

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:

Task

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: same key is used to lock and unlock message.

Advantages:

Disadvantages:

Assymetric encryption: different keys are used to encrypt and decrypt the message

Advantages:

Disadvantages:

Encryption algorithms:

Advantages:

Disadvantages:

Hash algorithms:

Advantages:

Disadvantages:

Compression:

Advantages:

Disadvantages:

Hashing:

Advantages:

Disadvantages:

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. The type of

Limitation: the hidden image quality is losses due to loss of information. 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.

* 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. 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 (ll, ss, …) in English.

Knowing that the

Task 4

1. A

Task 5

1. A

Task 6

Task 7

Bibliography

[1]

[2]

[3]