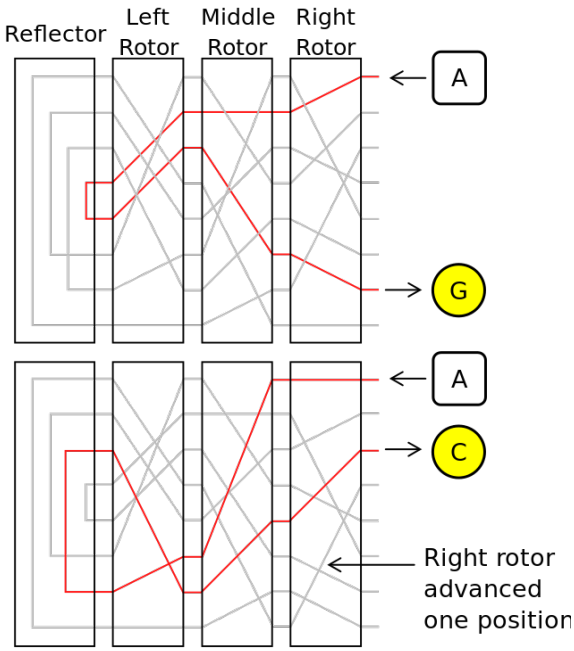
heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

L a b o r a t o i r e

Unité : INF2	Labo no : 03	Machine « Enigma »

But

La machine *enigma* fût intensément utilisée pour transcoder des messages secrets en particulier pendant la deuxième guerre mondiale par les allemands. Afin de déchiffrer un message, il est nécessaire d'avoir exactement les mêmes configurations entre les différentes machines. Ces configurations changeaient tous les jours.



Alan Turing développa une machine « bombe » permettant de cracker ces paramètres et ainsi décoder les messages ennemis. Ceci reste un véritable exploit compte tenu de la technologie du moment.

Pourtant le fonctionnement de la machine *enigma* est relativement simple mais offrait un nombre considérable de possibilités.

Ce laboratoire vise à reproduire cette machine.
Avant de continuer, il est utile de consulter ces liens

- Vidéo https://www.youtube.com/watch?v=mcX7iO_XCFA
- Wiki https://en.wikipedia.org/wiki/Enigma_rotor_details
- Simulateur https://piotte13.github.io/enigma-cipher

Implémenter les classes nécessaires afin d'implémenter la machine *enigma* avec les codes disponibles suivants. Pour simplifier ce développement, nous ignorons le *plugboard*.

Component	Wiring	Id	Notch
ENTRY	ABCDEFGHIJKLMNOPQRSTUVWXYZ		
Rotor	EKMFLGDQVZNTOWYHXUSPAIBRCJ	I	Q
	AJDKSIRUXBLHWTMCQGZNPYFVOE	II	E
	BDFHJLCPRTXVZNYEIWGAKMUSQO	III	V
	ESOVPZJAYQUIRHXLNFTGKDCMWB	IV	J
	VZBRGITYUPSDNHLXAWMJQOFECK	V	Z
Reflector	EJMZALYXVBWFCRQUONTSPIKHGD	UKW-A	
	YRUHQSLDPXNGOKMIEBFZCWVJAT	UKW-B	
	FVPJIAOYEDRZXWGCTKUQSBNMHL	UKW-C	

Sur ces bases, écrire un programme pour décoder le message

CLZJVMUOAQAGFQJSMOYQLPLCTN

… avec les configurations

Component	Id	Position
Rotor - LEFT	II	C
Rotor - MIDDLE	IV	K
Rotor - RIGHT	I	M
Reflector	UKW-B	

L a b o r a t o i r e

A faire

Par les différents fichiers et classes, vous devez mettre à disposition de quoi :

- créer un objet de type *Enigma* en passant les rotors et le réflecteur utilisés
- changer le réflecteur
- changer un rotor
- changer la position d'un rotor
- convertir un caractère
- convertir une chaine de caractères
- choisir d'afficher les informations de cheminement (debug) tant pour les constructeurs que pour les conversions (**voir exemple en dernière page**)

Contraintes

- Lire les documentations proposées et liens afin de bien comprendre le sujet
- Utiliser au mieux la théorie et les éléments vus à ce jour
- Ne rien utiliser qui n'est pas encore étudié en théorie (ie héritage …)
- Répartir les différentes classes dans des fichiers distincts

Temps à disposition : 10 périodes

Laboratoire

CONFIGURATION SIMPLE

LEFT rotor
```
rotor id   : III
entry      : ABCDEFGHIJKLMNOPQRSTUVWXYZ
wiring     : BDFHJLCPRTXVZNYEIWGAKMUSQO
notch      : V
position   : A
```

CENTER rotor
```
rotor id   : II
entry      : ABCDEFGHIJKLMNOPQRSTUVWXYZ
wiring     : AJDKSIRUXBLHWTMCQGZNPYFVOE
notch      : E
position   : A
```

RIGHT rotor
```
rotor id   : I
entry      : ABCDEFGHIJKLMNOPQRSTUVWXYZ
wiring     : EKMFLGDQVZNTOWYHXUSPAIBRCJ
notch      : Q
position   : A
```

Reflector
```
reflector  : UKW-B
entry      : ABCDEFGHIJKLMNOPQRSTUVWYXZ
wiring     : YRUHQSLDPXNGOKMIEBFZCWVJAT
```

DEROULEMENT
https://piotte13.github.io/enigma-cipher

```
rotor id   : I
entry      : ABCDEFGHIJKLMNOPQRSTUVWXYZ
wiring     : EKMFLGDQVZNTOWYHXUSPAIBRCJ
notch      : Q
position   : B
result     : [M <= C] <= B

rotor id   : II
entry      : ABCDEFGHIJKLMNOPQRSTUVWXYZ
wiring     : AJDKSIRUXBLHWTMCQGZNPYFVOE
notch      : E
position   : A
result     : [H <= L] <= M

rotor id   : III
entry      : ABCDEFGHIJKLMNOPQRSTUVWXYZ
wiring     : BDFHJLCPRTXVZNYEIWGAKMUSQO
notch      : V
position   : A
result     : [P <= H] <= H

reflector  : UKW-B
entry      : ABCDEFGHIJKLMNOPQRSTUVWYXZ
wiring     : YRUHQSLDPXNGOKMIEBFZCWVJAT
result     : [P => I]

rotor id   : III
entry      : ABCDEFGHIJKLMNOPQRSTUVWXYZ
wiring     : BDFHJLCPRTXVZNYEIWGAKMUSQO
notch      : V
position   : A
result     : I => [I => Q]

rotor id   : II
entry      : ABCDEFGHIJKLMNOPQRSTUVWXYZ
wiring     : AJDKSIRUXBLHWTMCQGZNPYFVOE
notch      : E
position   : A
result     : Q => [Q => Q]

rotor id   : I
entry      : ABCDEFGHIJKLMNOPQRSTUVWXYZ
wiring     : EKMFLGDQVZNTOWYHXUSPAIBRCJ
notch      : Q
position   : B
result     : Q => [R => X]

B => W
```

L a b o r a t o i r e