Assignment 1

Encryption
Practical work #1

February 7, 2016

Author: Sarpreet Singh Buttar
Supervisor: Ola Flygt
Semester: VT 2016
Course: Computer Security, 1DV700

Contents

1 Introduction

The report gives information about the different methods used in cryptography. It begins with the differnces in some well known methods such as symmetric and asymmetric encryption. Furthermore, it covers some other methods including their pupose and usage. The report also consits of some practical tasks[1] such as hidden messages and encryption using a key. At last, it shows the personal experince while encrypting other's cipher text files as well as using the hash function.

2 Differences between Symmetric and Asymmetric encryption

Following are the key differences between Symmetric and Asymmetric encyrption in terms of cryptography:

2.1 Symmetric encryption

In symmetric encryption, both parties *(sender and receiver)* use a single key to perform encryption and decryption, also known as private/secret or single key cryptography. Both parties are at the same position in symmetric encryption. Due to the single key, algorithms are not complex which causes them to run extremely fast and become easier to implement in hardware. All the participants in the encryption must be configured before, by using the secret key. If the key is exposed under any circumstances, communiction will be compromised or negotiated. DES, RC4 and AES are the names of algorithms which are commonly used in symmetric encryption. The mathematical notation for symmetric encryption is P = D(K, E(K,P)) where P stands for plaintext (original text), D for decrypted text, E for encrypted text and key is denoted by K.

2.2 Asymmetric encryption

In asymmetric encryption, both parties *(sender and receiver)* uses two seperate keys *(the public key and the private key)* to perform encryption and decryption, thus both parties are not equal. The public key is available to everyone to encrypt the message, but only authorized persons can access the private key and decrypt the message. Compared to symmetric encryption, algorithms are much more complex which demands high computational work, therefore they work quite slow. Building a secure connection over an inesecure medium such as the internet is the major advantage of asymmetric encryption. RSA is the most common algorithm in asymmetric encryption. The mathematical notation for asymmetric encryption is $P = D(K_D, E(K_E, P))$ where K_D denotes to decryption key and K_E denotes to encryption key.

[1] Excercise 4 can be found in the zip file and excercise 5 is uploaded with name "SarpreetSinghButtar.substitution".

3 Differences between Encryption and Hash algorithms

The key difference between both algorithms is that messages encrypted by encryption algorithms can be reversed back to the original form by using the special key, whereas it is almost imossible to reverse a hash back to its original string form. Hash algorithms such as MD5 and SHA are most commonly used to generate a fixed length string or number from a string of text to increase the integrity of the data. Hashing is very helpful to secure the data such as the last digits of a credit card or a password because hashes are genetically one way, if any minor change occurs in the input it makes a significant change in the output whick makes harder for the crypanalyst to steal the data. On the other hand, encryption algorithms such as AES and PGP are more helpful than hashing algorithms for sending secure messages in the form of cipher - text which can be decrypted by using the special key. Sometimes, encryption can be used over hashing when some part of the file or data is not neccesary for the receiver to know.

4 Differences between Compression and Hashing

Following are the key differences between Compression and Hashing in terms of cryptography:

4.1 Compression

Compression is a process which combines the length of two data files and produces a single output which is the same size as one of the input files. The compression can be performed in different forms such as lossless *(Output is exactly same as orginal contents of file)* and lossy *(data can be lost)*. There is no security in data compression unless the file is first compressed and later encrypted. This form of encryption is very difficult to break. Compression can be measured by the following notataion:

$$\text{Compression Factor} = (1 - (\frac{CompressedSize}{UncompressedSize})) * 100$$

4.2 Hashing

Hashing is a process which produces a fixed length of string or number of input file. It produces binary numbers which are almost impossible to revert for getting the original content of file. Hash always provides better security even without combining it with encryption. In mathematica, hash function looks like

$$f : A \rightarrow B \text{ where } |A| > |B|$$

So, the key difference is that if compression is performed alone, data might be stolen or lost or damaged *(especially photos and videos)* whereas if hashing is performed with strong algorithims, it can never be decrypted. Furthermore, compressed files can be decrypted successfully *(depends on compression factors)*, but hashing cannot.

5 Differences between Steganography, Encryption and Digital Watermarking

Steganography is a process of hiding data or files within another file, such as an image. Encryption is a process of converting original data *(plain-text)* into unreadable text format *(cipher-text)*, to protect it from human interaction. Digital watermarking, on the other hand, is a process of inserting digital information *(signature, which can be vsible or invisible)* in to digital files such as images or signals. It is often used to verify the owner's identity and authentication. The key difference between these methods is that steganography is hard to indetify with the naked eye whereas encryption is always visible, and watermarking can be both.

5.1 Purpose and usage of Steganography

Hiding a message in such a unique way that is not visible with the naked eye is the pupose behind the steganography. It can be used in linguistic or technical ways. In linguistic steganography, the message is hidden within the other text and in technical, the message is hidden in the digital files such as an image.

5.2 Purpose and usage of Encryption

Converting a meaningfull message into unmeaningful words is the purpose behind the encryption. The encryption is used with the help of algorithms and in symmetric or asymmetric methods. However, encryption can also be used with other types of cryptography methods such as steganography, hash function and compression which helps to increase the security of the message.

5.3 Purpose and usage of Digital Watermarking

Inserting logos or seals on digital mediums which represents the legal ownership of organization or a person, also known as copyright, is the purpose behind digital watermarking. It is often used to extend the information on digital products for preventing false ownership.

6 Hidden message in the text

The hidden message is *George your package ready by friday the 21st room three. Please destroy this immediately.*

7 Decrypted message and motivation

The decrypted message is *"encrypted message"*. No, it will not be easy to decrypt without key because the position of the letters is not in a particular order, and it's difficult to find their position without a key. It does not matter even if letter 'H' appeared three times in the cipher - text and its value is just 3 letter before, because I tried to write all the letters in substitution method +3 and -3, its still hard to find the original content.

8 How I encrypted some cipher - text files

I downloaded, some files from MyMoodle and tried to decrypted them. I managed to decrypt two files succesfully with my own java program. Both files used substitution encryption. The text in first file was shifted 5 letters forward. I input different key number and found it easily. Following is the decrypted text:
"COMPUTER SECURITY IS SECURITY APPLIED TO COMPUTING DEVICES SUCH AS COMPUTERS AND SMARTPHONES, AS WELL AS COMPUTER NETWORKS SUCH AS PRIVATE AND PUBLIC NETWORKS, INCLUDING THE WHOLE INTERNET. THE FIELD COVERS ALL THE PROCESSES AND MECHANISMS BY WHICH DIGITAL EQUIPMENT, INFORMATION AND SERVICES ARE PROTECTED FROM UNINTENDED OR UNAUTHORIZED ACCESS, CHANGE OR DESTRUCTION, AND IS OF GROWING IMPORTANCE DUE TO THE INCREASING RELIANCE OF COMPUTER SYSTEMS IN MOST SOCIETIES. BY LI CHUNG HEI".
The other file takes bit more time because I never expected that we can exchange the letters with 17 letters behind the original letter. I thought as it is mentioned in the question that we must set the maximun size upto eight bits $2^8 = 256$. So, I was expecting with range of 4. At last I run the for loop on some files and decrypted the another file. Below is the text:
"WE DID THE THE ASSIGNMENT IN ONLY 2 DAYS. IT WAS HARD ESPECIALLY THE THIRD QUESTION. THE SECRET KEY IS SEVENTEEN. YASSER ALMODHI,MOHAMMED ALMNAEA."

9 How hash function works

I solved this exercise with the help of hexadecimal table. First write all the hexadecimal value of given input

unsigned int hash = 0xDECAFBAD

According to hexa tabel:

D = 13
E = 14
C = 12
A = 10
F = 15
B = 11
A = 10
D = 13

Above values in the binary form (base 2)

Eg: D (13) = 1101 ($1*2^3+1*2^2+0*2^1+1*2^0=13$)
E (14) = 1110
C (12) = 1100
A (10) = 1010
F (15) = 1111
B (11) = 1011
A (10) = 1010
D (13) = 1101

Now write the binary number all together

$$11011110110010101111101110101101 \tag{1}$$

Shift the (1) binary number 5 bits to the left

$$11011110110010101111101110101101 00000 \tag{2}$$

Also, Shift the (1) binary number 27 bits to the right

$$1101111011 \tag{3}$$

Now, Perform XOR operation between (2) and (3). We also must include the XOR of msg[i] which meas the value of msg[ ] array at postion. But in this case we do not know the value of msg[ ] array, we skip it. In XOR method, if the number is 0,1 it chnages to 1, if 0,0 it remains 0 and 1,1 also changes to 0. Below is the solution:

$$11011110110010101111101110100110110 11 \tag{4}$$

0x7FFFFFFF is the another equation in the exercise. Accordind to the hexa value of 7 = 7 and F = 15. In the binary form 7 = 0111 and F = 1111. Below is the binary eqaution of this:

$$01111111111111111111111111111111 \tag{5}$$

The binary number which starts from 0 is negative number. In AND operation if both values are same then output remains same and if one of the number is different from other then its always 0. Now perform AND operation between (4) and (5):

$$00000101110010101111101110100110101 1 \tag{6}$$

(6) is the new binary number after all the operation.

9.1 Motivation

According to my opinion, this is not a good cryptographic hash function because a good hash function is expected to generate the same output as given input value. Moreover, good hash function mostly provides same fixed size output. And this hash function has provided different size of output.