MID-TERM PROJECT REPORT

# Introduction

The project is on a new counter mode cipher which comprises of an encryption using recurring stages of substitution and transposition with a 64-bit symmetric key. It will include a functional UI and will be able to encrypt/decrypt files of variable types.

# Literature Survey

The encryption algorithm uses rounds of substitution and transposition. The substitution cipher derives from a classic vigenere cipher but has a twist in its implementation. The transposition cipher does not have any classical roots but uses an array of indices generated using the key, and transposes the characters in the 64-bit block accordingly.

# Objectives

The objectives of the project include:

* Encryption/Decryption using multiple stages of substitution and transposition.
* Block chaining using counter mode.
* Dispersion of relative frequencies of characters.
* Dispersion of relative frequencies of digrams and trigrams.
* Ability to handle files of various types.
* Reasonable confusion and diffusion.

# Methodology

## Substitution cipher

The key and plaintext blocks are divided into 4-bit blocks. The (2i)th and (2i+1)th nibbles of the key are added to the ith nibble of plaintext. However, after the 8th nibble of plaintext, the 16th nibble of the key will be exhausted. To avoid reuse of the same nibble pairs of the key, the key is right circular shifted by 4 bits. This gives a new key set of 64 bits which is used to encrypt the remaining 32 bits of the plaintext in the same fashion.

## Transposition cipher

An array of integers from 0 to 7 is taken. This array is then shuffled using the key to perform the shuffle. The reordered array provides the new order of indices of the bytes in the 64-bit block of plaintext.

This substitution and transposition process is carried out in 10 repeating stages using a key and a changing numeric counter.

# Work Done So Far

Encryption part of the cipher is completed and operational. The program takes an input text file, parses it and encrypts it using the substitution and transposition cipher techniques.

Relative frequency analysis using some plaintext-cipher text pairs has also been done.

# Results

For the plaintext: FitAR0^,exol(pOo(.=w\_CaFpLnP>t't7^+MWDg9;0$tU%]:Lswf&1+GKB78za=

Using the key: abcdefgh

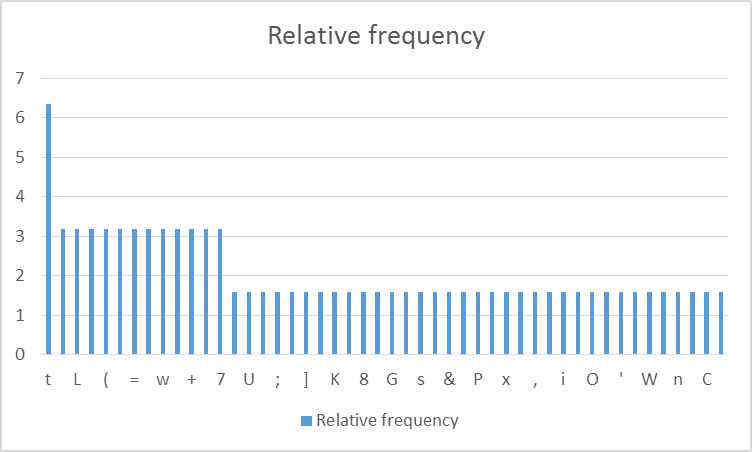
The cipher results in the following cipher text: ÞÉ€PÛÄI»‰ŠÝ¹yI‹³ØÚÏƒÜÎŸPüÎÞ¬vié“ª)5Q"~)W¡eFâTÔGœêà‹

# Work Remaining

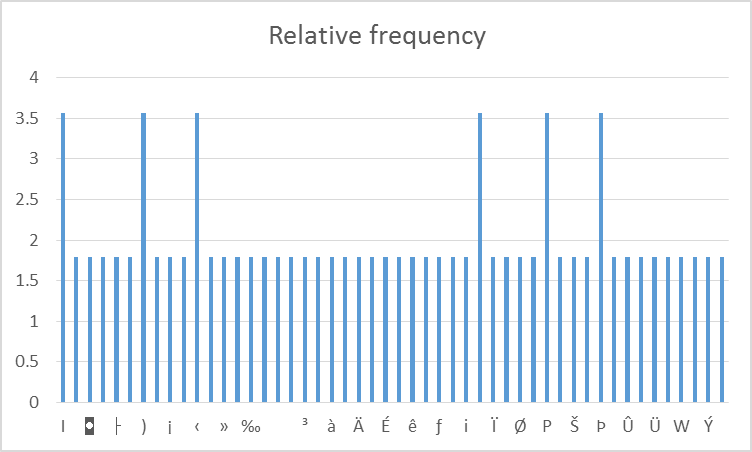
Decryption stage of the cipher, ability to handle various file types and a minimal GUI to be worked on further.

# Conclusions

Relative frequencies of characters in the plaintext:



Relative frequencies of characters in the cipher text:



# References

* <http://www.dcode.fr/frequency-analysis>
* <http://randomtextgenerator.com/>
* <http://stackoverflow.com/>
* <http://www.geeksforgeeks.org/>