthur Scherbius en 1919. Elle a été utilisée durant la Seconde Guerre mondiale pour la communication secrète entre les différentes unités de l'armée allemande. La machine est constituée de cinq rotors dont un réflecteur, d'un clavier, d'un tableau de permutation et de lampes pour chaque lettre. Pour l'allumer il faut une batterie de 4,5 Volt. Le principe est simple : Lorsqu'on appuie sur une lettre du clavier, un courant électrique va être envoyé au tableau de permutation dans lequel la lettre entrée est échangée avec une autre lettre si elles sont connectées. Puis il passera la première fois par les quatre rotors : Dans chacun des trois rotors au milieu il y a un décalage des lettres qui s'opère. À la fin les lettres sont permutees encore une fois dans le réflecteur qui les renvoie par les rotors au tableau de permutation ce qui permettra à une lampe correspondant à une lettre de s'allumer. Ainsi pour chaque lettre on relève la lettre codée, on obtient alors notre message crypté.



*Sites de référence :*

- <https://fr.wikipedia.org/wiki/Cryptographie>
- <http://www.bibmath.net/crypto/>
- [https://fr.wikipedia.org/wiki/Chiffrement\\_par\\_d%C3%A9calage](https://fr.wikipedia.org/wiki/Chiffrement_par_d%C3%A9calage)
- [https://fr.wikipedia.org/wiki/Chiffre\\_de\\_Vigen%C3%A8re](https://fr.wikipedia.org/wiki/Chiffre_de_Vigen%C3%A8re)
- [https://fr.wikipedia.org/wiki/Enigma\\_\(machine\)](https://fr.wikipedia.org/wiki/Enigma_(machine))
- photo d'Enigma : Von William Warby from London, England - Enigma, CC BY 2.0, <https://commons.wikimedia.org/w/index.php?curid=46848023>

## 1.2 Fonctionnement du programme

### 1.2.1 Accueil et choix de la langue

Pour exécuter notre programme, il est nécessaire de l'ouvrir avec le logiciel Pycharm, d'aller dans le fichier "main\_module" et d'appuyer sur "run" - "run" - "run main\_module". Les instructions du programme seront affichées dans la console qui s'ouvre en bas de l'interface comme montrés ci dessous :

```
Hello and welcome to the cryptography program  
Please select your language:  
'f' for Français, 'e' for English.
```

Fig. 1 – Écran d'accueil

Vous venez d'entrer dans le programme Cryptographie, vous devez entrer la lettre ' f ' pour avoir les instructions en français et ' e ' pour les avoir en anglais. Si la lettre entrée est ' e ', les prochaines instructions seront donc en anglais.

Note : Vous retrouverez les mêmes interfaces en français.

Une nouvelle fenêtre va ensuite apparaître :

```
What do you want to do - encrypt or decrypt a message?  
Enter 'c' for encrypting or 'd' for decrypting.  
Enter 's' to change settings(language)  
or 'q' to exit :(
```

Fig. 2 – Menu principal

Le programme demande maintenant ce que vous voulez faire, vous devez entrer ' c ' si vous voulez que le programme crypte votre texte ou ' d ' si vous voulez qu'il le décrypte. Si vous voulez changer de langue entrez ' s ' et si malheureusement vous voulez quitter le programme entrez ' q ' .

Si la lettre entrée est ' s ' , une nouvelle fenêtre permettant de changer la langue va alors apparaître.

```
Please select your language:  
'f' for Français,    'e' for English.
```

Fig. 3 – Paramètres

Vous devez entrer la lettre ' f ' pour avoir les instructions en français et ' e ' pour les avoir en anglais.

Si la lettre entrée est ' f ' les prochaines instructions seront donc en français.  
Vous reviendrez sur les instructions précédentes cette fois-ci en français.

### 1.2.2 Crypter/Décrypter

```
Bonjour et bienvenue sur le programme de cryptographie.  
Que voulez vous faire-crypter ou décrypter un message?  
Insérez 'c' pour crypter ou 'd' pour décrypter.  
Insérez 's' pour changer les paramètres(langue)  
ou 'q' pour quitter le programme :(
```

Fig. 4 – Menu principal

Vous devez entrer ' c ' si vous voulez que le programme crypte votre texte ou ' d ' si vous voulez qu'il le décrypte.

Si vous voulez changer de langue entrez ' s ' et si malheureusement vous voulez quitter le programme entrez ' q ' .

Si la lettre entrée est ' c ' , le programme va donc être servi pour le cryptage d'un texte.  
Il existe trois méthodes par lesquelles le texte peut être crypté, nous allons donc détailler les différentes manières.

### 1.2.3 Choix du principe

Si vous avez choisi de crypter votre texte, il vous faut maintenant choisir quelle méthode vous voulez utiliser, trois choix s'offrent à vous.

**De quelle manière voulez-vous crypter votre texte?**

Insérez 'c' pour le cryptage par la méthode du chiffre de César, insérez 'v' pour le cryptage par la méthode du chiffre de Vigenère ou insérez 'e' pour le cryptage par la méthode de la machine Enigma.

Insérez 'h' pour ouvrir l'aide dans laquelle il y a plus d'informations sur les différents principes.

Insérez 'm' pour retourner au menu principal.

Fig. 5 – Cryptage

Vous devez entrer ' c ' si vous voulez que le programme crypte votre texte par la méthode du chiffre de César, ' v ' par la méthode du chiffre de Vigenère et enfin ' e ' par la méthode de la machine Enigma.

Si tout autre fois vous voulez retourner au menu principal, entrez ' m '.

De la même manière, si à l'interface précédente vous aviez choisi le mode décryptage, vous allez devoir choisir la méthode par laquelle vous voulez déchiffrer votre texte. Les commandes pour choisir la méthode de déchiffrement sont alors les mêmes que pour un texte à crypter : ' c ' pour César, ' v ' pour Vigenère, ' e ' pour Enigma et ' m ' pour retourner au menu principal.

**De quelle manière voulez-vous déchiffrer votre texte?**

Insérez 'c' pour le cryptage par la méthode du chiffre de César, insérez 'v' pour le cryptage par la méthode du chiffre de Vigenère ou insérez 'e' pour le cryptage par la méthode de la machine Enigma.

Insérez 'h' pour ouvrir l'aide dans laquelle il y a plus d'informations sur les différents principes.

Insérez 'm' pour retourner au menu principal.

Fig. 6 – Déchiffrement

Dans les deux cas vous pouvez consulter l'aide en entrant ' h ' qui vous rappellera les principes de cryptage utilisé pour les différentes méthodes César, Vigenère ou Enigma :

\*\*\*\*\* AIDE \*\*\*\*\*

Voici les explications pour les différents principes de (dé)cryptage.

- Le chiffre de César :

Ce procédé a été inventé lors de l'époque romaine par Jules César pour ses communications secrètes. En décalant l'alphabet par un entier donné chaque lettre est associée à une nouvelle lettre, ainsi on peut crypter le message initiale en remplaçant chaque lettre par la nouvelle lettre attribuée.

- Le chiffre de Vigenère :

Il a été inventé au 16e siècle par Blaise de Vigenère et est basé sur le tableau de Vigenère (tableau avec deux fois l'alphabet). Une clé (un mot) est répétée et mise sous le message et de cette manière on peut trouver les lettres correspondantes à partir du tableau.

- Le principe de la machine Enigma :

L'Enigma est une machine de cryptographie inventée par Arthur Scherbius en 1919. Elle a été utilisée durant la Seconde Guerre mondiale pour la communication secrète entre les différentes unités de l'armée allemande.

La machine est constituée de cinq rotors dont un réflecteur, d'un clavier, d'un tableau de permutation et de lampes pour chaque lettre.

Lorsqu'on appuie sur une lettre du clavier, un courant électrique va être envoyé au tableau de permutation dans lequel la lettre entrée est échangée avec une autre lettre si elles sont connectées. Puis il passera la première fois par les quatre rotors : Dans chacun des trois rotors au milieu il y a un décalage des lettres qui s'opère. À la fin les lettres sont permutees encore une fois dans le réflecteur qui les renvoie par les rotors au tableau de permutation ce qui permettra à une lampe correspondant à une lettre de s'allumer. Ainsi pour chaque lettre on relève la lettre codée, on obtient alors notre message crypté.

Insérez 'm' pour retourner au menu principal.

Fig. 7 – Aide

*Le chiffre de César :*

Imaginons que vous ayez choisi de crypter ou décrypter votre texte par la méthode du chiffre de César, l'interface suivante apparaîtra :

Vous avez choisi <<César>>;  
Insérez votre clé (un nombre compris entre 1 et 25);  
Insérez 'm' pour retourner au menu principal.

Fig. 8 – Le chiffre de César

Vous devez maintenant choisir la clé à utiliser pour (dé)crypter votre texte. Cette clé doit être un nombre compris entre 1 et 25 et correspondra au décalage de l'alphabet lors du (dé)cryptage de chaque lettre. Vous avez également la possibilité de retourner au menu principal en entrant 'm'.

*Le chiffre de Vigenère :*

Si votre choix se porte sur le (dé)cryptage par la méthode du chiffre de Vigenère, vous verrez alors le message suivant :

```
Vous avez choisi <<Vigenère>>:  
Insérez votre clé (un mot).  
  
Insérez 'm' pour retourner au menu principal.
```

Fig. 9 – Le chiffre de Vigenère

Vous devez maintenant entrer la clé que vous souhaitez utiliser. Cette clé doit être un mot composé uniquement de lettres (minuscules ou majuscules) sans espace ni tiret. Vous pouvez aussi entrer ' m ' si vous voulez retourner au menu principal.

*La machine Enigma :*

Si vous avez sélectionné le (dé)cryptage par la méthode de la machine Enigma, le message suivant apparaîtra :

```
Vous avez choisi <<Enigma>>:  
Insérez votre clé (composée de trois lettres enmajuscules).  
  
Insérez 'm' pour retourner au menu principal.
```

Fig. 10 – Le cryptage par la machine Enigma

Le programme attend de vous que vous entriez la clé de (dé)cryptage. Cette clé doit se présenter sous la forme de trois lettres majuscules.

Vous avez toujours, comme précédemment la possibilité de retourner au menu principal en entrant ' m '.

Quelle que soit la méthode de (dé)cryptage choisie vous serez confronté au message suivant qui vous indique d'entrer le texte à traiter. Il est important de savoir que dans le texte tous les caractères spéciaux seront normalisés et les chiffres et signes de ponctuation seront enlevés.

À ce stade vous pouvez aussi entrer ' m ' pour retourner au menu principal.

```
Insérez votre texte.  
  
Insérez 'm' pour retourner au menu principal.
```

Fig. 11 – Entrée du texte

Enfin le programme s'exécute pour effectuer l'opération que vous lui avez demandé, et l'un des message suivant apparaîtra suivi de votre texte crypté ou décrypté.

**Voici votre texte crypté:**

Fig. 12 – Affichage du texte crypté

**Voici votre texte décrypté:**

Fig. 13 – Affichage du texte décrypté

Message de fin :

**Merci d'avoir utilisé notre programme.**

**Bonne journée, au revoir.**

Fig. 14 – Sortie du programme

## 2 Guide de maintenance

### 2.1 Fonctionnalité

#### 2.1.1 En général

- Quand l'utilisateur lance le programme on lui demande de choisir la langue, soit français, soit anglais.
- Notre programme va proposer à l'utilisateur trois façons différentes de (dé)crypter un texte de complexité croissante et demander une clé.
- Les différentes manières sont le principe du chiffre de César, du chiffre de Vigenère et de la machine Enigma.

#### 2.1.2 Différents états du programme

Les différents états du programme sont représentés dans le diagramme ci-dessous. Dès que le programme est lancé, il est généralement toujours dans un état en attendant des saisies de l'utilisateur. La seule exception est l'état en cryptant ou décryptant. Sur les flèches on peut voir ce qu'il faut faire pour accéder à un autre état, soit le précédent, soit le suivant. Avant que le programme est fermé, il affichera un petit message de remerciement.

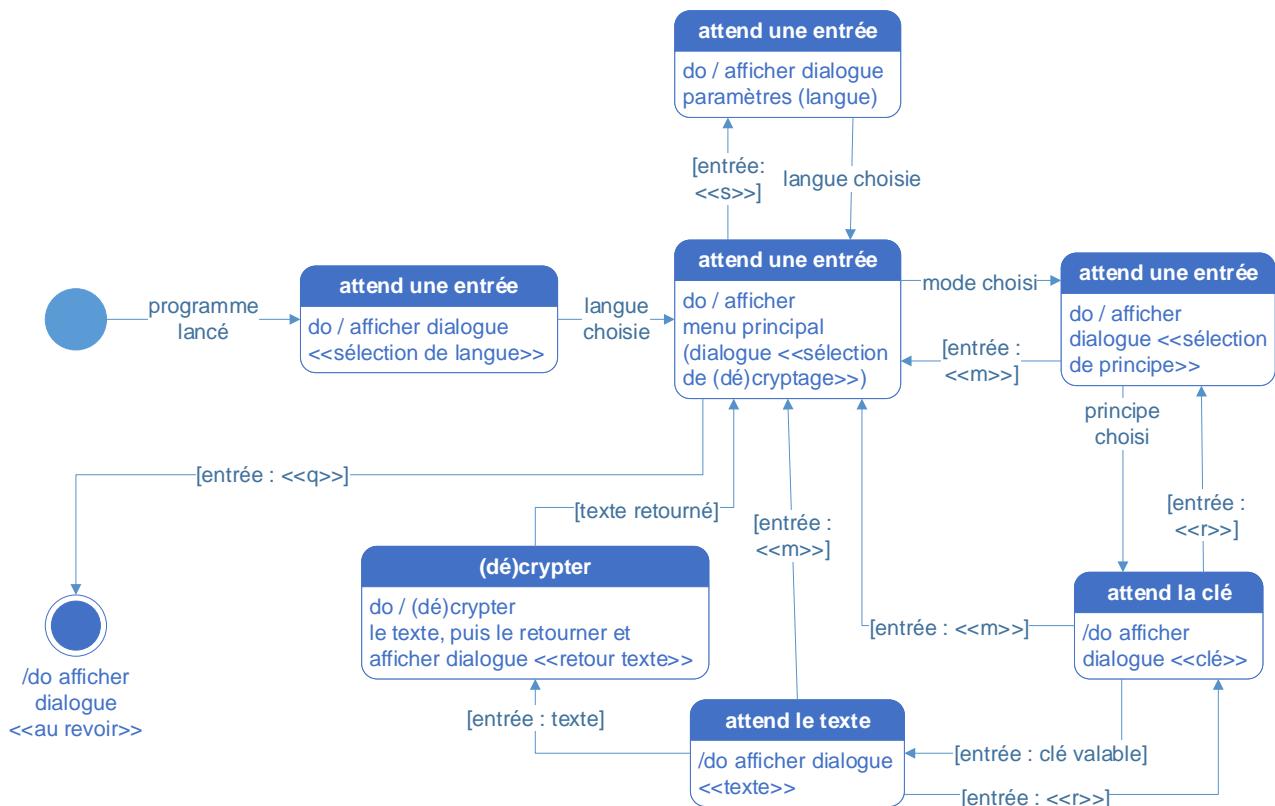


Fig. 15 – Diagramme états-transitions du programme

### 2.1.3 En détail et coupé en modules

- *Avant de commencer le (de)cryptage :*

On va créer une méthode qui formatera le texte (enlever les accents, les caractères spéciaux, les signes de ponctuation et les espaces, puis mettre tout en majuscule).

- *(Dé)Cryptage César :*

On compte transformer les lettres du texte en nombres par le système unicode, ensuite on additionne la clé (nombre) aux nombres obtenus par le système. On reconvertis alors les lettres en caractères et retourne le texte. Pour le décryptage, il suffit de soustraire au lieu d'additionner.

- *(Dé)Cryptage Vigenère :*

Dans un premier temps on crée une matrice de 26 x 26 lettres contenant l'alphabet représentant le tableau de Vigenère et une matrice à deux lignes pour le texte et la clé. Dans un deuxième temps on prend le texte et on insère tour à tour les caractères individuels dans la première ligne de la matrice et la clé dans la deuxième. Chaque lettre du texte doit être attribuée à un caractère de la clé (mot) ce qui est permis en répétant le mot tant qu'ils restent des lettres du texte. Le cryptage est fait caractère par un caractère. Pour trouver la lettre cryptée on regarde en premier la lettre du texte et on cherche la colonne de la matrice qui appartient à la lettre et on la mémorise. Par la suite on considère le caractère de la clé auquel la lettre du texte est attribuée et on cherche la ligne de la matrice qui appartient au caractère. Dès qu'on a trouvé les deux, la lettre de la matrice qui est enregistré sur cette case est la lettre cryptée laquelle est mémorisée dans une chaîne de caractère. Lorsqu'on a crypté toutes les lettres du texte, on retourne la chaîne de caractère qui est le texte crypté. Pour le décryptage, on possède la matrice à deux lignes avec le texte crypté sur une ligne et la clé répétée sur l'autre. Pour chaque lettre du texte crypté, on parcourt dans le tableau de Vigenère (matrice) la ligne correspondant à la lettre de la clé répétée et lorsqu'on trouve la lettre cryptée cherchée on remonte la ligne pour obtenir le caractère décrypté correspondant à cette lettre. De la même manière que pour le cryptage on mémorise les lettres obtenues dans une chaîne de caractère ce qui permet d'avoir au final le message décrypté.

- *(Dé)Cryptage Enigma :*

Pour commencer nous créons cinq listes : La première correspond au tableau de permutation, les trois suivantes aux rotors au milieu et la dernière au réflecteur. Au début de la programmation on choisit un décalage fixe ; si possible on essayera plus tard de changer le décalage automatiquement. Pour les connecteurs, il y en aura dix ainsi 20 lettres seront connectées entre elles et six qui ne le seront pas. Nous allons créer une fonction qui, si la lettre est connectée, va retourner la lettre associée. On appelle ensuite des fonctions qui exécutent les décalages au niveau des trois rotors et après on utilise la fonction correspondant au réflecteur pour permuter les lettres. On repasse finalement à nouveau par les rotors et on obtient une certaine lettre. Si la lettre est connectée à une autre, on retourne l'autre lettre, sinon on garde la même, celle-ci est alors la lettre (dé)cryptée.

## 2.1.4 Structure du programme

main_module	screen_module	tests
<pre>normalise_letter(x) format_text(text) run()</pre>	<pre>show_start_ask_language() show_language_settings() show_main_menu(english: Boolean) show_principles(english: Boolean, encrypting: Boolean) show_ask_key(english: Boolean, principle: char) show_ask_text(english: Boolean) show_treated_text(english: Boolean, encrypting: Boolean) show_help_principles(english: Boolean) show_quit_message(english: Boolean)</pre>	<pre>test_caesar_encryption() test_caesar_decryption() test_create_table_of_vigenere() test_vigenere_encryption() test_vigenere_decryption() test_enigma() test_format_and_normalise() test_run() run_all_tests()</pre>
<pre>screen_constants</pre>		
<pre>STARTASKLANGUAGE LANGUAGE_SETTINGS ENGLISH_MAIN_MENU ENGLISH_PRINCIPLES_ENCRYPTING ENGLISH_PRINCIPLES_DECRYPTING ENGLISHASKKEYCAESAR ENGLISHASKKEYVIGENERE ENGLISHASKKEYENIGMA ENGLISHASKTEXT ENGLISH_ENCRYPTED_TEXT ENGLISH_DECRYPTED_TEXT ENGLISH_HELP_PRINCIPLES ENGLISH_QUIT_MESSAGE FRENCH_MAIN_MENU FRENCH_PRINCIPLES_ENCRYPTING FRENCH_PRINCIPLES_DECRYPTING FRENCHASKKEYCAESAR FRENCHASKKEYVIGENERE FRENCHASKKEYENIGMA FRENCHASKTEXT FRENCH_ENCRYPTED_TEXT FRENCH_DECRYPTED_TEXT FRENCH_HELP_PRINCIPLES FRENCH_QUIT_MESSAGE</pre>	<pre>text_module</pre>	<pre>encrypt_caesar(text: string, key: int) decrypt_caesar(text: string, key: int) create_vigenere_table() create_table_text_key(text: string, key: string) encrypt_vigenere(text: string, key: string) decrypt_vigenere(text: string, key: string) create_initial_list() search_index(initial_list: list, letter: char) plugboard(letter: char) permutation_reflector(letter: char) shift_first_rotor(return_path: Boolean, index: int, offset: int) shift_second_rotor(return_path: Boolean, index: int, offset: int) shift_third_rotor(return_path: Boolean, index: int, offset: int) enigma(text: string, key: string)</pre>

Fig. 16 – Structure du programme en modules

## 2.1.5 Explications des modules, constantes et fonctions

### Explications du module *screen\_constants* :

Ce module contient toutes les constantes nécessaires pour le screen\_module, c'est-à-dire tous les textes de l'interface utilisateur.

- **STARTASKLANGUAGE** :  
dialogue de démarrage (voir fig. 1)
- **LANGUAGE\_SETTINGS** :  
dialogue des paramètres de langue (voir fig. 3)
- **ENGLISH\_MAIN\_MENU** et **FRENCH\_MAIN\_MENU** :  
menu principal (voir fig. 2 et 4)
- **ENGLISH\_PRINCIPLES\_ENCRYPTING** et  
**FRENCH\_PRINCIPLES\_ENCRYPTING** :  
dialogue de sélection du principe de cryptage (voir fig. 5)

- **ENGLISH\_PRINCIPLES\_DECRYPTING** et **FRENCH\_PRINCIPLES\_DECRYPTING** : dialogue de sélection du principe de décryptage (voir fig. 6)
- **ENGLISH\_ASK\_KEY\_CAESAR** et **FRENCH\_ASK\_KEY\_CAESAR** : dialogue de demande de la clé pour (dé)crypter par César (voir fig. 8)
- **ENGLISH\_ASK\_KEY\_VIGENERE** et **FRENCH\_ASK\_KEY\_VIGENERE** : dialogue de demande de la clé pour (dé)crypter par Vigenère (voir fig. 9)
- **ENGLISH\_ASK\_KEY\_ENIGMA** et **FRENCH\_ASK\_KEY\_ENIGMA** : dialogue de demande de la clé pour (dé)crypter par Enigma (voir fig. 10)
- **ENGLISH\_ASK\_TEXT** et **FRENCH\_ASK\_TEXT** : dialogue de demande du text à (dé)crypter (voir fig. 11)
- **ENGLISH\_ENCRYPTED\_TEXT** et **FRENCH\_ENCRYPTED\_TEXT** : dialogue du texte crypté (voir fig. 12)
- **ENGLISH\_DECRYPTED\_TEXT** et **FRENCH\_DECRYPTED\_TEXT** : dialogue du texte décrypté (voir fig. 13)
- **ENGLISH\_HELP\_PRINCIPLES** et **FRENCH\_HELP\_PRINCIPLES** : dialogue d'aide (voir fig. 7)
- **ENGLISH\_QUIT\_MESSAGE** et **FRENCH\_QUIT\_MESSAGE** : message de sortie (voir fig. 14)

#### **Explications du module *screen-module* :**

Ce module est responsable de l'interface utilisateur, c'est-à-dire il montre le bon texte dans la langue choisie.

<b>show_start_ask_language</b>	(ligne 8)
Déclaration	show_start_ask_language()
Rôle	demande à l'utilisateur la langue qu'il veut utiliser au début du programme
Paramètre	aucun
Retour	la chaîne de caractère choisie par l'utilisateur : ' f ' pour le français ' e ' pour l'anglais
Appelé par	run()
Appelle	aucun

<b>show_language_settings</b>	(ligne 18)
Déclaration	show_language_settings()
Rôle	demande à l'utilisateur la langue qu'il veut utiliser au cours du programme
Paramètre	aucun
Retour	la chaîne de caractère choisie par l'utilisateur : ‘ f ’ pour le français ‘ e ’ pour l'anglais
Appelé par	run()
Appelle	aucun
<b>show_main_menu</b>	(ligne 28)
Déclaration	show_main_menu(english)
Rôle	demande à l'utilisateur ce qu'il veut utiliser la fonction cryptage ou décryptage du programme
Paramètre	english : booléen
Retour	True si la langue choisie est l'anglais False si la langue choisie est le français la chaîne de caractère choisie par l'utilisateur : ‘c’ pour cryptage ‘d’ pour décryptage ‘s’ pour changer de langue ‘q’ pour quitter le programme
Appelé par	run() (attention à vérifier)
Appelle	aucun
<b>show_principles</b>	(ligne 50)
Déclaration	show_principles(english, encrypting)
Rôle	demande à l'utilisateur la méthode qu'il veut utiliser pour (dé)crypter
Paramètre	english : booléen
Retour	True si la langue choisie est l'anglais False si la langue choisie est le français encryption : booléen True si l'utilisateur veut crypter False s'il veut décrypter la chaîne de caractère choisie par l'utilisateur : ‘c’ pour la méthode César ‘v’ pour la méthode Vigenère ‘e’ pour la méthode de la machine Enigma ‘m’ pour retourner au menu principal
Appelé par	run() (attention à vérifier)
Appelle	aucun

<b>show_ask_key</b>	(ligne 81)
Déclaration	show_ask_key/english, principle)
Rôle	demande à l'utilisateur la clé pour la méthode qu'il veut utiliser pour (dé)crypter
Paramètre	english : booléen True si la langue choisie est l'anglais False si la langue choisie est le français
	principle : char 'c', 'v' ou 'e' selon la méthode de (dé)cryptage qu'il a choisi
Retour	la clé ou 'm' pour retourner au menu principal
Appelé par	run() (attention à vérifier)
Appelle	aucun
<b>show_ask_text</b>	(ligne 115)
Déclaration	show_ask_text/english)
Rôle	demande à l'utilisateur le texte qu'il veut (dé)crypter
Paramètre	english : booléen True si la langue choisie est l'anglais False si la langue choisie est le français
Retour	la clé ou 'm' pour retourner au menu principal
Appelé par	run() (attention à vérifier)
Appelle	aucun
<b>show_treated_text</b>	(ligne 135)
Déclaration	show_treated_text/english, encrypting)
Rôle	retourne le message d'affichage du texte (dé)crypté
Paramètre	english : booléen True si la langue choisie est l'anglais False si la langue choisie est le français
	encryption : booléen True si l'utilisateur veut crypter False s'il veut décrypter
Retour	le message d'affichage du texte (dé)crypté
Appelé par	run() (attention à vérifier)
Appelle	aucun
<b>show_help_principles</b>	(ligne 162)
Déclaration	show_help_principles/english)
Rôle	Affiche une aide dans laquelle le principe
Paramètre	english : booléen True si la langue choisie est l'anglais False si la langue choisie est le français 'm'
Retour	run() (attention à vérifier)
Appelé par	aucun
Appelle	

<b>show_quit_message</b>	(ligne 180)
Déclaration	show_quit_message/english)
Rôle	Affiche un message de fin d'utilisation du programme
Paramètre	english : booléen
	True si la langue choisie est l'anglais
	False si la langue choisie est le français
Retour	aucun
Appelé par	run() (attention à vérifier)
Appelle	aucun

#### ***text\_module :***

- **encrypt\_caesar(text, key)** :  
crypte le texte formaté par la méthode César
- **decrypt\_caesar(text, key)** :  
décrypte le texte formaté par la méthode César
- **create\_vigenere\_table()** :  
TODO
- **create\_table\_text\_key(text, key)** :  
TODO
- **encrypt\_vigenere(text, key)** :  
crypte le texte formaté par la méthode Vigenère
- **decrypt\_vigenere(text, key)** :  
décrypte le texte formaté par la méthode Vigenère
- **create\_initial\_list()** :  
TODO
- **search\_index(initial\_list, letter)** :  
cherche l'indice d'une lettre donnée dans une liste donnée
- **plugboard(letter)** :  
modélise le tableau de permutation, 10 lettres sont associées à dix autres lettres. Si la lettre donnée est associée à une autre lettre celle-ci va être retournée. Il y a six lettres qui ne sont associées à aucune autre lettre.
- **permutation\_reflector(letter : char)** :  
modélise le réflecteur ; même principe que plugboard(letter), mais cette fois-ci toutes les lettres sont associées à une autre lettre
- **shift\_first\_rotor(letter : char)** :  
modélise le premier rotor, exécute le décalage des lettres par indices et retourne la lettre

- correspondante
- **shift\_second\_rotor(letter : char) :**  
modélise le deuxième rotor, exécute le décalage des lettres par indices et retourne la lettre correspondante
  - **shift\_third\_rotor(letter : char) :**  
modélise le troisième rotor, exécute le décalage des lettres par indices et retourne la lettre correspondante
  - **enigma(text, key) :**  
(dé)crypte le texte formaté par la méthode Enigma
- main\_module :***
- **normalise\_letter(x) :**  
normalise une lettre si elle est par exemple un caractère spécial
  - **format\_text(text) :**  
formate le texte, c'est-à-dire le texte donné est mis en majuscules, les virgules, espaces, chiffres, symboles, etc. sont enlevés et les caractères spéciaux sont normalisés
  - **run() :**  
démarrer le programme et contrôle son déroulement
- tests :***
- **test\_caesar\_encryption() :**  
TODO
  - **test\_caesar\_decryption() :**  
TODO
  - **test\_create\_table\_of\_vigenere() :**  
TODO
  - **test\_vigenere\_encryption() :**  
TODO
  - **test\_vigenere\_decryption() :**  
TODO
  - **test\_enigma() :**  
TODO
  - **test\_format\_and\_normalise() :**  
TODO

- **test\_run()** :  
TODO
- **run\_all\_tests()** :  
TODO

### 3 Annexe : Code du programme