Name: Le Dao
CS166-02
Date: Feb 9 2017

Homework 2

Due February 10, 2017

Chapter 2 problems [1 pt each]:
Do numbers **1**,**5**,**6**,**8**,**10**,12,14,19,22,&26.

For problem 12, you may provide your code in Java or C.
Note that problem 12 will help you with problem 10.

The ciphertext for problem 10 is:
MXDXBVTZWVMXNSPBQXLIMSCCSGXSCJXBOVQXCJZMOJZCVCTVWJCZAAXZBCSSCJ
XBQCJZCOJZCNSPOXBXSBTVWJCJZDXGXXMOZQMSCSCJXBOVQXCJZMOJZCNSPJZH
GXXMOSPLHJZDXZAAXZBXHCSCJXTCSGXSCJXBOVQX

The first word of the plaintext is 'never'.

Problem 1

a. Kerckhoffs' Principle in the context of cryptography means that good crypto does not depend on its secrecy. It should be secure even if everything about the system, except the key, is known by the public.
b. Real world violated Kerckhoffs' Principle is writing the password on a note then hide it under the keyboard. If someone manages to find the piece of paper, worst things will happen.
c. Kerckhoffs' Principle in other aspects besides cryptographic definition: security in general, openness provides ductility, according to Bruce Schneier.

Problem 5

Computer tests 2^40 key per second

a. Expected time to find a key by exhaustive search if keyspace if of size 2^88
   892551.30 decades, or **8925512.96 years**
b. Keyspace is 2^112
   1.50 * 10^14 years
c. Keyspace is 2^256
   3.34 * 10^57

Problem 6

The weak ciphers used during the election of 1876 employed a fixed permutation of the words for a given length sentence. To see that this is weak, find the permutation of (1 , 2 , 3 , . . . , 10) that was used to produce the scrambled sentences below, where "San Francisco" is treated as a single word. Note that the same permutation was used for all three sentences.

first try try if you and don't again at succeed
only you you you as believe old are are as
winter was in the I summer ever San Francisco coldest spent

The permutation is **4 9 1 5 7 10 2 6 3 8**

Decoded scripts:
If at first you don’t succeed try and try again
You are only as old as you believe you are
The coldest winter I ever spent was summer in SF

Problem 8

This problem deals with the concepts of confusion and diffusion
a. Define the terms confusion and diffusion as used in cryptography.
Confusion is keeping the plaintext and the ciphertext away from each other. Diffusion is spreading the plaintext statistics through the ciphertext.
b. Which classic cipher discussed in this chapter employs only confusion?
Substitution cipher and one-time pad

c. Which classic cipher discussed in this chapter employs only diffusion?
Double transposition
d. Which cipher discussed in this chapter employs both confusion and diffusion?
Block cipher

Problem 10
MXDXBVTZWVMXNSPBQXLIMSCCSGXSCJXBOVQXCJZMOJZCVCTVWJCZAAXZBCSSCJ
XBQCJZCOJZCNSPOXBXSBTVWJCJZDXGXXMOZQMSCSCJXBOVQXCJZMOJZCNSPJZH
GXXMOSPLHJZDXZAAXZBXHCSCJXTCSGXSCJXBOVQX

NEVER IMAGINE YOURSELF NOT TO BE OTHERWISE THAN WHAT IT MIGHT APPEAR TO OTHERS THAT WHAT YOU WERE OR MIGHT HAVE BEEN WAS NOT OTHERWISE THAN WHAT YOU HAD BEEN WOULD HAVE APPEARED TO THEM TO BE OTHERWISE