

HW # 5

Due Date: Wednesday, October 10th, 2007, 7:20 PM
at the beginning of class

Reading Assignment:

- W. Stallings, *Cryptography and Network Security*, Chapter 2
- A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, Chapter 7.3

Problems:

Please use very legible handwriting or type the answers. In either case you can draw diagrams and write formulae by hand but they have to be legible and the diagrams have to be labeled clearly. Answers that neither the TA nor the instructor can read receive 0 points. You are allowed to work in groups on these problems but you have to **write your own solution** in your own words. Copying the solution from someone else (in class or otherwise e.g. Internet) is a serious honor code violation and will be treated as such.

1. (10 points) Decipher the following short English message using the Vigenere Cipher and the key "FAUST".

BHIWO JRQAL MEMLH PEYHT XEWJX YMOKM MIXWM MEZSV YTBSM MEJGL
XEMKX XOHWZ TENZX

Please note that all spaces and punctuation characters have been removed from the message before encryption, and the letters of the ciphertext have been arranged for convenience and increased readability in the groups of five characters.

2. (10 points) Encrypt the message "Secrets travel fast in Paris" using the Playfair cipher (following the exact specification given in the Stallings book) using the key: NAPOLEON. Note: You should never use a password/key for a real cryptosystem that is so closely associated with the plaintext.
3. (10 points) Encrypt the message from question 2 using the Hill Cipher and the key

$$\begin{pmatrix} 3 & 12 \\ 19 & 5 \end{pmatrix}$$