Islam Ibragimov 1,2,5

Braeden Olney 3,4

CS430

4/8/23

1. Edgar Allen Poe's 1843 short story, "The Gold Bug", features a cryptanalytic attack.

What type of cipher is broken and how?

**- The cipher that was cracked was a simple substitution cipher, and the method used to break it relied on analyzing the frequency of symbols.**

What happens as a result of this cryptanalytic success?

**- The breakthrough in deciphering the cipher led to the discovery of shortcuts, making it feasible to handle an overwhelmingly large number of possible keys. It became apparent that simple substitution was not sufficient, as there are 26 factorial keys to consider, and statistical analysis alone was inadequate for effective decryption. As a result, cryptanalysis techniques evolved to incorporate more advanced methods of confusion and encryption.**

1. Find the plaintext and the key of the following ciphertext. Hint: the key is a shift of the alphabet, n.

CSYEVIXIVQMREXIH

* **I created a table for all 4 keys. All three keys before key 4 didn’t make any sense, only key 4 gave me meaningful output. So, I put a photo of only key 4 here, but if it is necessary can provide the work for other three keys too.**

A sheet of music

Description automatically generated with medium confidence

3) Write a program to help an analyst decrypt a simple substitution cipher. Your program should take the ciphertext as input, compute letter frequency counts, and display these for the analyst. The program should then allow the analyst to guess a key and display the results of the corresponding "decryption" with the putative key.

The source code for this question will be in a java file with the submission.

Report for implementation:

For the implementation of the program, it starts by asking the user for a string to decrypt, then the string is counted for each letter’s occurrence, then the stats are printed for each letter if it has 1 or more occurrences. Then the user is prompted to try putting in a possible key for the cipher until the user types “end” where the program exits. Implementation for this was straightforward and there are no known bugs, no real data structures were used for this just java collections resources and string/char manipulation.

4) Use this program to determine the plaintext and key for the ciphertext that appears in the following Alice in Wonderland quote:

**MXDXBVTZWVMXNSPBQXLIMSCCSGXSCJXBOVQXCJZMOJZCVCTVWJCZAAXZBCSSCJXBQCJZCOJZCNSPOXBXSBTVWJCJZDXGXXMOZQMSCSCJXBOVQXCJZMOJZCNSPJZHGXXMOSPLHJZDXZAAXZBXHCSCJXTCSGXSCJXBOVQX**

The key for the ciphertext is prtvEFbdfhKlnywusRomUigeYa where the capitalized letters aren’t used in the ciphertext.

The plain text for the ciphertext is neverimagineyourselfnottobeotherwisethanwhatitmightappeartoothersthatwhatyouwereormighthavebeenwasnototherwisethanwhatyouhadbeenwouldhaveappearedtothemtobeotherwise

5) Decrypt the ciphertext:

IAUTMOCSMNIMREBOTNELSTRHEREOAEVMWIH

TSEEATMAEOHWHSYCEELTTEOHMUOUFEHTRFT

This message was encrypted with a double transposition (of the type discussed in the text) using a matrix of 7 rows and 10 columns.

Hint: The first word is "there." Put the ciphertext in a 7 x 10 array. Then the letters of "there" will all appear (in scrambled order) in one row. This gives a start on the column permutation. Once the column perms are known, the row perms are easily determined.

Text, letter

Description automatically generated

Text, letter

Description automatically generated

Text, letter

Description automatically generated

Text, letter

Description automatically generated

Text, letter

Description automatically generated

Text, letter

Description automatically generated

Text, letter

Description automatically generated