Linnéuniversitetet
Kalmar Växjö

Linnaeus University

1DV700 - Computer Security
Assignment 1

Student: Zejian Wang
Personal number: 19900227T691
Student ID: zw222bb@student.lnu.se

Linnéuniversitetet
Kalmar Växjö

Faculty of Te
Department

Setup Premises

Windows 10, Chrome web browser, Python in VSC, Matplotlib are used.

Task 1

a) Symmetric encryption – Asymmetric encryption:

The speed of symmetric encryption is fast, while the speed of asymmetric encryption is slow; symmetric encryption: one key for encryption and decryption, the key is secret, Asymmetric encryption: one key for encryption, a different key for decryption, one of the keys is public, the other one is secret; The symmetric key size is not more than 256 bits, whereas asymmetric key size is unlimited, typically no less than 256; It is much more difficult to manage symmetric keys than to manage asymmetric keys. [1]

Encryption algorithms – Hash algorithms:

Encryption algorithms is a function of encoding plaintext as cyphertext, which can be decrypted with a correct key. However, the hash algorithm is a one-way encryption process and a hash value cannot be reversely processed to get to the plaintext. [2]

Compression – Hashing

Hashing is scrambling data and convert it into a numerical value, and no matter how long the input is, the output value is always of the same length. However, compression is the process of reducing bits by identifying and eliminating statistical redundancy, and the compression process can be reversed as decompression while hashing cannot be reversed. [3]

b)

The information is hided within an ordinary file or message in using steganography, the information can be encrypted or not, the communication is covert, while in encryption, the information is converted into a secret code that only particular people or organisation can read it using key and the communication may not covert, however, the information in a digital media with digital watermarking is readable. The purpose of steganography is to transmit information when do not want the third party to know the existence the communication. The purpose of encryption is to intend to make a message unreadable by a third party when transmitting some confidential information. The digital watermarking is used to verify the credibility of the content or to recognize the identity of the digital content's owner. [4]

Task 2

a) From the table of plain and cipher, the message can be decrypted, the message is “HKPUFCMHY BHDDXZH”, and each letter in the message is corresponding to “encrypted message” from the plain line, hence, the message is decrypted.

b) Decrypt the message（ QMJ BPZ B XPJZ RZWJPAXQ LAD ）without a key using brutal force.

First look at the three characters “QMJ” and “BPZ”, google most frequently used English words with 3 letters “the, and, are, for, not, but, had, has, was, all, any, one, man, out, you ”, a combination of two words among them that make sense maybe be “you are”, try “you are”, and we get the corresponding key are “QMJ BPZ”, then we can get that the message is “you are a Xrue ReWurAty LAD”, then we can find “Xrue” could be “true”, so the message now is “you are a true ReWurAty LAD”, then google 8 letter words ending in “ty” and “ur” in the middle, we can find “security”, now the message is “you are a security LiD”, and we can find that the last word “LiD”, “LD” are among the letters that are not been used(“dghjklmnpqvwxz”), and combined with googling 3 words with middle letter “i”, we can find that “LiD” is “wiz”, so the decrypted message is “you are a true security wiz”.

c) We can see from above that it is much more time consuming without a key when decrypting a message, we use brutal force to do the decryption, just try every possible letter or letter combinations to see whether it makes sense. The process is time-consuming and boring, so the motivation to do it is much more important, like I do this, the motivation for me is to finish the assignment, or else, I would not spend time on this.

Task 3

Use Caesar method for the substitution encryption, each character is substituted by another character using a formula (eg: chr((ord(c) + key-65) % 26 + 65)), the key is the number of moves of letters forward in the alphabet, Ascii is used, then each encrypted letter is added in an empty string, the cipher text is done. Decryption is almost the same formula, the only difference between those two formulas is the key for decryption is the number of moves of letter backward in the alphabet. Then each decrypted letter is added in an empty string, then is the decrypted text.

Use columnar method for transposition. Make a table, number of columns is the key (which is converted to an integer in the program), each letter in the plaintext is added to each bucket in the table row by row, and then fill each empty buckets in the last row with symbol that different from the plaintext. Then add each letter in the table to an empty string column by column (using for loop and index), then is the ciphertext. Decryption is almost the same algorithms, the difference is the number of columns is the result of the formula (ceil (length of text // key))(key is converted to an integer), which, the key is the same as used in the encryption, add each character in the ciphertext to the table row by row, fill each empty buckets in the last row with symbol that is different from the plaintext, then add each letter in the table to an empty string column by column, then remove the symbols that are added, then the text is the plaintext.

Create a function to read text from a text path and a function to output text to a path. Ask users for which encryption method will be used and a key, the program would execute the encryption process and output the encrypted text, then it will ask users for which decryption method (corresponding to the encryption method) will be used and the corresponding key that is the same as the encryption, the program would execute the decryption process and output the decrypted text to a path that has been created already.

Task 4

The file with secret message has been created, I use the substitution method to encrypt the file, processing it with the program of Task 3, the file is the output text, the key used is “k”, the file with my name has been uploaded.

Task 5

I have successfully decrypted one file (Zaid Abudal Khadam.txt) using the substitution program I created. At the top of the page, 'FRPERG ZRFFNTR' obviously is the 'Secret message', then I use a part of the program of substitution encryption I created in Task3 to decrypt it using key (a number not a letter) 1,2,3, …, then after try 12 times, the number 13 is the key to decrypt the 'FRPERG' as 'secret', then use the key to decrypt the whole file. The decrypted message is: "THE MOST THING IN YOUR LIFE YOU HAVE TO FIGHT YOUR DREAM TO REACH TO YOUR AIM AND THERE IS NOTHING EASY TO REACH IT FAST, A PERSON HAS TO SEEK HIS GOOL THROUGH OUT HIS PATIENCE."

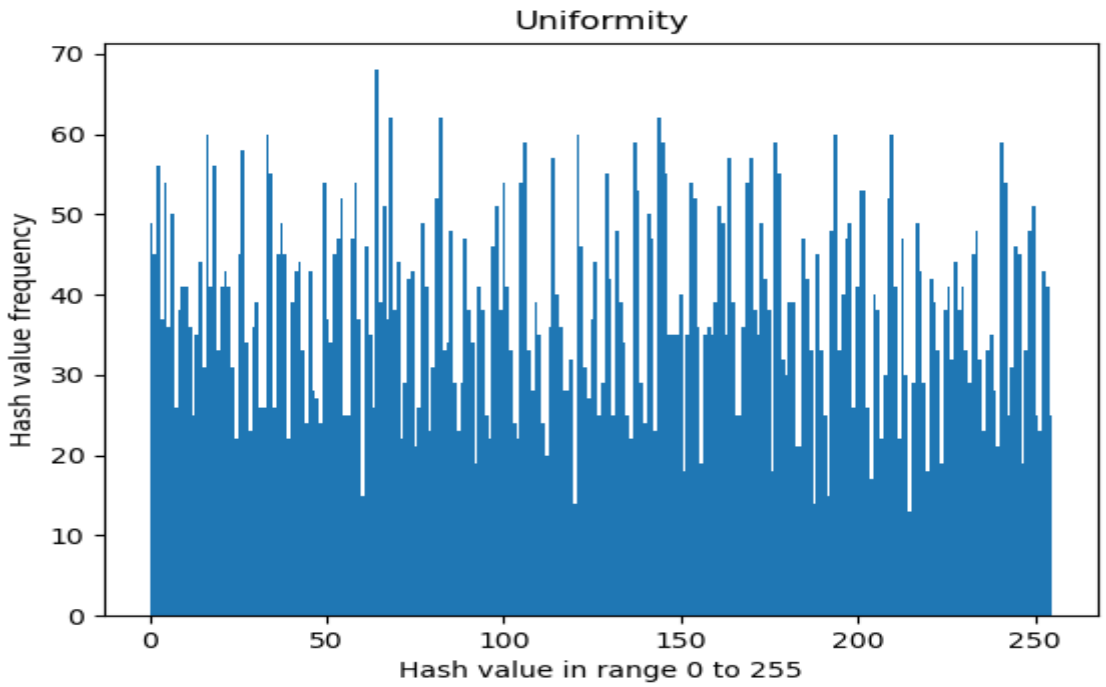
Another file I decrypted is Ahmad_nofal.txt, using the same method and process as I did above, the key is 23, and the decrypted message is: "I am Ahmad Nofal I like swimming, and reading. I studied Network design in Halmstad School, I have two brothers, I live with my family. I have friends from almost the whole world .best regards

For some file for example MitchellSandberg.txt, It is difficult to recognize what method he or she used to encrypt the message, without the key or the algorithms used, I cannot read this encrypted message.

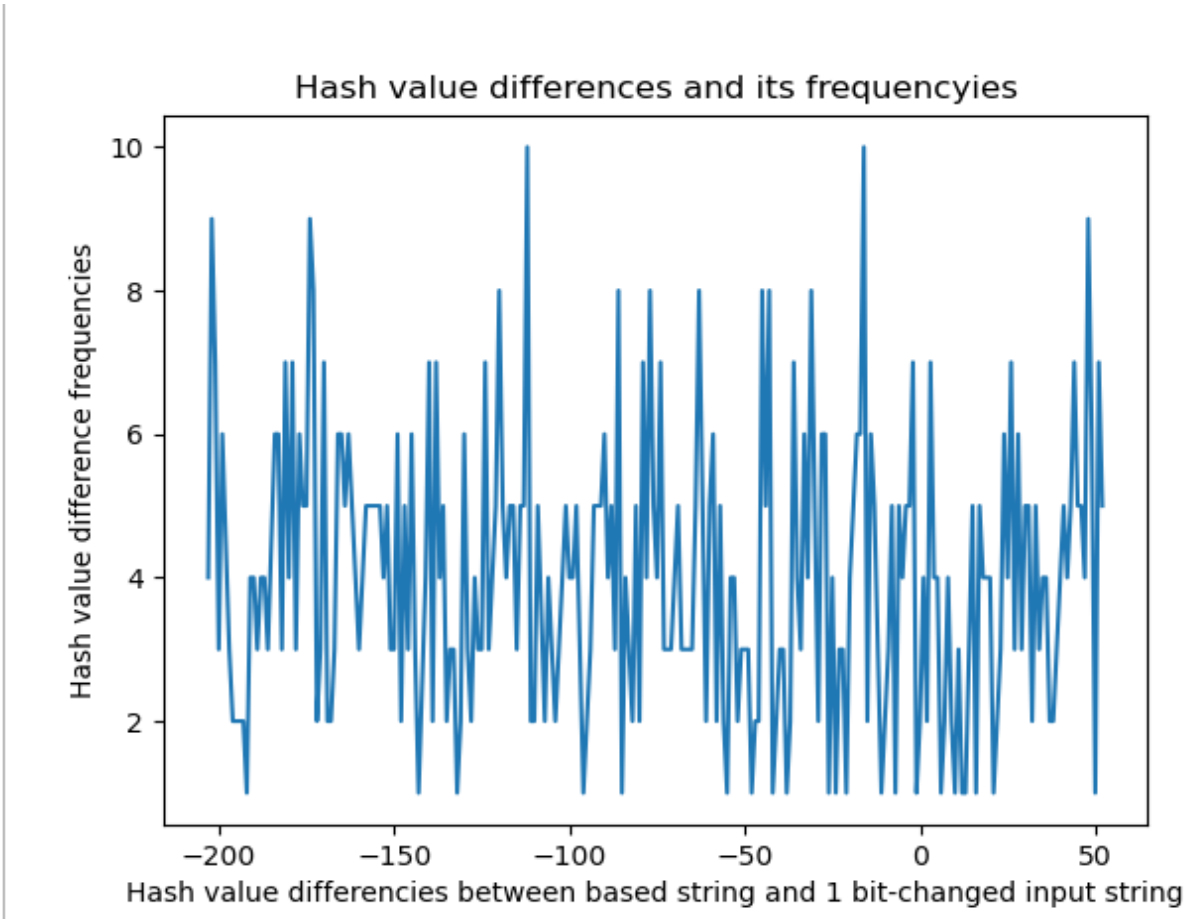
Task 6

a) The hash function I made is very simple, for every element in the input string, computing the value of each element using formula: randint(0, ord(e))**2, sum up all the value of each element and then modulo 256, the hash value generated is within the range of 0 to 255.

b) In order to test the first property, at least a couple of thousand test strings will be tested, the file holygrail.txt is used. In the program, a list is created containing all the strings in the file, all the strings are used to compute the hash function. Thousands of hash values are included in the list. A dictionary with the key for hash value and value of frequency is created, and then we use matplotlib to show the uniformity of the hash function. As the graph showed below, the uniformity of this hash function is not performed very well.



To test the second property, a program has been created that input strings that are very similar (only differ in 1 bit). The based string is 'Unanswered question', a string are slightly different (1 bit) from the based string, then a random letter is chosen and change the letter to binary bits, and then randomly select one of the binary bits and change it to 0 or 1 that is different from original bit. The new binary bits are made and then convert it to a symbol using Ascii, and then replace the original letter with the new symbol, that's how the one bit is changed. Then use the hash function, compute the hash value. A dictionary is created, and the difference between the new string and the old one is the key for the dictionary, and the value for the dictionary is the frequency of the difference. 1000 times(1000 1-bit different strings) to test the second property of the function is showed below, it showed that the hash function's second property is not performed very well.



c)The difference between normal hash functions and secure hash functions is that collisions hardly occur when using secure hash functions while normal hash functions does. My hash function is not a secure hash function, because the range of hash value is narrow, causing a lot of collisions, that's why my hash function is not secure. [5]

Bibliography

[1] Charles P.Pfleeger, "Toolbox: Authentication, Access Control, and Cryptography" in *Security in computing*, fifth ed. pp104
[2] ClickSSL, "Hashing vs Encryption–What Are the Difference?", [2021-06-20], url:[https://www.clickssl.net/blog/difference-between-hashing-vs-encryption]
[3] "Data compression", url: [https://en.wikipedia.org/wiki/Data_compression]s
[4] "Digital Watermarking", url: [https://www.techopedia.com/definition/24927/digital-watermarking]
[5] "What is the difference between a Hash Function and a Cryptographic Hash Function?", url:[https://security.stackexchange.com/questions/11839/what-is-the-difference-between-a-hash-function-and-a-cryptographic-hash-function]