Faculty of Computers, Informatics and Microelectronics
Technical University of Moldova

Information Security

Lab#3

Author:

Valeria BEGA

Supervisor:

Mihai COSLET

Chisinau 2017

Topic :

Breaking the shift cypher.

Implementation :

How?

By using the frequency analysis method. As I read lots of info and watched videos, there are multiple ways to break shifts, especially this one. For this laboratory was requested the frequency analysis thing. This way, when you look at an already encrypted sentence you can check the most common letter. Assuming that a text is in English, the most common letter in this language is E, next T and the logic goes on. It will be easy to decipher the sentence.

The main problem here is, that it gets more difficult when you don't know in which language the ciphered text is. Even though the letter frequency might be quite similar, still there are differences, and lots of languages such as Romanian, French, Russian have lots of different letters, accents and other weirdos.

In order to implement the requirements we need :

1. To remove all the symbols and everything which is not a letter, so the text can be parsed.
2. Count the number of times a letter appears in the text and create the possible permutations.
3. Shift the letters based on the permutations to get the text.
4. In the end, to check if the text makes sense I have a list of popular valid English words and check the text if it contains them.

Result example :

```
C:\Python27\python.exe C:/Users/begav/Desktop/UniStuff/SI/Lab2_SI/lab3.py
MAXIMUS: MY NAME IS MAXIMUS DECIMUS MERIDIUS, COMMANDER OF THE ARMIES OF THE NORTH, GENERAL (
EVERY PLAN IS TO BE CONSIDERED, EVERY EXPEDIENT TRIED AND EVERY METHOD TAKEN BEFORE MATTERS A
MY LOVE FOR THE ROMAN EMPIRE IS UNDENIABLY GREATER THAN FOR MYSELF. THE GREATEST EMPIRE EVER

Process finished with exit code 0
```

Conclusion :

This laboratory was fun to work on because encryption/decryption is always an interesting topic, and there are so many algorithms out there, that it feels nice to know at least how to break one. The frequency analysis was also interesting, especially because it makes playing with languages such as French and Russian more challenging.