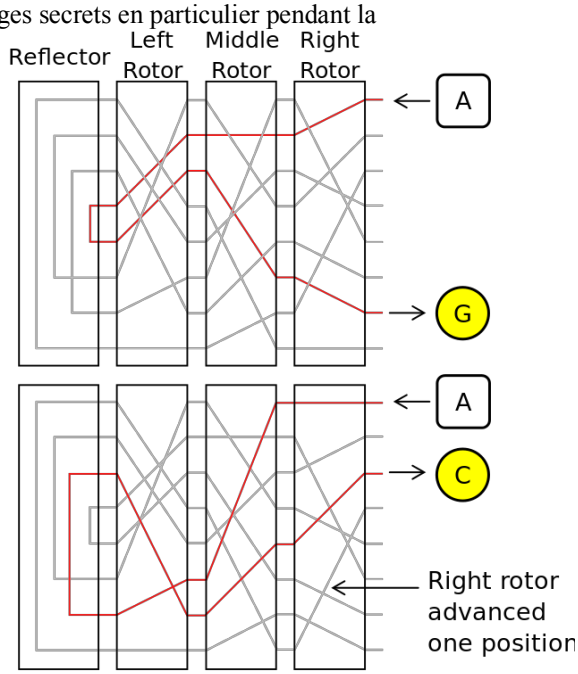
heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

L a b o r a t o i r e

Unité : INF2	Labo no : 02	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
- Simulateur https://cryptii.com/enigma-machine
- Wiki https://en.wikipedia.org/wiki/Enigma_rotor_details
- Exemple https://www.codesandciphers.org.uk/enigma/example1.htm

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	R
	AJDKSIRUXBLHWTMCQGZNPYFVOE	II	F
	BDFHJLCPRTXVZNYEIWGAKMUSQO	III	W
	ESOVPZJAYQUIRHXLNFTGKDCMWB	IV	K
	VZBRGITYUPSDNHLXAWMJQOFECK	V	A
Reflector	EJMZALYXVBWFCRQUONTSPIKHGD	UKW-A	
	YRUHQSLDPXNGOKMIEBFZCWVJAT	UKW-B	
	FVPJIAOYEDRZXWGCTKUQSBNMHL	UKW-C	

Sur ces bases, écrire un programme pour décoder le message

MDXMDAORNSLZBJTCDSABGHLVWA

… avec les configurations

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

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

Hes·so
Haute Ecole Spécialisée
de Suisse occidentale

L a b o r a t o i r e

- 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

A réaliser **le 5, 7, 11, 12 et 14 mars 2019**
☐ individuellement
☒ par groupes de **trois** étudiants

Travail à rendre **14 mars à 16h30**
☒ print
☒ fichiers **Labo_02_<nom>.zip** dans notre CyberLearn

Laboratoire

Configuration initiale

LEFT rotor
```
rotor id   : II
entry      : ABCDEFGHIJKLMNOPQRSTUVWYXZ
def wiring : AJDKSIRUXBLHWTMCQGZNPYFVOE
position   : C
pos wiring : DKSIRUXBLHWTMCQGZNPYFVOEAJ
notch      : F
```

MIDDLE rotor
```
rotor id   : IV
entry      : ABCDEFGHIJKLMNOPQRSTUVWYXZ
def wiring : ESOVPZJAYQUIRHXLNFTGKDCMWB
position   : K
pos wiring : UIRHXLNFTGKDCMWBESOVPZJAYQ
notch      : K
```

RIGHT rotor
```
rotor id   : I
entry      : ABCDEFGHIJKLMNOPQRSTUVWYXZ
def wiring : EKMFLGDQVZNTOWYHXUSPAIBRCJ
position   : R
pos wiring : USPAIBRCJEKMFLGDQVZNTOWYHX
notch      : R
```

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

Exemple de codage de la lettre 'B'

```
rotor id   : I
entry      : ABCDEFGHIJKLMNOPQRSTUVWYXZ
def wiring : EKMFLGDQVZNTOWYHXUSPAIBRCJ
position   : S
pos wiring : SPAIBRCJEKMFLGDQVZNTOWYHXU
notch      : R
result     : P<=B

rotor id   : IV
entry      : ABCDEFGHIJKLMNOPQRSTUVWYXZ
def wiring : ESOVPZJAYQUIRHXLNFTGKDCMWB
position   : L
pos wiring : IRHXLNFTGKDCMWBESOVPZJAYQU
notch      : K
result     : E<=P

rotor id   : II
entry      : ABCDEFGHIJKLMNOPQRSTUVWYXZ
def wiring : AJDKSIRUXBLHWTMCQGZNPYFVOE
position   : D
pos wiring : KSIRUXBLHWTMCQGZNPYFVOEAJD
notch      : F
result     : U<=E

reflector  : UKW-B
wiring     : YRUHQSLDPXNGOKMIEBFZCWVJAT
result     : U=>C

rotor id   : II
entry      : ABCDEFGHIJKLMNOPQRSTUVWYXZ
def wiring : AJDKSIRUXBLHWTMCQGZNPYFVOE
position   : D
pos wiring : KSIRUXBLHWTMCQGZNPYFVOEAJD
notch      : F
result     : M=>C

rotor id   : IV
entry      : ABCDEFGHIJKLMNOPQRSTUVWYXZ
def wiring : ESOVPZJAYQUIRHXLNFTGKDCMWB
position   : L
pos wiring : IRHXLNFTGKDCMWBESOVPZJAYQU
notch      : K
result     : M=>M

rotor id   : I
entry      : ABCDEFGHIJKLMNOPQRSTUVWYXZ
def wiring : EKMFLGDQVZNTOWYHXUSPAIBRCJ
position   : S
pos wiring : SPAIBRCJEKMFLGDQVZNTOWYHXU
notch      : R
result     : K=>M
```