

Homework 1

Due date: September 21

1. (5 pts) What are the three basic components of network security? Please list at least three threats of network security, preferably covering more than one components.
2. (35 pts) As we know, although the Hill cipher is strong against a ciphertext-only attack, it is vulnerable to known plaintext attacks. In this problem, you will have the opportunity to practice such an attack. On the webpage of CS 291, you could get a ciphertext file (encoded.out) which is encrypted using Hill cipher, it is your responsibility to analyze it and to restore it. Below is some information about the original and the encrypted files:
 - The plaintext is a .ps file developed with TeX Version 3.14 (MikTeX 2.3), and dvips 5.90.
 - It was encrypted using Hill Cipher with a key of 2×2 matrix in electronic codebook (ECB) mode. In this mode the plaintext is decomposed into blocks of appropriate size (depending on the key size). Each block of plaintext is encrypted using the same key independently. For more information on ECB mode, please refer to our textbook [WS] Section 3.7.
 - The numerical value of each character is determined by its ASCII value (range 0 – 255).
 - The encrypted file you received may not be the same size as the original .ps file. There is an additional four-byte integer at the beginning of the encrypted file which you need to skip.

In the homework, you need to do the following:

- explain in detail your analysis and restoration procedure; (20 pts)
- write down the key matrix and the message that is carried in the original .ps file; (10 pts)
- discuss the possible approaches to improve the security of the encryption procedure; (5 pts)

(Hint: you may wish to do a little research into .ps file's structure.)

3. (30 pts) Playfair cipher is one of the most widely used multiple-letter ciphers due to its simple yet effective design of key table. In this problem, you will take the challenge to design a cipher that outperforms the Playfair cipher.

The first step is to understand the fundamentals of multiple-letter ciphers and the limitation of Playfair cipher. The questions which you need to answer are:

- How many different plaintext-to-ciphertext block transformations can be provided by a two-letter cipher, and in a general setting, n-letter cipher? (please also explain your results.) (5 pts)
- How many possible plaintext-to-ciphertext transformations can be achieved in Playfair cipher? If your answer to this question is smaller than the result in the previous question, that means some plaintext-to-ciphertext transformations are impossible in Playfair cipher, please give an example of such transformations. (5 pts)

Now you are going to design a *two-letter* cipher of your own. The cipher will be named “Myal Cipher” (My Alphabetic Cipher). You are facing the following issues:

- How the key is designed, what is the key length, how many keys does Myal cipher has for encryption/decryption. (8 pts)
- How the rules are defined to transform a plaintext to a ciphertext based on the key. How many possible transformations can be achieved by Myal cipher. Please use examples to illustrate the transformations over different two-letter combinations (digrams) in Myal cipher. (9 pts)

Upon finishing designing Myal cipher, please discuss the security and usability of Myal cipher in comparison with Playfair cipher. (3 pts)