Assignment 2

1. **Edgar Allan Poe’s 1843 short story, “The Gold Bug,” features a cryptanalytic attack.**
   1. What type of cipher is broken and how?

The cipher that was broken was a simple substitution cipher and it is broken by using letter frequency.

* 1. What Happens as a result of this cryptanalytic success?

This cryptanalytic success led Legrand to find the location of the hidden treasure.

1. **Suppose that we have a computer that can test 240 keys each second.**
   1. What is the expected time (in years) to find a key by exhaustive search if the keyspace is of size 288?

The expected time to find a key by exhaustive search is 288/240 seconds, which equals to around 8925513 years (8.926 million years).

* 1. What is the expected time (in years) to find a key by exhaustive search if the keyspace is of size 2112?

The expected time to find a key by exhaustive search is 2112/240 seconds, which equals to around 149745258842898 years (149.7 trillion years).

* 1. What is the expected time (in years) to find a key by exhaustive search if the keyspace is of size 2256?

The expected time to find a key by exhaustive search is 2256/240 seconds, which equals to around 3.339 x 1057 Years.

1. **This problem deals with the concepts of confusion and diffusion.**
   1. Define the terms confusion and diffusion as used in crytography

Confusion is when a cipher tries to hide relation between the plaintext and the ciphertext.

Diffusion is when a cipher tries to spread the statistics of a plaintext through the whole ciphertext.

* 1. Which classic cipher discussed in this chapter employs only confusion?

The One-Time Pad and the Simple substitution cipher are example of ciphers that only employs confusion.

* 1. Which classic cipher discussed in this chapter employs only diffusion?

Double transposition cipher is the example of a cipher that only employs diffusion.

* 1. Which cipher discussed in this chapter employs both confusion and diffusion?

The codebook cipher is an example of a cipher that employs both confusion and diffusion.

1. **Recover the plaintext and key for the simple substitution example that appears in (2.2) on page 24.**

THE TIME HAS COME THE WALRUS SAID TO TALK OF MANY THINGS OF SHOES AND SHIPS AND SEALING WAX OF CABBAGES AND KINGS AND WHY THE SEA IS BOILING HOT AND WHETHER PIGS HAVE WINGS BUT WAIT A BIT THE OYSTERS CRIED BEFORE WE HAVE OUR CHAT FOR SOME OF US ARE OUT OF BREATH AND ALL OF US ARE FAT NO HURRY SAID THE CARPENTER THEY THANKED HIM MUCH FOR THAT A LOAF OF BREAD THE WALRUS SAID IS WHAT WE CHIEFLY NEED PEPPER AND VINEGAR BESIDES ARE VERY GOOD INDEED NOW IF YOURE READY OYSTERS DEAR WE CAN BEGIN TO FEED

(proof of the problem solved using the code from problem 12 is in “output.txt”)

1. **Write a program to help an analyst decrypt a simple substitution cipher. Your program should take the ciphertext as input, compute letter frequency counts, and display these for the analyst. The program should then allow the analyst to guess a key and display the result of the corresponding “decryption” with the putative key.**

Program included in hwk.zip, called “SubstitutionCipherDecodeHelper.java”

1. **Decrypt the ciphertext**

**IAUTMOCSMNIMREBOTNELSTRHEREOAEVMWIH**

**TSEEATMAEOHWHSYCEELTTEOHMUOUFEHTRFT**

**This message was encrypted with a double transposition using matrix 7 rows and 10 columns**

IAUTMOCSMN

IMREBOTNEL

STRHEREOAE

VMWIHTSEEA

TMAEOHWHSY

CEELTTEOHM

UOUFEHTRFT

STRHEREOAE

IMREBOTNEL

IAUTMOCSMN

VMWIHTSEEA

TMAEOHWHSY

CEELTTEOHM

UOUFEHTRFT

THEREARESO

METOBERLIN

ATCOMMUNIS

MISTHEWAVE

MEWHOSAYTH

ELETTHEMCO

OFTHEFUTUR

THEREARESO

MEWHOSAYTH

ATCOMMUNIS

MISTHEWAVE

OFTHEFUTUR

ELETTHEMCO

METOBERLIN

THERE ARE SOME WHO SAY THAT COMMUNISM IS THE WAVE OF THE FUTURE LET THEM COME TO BERLIN

1. **Using the letter encodings in Table 2.1, the following ciphertext message was encrypted with a one-time pad:**

**KITLKE**

* 1. If the plaintext is “thrill,” what is the key?

Ciphertext 011 010 111 100 011 000

Plaintext 111 001 101 010 100 100

**Key= C xor P 100 011 010 110 111 100**

* 1. If the plaintext is “tiller,” what is the key?

Ciphertext 011 010 111 100 011 000

Plaintext 111 010 100 100 000 101

**Key= C xor P 100 000 011 000 011 101**

1. **Suppose that the following is an excerpt from the decryption codebook for a classic codebook cipher**

**123 once**

**199 or**

**202 maybe**

**221 twice**

**233 time**

**332 upon**

**451 a**

**Decrypt the following ciphertext**

**242, 554, 650, 464, 532, 749, 567**

**Assuming that the following additive sequence was used to encrypt the message**

**119, 222, 199, 231, 333, 547, 346**

242 – 119 = 123 once

554 – 222 = 332 upon

650 – 199 = 451 a

464 – 231 = 233 time

532 – 333 = 199 or

749 – 547 = 202 maybe

567 – 346 = 221 twice

**once upon a time or maybe twice**

1. **In this chapter, we discussed a forward search attack.**
   1. Explain how to conduct a forward search attack.

To conduct a forward search attack, we are required to guess the whole plaintext and encrypt it with the public key and then compare it with the ciphertext that we intercepted, if it is the same, then we have found the plaintext, if not, then we just have to keep guessing.

* 1. How can you prevent a forward search attack against a public key cryptosystem?

To prevent a forward search attack against a public key cryptosystem, we have to ensure that the size of the plaintext is large enough so that the attacker cannot simply encrypt all possible plaintext messages.

* 1. Why can’t a forward search attack be used to break symmetric cipher?

Because a public key can only be used to encrypt plaintext and cannot be used to decrypt, in the case of symmetric cipher, the key is used to encrypt and decrypt. In forward search attack it requires you to have a key to encrypt, but in a symmetric cipher we don’t know the key, else we wouldn’t need to guess what the plaintext is, because we can use the symmetric key to decrypt the ciphertext.

1. **Suppose that a particular cipher uses a 40-bit key and the cipher is secure.**
2. How much work, on average, is an exhaustive search attack?

For a 40 bit key, there are 240 different keys and the average is half of it. Which is 240 /2 = **239**

**It requires on average to try 239 keys in order to break the cipher**

1. Outline an attack, assuming that known plaintext is available.

By doing a known plaintext attack, we can try to decipher the ciphertext by finding the relation between the known plaintext and the ciphertext, and find what kind of cipher method was used and partially find out the key of the ciphertext.

1. How would you attack this cipher in the ciphertext-only case?

To attack this cipher in the ciphertext-only case, we would need to do an exhaustive search attack, because other than the algorithm and ciphertext we don’t know any other information.