Goal

In this Lab, you will attempt to cryptanalyse texts encrypted using two classical cryptosystems: the Vigenère cipher, and the monoalphabetic substitution cipher. We provide you with scripts to help you in your cryptanalysis.

Preliminaries

Download the archive Lab1.zip.

```
$ wget https://www.enseignement.polytechnique.fr/informatique/INF558/TD/td_1/Lab1.zip
```

Unzip the file.

```
$ unzip Lab1.zip
```

Change directory into `Lab1`.

```
$ cd Lab1
```

Vigenère cipher

Open the Jupyter notebook `Vigenere.ipynb`

```
$ jupyter3 notebook Vigenere.ipynb
```

to start the given notebook `Vigenere.ipynb` and follow the instructions. Basically, you need to type return in each cell, or use one of the buttons. Ask for help if your get stuck.

Depending on your configuration, you might need to replace `jupyter3` by `jypyter` (without the `3`) in the command.

Modify the language and the target ciphertext. Your goal is to decrypt the message that was sent to you by email, but you can also attempt to break other ciphertexts.

Monoalphabetic substitution

Open the Jupyter notebook `Monoalphabetic.ipynb`

```
$ jupyter3 notebook Monoalphabetic.ipynb
```

to start the given notebook `Monoalphabetic.ipynb` and follow the instructions.

Depending on your configuration, you might need to replace `jupyter3` by `jypyter` (without the `3`) in the command.

Modify the language and the target ciphertext. Your goal is to decrypt the message that was sent to you by email, but you can also attempt to break other ciphertexts.

Homework for next week

You will receive by email a text encrypted using a monoalphabetic substitution cipher. Your goal is to cryptanalyse it.

See the details of the assignment on the dedicated page on Moodle.

Good luck!