## Adeen Ayub

## Aphichaya Piyapinansook

## Rony Xavier

## CS6903 Project 1

Cryptanalysis based on Unit Frequency Characters in the key

This team consists of Adeen Ayub, Aphichaya Piyapinansook, and Rony Xavier. We are submitting one cryptanalysis approach as follows:

## Cryptanalysis APPROACH for test1

The cryptanalysis approach we used in our program utilizes the fact that seven of the alphabets ( 'b', 'j', 'k', 'v', 'q', 'x', 'z' ) have the average frequency of one, which means that their corresponding ciphertext will be same and repeated. For example, the letter j has an average frequency of 1 and the key value would be k(j,1), for any randomly chosen key, Its ciphertext will always be identical.

We pre-process the known plaintexts to map out occurrences of all the unit frequency characters. In other words, we collected and saved all the known unit frequency character positions that help us determine which one of the five plaintexts is given as ciphertexts.

The decryption scheme will work regardless of the scheduling algorithm used in the encryption scheme. The Scheduling algorithm does not play a crucial role in this decryption scheme due to the weakness that several alphabets only have an average frequency of 1. This results in those letters being mapped to the same number.

## IMPLEMENTATION for test1

As stated above, the decryption scheme preprocesses the known plaintexts to map the occurrences of all the unit frequency characters using the method GENERATE\_UNIT\_FREQ\_CHAR\_POSITIONS.

**procedure** GENERATE\_UNIT\_FREQ\_CHAR\_POSITIONS

PLAINTEXT\_LIST 🡨 List of known plaintext strings

UNIT\_FREQUENCY\_CHARS 🡨 List of unit frequency chars { 'b', 'j', 'k', 'v', 'q', 'x', 'z' }

**for** each string *plaintext* in the PLAINTEXT\_LIST **do**

**for** each character *char* in UNIT\_FREQUENCY\_CHARS **do**

**for** each character *letter* in *plaintext* **do**

**if** *char == letter* **do**

insert into vector *positionlist* index of *letter* in *plaintext*

**end if**

**end for**

insert into map *unitFreqCharPositions* vector *positionlist* at key *char*

**end for**

insert into vector *unitFreqCharPositionsList* map *unitFreqCharPositions*

**end for**

**return** *unitFreqCharPositionsList*

**end procedure**

The ciphertext is received from the user from STDIN as series of integers delimited by commas. The method DECRYPT\_CIPHERTEXT shown below performs the decryption and returns an index which gives the guessed plaintext or returns ‘-1’ indicating failure to decrypt.

**procedure** DECRYPT\_CIPHERTEXT

CIPHERTEXT 🡨 vector of integers that form the provided ciphertext

*unitFreqCharPositionsList* 🡨 from GENERATE\_UNIT\_FREQ\_CHAR\_POSITIONS

**for** each map *unitFreqCharPositions* in *unitFreqCharPositionsList* **do**

**for** each key *char* in *unitFreqCharPositions* **do**

vector*positions* **🡨** *unitFreqCharPositions* value at key *char*

**for** eachinteger *position*in *positions* **do**

insert into vector *list* values of CIPHERTEXT at index *position*

**end for**

**if** length of *list >* 1 **AND** all elements of *list* are equal

/\* return index which is the index of guessed plaintext \*/

**return** index of *unitFreqCharPositions* in *unitFreqCharPositionsList*

**end if**

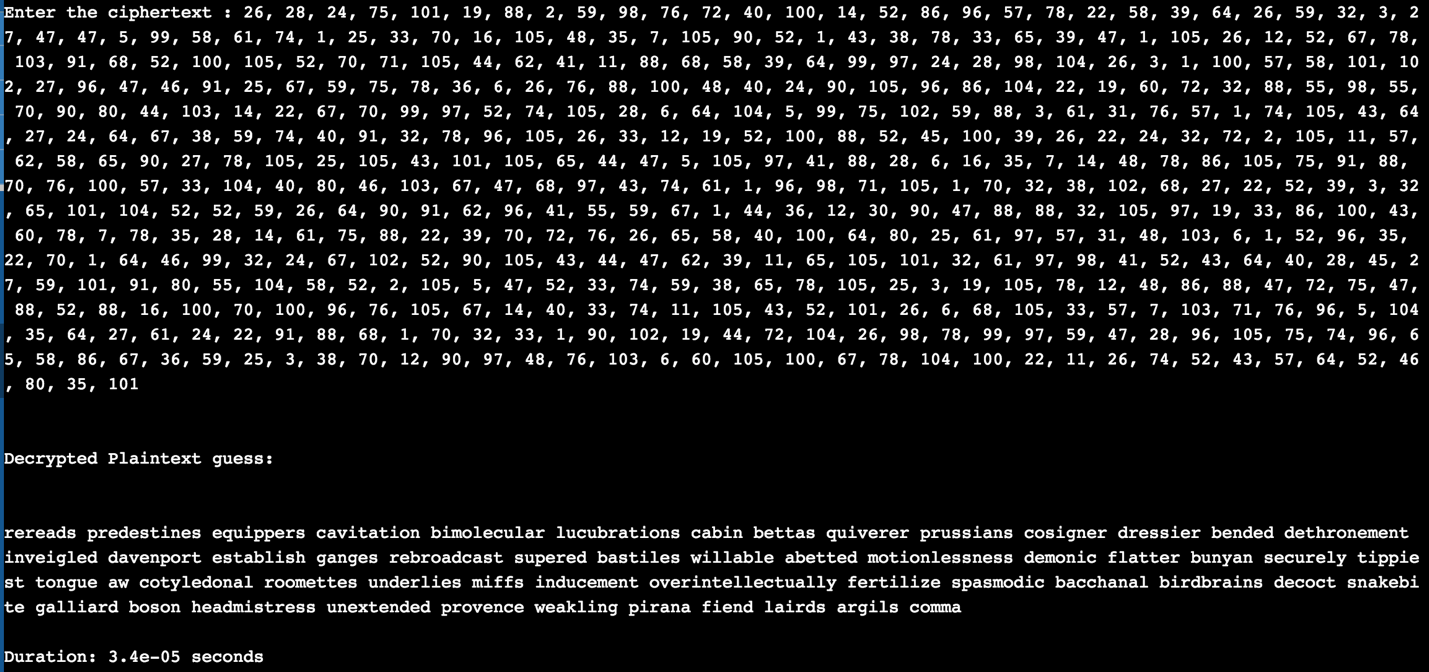
**end for**

**end for**

**return** -1 /\* indicating failure \*/

**end procedure**

## Trial run for test1:



## Conclusion

The decryption scheme could effectively decrypt ciphertexts of known plaintexts thus the encryption scheme fails the *indistinguishability* notion. The proposed scheme does not address test2.