**CS 430 – Introduction to Computer Security**

**Project 0 – not graded, do not submit**

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

a. What type of cipher is broken and how?

b. What happens as a result of this cryptanalytic success?

1. Given that the Caesar's cipher was used, find the plaintext and the shift that corresponds to the following ciphertext:

CSYEVIXIVQMREXIH

**Hint:** You may use, for instance: <http://www.dcode.fr/caesar-cipher>

1. 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.
2. Use the program to determine the plaintext and key for the ciphertext that appears in the following *Alice in Wonderland* quote:

"Begin at the beginning," the King said, very gravely," and go on till you come to the end: then stop."

The message was encrypted with a simple substitution cipher and the plaintext has no spaces or punctuation.

1. Decrypt the ciphertext:

IAUTMDCSMNIMREBOTNELSTRHEREOAEVMWIH

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.