

Cryptographie

Léa MENERET, Fathima SAHADATTALY, Ulrike KULZER
21 novembre 2017

1 Contexte

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.

1.2 Histoire

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 initial en remplaçant chaque lettre par la nouvelle lettre attribuée.

— *le chiffre de Vigenère :*

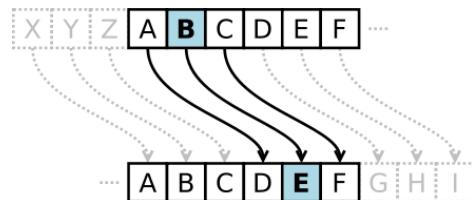
Il a été inventé au 16e siècle par Blaise de Vigenère et est basé sur le tableau à droite. Une clé (un mot) est répétée et mis sous le message et de cette manière on peut trouver les lettres correspondantes à partir du tableau.

Exemple :

clé : musique
Texte : j'adore écouter la radio toute la journée.
Texte en clair 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.



		Lettre en clair																									
		26 lettres chiffrées																									
		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	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	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	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	

— *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/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>

2 Fonctionnalité

2.1 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.

2.2 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.

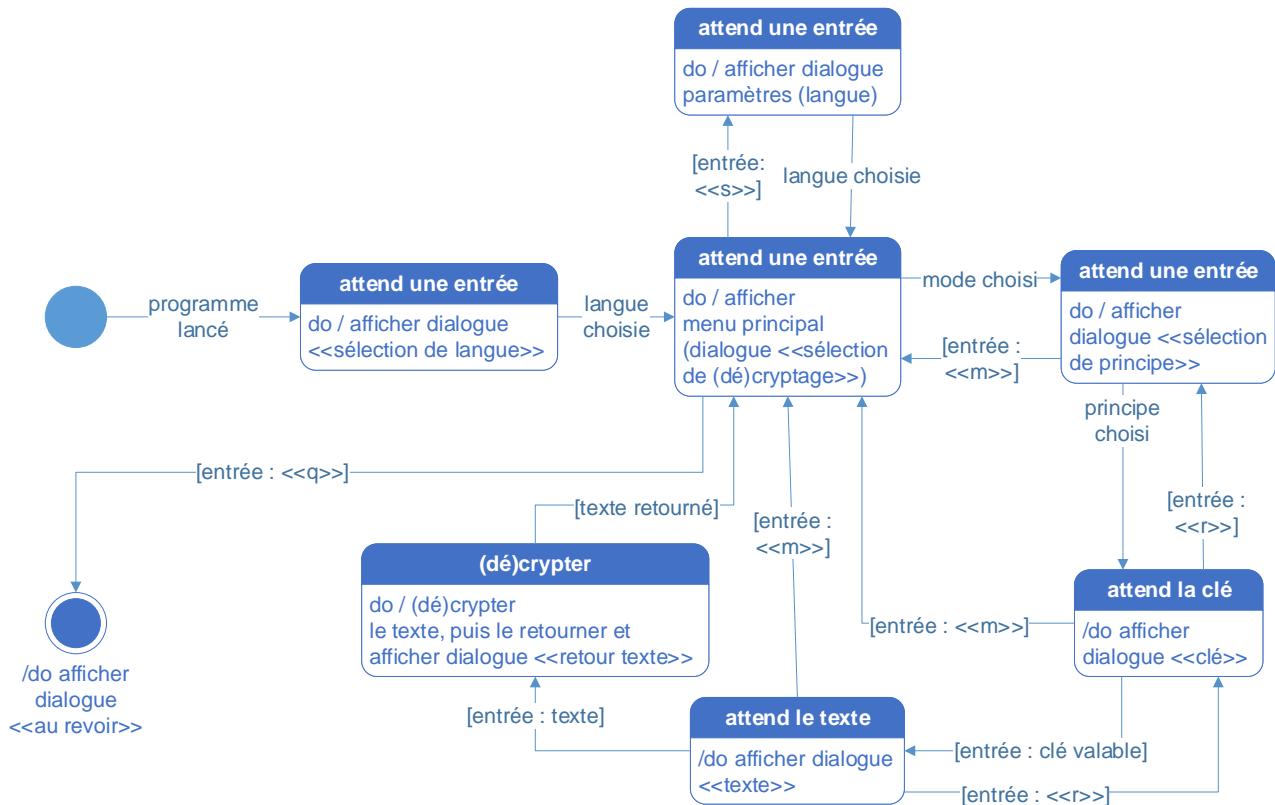


Fig. 1 – Diagramme états-transitions du programme

2.3 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.

2.4 Structure du programme

2.4.1 Diagramme de classes

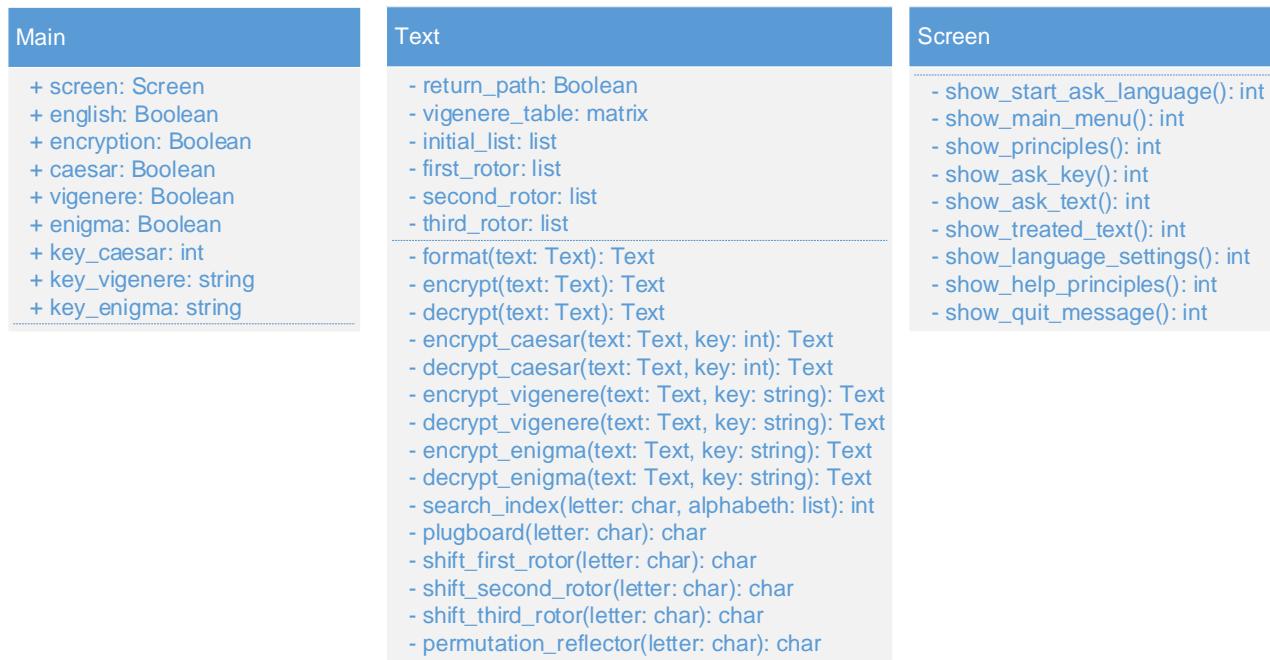


Fig. 2 – Diagramme de classes

2.4.2 Explication du diagramme

- *Le module Main*
 - **module** : démarre le programme et contrôle son déroulement
- *La classe Text*
 - **format(text : Text)** : formate le texte pour avoir un texte en majuscule sans virgules, espaces, chiffres, symboles, ...
 - **encrypt(text : Text)** : appelle l'un des trois principes choisi par l'utilisateur pour crypter le texte
 - **decrypt(text : Text)** : appelle l'un des trois principes choisi par l'utilisateur pour décrypter le texte
 - **encrypt_caesar(text : Text, key : int)** : crypte le texte formaté par la méthode César
 - **decrypt_caesar(text : Text, key : int)** : décrypte le texte formaté par la méthode César

- **encrypt_vigenere(text : Text, key : string)** : crypte le texte formaté par la méthode Vigenère
- **decrypt_vigenere(text : Text, key : string)** : décrypte le texte formaté par la méthode Vigenère
- **encrypt_enigma(text : Text, key : string)** : crypte le texte formaté par la méthode Enigma
- **decrypt_enigma(text : Text, key : string)** : décrypte le texte formaté par la méthode Enigma
- *méthodes utilisées pour le (dé)cryptage par «Enigma» :*
 - **search_index(letter : char, alphabeth : list)** : cherche l'indice d'une lettre donnée dans une liste donnée
 - **plugboard(letter : char)** : 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.
 - **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
 - **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
- *La classe Screen*
 - **show_start_ask_language()** : affiche le dialogue de démarrage (voir fig. 4)
 - **show_main_menu()** : affiche le menu principal (voir fig. 5 et 16)
 - **show_principles()** : affiche le dialogue de sélection du principe (voir fig. 7, 8, 18 et 19)
 - **show_ask_key()** : affiche le dialogue de demande de la clé pour (dé)crypter ce qui dépend de la choix du principe (César, Vigenère ou Enigma ; voir fig. 9, 10, 11, 20, 21 et 22)

- **show_ask_text()** : affiche le dialogue de demande du text à (dé)crypter (voir fig. 12 et 23)
- **show_treated_text()** : affiche le texte (dé)crypté (voir fig. 13, 14, 24 et 25)
- **show_language_settings()** : affiche les paramètres (voir fig. 6 et 17)
- **show_help_principles()** : affiche le dialogue de démarrage (voir fig. 27)
- **show_quit_message()** : affiche le message de sortie (voir fig. 15 et 26)

2.4.3 Diagramme de communication

Le diagramme ci-dessous montre le déroulement général du programme.

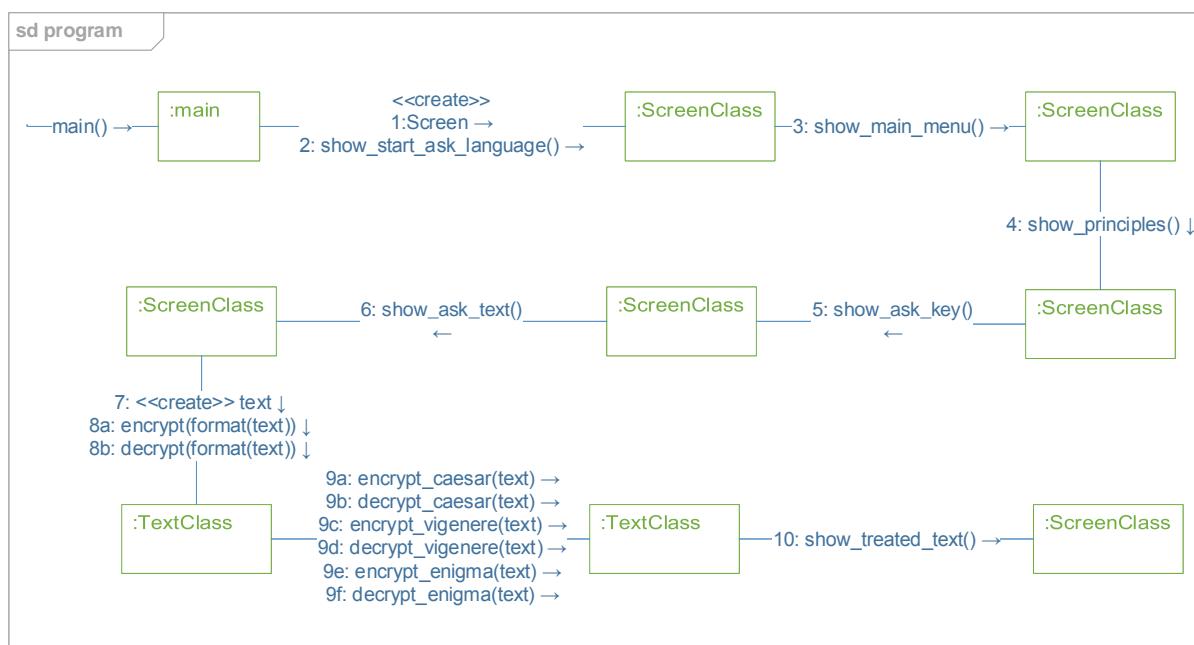


Fig. 3 – Diagramme états-transitions du programme

3 Interfaces utilisateurs

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

Fig. 4 – Écran d'accueil

3.1 En anglais :

```
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. 5 – Menu principal

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

Fig. 6 – Paramètres

```
How do you want to encrypt your text?  
Enter 'c' for Cesar's cypher,  
enter 'v' for Vigenère's cypher  
or enter 'e' for the encryption/decryption by the Enigma machine.  
Enter 'm' to go back to the main menu.
```

Fig. 7 – Cryptage

```
How do you want to decrypt your text?  
Enter 'c' for Cesar's cypher,  
enter 'v' for Vigenère's cypher  
or enter 'e' for the encryption/decryption by the Enigma machine.  
Enter 'm' to go back to the main menu.
```

Fig. 8 – Décryptage

```
You chose "Cesar":  
Please enter your key (a number between 1 and 25 included).  
Enter 'm' to go back to the main menu  
or 'r' to go back to the previous menu.
```

Fig. 9 – Le chiffre de César

```
You chose "Vigenère":  
Please enter your key (a word).  
Enter 'm' to go back to the main menu  
or 'r' to go back to the previous menu.
```

Fig. 10 – Le chiffre de Vigenère

```
You chose "Enigma":  
Please enter your key (composed of three upper case letters).  
Enter 'm' to go back to the main menu  
or 'r' to go back to the previous menu.
```

Fig. 11 – Le cryptage par la machine Enigma

```
Please enter your text.  
Enter 'm' to go back to the main menu  
or 'r' to go back to the previous menu.
```

Fig. 12 – Entrée du texte

```
Here is your encrypted text:  
...
```

Fig. 13 – Affichage du texte crypté

```
Here is your decrypted text:  
...
```

Fig. 14 – Affichage du texte décrypté

```
Thank you for using our program.  
Good bye and have a nice day.
```

Fig. 15 – Sortie du programme

3.2 En français :

```
Bonjour. Bienvenue sur le programme de cryptographie.  
Qu'est-ce que vous voulez 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. 16 – Menu principal

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

Fig. 17 – Paramètres

```
De quelle manière voulez vous crypter votre texte?  
Insérez 'c' pour le cryptage par le chiffre de César,  
insérez 'v' pour le cryptage par le chiffre de Vigenère  
ou insérez 'e' pour le cryptage par la machine Enigma.  
Insérez 'm' pour retourner au menu principal.
```

Fig. 18 – Cryptage

```
De quelle manière voulez vous décrypter votre texte?  
Insérez 'c' pour le décryptage par le chiffre de César,  
insérez 'v' pour le décryptage par le chiffre de Vigenère  
ou insérez 'e' pour le décryptage par la machine Enigma.  
Insérez 'm' pour retourner au menu principal.
```

Fig. 19 – Décryptage

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

Fig. 20 – Le chiffre de César

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

Fig. 21 – Le chiffre de Vigenère

**Vous avez choisi <<Enigma>>:
Insérez votre clé (composée de trois lettres en majuscule).
Insérez 'm' pour retourner au menu principal
ou 'r' pour retourner au dernier menu.**

Fig. 22 – Le cryptage par la machine Enigma

**Insérez votre texte.
Insérez 'm' pour retourner au menu principal
ou 'r' pour retourner au dernier menu.**

Fig. 23 – Entrée du texte

**Voici votre texte crypté:
....**

Fig. 24 – Affichage du texte crypté

**Voici votre texte décrypté:
....**

Fig. 25 – Affichage du texte décrypté

**Merci d'avoir utilisé notre programme.
Bonne journée, au revoir.**

Fig. 26 – Sortie du programme

***** 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 mis 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. 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.

Insérez 'm' pour retourner au menu principal.

Fig. 27 – Aide