CSC564A Computer Security

Project 1

(due by midnight on Friday, February 17)

Version 1

Project 1 must be submitted electronically, using the Blackboard Digital Dropbox facility of the course website. Remember that the dropbox is a two stage process. If you don't do it right, I won't receive the assignment, and you will get a zero for the assignment.

Each assignment must be prepared with a word processor. I'll take ASCI text documents (like those prepared with NOTEPAD), MS Word 2003 compatible documents, and PDF. You should clear with me in advance any other formats. Please do NOT send me multiple files for a single homework assignment - get it into one file. Zipped files will not be accepted!

Use the following naming conventions. If your name is John Smith, then your file name must be jsmith.doc, or jsmith.txt, or jsmith.pdf.

Problem 1. (Substitution cipher) (50 points) Break the following ciphertext if you know that it has been encrypted with an affine cipher. You also know that ciphertext *e* decodes to plaintext *i* and ciphertext *d* decodes to plaintext *f*.

sgivkrulgxukxujcuffuxzngt

Problem 2 (Transposition cipher) (50points) Break the following ciphertext. You know that it has been created using a transposition cipher.You have two choices:

- To write a program (in a language of your choice) that breaks the ciphertext using a brute force attack. Document and explain the program. Attach the source code.
- To break the ciphertext manually without a program. In this case, you are not allowed to apply a brute force attack. Show all your work. Answer the following questions: What are the weaknesses of this cipher? How could the cipher be improved? What are the weaknesses of the ciphertext that make it easy to break?

aicasugdtyyetyarfrntoaepl