Assignment

This exercise involves decrypting two different pieces of ciphertext using two different methods to find the encryption keys and the original plaintext messages. Please refer to the file: "studentAssignmentInfo_Moodle.csv" on Moodle to locate your ciphertexts.

All of the secret messages have been encrypted by an 8-rotor encryption machine written in Java. The source code for the Rotor Machine is available on Moodle as the file **`Rotor96Crypto.java`**. You just need to write the code to use it to search for the various keys. All the keys have been taken for a file of common passwords called **`passwords`**, which is also available on Moodle.

Once you have finished your exercise, submit a zip file containing your **report** and your **two programs**, called **`KPA.java`** (for Known Plaintext Attack) and **`COA.java`** (for Ciphertext Only Attack) using Moodle. Your zip file should have the form **`lastname_firstname.zip`** - mine would be called **`nguyen_truong.zip`.**

Deadline Saturday 10th March 2025 at 11.30 p.m. This exercise is worth 20% of your mark for this module.

Known Plaintext Attack (KPA):

You will be given a chunk of ciphertext, together with the **first two characters (i.e., "W" and "e")** of the plaintext.

(1) Write a program to perform a ***dictionary attack*** to find the key. Use this key to decode the rest of the message. Your report should contain the key you found and the decoded message.

(2) Some of you may find more than one possible keys that produce decoded messages starting with the first two characters, but only one of them is an English sentence. All of you need to explain in words why this happens (even though in your specific case, only 1 key is found), and how you choose the correct key (You do not need to program to choose the right key, just explain in words).

(3) Calculate the probability of this occurrence (i.e., finding more than one keys that produce decoded messages starting with the two provided characters).

Ciphertext Only Attack (COA):

You will be given another chunk of ciphertext, as above, but **no information** about plaintext.

(1) You will need to perform a ***dictionary attack as before***, but now decide whether a key produces the correct plaintext, given that the plaintext is an English language message.Your report should contain the key you found and the decoded message.

(2) You should explain and elaborate your method on how you decide whether a decoded message is the correct plaintext or not.

(3) You will need to perform some experiment to find out how many ciphertext characters were needed to decode the message unambiguously. You should also include a theoretical calculation of the number of ciphertext letters needed before unambiguous decoding is possible, together with the actual number of letters needed for your particular message, as found by your experiment. Explain the difference.

My Supporting Code

My code is in a class called **`Rotor96Crypto`**, which implements an 8-rotor machine. Each rotor has 96 characters, the complete ASCII character set. There is one public method:

```
public String encdec(int mode, String key, String text)
```

`mode` is either `ENC=1` for Encryption, when `text` is the plaintext and the ciphertext is returned, or `DEC=2` for Decryption, when `text` is the ciphertext and the plaintext is returned.

Further support:

https://www3.nd.edu/~busiforc/handouts/cryptography/cryptography%20hints.html