

Linnaeus University

1DV700 - Computer Security

Assignment 1

Student: Evan Huynh

Personal number: 970330-4130

Student ID: eh223im@student.lnu.se



Setup Premises

Explain your setup such as, OS, web browser, tools being used, development environment, and whatever else is necessary…

OS: OS X 10.13 on MBP mid 2012

IDE: IntelliJ IDEA 2019.3

Java version: 13

Web browser: Google Chrome (ver 79 as the time of writing)

Specific tool used:

All specific tools will be mentioned in the

# Task 1

1. The first task is to investigate different terms within cryptography and related areas.
   1. Different between pairs of methods:

Symmetric encryption: Alice wants to send Bob the message P. She encrypts the message using key K which results . If Bob wants to read P, he has to decrypt using the decryption process which results We can see that the same key is used to lock and unlock message. The algorithm to obtain the plaintext is because Decryption and Encryption are the mirror image of the process using the same key K. [1]

Advantages: Using the same key K both to encrypt and decrypt, the algorithm is faster since only one shared key is used.

Disadvantages: If the key K is lost then all the messages are available to the attackers. The transmission of key K which can be both hard and dangerous, due to physical constrain or the communication method.

Asymmetric encryption: different keys are used to encrypt and decrypt the message. The process can be described using [1]. This means that the encryption uses key and the decryption process use key , which is totally different than each other.

For example, Alice wants to send Bob the message

Advantages:

Disadvantages:

Encryption algorithms:

Hash algorithms:

Compression:

Hashing:

# Task 2

1. Steganography
   1. According to the website, they used the classical technique of hiding the image within image using the least significant bit to achieve it.

Limitation: the hidden image quality is losses due to loss of information. Storing picture within pictures will results the recovered image quality is loss since there are not enough information that could be recovered from the steganographed file.

Also, if the message is too large, the original picture quality might be modified too much that the attacker can notice something wrong with it. For example, hiding 7 bits in the original image might results the low-quality exported image, which indicates something is wrong with the data being sent.

* 1. A
  2. Since the image is mostly black and white, those white regions are represented in 00 bit. However, I noticed there are a lot of irregularity starting from bit #54 (reference to my Java program). In this image, most of the black pixels are represented by FE, however there are some that are represented by FF which caught my attention. Most of the black are represented by FE, throughout the rest of the file.  
     By running this program, I was able to extract specific region that contain the message. The algorithm was pretty simple, take the bit number, convert to integer and take the modulus 2. If it is even, that bit has a 0 hidden in the LSB, otherwise 1.  
     The rest of the program is just for decorating and house-keeping purpose. I just simply split the string every 8th bit and convert binary string to ASCII.

The final message is “Congratulation!”

# Task 3

1. Message decryption
   1. With pen and paper: “encrypted message”.
   2. It could be decrypted without the key. Since this is a monoalphabetic cipher, it could be decrypted with ease. Although frequency analysis of single character might not work 100%, there are also some more popular bigrams (th, he, …), trigrams (the, and, …), not to mention double letters (ss, ee, ll, …) in English.

Knowing that the

# Task 4

# Task 5

1. Encrypted file

In this task I added the soliloquy by Prince Hamlet in act 3, scene 1 of William Shakespeare’s play Hamlet, mostly known as “To be or not to be”. This file is encrypted using my substitution method with the key ‘123’ and uploaded in my name. Below are the images showing what the file should looks like on my machine before and after encrypting it.

Of course, the encrypted file does contain some special characters and non-printable characters as well.

|  |  |
| --- | --- |
| Original | Encrypted |
|  |  |

# Task 6

1. Cryptanalysis

# Task 7

1. Hash function

In this task

# Bibliography

|  |  |
| --- | --- |
| [1] | C. P. Pfleeger, Security in Computing. |

Bibliography

[1]

[2]

[3]