Linnéuniversitetet
Kalmar Växjö

Linnaeus University

1DV700 - Computer Security
Assignment 1

Student: Abdulrahman Racheed
Personal number: 021225-1292
Student ID: ar224ee@student.lnu.se

Setup Premises

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

Task 1

A)
Symmetric encryption is an encryption method where you use a specific secret key to both encrypt and decrypt data. An example of this encryption method is the Caesar cipher. Asymmetric encryption on the other hand uses a pair of keys instead of only one, they are the public and private keys. The public key is used to encrypt data whilst the private key decrypts it. This means that the private key must be kept private as the name suggests to increase security [1].
Encryption algorithms are used to encrypt data while the data can be decrypted with a secret key. This ensures that the data is encrypted and kept safe while still being able to be viewed by people with its corresponding security key. Hash algorithms on the other hand use a one-way encryption method. This means that once the data is encrypted, it cannot be recovered. This is why it is used for managing file-identifiers such as file-ID's, passwords authentication [2][3].
Compression is a method used to decrease the size of a folder, file or data in order to make it easier to share. This method can be reversed to access the old data. Hashing in the other way is a method made to be a one-way encryption method. This means that once the data has been hashed, it cannot be reversed. This is because hashing creates a fixed-sized output [2][4].

B)
Stenography is a method that is used to conceal information inside files, images, videos and more. The goal is to hide the information rather than encrypting it. This method is used when the message needs to be delivered undetected. Such as a spy sending information to a rival company.

Encryption is a method that converts plaintext into encrypted information. This information cannot be decrypted if you do not know the specific algorithm used or if you don't have authority to clear the decryption. This is a method used to protect data from unauthorized access. It is used in a variety of situations, such as computer files, company data and more.

Lastly we have Digital watermarking. This method is used by embedding information onto a file, such as an image or your name. These watermarks are used to identify the owner of the information. Digital watermarks are used in a different way than the two recently mentioned methods. It wants to clearly identify the owner instead of concealing/protecting it.
- Stenography conceals information
- Encryption protects information
- Digital watermarking Identifies the owner

Task 2

A)
For this task I simply used the table we were supplied with, the deciphered message said “encrypted message”.
B)
My approach to this was to try to brute force it. I tried a multitude of different keys but the end result was all gibberish for all my tries.
C)
2b was very difficult trying to decipher. I did not know the key which made me try as many keys as i could. My method would work in the end, but it was very time consuming and inefficient. I could have created a program that took in a specific key and deciphered the message but that would have been even more time consuming.

Task 3

I used caesar shift cipher and a columnar cipher. I wrote two different functions for each cipher, one for encryption and the other for decryption. I also created two additional functions for file handling, they respectively read from files and write into files.

The caesar shift cipher takes in text and the selected key, then we loop through each character in the given text while getting its ASCII value. When we retrieve that, we add the key and modulo it by 255 to get the new position of the value. Then we use chr() to get the newly shifted character and lastly we return the cipher.

For the columnar cipher we need to create a box that will contain the ciphers, but to determine the size of it we need the key length. Keys for this cipher are words instead of numbers, so both the letters and length of the key matter in this case. Now that we have the dimensions for the box, we convert the text and the key into lists while fillers are added if needed to complete the rectangular shape. The box is then filled with the text and the cipher is retrieved by reading the columns in the order specified by the keyword.

Task 4

I used my columnar cipher and I set my key to “mother”.

Task 5

oa222sv.txt: I took a random cipher and searched for tools that searched cracked ciphers. I found two websites. Boxentriq and CipherTools. They took in a cipher and tried to decipher it using the caesar cipher. At last i found that the translated message that both websites agreed upon.[5][6]

```
**********************************************************************************************
*                                                                                            *
*                                Secret message - Top Secret                                 *
*                                                                                            *
*                      MaY onlY be read bY secUritY passed personnel                         *
*                                                                                            *
**********************************************************************************************

CompUter secUritY is the protection of the items YoU ValUe, called the assets of a
compUter or compUter sYstem. There are manY tYpes of assets, inVolVing hardWare,
softWare, data, people, processes, or combinations of these. To determine What to protect,
We mUst first identifY What has ValUe and to Whom.
A compUter deVice (inclUding hardWare, added components, and accessories) is§
certainlY an asset. BecaUse most compUter hardWare is prettY Useless WithoUt programs,
the softWare is also an asset. SoftWare inclUdes the operating sYstem, Utilities and deVice
handlers; applications sUch as Word processing, media plaYers or email handlers; and eVen
programs that YoU maY haVe Written YoUrself. MUch hardWare and softWare is off the shelf,
meaning that it is commerciallY aVailable (not cUstom-made for YoUr pUrpose) and
that YoU can easilY get a replacement. The thing that makes YoUr compUter UniqUe and
important to YoU is its content: photos, tUnes, papers, email messages, projects, calendar
information, ebooks (With YoUr annotations), contact information, code YoU created, and
the like. ThUs, data items on a compUter are assets, too. unlike most hardWare and
softWare, data can be hard—if not impossible—to recreate or replace

      Osamah Ali

**********************************************************************************************
```

Figure 1: Decoded oa222sv message

mo223tz.txt: After i was done with the previous cipher, i picked the second one at random, and it looked quite similar to the previous cipher. So with that knowledge in mind i went back to the online tools i found and it cracked the cipher once again. Both the websites seemed to agree upon the result aswell [5][6]. Figure 2 shows the result.

```
*****************************************************************************************************
*                                                                                                   *
*                                Secret message - Top Secret                                        *
*                                                                                                   *
*                      May only be read by security passed personnel                                *
*                                                                                                   *
*****************************************************************************************************

Inequality is defined as both unjust and unequal distributions and outcomes.
The focus here is on economic inequality, because most of the worlds population lives in
capitalist societies where access to and quality of various elements of social well-being z◆◆
including nutrition, shelter, health, education, employment opportunities, clean environments,
leisure, security, social stability, and so forth- are increasingly determined by
purchasing ability.
Economic inequality inevitably creates social inequality, as some groups are denied
access to these basic elements of social well-being.
Geographers first became interested in the spatial implications of inequality during the
1970s, particularly within two key foundational subfields (Marxist urban political economy
and welfare geography).
The waning geographical interest in inequality during the 1980s was re-energized by the
resurgence of global(ized) inequality in the 1990s and beyond, focusing on terms of income
polarization and concentrated poverty. The role of the welfare state in mediating inequality §
is also discussed, including the sense that the state is now magnifying, rather than countering
or ignoring, inequality. Similar issues are then highlighted in the less-developed world,
particularly with regard to the urbanization of poverty and the spatial separation of the classes.
Finally, a glimpse is offered into how geographers are currently studying inequality.

Martim Oliveira
§
*****************************************************************************************************
```

Figure 2: Decoded mo223tz message

Task 6

I took my hash function from the python course and modified it. I used the ASCII values of the characters multiplied by a counter plus a constant of 303 (prime number). I received my one bit word text file from a friend that has previously done the course while i got my 10k words from a GitHub repository. I found [7]. My graphs look like this:

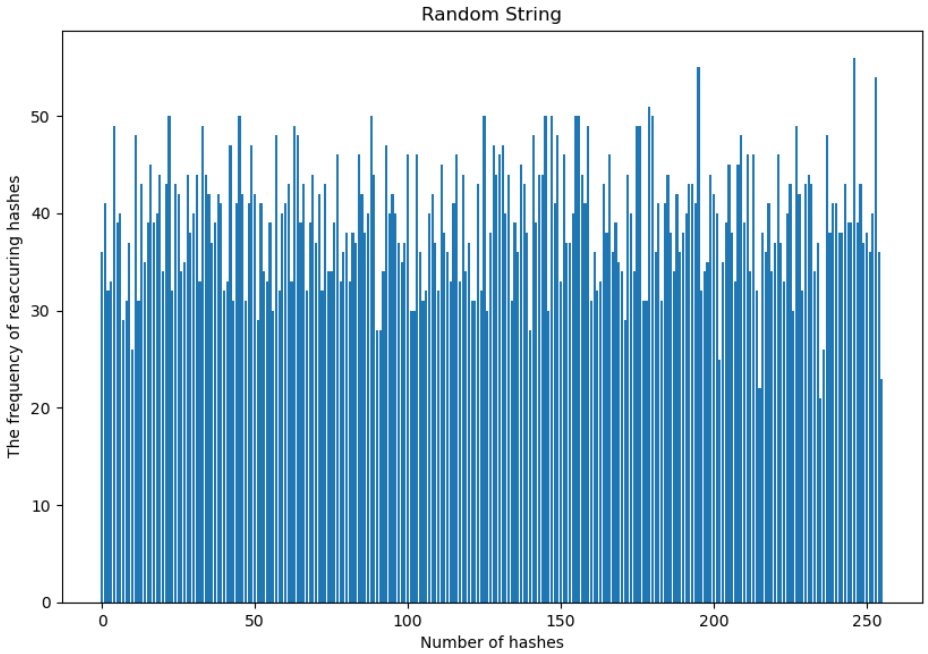

Figure 3: Bar graph

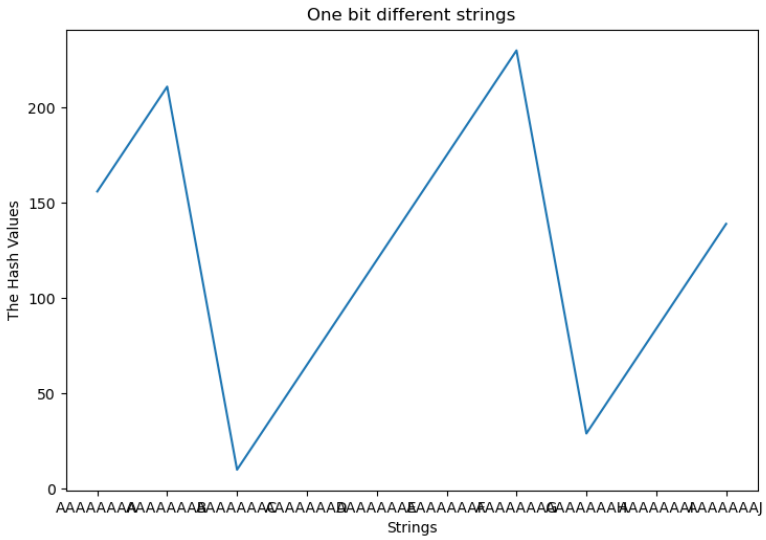

Figure 4: Line Graph

I created a collision test and an avalanche test to analyse the effectiveness of my hash function. The collision test analyses the frequency of recurring hash values while the avalanche test measures the hash function's sensitivity to minor changes in input values. The results from both test show that there are frequent duplicate hash values which means that the hash function is not very good.

A secure hash function efficiently computes hashes while also keeping the number of collisions stay to a minimum. That means that the program should be able to calculate the hash values quickly while also reducing the number of recurring hash values [8][9]. My hash value is not particularly secure since collisions often occur as shown on figure 3.

Bibliography

[1] https://www.geeksforgeeks.org/difference-between-symmetric-and-asymmetric-key-encryption/

[2] https://www.techtarget.com/searchdatamanagement/definition/hashing

[3] https://www.encryptionconsulting.com/education-center/encryption-vs-hashing/#:~:text=Since%20encryption%20is%20two%2Dway,salt%2C%20that%20cannot%20be%20decrypted.

[4] https://www.barracuda.com/support/glossary/data-compression#:~:text=Data%20compression%20is%20the%20process,bits%20than%20the%20original%20representation.

[5] https://www.boxentriq.com/

[6] https://ciphertools.co.uk/

[7] https://github.com/first20hours/google-10000-english/blob/master/google-10000-english.txt

[8] https://en.wikipedia.org/wiki/Hash_function#:~:text=A%20good%20hash%20function%20satisfies,of%20output%20values%20(collisions).

[9] https://www.geeksforgeeks.org/what-are-hash-functions-and-how-to-choose-a-good-hash-function/