Project 1: Cracking Encryption

Due Wednesday, September 13

For this assignment, you are given 6 files containing ciphertext from 4 different ciphers. In order to receive full credit, you must provide (for each file):

- Plaintext
- The cipher and key used for encryption
- A description of how you decrypted the file, including any computer programs you wrote to assist in this task

A complete report describing all of the above will be somewhat lengthy. Computer programs may be in any language.

Each of your 6 files may be encrypted with any of the 4 methods (shift, stream, permutation, and Vigenere). At least one file will be encrypted with each method. The plaintext is taken from articles on Wikipedia. All articles were written in English, but may contain names from other languages. Since the text was harvested some years ago, it may not match any current article exactly.

Standard letter frequencies can be found here:
http://en.wikipedia.org/wiki/Letter_frequency

Key Limitations

For the permutation cipher, the block is restricted to no more than 15 by 15. For the vigenere cipher, the key is a single word.

Allowed Methods

Although it is possible to decrypt all the files purely by hand, a computer is strongly recommended. There are websites which will crack historical ciphers, but this is not an allowed method. Write your own software for the task. Consulting with your peers is recommended, particularly in identifying which ciphertext was produced by which cipher, but do write your own decryption programs.

Turning in the assignment

Upload a single file (zip or tar archive) containing programs you wrote or used for this project along with your report. Any common format for the report is acceptable, but .pdf is preferred. Formatting in Microsoft Office is not always preserved when opening documents in alternate word processors! Reports should not be encrypted.