Linnéuniversitetet
Kalmar Växjö

Linnaeus University

1DV700 - Computer Security
Assignment 1

Student: Mario Guerra Pérez
Personal number: 02097-
Student ID: mg224in@student.lnu.se

Setup Premises

OS used: linux subsystem in windows (WSL).
Web Browser: OperaGX
Development environment: Visual Studio Code
Extra information: In exercise 3, you will need to introduce the document to encrypt or decrypt by shell.

Task 1

A)

a. On one hand, symmetric encryption just uses a secret key to cipher and decipher information so it's fast in the moment of execution. For this reason, it's used to send big data amounts, besides that the size of the cipher text is the same or smaller than the original plain text. However, it has some problems, as, for example, it isn't scalable, given that it isn't suitable for various users. Also, it just provides confidentiality, given that any user could use the key if it has it.
On the other hand, asymmetric encryption works with 2 keys: one public key that it's available for anyone who wants to send a message, and a private key that is private for each user. For any message encrypted with a public key, to decrypt it is necessary to use a private key. However, for any message encrypted with a private key, it's just necessary to use a public key to decrypt it. This complexity of using 2 keys makes the process is slower than the symmetric encryption, so it's used to send small messages. However, unlike symmetric encryption, thanks to the use of 2 keys, this method provides in addition to confidentiality, authenticity, and non-repudiation. [1][2]

b. An encryption algorithm is a 2-way process in which plane text is modified through an algorithm and a key, so it's reversible. It's important to highlight that the size of the output produced has a variable length given that each part of the text is changed for another. They are used primarily to maintain data confidentiality during transmission and storage.
On the other hand, the hash algorithm is a 1-way process in which any data is turned into a fixed-size hash value using a hash algorithm. This size is always the same, it doesn´t matter the size of the input. However, it isn't reversible compared with the encryption algorithm given that the size of the output is always the same, so it isn't impossible to make differences to recover the original value. For this reason, hash algorithms are used to verify data integrity. [3][4][5][6]

c. On one hand, data compression is the process of reducing the size of a file with the goal of having more efficient storage and transmissions through the internet and networks. There are two types of compression. The first one compresses files by removing data from the proper file. The second one reduces the size without losing information.
On the other hand, in cryptography, compression is used to transform the data to something that is difficult to reverse this transformation. A hash function does this basically, processing an arbitrary-length message into a fixed-length output which is difficult to return to its original form. [7][8]

B) Steganography, on the one hand, is the technique to hide information, especially used with texts, images, videos…, and other kinds of files without making any visual change in the original file and the file with the embedded. It's often mixed with cryptography, so this combination means that only the recipients can recover the original files.
On the other hand, encryption is the process of converting plaintext into ciphertext using an encryption key. This text can be only decrypted by the receptor using the same key. It turns sensitive information into an unreadable format, unlike steganography which visually, the file doesn't change.
Finally, digital watermarking is the process of inserting information into a digital element, like an image, video, or audio file with the aim of protecting the copyright and intellectual property rights of the content creator. They are the watermarks that are sometimes in different images, for example.

In conclusion, stenography hides information without changing the elements, encryption changes the proper element to something unreadable, and digital watermarking helps to protect copyright and intellectual property rights. [9][10][11]

Task 3

A. The result of decrypting the message is HELLOCHATGPT HOWAREYOU.

Task 4

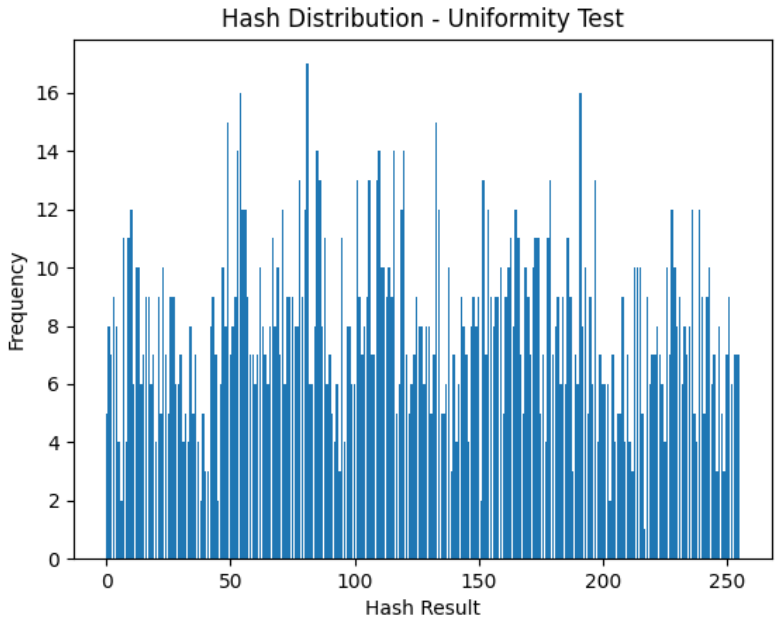
In this exercise, it was requested the implementation of 2 encrypt and decrypt functions: one with substitution method and another with transposition method. The code implementation in the substitution method was to take the key that the user gives, summarize the ASCII value it has, and make the module 255 (size of ASCII table). Once we have this value, we just have to take the text and take every digit summarize the value of the digit plus the value of the key, and then, return the digit. The decryption was the opposite operation.
On the other hand, the transposition method consisted of taking the text and dividing it in a matrix with the size of the key columns (that means if the key is 135462, there will be 6 columns). After that, we take every column and put it in the position they key gave. For example, if the key is 135462, the first column will be moved to the first position, and the third column will be moved to the second position… The decrypt is made the opposite operation. The principal problem was to divide these columns and manipulate them, so it was necessary to use a dictionary.

Task 5

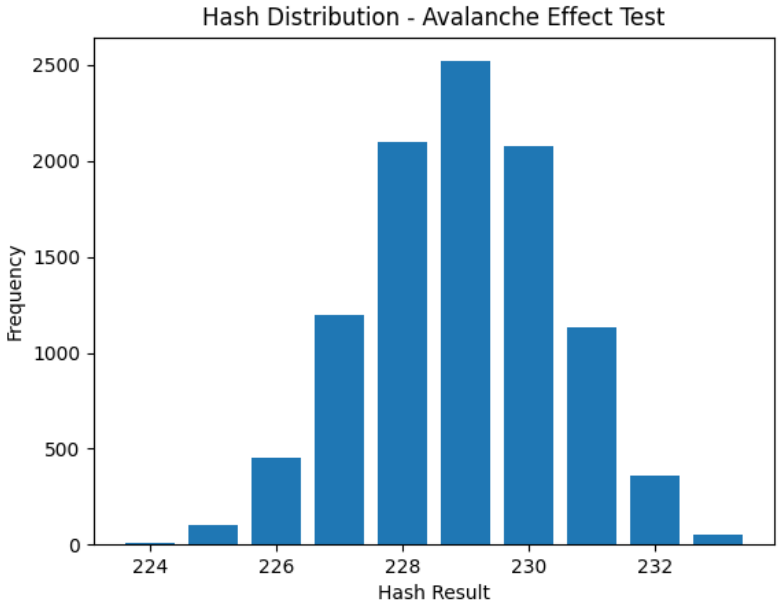
A. In this task, is required to decrypt a text given by another person. In my case, the files were encrypted with the substitution encryption method, so I just had to modify a bit substitution decrypt method, which consisted of adding a method that tries all the values of the ASCII table and as the begins of the files are all the same, when the first 7 lines of the text to decrypt (7 because are the lines that are common for every file) are the same than the original one, the text is already decrypted, given that any key is given.

Task 6

B. Once the tests are done, let's analyze the results. From one side, we have the results of the Uniformity Test, which shows that the frequencies are showing some variations (the mean frequency is 7.8125), which means that the hash values are not correctly distributed. Besides, the variance and the standard deviation are high (10,1132 and 3,18 respectively), given that they reiterate that the distribution is not perfectly uniform.



On the other side, in the Avalanche Effect Test (which basically are test with small changes), the frequencies show a trend, where some values appear much more than others. This means that small changes in the input make hash values not uniformly distributed. The variance and standard deviation have high values also, reinforcing that small changes in the input generate hash values with varied frequencies.



In conclusion and to summarize, on one hand, the Uniformity Test indicates that the hash function is not uniform given that there are some values that appear more frequently than others, and, on the other hand, the Avalanche Effect Test indicates that small changes result in hash values that are not uniform distributed, given that this distribution shows a clear pattern, which is not ideal for a good hash function.

C. The principal difference is the security properties they provide, given that the secure hash function (also called cryptographic hash function) has some security function as collision

resistance, which means that in this hash function is difficult to find two input values that produce the same output hash; and pre-image resistance, which means that in this function should be difficult to find the input value giving the output value, among others examples.

The easiest way to prove this difference is with these security properties: the collision resistance and the pre-image resistance. It's important to highlight that there are other security properties that can be used to prove this, for example, the one-way functions, which is similar to pre-image resistance given that it consists in that the secure hash function must be difficult to reverse; and the avalanche effect, which means that even a small change in the input should completely change the output value of the function.
Testing a hash function with these properties can determine if a hash function is secure or not. [12][13]

Bibliography

[1] SSL Information, ” Symmetric vs. Asymmetric Encryption – What are differences?”, [2015-2-22], url: [https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences].
[2] gluttony777 & geeksforgeeks, “Difference Between Symmetric and Asymmetric Key Encryption” [2023-05-22] , url: [https://www.geeksforgeeks.org/difference-between-symmetric-and-asymmetric-key-encryption/]
[3] encryptionconsulting, “What is difference between Encryption and Hashing? Is Hashing more secure than Encryption?” [2020-11-20], url: “https://www.encryptionconsulting.com/education-center/encryption-vs-hashing/”
[4] Patrick Nohe, “The difference between Encryption, Hashing and Salting” [2018-12-19], url: “https://www.thesslstore.com/blog/difference-encryption-hashing-salting/”
[5] Margaret Rouse, “Encryption Algorithm” [2023-09-4], url: “https://www.techopedia.com/definition/1778/encryption-algorithm”
[6] Deepak Mishra, “Why are Hash Functions Irreversible?” [2019-07-24], url: “https://metamug.com/article/security/cryptographic-hash-irreversible-collision-free.html”
[7] Shannon -JJ Behrens, “Hashing, Encryption, Encoding, Compression, Oh My!” [2020-09-26], url:“ https://www.javacodegeeks.com/2020/09/hashing-encryption-encoding-compression-oh-my.html ”
[8] Anonymous, “Unit 1.3.1 Compression, Encryption and Hashing” [2020-02-26], url: “ https://en.wikibooks.org/wiki/A-level_Computing/OCR/Unit_1.3.1_Compression,_Encryption_and_Hashing ”
[9] Ganv, “Steganography and Digital Watermarking” [2009-04-12], url: “ http://wiki.cas.mcmaster.ca/index.php/Steganography_and_Digital_Watermarking ”
[10] Anonymous, “How does steganography work and does it threaten enterprise data?”[2014-01-30], url: “https://moodle.lnu.se/pluginfile.php/8283582/mod_resource/content/1/How%20does%20steganography%20work%20and%20does%20it%20threaten%20enterprise%20data%3F.pdf”
[11] Hardikkumar V. Desai, “Steganography, Cryptography, Watermarking: A Comparative Study” [2012-12-12], url: “https://www.rroij.com/open-access/steganography-cryptography-watermarking-a-comparative-study-33-35.pdf”
[12] Anderson Dadario, “Cryptographic and Non-Cryptographic Hash Functions” [2017-02-26], url: “https://dadario.com.br/cryptographic-and-non-cryptographic-hash-functions/ “
[13] Anonymous, “What is the difference between a Hash Function and a Cryptographic Hash Function?” [2014-08-18], url: “https://security.stackexchange.com/questions/11839/what-is-the-difference-between-a-hash-function-and-a-cryptographic-hash-function “