



# **MANUEL D'UTILISATION**

Licence Informatique – Troisième année

Groupe 1 Info

**Atelier de cryptographie pour la fête de science**

**Réalisé par :**

Mme. BENTABE Rania

M. FALL Mouhamed

**Encadré par :**

M. FURST Frederic

Mme. LI Yu

Mme Ionica Sorina

**Année universitaire 2024-2025**

## Table des matières

I.	Introduction .....	1
II.	Installation .....	1
III.	Guide d'utilisation .....	2
IV.	Gestion des erreurs .....	6
V.	Contacts et support .....	7

# I. Introduction

Ce document présente le manuel d'utilisation de notre application complète.

Ce manuel d'utilisation a pour objectif de guider clairement et simplement les utilisateurs dans la prise en main de l'application. Il explique les différentes fonctionnalités disponibles et comment les utiliser efficacement. Le document est organisé en sections logiques, permettant à l'utilisateur de trouver rapidement l'information recherchée.

## II. Installation

Pour l'utilisation de notre application, une installation au préalable de python3 ainsi que certaines bibliothèques est requise.

Voici les différentes étapes de l'installation sur linux :

### A. Installation python3

- ❖ Ouvrir le terminal
- ❖ Mettre à jour les dépôts : `sudo apt update`

```
momo@momo:~/Documents/SAE_4$ sudo apt update
[sudo] Mot de passe de momo :
Réception de :1 http://repo.mysql.com/apt/debian buster InRelease [22,1 kB]
Atteint :2 http://deb.debian.org/debian bullseye InRelease
Atteint :3 http://security.debian.org/debian-security bullseye-security InRelease
Atteint :4 http://deb.debian.org/debian bullseye-updates InRelease
Atteint :5 https://packages.sury.org/php bullseye InRelease
Réception de :6 http://archive.ubuntu.com/ubuntu focal InRelease [265 kB]
Err :1 http://repo.mysql.com/apt/debian buster InRelease
```

- ❖ Entrer la commande : `sudo apt install python3 python3-pip python3-venv`

```
momo@momo:~/Documents/SAE_4$ sudo apt install python3 python3-pip python3-venv
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
python3-pip est déjà la version la plus récente (20.3.4+deb11u1).
python3 est déjà la version la plus récente (3.9.2-3).
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  debsumo-archive-keyring libapache2-mod-php7.4 libdbus-glib-1-2 libpcre2-posix2 libwpe-1.0-1 libwpebackend-fdo-1.0-1 linux-image-5.10.0-10-amd64 linux-image-5.10.0-25-amd64
  php7.4 php7.4-dev php7.4-gd php7.4-mysql rlinetd tcpd
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
Les paquets supplémentaires suivants seront installés :
  libpython3.9 libpython3.9-dev libpython3.9-minimal libpython3.9-stdlib python3.9 python3.9-dev python3.9-minimal python3.9-venv
Paquets suggérés :
  python3.9-doc binfmt-support
Les NOUVEAUX paquets suivants seront installés :
  python3-venv python3.9-venv
Les paquets suivants seront mis à jour :
  libpython3.9 libpython3.9-dev libpython3.9-minimal libpython3.9-stdlib python3.9 python3.9-dev python3.9-minimal
7 mis à jour, 2 nouvellement installés, 0 à enlever et 5 non mis à jour.
Il est nécessaire de prendre 6 596 o/11,5 Mo dans les archives.
Après cette opération, 42,0 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n]
```

### B. Installation des bibliothèques requises

- ❖ Pour l'utilisation de la bibliothèque tkinter : `sudo apt install python3-tk`
- ❖ Pour l'utilisation de la bibliothèque PIL : `pip install pillow`
- ❖ Pour l'upgrade de POP : `python3 -m pip install --upgrade pip`

### III. Guide d'utilisation

Dans cette partie, nous allons décrire les différentes fonctionnalités principales de notre application et leur utilisation.

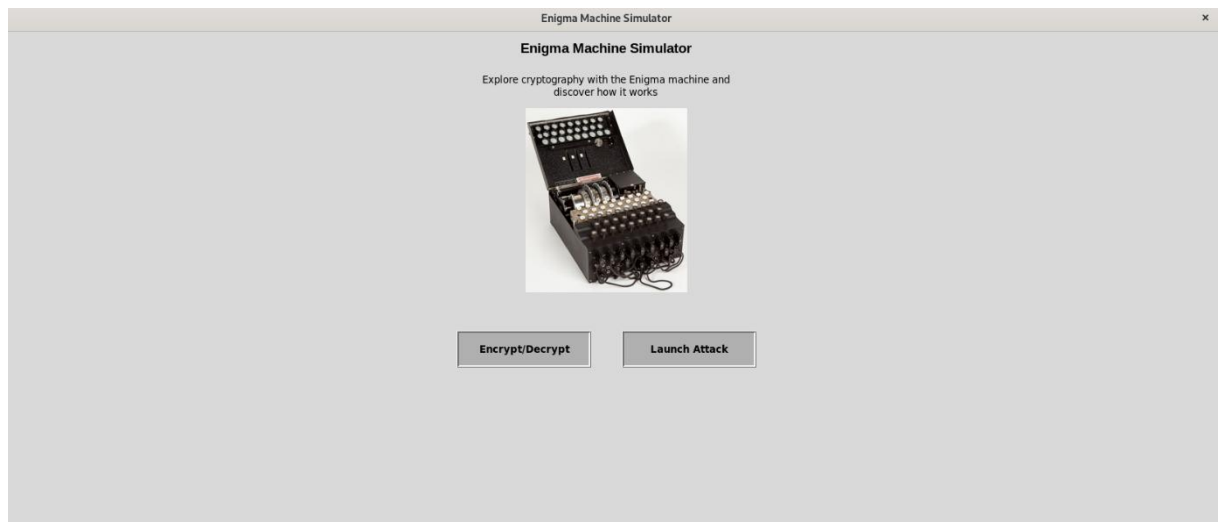
#### a) Chiffrement/Déchiffrement :

Cette fonctionnalité permet à l'utilisateur d'effectuer le chiffrement ou déchiffrement d'un texte saisi.

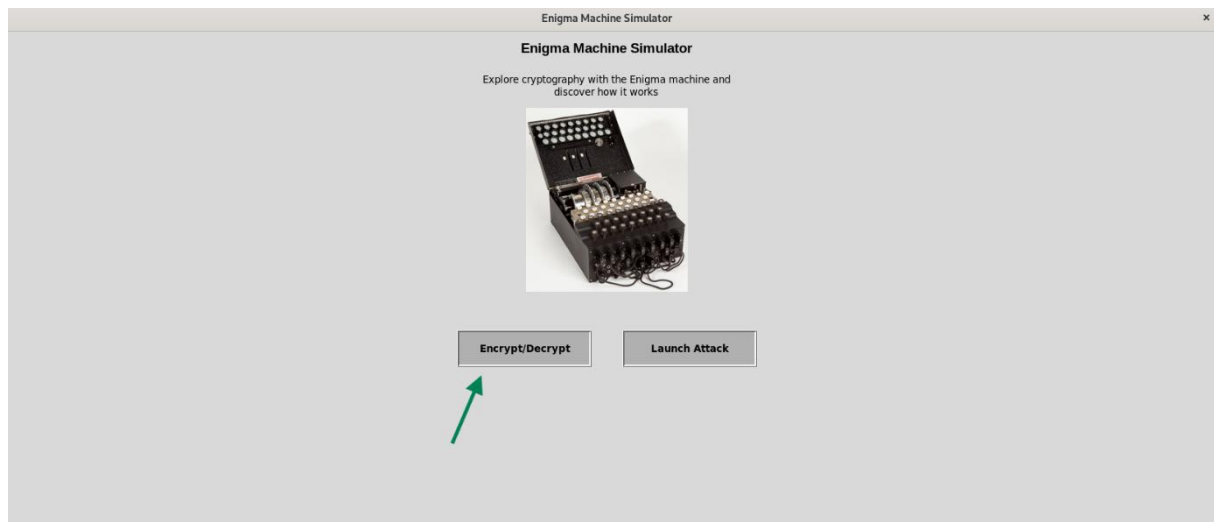
Pour réaliser un chiffrement ou déchiffrement, voici les différentes étapes à suivre :

- D'abord, lancer l'accueil avec la commande suivante : **python3 Accueil.py**

```
momo@momo:~/Documents/SAE_4$ ls
Accueil.py  Attack.py  config  I_Attack.py  I_chiffrement.py  Machine.py  pycache  ressource
momo@momo:~/Documents/SAE_4$ python3 Accueil.py
```

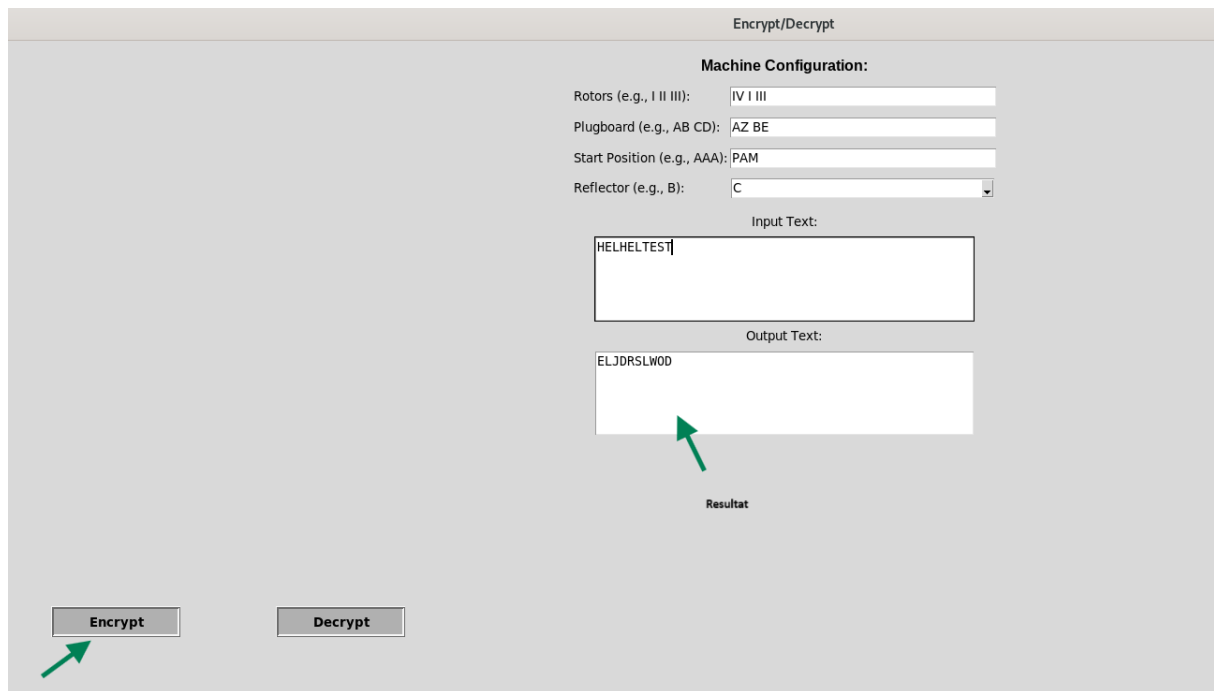


- Une fois sur la page d'accueil, appuyer sur le bouton « **Encrypt/Decrypt** »



- Maintenant on peut commencer le chiffrement/déchiffrement en renseignant le texte et la configuration de la machine avec les champs suivants :
  - **Rotors** : Ce champ permet de spécifier l'ordre des rotors de droite à gauche. Les rotors autorisés sont : I II III IV V.
  - **Plugboard** : Ce champ permet de spécifier les différentes connexions des lettres .il est optionnel.
  - **Start position** : Ce champ permet de spécifier les positions initiales des rotors de droites à gauche.
  - **Reflector** : Ce champ permet d'indiquer le type de réflecteur à utiliser pour le chiffrement/déchiffrement.
  - **Input text** : Text à chiffrer/déchiffrer.

### Exemple du chiffrement du texte « HELHELTEST »

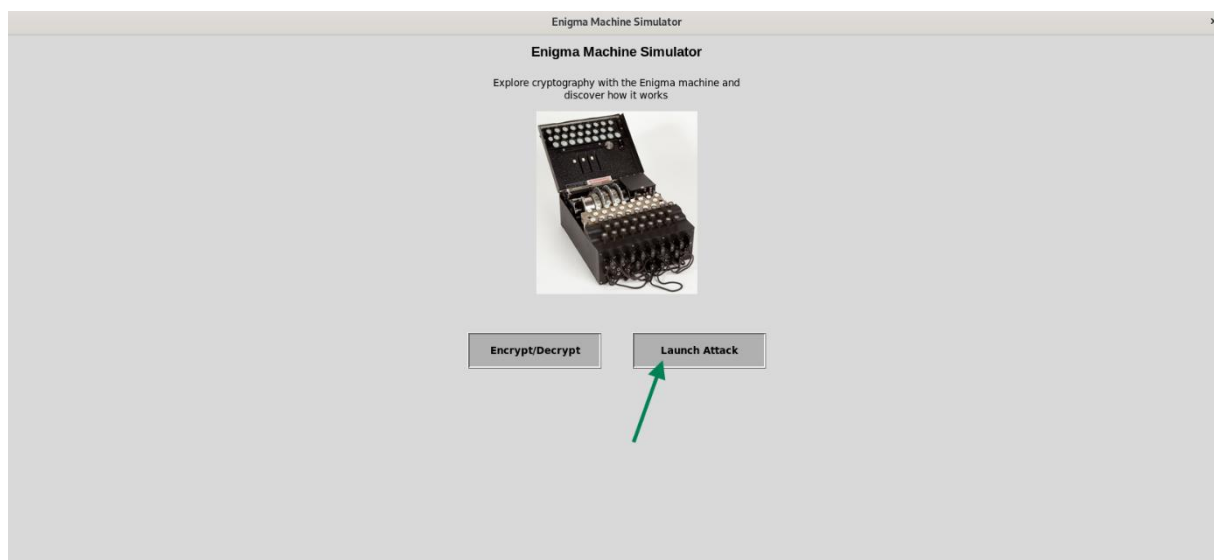


## b) Attaque

Cette fonctionnalité permet à l'utilisateur de procéder à une attaque afin de retrouver la configuration de la machine(clé).

Pour réaliser une attaque, voici les différentes étapes à réaliser :

- ❖ Sur la page d'accueil, appuyer sur le bouton « **Launch Attack** »



Attack

Plain Text:

Cipher Text:

Launch Attack

Encryption Key Details:

Rotors (e.g., I II III):

Plugboard (e.g., AB CD):

Start Position (e.g., AAA):

Reflector (e.g., B):

Test

- ❖ Une fois sur la page d'accueil, avant d'appuyer sur « **Launch Attack** », renseigner le texte en clair et le texte chiffré.

Attack

Plain Text:

AZEAEZTEST

Cipher Text:

NMIPQJCGDI

Launch Attack

Démarrer l'attaque

Encryption Key Details:

Rotors (e.g., I II III):

Plugboard (e.g., AB CD):

Start Position (e.g., AAA):

Reflector (e.g., B):

Test

Plain Text:

AZEAEZTEST

Cipher Text:

NMIPQJCGDI

Launch Attack

Clé retrouvé !

Encryption Key Details:

Rotors (e.g., I II III):

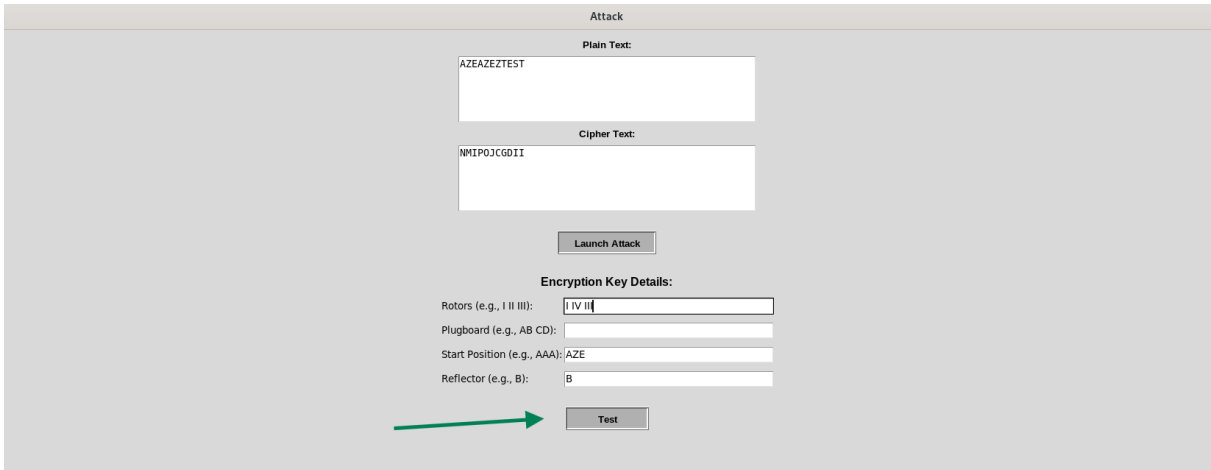
Plugboard (e.g., AB CD):

Start Position (e.g., AAA):

Reflector (e.g., B):

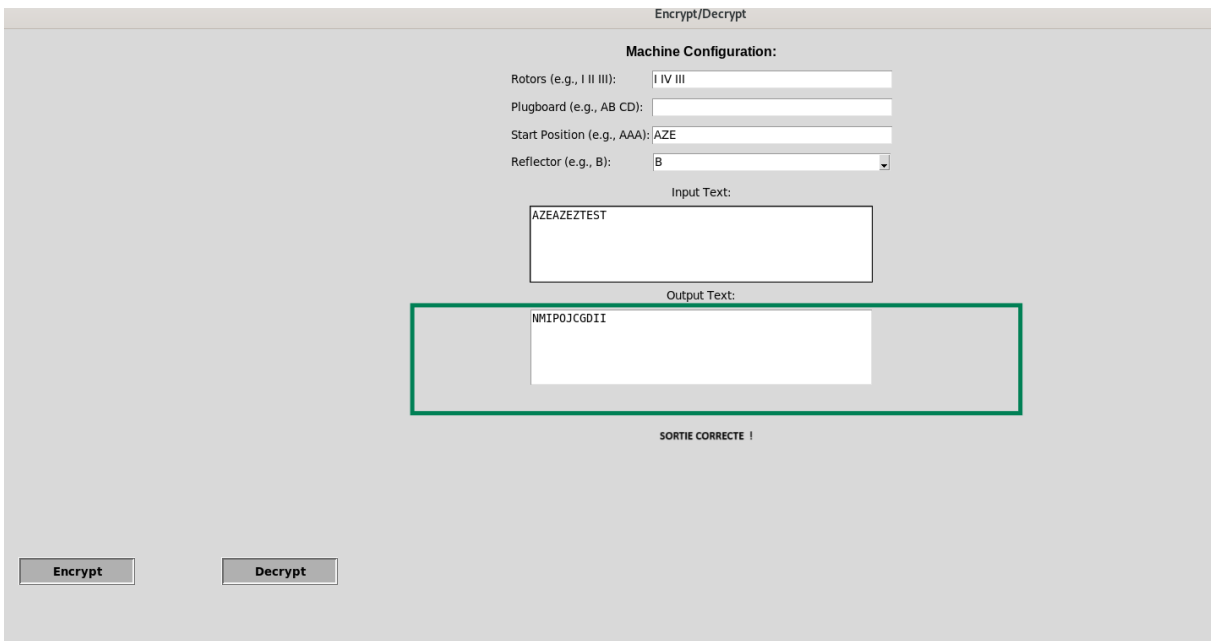
Test

Une fois la clé retrouvée, pour faire une vérification, l'utilisateur peut appuyer sur le bouton « **test** » puis renseigner le texte en clair initial afin de savoir s'il obtiendra le texte chiffré intercepté au départ.



The 'Attack' interface contains the following elements:

- Plain Text:** A text box containing 'AZEAEZTEST'.
- Cipher Text:** A text box containing 'NMIP0JCGDII'.
- Launch Attack:** A button.
- Encryption Key Details:**
  - Rotors (e.g., I II III):** A dropdown menu showing 'I IV II'.
  - Plugboard (e.g., AB CD):** An empty text box.
  - Start Position (e.g., AAA):** A text box containing 'AZE'.
  - Reflector (e.g., B):** A dropdown menu showing 'B'.
- Test:** A button with a green arrow pointing to it from the left.



The 'Encrypt/Decrypt' interface contains the following elements:

- Machine Configuration:**
  - Rotors (e.g., I II III):** A dropdown menu showing 'I IV III'.
  - Plugboard (e.g., AB CD):** An empty text box.
  - Start Position (e.g., AAA):** A text box containing 'AZE'.
  - Reflector (e.g., B):** A dropdown menu showing 'B'.
- Input Text:** A text box containing 'AZEAEZTEST'.
- Output Text:** A text box containing 'NMIP0JCGDII', which is highlighted with a green rectangular border.
- SORTIE CORRECTE !** A message displayed below the output text box.
- Encrypt:** A button.
- Decrypt:** A button.

## IV. Gestion des erreurs

L'application intègre déjà des messages clairs pour informer l'utilisateur des erreurs de saisie et des éventuelles mauvaises configurations.

Si une erreur persiste ou que l'utilisateur rencontre une situation non prévue, il peut contacter le support technique via les coordonnées fournies dans la section « Contacts et support ».



## V. Contacts et support

Pour toute information relative au fonctionnement de la machine Enigma, veuillez-vous référer au document suivant :

<https://razvanbarbulescu.pages.math.cnrs.fr/ImageDesMaths/enigma.html>

### **Contacts**

Rania BENTABE : [rania.bentabe@etud.u-picardie.fr](mailto:rania.bentabe@etud.u-picardie.fr)

Mouhamed FALL : [mouhamed.fall@etud.u-picardie.fr](mailto:mouhamed.fall@etud.u-picardie.fr)