Tutorial 1: Introduction to Info Security

Discuss Q1-Q5 from **Assignment 1.**

1. Some authors distinguish between secrecy, privacy, and confidentiality. In this usage, secrecy is equivalent to our use of the term confidentiality, whereas privacy is secrecy applied to personal data, and confidentiality (in this misguided sense) refers to an obligation not to divulge certain information.

   a. Discuss a real-world situation where privacy is an important security issue.

   b. Discuss a real-world situation where confidentiality (in this incorrect sense) is a critical security issue.

2. Given that the Caesar's cipher was used, find the plaintext that correspond to the following ciphertext:

   VSRQJHEREVTXDUHSDQWU

3. Find the plaintext and the key, given the ciphertext:

   CSYEVIXIVQMREXIH

   Hint: The key is a shift of the alphabet.

4. Determine the plaintext and key for the ciphertext that appears in the Alice in Wonderland quote at the beginning of this chapter.

   MXDXBVTZWVMXNSPBQXLIMSCCSGXSCJXBOVQXCJZMOJZCVC

   TVWJCZAAXZBCSSCJXBQCJZCOJZCNSPOXBXSBTVWJC

   JZDXGXXMOZQMSCSCJXBOVQXCJZMOJZCNSPJZHGXXMOSPLH

   JZDXZAAXZBXHCSCJXTCSGXSCJXBOVQX

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

5. Encrypt the message

we are all together

using a double transposition cipher (of the type described in the text) with 4 rows and 4 columns, using the row permutation

(1,2,3,4)—> (2,4,1,3)

and the column permutation

(1,2,3,4)—> (3,1,2,4).

6. Suppose that we have a computer that can test 2^{40} keys each second.

a. What is the expected time (in years) to find a key by exhaustive search if the keyspace is of size 2^{88}?

b. What is the expected time (in years) to find a key by exhaustive search if the keyspace is of size 2^{112}?

c. What is the expected time (in years) to find a key by exhaustive search if the keyspace is of size 2^{256}?

7. Decrypt the ciphertext:

IAUTMOCSMNIMREBOTNELSTRHEREOAEVMWIH

TSEEATMAEOHWHSYCEELTTEOHMUOUFEHTRFT

This message was encrypted with a double transposition (of the type discussed in the LECTURE 2) using a matrix of 7 rows and 10 columns.

Hint: The first word is "there."