

# Partajoux

DANG Hung Hoang, FUDITPHU Yan-Guillaume, KULZER Ulrike  
19 janvier 2018

## Table des matières

|          |   |          |
|----------|---|----------|
| <b>1</b> | <b>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        |
| 1.3      | Structure du programme . . . . .        | 5        |
| <b>2</b> | <b>Annexe : Code du programme</b>       | <b>5</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 abouties 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 :

— *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 permutées 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.

## 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 :

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 :

## 1.3 Structure du programme

## 2 Annexe : Code du programme

*L'ordre des modules :*

1. main\_module
2. screen\_module
3. screen\_constants
4. text\_module
5. tests