# Ransomware Attack

Mariam Mohammed 3910160

Renad Al Ahmadi 3810057

Sondos Ehab 3810121

Haya Baqais 3910002

Dept. of Cyber Security and Forensic Computing

Faculty of Computer Science and Information Technology

University of Prince Mugrin, Madinah KSA

This project report is submitted to the Department of Cyber Security and Forensic Computing at University of Prince Mugrin in partial fulfillment of the requirements for the course Applied Cryptography FC421.

**Author(s):**

Mariam Mohammed
3910160@upm.edu.sa
Renad Alahmadi
3810057@upm.edu.sa
Sondos Ehab
3810121@upm.edu.sa
Haya Baqais
3910002@upm.edu.sa

**University supervisor(s):**

Dr. Mohammed Abdulrahman
Department of Cyber Security and Forensic Computing University of Prince Mugrin
Address: Medina, Saudi Arabia
Email: m.arahman@upm.edu.sa

# ABSTRACT

The attacks against organizations and users are increasing every year introducing new vulnerabilities and costing a lot of damage. One of the most common attacks is ransomware attacks that use crypto algorithms along with other malicious techniques to gain control of the victim's system and encrypt their files. This report explains ransomware along with the cryptographic operations and algorithms that were used in creating ransomware.

# TABLE OF CONTENTS

# Chapter 1 – Introduction

## 1. Introduction

Nowadays, technology is developing rapidly, and it is integrated in every part of people's daily lives from chatting and ordering food to sending sensitive data. With these advancements of technology, cryptography is also being used heavily. Cryptography as defined by Kaspersky (2021) is: "the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents". The term is derived from the Greek word "kryptos" which means hidden. Cryptography is a vital component to achieve confidentiality, integrity, availability, and non-repudiation. Cryptography involves two main operations: encryption and decryption. Encryption's role is to transform the data to an unreadable format, while decryption's role is to restore the format of the encrypted data. Cryptography is crucial and applied in many helpful areas such as authenticating users, storing passwords in a hashed format, encrypting emails and chat messages, disk encryption to keep important files safe, SSL in HTTPS, and even in GSM communications to preserve the secrecy of phone calls and SMS. However, it can also be used for evil malicious purposes such as ransomware attacks to encrypt the files of the user and blackmail him/her to pay a ransom to get their files in the decrypted format. Two major types of modern cryptography are symmetric-key cryptography and asymmetric-key cryptography. Symmetric-key cryptography, also known as secret key cryptography, uses one shared key between the sender and the receiver to encrypt and decrypt messages. Asymmetric key cryptography, also known as public-key system, uses pair of keys in which each pair consists of two keys: public key and private key.

In our project, we are going to showcase one of the most popular attacks that involves cryptography which is ransomware attack and explain the role of cryptography algorithms in this attack and how it uses both symmetric and asymmetric cryptography.

# Chapter 2 – Ransomware

## 2.1 Ransomware

Over the past few years, the business industry has been highly targeted by ransomware attacks. The attack has targeted high-profile organizations and companies in different countries. According to Cognyte CTI Research Group (2021), 2021 year has seen an increase in the number of ransomware attacks. As defined by FBI government (2020) "Ransomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return". This type of attack can exploit vulnerabilities on the network or system or take advantage of human errors. Once it compromises the system, it will encrypt the user's files to prevent the user from accessing his/her own data and won't decrypt them back unless the victim pays the required amount of money/ransom to the attacker, usually by electronic currencies. In 2021, ransomware attacks have affected 1,097 organizations in the first half period, while in 2020, about 1,112 organizations were hit by ransomware attacks. The statics of the attack are not enough to prove the severity of the attack, but also it has a great impact on the continuity of the organization's business and its financial status. For example, the hacker takes advantage of the pandemic and attacks healthcare systems, consequently, many of the hospitals were victimized by ransomware. A study by Paul Bischoff (2021), shows that more than 600 hospitals, clinics, and patient records were affected by ransomware attacks only in 2020, and the overall cost of the attacks is about $20.8 billion. When this happens in the healthcare industry, it will slow the operations of the hospitals and their critical information might be encrypted and exfiltrated by the attacker till the ransom is paid. Furthermore, there are many types of ransomware attacks that have a significant impact and cause great damage to systems and organizations. This will be explained in the following sections.

## 2.2 Ransomware Real Life Examples

The following points are real examples of ransomware attacks, that have the same goal but differ in the way they spread and work.

### 2.2.1 Ryuk Ransomware

In Ryuk ransomware attack, the attacker uses phishing emails as threat vector to trigger the users into opening a malicious document that causes the Macro to run CMD and execute PowerShell command. As described by Malwarebytes company (n.d), after the PowerShell is executed, it attempts to download Trojan Emotet malware. This malware can affect the system with additional malwares such as Trickbot. Once the Trickbot payload is executed it will collect critical information about the infected system such as admin credentials, theses information can be used later to beyond the scope of the attack and access the assets they want to infect. Finally, the threat vectors will establish a connection with the target servers via remote desktop protocol to execute Ryuk payload. A combination of different malwares gives the attacker the opportunity to control the target system and hit its goal.

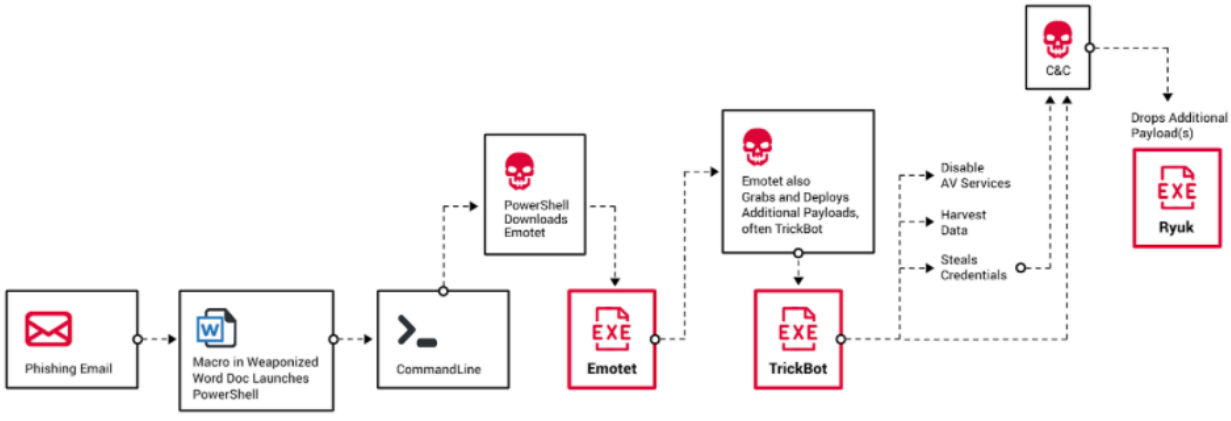


Figure. 1. The Ryuk Ransomware Technique.

### 2.2.2 WannaCry Ransomware

This type of ransomware had a significant impact in 2017. Cyware Social (2018) reported that more than 200,000 machines were affected by WannaCry in 150 countries such as Russia and China. As defined by NCCIC (n.d.) "WannaCry is ransomware that contains a worm component. It attempts to exploit vulnerabilities in the Windows SMBv1 server to remotely compromise systems, encrypt files, and spread to other hosts." If the computer systems are using the vulnerable server message block version 1(SMBv1) which is a file sharing protocol, they cannot avoid the caused damage that resulted from being attacked by WannaCry. An EternalBlue exploit was used to take advantage of the vulnerability, the exploit was developed by NSA for cyberattack purposes and the tool was leaked in 2017 successfully by a group of cybercriminals called Shadow Brokers. Furthermore, WannaCry attack acts as a worm to spread itself throughout the victim machines and networks. The worm has the ability to copy itself without the need of the victim's interaction. This makes it different from other ransomware attacks that use the social engineering techniques as a threat vector to spread the attack.


Figure. 2. The WannaCry Ransomware Screen.

## 2.3 Ransomware Spreading Methods

The ransomware attack is like any other attack that needs to be distributed by a threat vector to infect the victim's system in order to deliver its payload.

### 2.3.1 Email Attachments

When people send e-mails, they often add attachments with this e-mail, and this is called e-mail attachments. The attackers use mail attachments to attach malicious files to damage the device on which these files will be downloaded and to grant the hacker the "mail sender" access and damage the target device. Because the mail automatically blocks malicious files if they exist, the attackers hide them inside other types of files so that they are not discovered by the mail client, and the victim thinks that the sender is a trusted person and that the attached file is a secure file, but the truth is the exact opposite, and the person becomes a victim to phishing emails and download the file which is the ransomware. When it runs on the device, it encrypts the files and, in some cases, exfiltrate them also. The attacker will ask for a ransom and the files won't be decrypted unless the required amount of money is paid.

### 2.3.2 Removable Media

As defined by techopidia (2011), removable media are devices used for storage, backup, or transportation of data. They are called removable media because it has the capability to be inserted and removed from a computer device without causing it to shut down such as a USB. The attacker uses this technique to inject malicious software into a USB flash or other type of removable devices and when the victim plugs the malicious USB into their machine, the malicious file compromises the machine.

### 2.3.3 Remote Desktop Protocol

RDP stands for Remote Desktop Protocol, and it runs on port 3389. It provides a service in which users can connect to another user's desktop while running this protocol. When a user connects to another user using RDP, he can have control over the

device such as accessing settings or downloading files. Attackers take advantage of this service and port and gain access to vulnerable machines and download ransomware.

#### 2.3.4 Malvertising

Malvertising is a type of attack that targets advertising websites. This attack works by injecting advertising pages with malicious code and usually redirecting the user to another malicious website. These are difficult to detect because the online advertising system is a complex network system, so the code is injected in unexpected places and cannot be easily discovered and accessed. Thus, the user is redirected to an advertising page that contains malicious programs, and this leads to downloading ransomware to the victim's computer.

# Chapter 3 – Ransomware Algorithms

## 3.1 Ransomware

Our ransomware consists of the two types of modern cryptography: symmetric and asymmetric cryptography. Furthermore, base64 and SHA-512 were used. First, ransomware will search files on the system. Then it is going to encrypt them using AES symmetric key algorithm and add "FC421RANSOM" as the extension of the files as well as changing the desktop wallpaper to a ransom note. Then for the ransomware to be more robust and efficient, the AES key that was used to encrypt the files will be encrypted using the attacker's public key that is generated using RSA algorithm. If the victim paid the ransom, the AES key will be decrypted using the attacker's private key and then the files are going to be decrypted using the retrieved AES key. During the process of generating the AES key, the key must be hashed using SHA-512 and then the key digest is going to be encoded using base64 to prepare it for the algorithm. During the process, we used multiple cryptographic components in our project. The following diagram explains the high-level idea of ransomware:

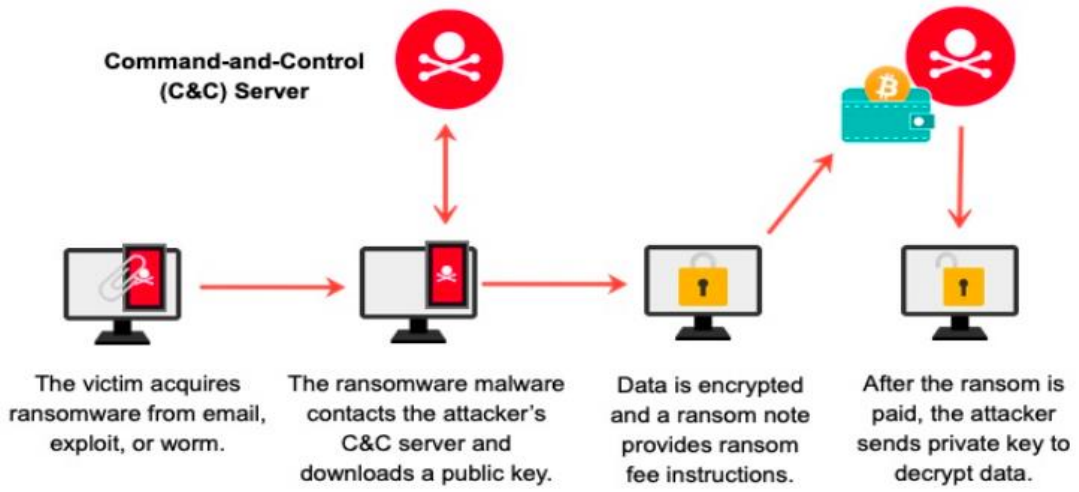


Figure. 3. Ransomware Technique.

## 3.2 Encryption Algorithm

### 3.2.1 Symmetric Cryptography- Advance Encryption Standard (AES)

AES is Advance Encryption System is a two-way encryption method. It allows users to encrypt the text to a scrambled form and get the original data by decrypting it in the opposite way. Also, this algorithm uses symmetric encryption which means that the encryption key is the same as the decryption key. Furthermore, AES have 3 main variations, AES-128, AES-192, and AES-256, which depend on the key size and the number of rounds. AES-128 uses 128 bits key size and consists of 10 rounds. On the other hand, AES-192 and AES-256 have 192 bits and 256 bits key respectively key size of 256 bits and consists of 14 rounds. The bigger the key size the stronger the encryption.

#### *3.2.1.1 Basic Configurations:*

Key size: 256 bits

Block Size: Fixed 128 bits

Mode: Cipher Block Chaining (CBC)

Number of Rounds: 14 rounds

### *3.2.1.2 Cipher Block Chaining (CBC):*

As mentioned above, AES is a block cipher encryption algorithm which divides the plaintext into chunks of fixed sized blocks. Furthermore, block cipher algorithms have multiple encryption modes which determine the way of handling the series of cipher blocks. In our project we have used Cipher Block Chaining (CBC) mode which gives an extra layer of randomness and hardens the plaintext recovery.

CBC is an advancement mode for Electronic Code Book (ECB) which was handling each block separately. As shown in the figure below, a block cipher that uses ECB mode will divide the plain text into fixed size blocks. Then, it will do the encryption on each block separately. Finally, the blocks of cipher text will be combined together as the encryption result. Handling each block separately was the main reason for it to be broken because it does not perform a diffusion layer which exposes the data pattern specially for identical plaintext.

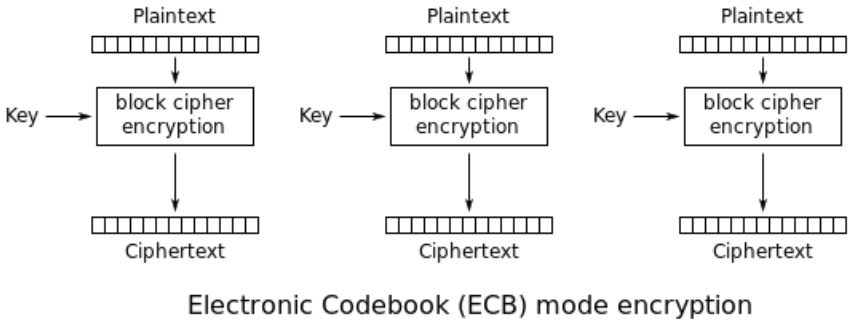


Figure. 4. ECB Encryption.

After ECB compromise, CBC model was proposed to solve the problem of data pattern. ECB approach was relying on chaining the blocks so data patterns cannot be exposed. Specifically, an extra randomness layer will be added before starting the encryption process where the plaintext block will be added to similar size vector. In the first step an Initialization Vector (IV), which is a random value, will be added to the first plaintext block. After the encryption process, the resulting ciphertext will be added to the next block of plaintext before it gets encrypted. As shown in the figure below, this block chaining will hide the pattern from the ciphertext even for matching plaintext as long as the Initialization Vector (IV) is different. Even though it applies better security measures, it still has the disadvantage of applying block cipher in parallel because each block ciphering relies on the previous block. (TechTarget, 2021)

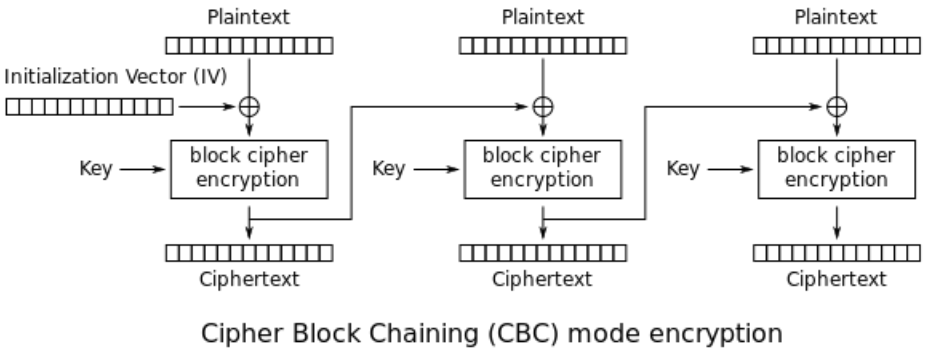


Figure. 5. CBC Encryption.

### *3.2.1.3 AES Key Expansion:*

From AES-256 name, we can indicate that it uses 256 bits key length while keeping the same block size as 128 bits. We also know that it consists of 14 rounds which requires more than the original key for the encryption process. Due to that, key scheduling process is being applied to derive new round keys from the original key.

In the beginning AES 256 bits cipher key will differ slightly from AES 128 bits. AES 256 bits key will consist of 8 words per round which is double the block size. Besides, it contains 14 rounds which will determine the number of round keys we must generate. The first step in the routine is to take the first four bytes W[0-3] from the original key. Then, the last selected word W[3] will be taken into the following functions:

1. Apply single left shift on the four bytes.
2. Apply a substitution box to the resulting four bytes. Each byte represented by two hexadecimal values where the first hex value will indicate the row index and the second hex value will indicate the column index.

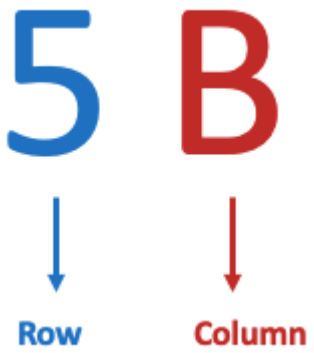


Figure. 6. Index of Substitution Table.

Next, the value will be looked up by finding the crossing point in the substitution table shown in the figure below and it will be returned. In the case of our sample above, the result will be 39.

| | | y | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | a | b | c | d | e | f |
| x | 0 | 63 | 7c | 77 | 7b | f2 | 6b | 6f | c5 | 30 | 01 | 67 | 2b | fe | d7 | ab | 76 |
| | 1 | ca | 82 | c9 | 7d | fa | 59 | 47 | f0 | ad | d4 | a2 | af | 9c | a4 | 72 | c0 |
| | 2 | b7 | fd | 93 | 26 | 36 | 3f | f7 | cc | 34 | a5 | e5 | f1 | 71 | d8 | 31 | 15 |
| | 3 | 04 | c7 | 23 | c3 | 18 | 96 | 05 | 9a | 07 | 12 | 80 | e2 | eb | 27 | b2 | 75 |
| | 4 | 09 | 83 | 2c | 1a | 1b | 6e | 5a | a0 | 52 | 3b | d6 | b3 | 29 | e3 | 2f | 84 |
| | 5 | 53 | d1 | 00 | ed | 20 | fc | b1 | 5b | 6a | cb | be | 39 | 4a | 4c | 58 | cf |
| | 6 | d0 | ef | aa | fb | 43 | 4d | 33 | 85 | 45 | f9 | 02 | 7f | 50 | 3c | 9f | a8 |
| | 7 | 51 | a3 | 40 | 8f | 92 | 9d | 38 | f5 | bc | b6 | da | 21 | 10 | ff | f3 | d2 |
| | 8 | cd | 0c | 13 | ec | 5f | 97 | 44 | 17 | c4 | a7 | 7e | 3d | 64 | 5d | 19 | 73 |
| | 9 | 60 | 81 | 4f | dc | 22 | 2a | 90 | 88 | 46 | ee | b8 | 14 | de | 5e | 0b | db |
| | a | e0 | 32 | 3a | 0a | 49 | 06 | 24 | 5c | c2 | d3 | ac | 62 | 91 | 95 | e4 | 79 |
| | b | e7 | c8 | 37 | 6d | 8d | d5 | 4e | a9 | 6c | 56 | f4 | ea | 65 | 7a | ae | 08 |
| | c | ba | 78 | 25 | 2e | 1c | a6 | b4 | c6 | e8 | dd | 74 | 1f | 4b | bd | 8b | 8a |
| | d | 70 | 3e | b5 | 66 | 48 | 03 | f6 | 0e | 61 | 35 | 57 | b9 | 86 | c1 | 1d | 9e |
| | e | e1 | f8 | 98 | 11 | 69 | d9 | 8e | 94 | 9b | 1e | 87 | e9 | ce | 55 | 28 | df |
| | f | 8c | a1 | 89 | 0d | bf | e6 | 42 | 68 | 41 | 99 | 2d | 0f | b0 | 54 | bb | 16 |

Figure. 7.Substitution Table.

3. Add the resulting word using Xor operation with a constant that will have the value of $2^{i-1}$ **00 00 00** where **i** is the index of round.
4. Add the resulting word with the first word W [0] using Xor operation. The resulting word will be counted as W [8] because the original key size is W [0-7].

The next word W [9] will get its value by Xor W [1] with the resulting word W [8] and the process will be done for the rest of the original key words. The new words will be getting their values with the following formula W[i]= W[i-1] Xor W[I-8]. The difference between AES-256 bits and the other variations is that it will apply S-box if i-4 is multiple of the key length, which is 8 words in 256 bits. Specifically, a substitution will take a place at the fourth word in the middle of each round. The key expansion will contain 60 words W [0-59]. (National Institute of Standards and Technology, 2001)

#### *3.2.1.4 Encryption Process:*

First, we should prepare our plaintext before the main encryption process. The plaintext is divided into blocks, each block with size 128 bits which is equivalent to 16 bytes.

The main three operations on each round are:

i. Randomness Layer which has adding round key operation.
i. Confusion Layer, and this has a byte substitution, or we can call it (s-box) operation.
ii. Diffusion Layer which has two sub operations: shift row and mix column. There is no mixed column operation for the last round.

At first, we will take a plain text which is 16 bytes and make it a 4 X 4 matrix as you can see in the figure (8), and we call it state.

Then we get the original key and do XOR operation with these two inputs (state, first 128 bits from the original key)

Next, we will take the result of first XOR operation and go to confusion step. In the confusion, we will do the substitution (s-box) operation. The state, which is 4 X 4 matrix, in each box in this matrix we have hex value. We will take the hex value with two numbers and the first one we imagine as (x) and the second one as (y) then we will go to (s-box) table and look for the (x) in row and (y) in column then take the intercept point and this will be the new value. We will complete all 15 s-boxes and get the new value for all.

After we get the new state, we will move on to the diffusion operation. The first step in diffusion is shift row. As you can see in figure (9) we will shift first row 0-bits, second row 1 bit, third row 2 bit and fourth row 3 bit.

After we do the shifting the matrix will be as you can see in the figure (10) then we will go to mix column also in diffusion step. In mix column we will have fixed matrix 4 X 4, and we will multiply it with the state we got after row shifting. Galois Fields should be taken into consideration to avoid passing 8 bits limit for each byte. To ensure this, we take the mod operation with the irreducible polynomial x^8+x^4+x^3+x+1.

Then the last step we will be added to the second 128 bits from the original key and again do the same steps 14 times because we have 14 rounds in AES-256. However, the last round which is round 14 will not undergo a mix column operation.


Normal plain text

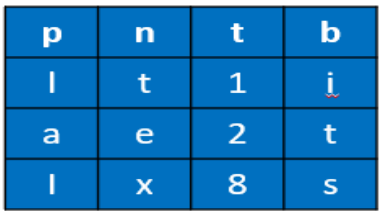


Figure.8. state.

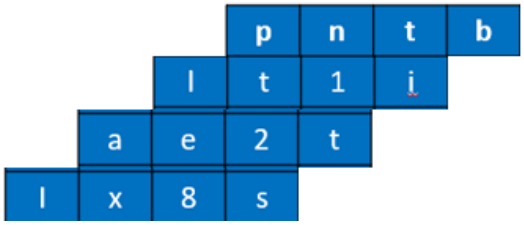


Figure.9. shift row.

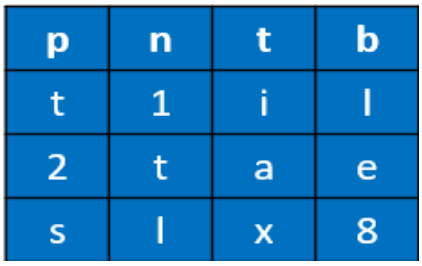


Figure. 10.Final Result for Shift Row.

### 3.2.2 Asymmetric Cryptography-RSA

Asymmetric cryptography depends on the use of two keys. These two keys (key pair) must be mathematically related to each other. The key pair consists of a public key and a private key. As the name implies, public keys can be available to anyone while on the other hand, private keys should be kept secret. When the data is encrypted using the public key, the private key is going to decrypt the encrypted data. If the data is encrypted with the private key this creates a digital signature. One of the most crucial and popular uses of asymmetric cryptography is key exchange. This solves the problem of symmetric cryptography which is how to securely exchange the shared key between the sender and the receiver.

RSA is a widely used asymmetric cryptosystem. It was invented by Ron Rivest, Adi Shamir, and Leonard Adleman, hence the name RSA. The main idea behind RSA is that it is hard to factorize a large integer. The private key is derived from two large prime numbers; therefore, the strength of the encryption relies on the key size. (GeeksforGeeks, 2021)

#### *3.2.2.1 Key Generation:*

1- Select two large prime numbers, P and Q
2- Calculate n using the equation n=P*Q
3- Calculate Φ(n) using the equation Φ(n)=(P-1) * (Q-1)
4- Select a small exponent e that must be an integer, not a factor of n, and 1 < e < Φ(n)

**Public key** consists of: (n,e)

**Private key** is a= e-1 mod Φ(n)

#### *3.2.2.2 Encryption:*

Y= $x^e$ mod n., where x is the plaintext

#### *3.2.2.3 Decryption:*

Y= $c^a$ mod n., where c is the ciphertext

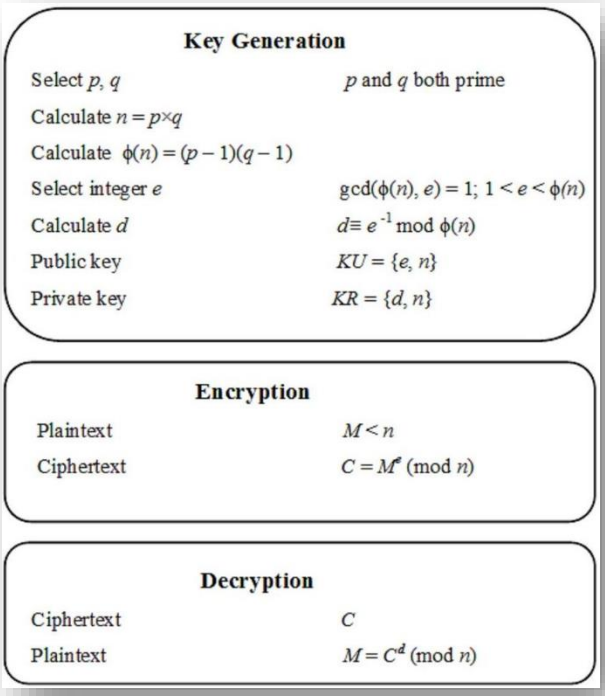


Figure. 11.RSA Algorithm.

### 3.2.3 Secure Hash Algorithm (SHA256)

Secure Hash Algorithm is a function that falls under hash functions. This cryptographic field focuses on generating fixed size digest regardless of the input size.

Hash main features:

- Fixed size output
- Collision resistance which means each input will give special output that cannot be generated with any other value. Specifically, H(x) = H(y) only of x=y.
- One way algorithm which means the original input cannot be recovered from the plaintext

- Avalanche effect which means any simple change in the input will make huge change in the output

The randomness in the value and the fixed size output will be useful for AES key generation. Besides, the collision resistance feature ensures that the user cannot brute force the key unless he/she got the specific input on generation which can vary in size and can be extremely large.

#### *3.2.3.1 General Configurations:*

Block size: 512 bits

Number of rounds: 64 rounds

#### *3.2.3.2 Hashing Process:*

In general, the hashing process start divide the input into a fixed size of chunks. At the end of the last block, the padding will be added which is consists of separator, completing zeros, and 64 bits length. Then, the algorithm will start initializing default buffer values. Next, the compression function will take a place for 64 rounds on each block then the output will be used to feed the next block input. The output of the last block will be output and used as hash or message digest. (Anand, 2019)

## 3.3 Scenario

The employees of a company called “Wobily” received an email message that appears to be from the ICT department of the company. The email asked them to download and setup an executable file on the company’s computer machines because it is needed for monitoring purposes as soon as possible. As a consequence, some employees downloaded the executable and all of a sudden, they found a desktop note that says that their files are encrypted, and they

won't get it back unless the company pays the required amount of money. Then they realized that this was a well-crafted phishing email that was sent by an attacker to target multiple computers in the company and ask for a huge ransom to gain money. This attack caused a lot of adverse consequences for the organization such as impacting the business continuity, loss of sensitive data, and affected the company's financial situation.

# Chapter 4 - Requirement Analysis

## 4.1 Functional Requirements

### 4.1.1- Attacker

- Attacker can encrypt multiple file extension
- Attacker can generate and access a symmetric key to encrypt the victim's file
- Attacker can encrypt the symmetric key with his/her public key
- Attacker can decrypt the symmetric key and files

### 4.1.2- Victim

- Victim can contact attacker to get the encryption key

## 4.2 Non-Functional Requirements

- The files will be encrypted in the background

## 4.3 Flow Diagram

### 4.3.1 Encryptor

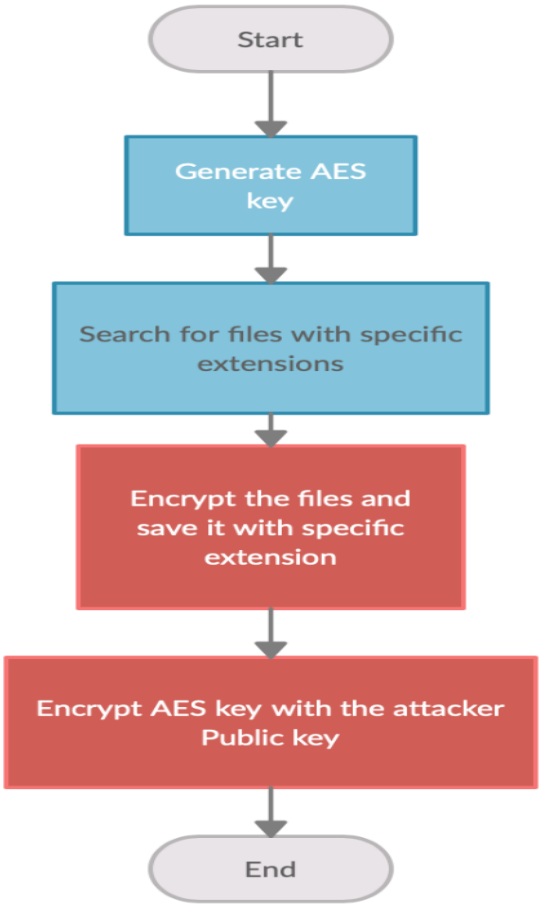


Figure. 12.Flow Diagram of Encryptor Function.

### 4.3.2 Decryptor

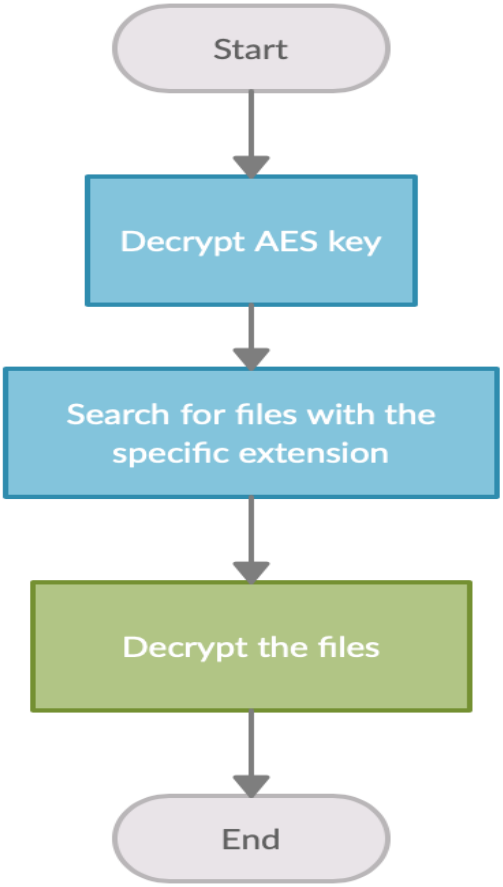


Figure. 13.Flow Diagram of Decryptor Function.

## 4.4 Processes Flow

1- Search for the files on the system and add them to a list
2- Change their extension to “FC421RANSOM”
3- Get the SHA-256 hash digest of the AES key
4- Use the encryptor function to encrypt the files

5- Add the ransom note
6- Encrypt the AES key using the attacker's public key that is generated using RSA
7- If the attacker decided to decrypt the files, then the decryptor function will work
8- The AES key will be decrypted using the attacker's private key that is generated using RSA
9- Search for files with the extension "FC421RANSOM"
10- Decrypt the files using the decryption process.

# Chapter 5 - Design Consideration

## 5.1 Hardware Requirements

- PC

## 5.2 Software Requirements

- Python 3.10
- Virtual box
- Kali iso
- Windows iso
- Pycharm community edition

## 5.3 Cryptographic Components

1. **RSA:**

   We used RSA from Crypto.PublicKey library in Python. The key length that was used is 4096 bits which is 512 bytes.

2. **AES:**

   We used AES from Crypto.Cipher library in Python

3. **SHA-512:**

   We used SHA256 from Crypto.Hash library in Python.

4. **Base64:**

   We used base64 library from python

### 5.4 Implementation

Code was uploaded on github for efficiency and readability on the following link:

https://github.com/hayabaq/RanSomeWhere

## Chapter 6 – Conclusion

As a conclusion, Cryptography can be used for bad intentions as well as their main security goals. Ransomware is one of the most popular example of abusing cryptography. Those service denials consequences can extend to affect many industry field such as health care system which might lead to loosing peoples' lives. This project consisted of creating a ransomware using python programming language as well as explaining all relevant cryptographic concepts and components such as symmetric and asymmetric Cryptography. Specifically, AES, RSA, and Hash algorithms.

# References

Anand, A. (2019, November 27). *Breaking Down : SHA-256 Algorithm*. infosecwriteups. Retrieved December 2021, from https://infosecwriteups.com/breaking-down-sha-256-algorithm-2ce61d86f7a3

Bischoff, P. (2021, July 27). *Ransomware attacks on US healthcare organizations cost $20.8bn in 2020*. Comparitech. Retrieved December 27, 2021, from https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/

*Cryptography definition*. www.kaspersky.com. (2021, January 13). Retrieved December 27, 2021, from https://www.kaspersky.com/resource-center/definitions/what-is-cryptography

Cyware. (2018, November 25). *Wannacry: What makes the ransomware still an active and prevalent threat?: Cyware Hacker News*. Cyware Labs. Retrieved December 27, 2021, from https://cyware.com/news/wannacry-what-makes-the-ransomware-still-an-active-and-prevalent-threat-889fe649

FBI. (2020, April 3). *Ransomware*. FBI. Retrieved December 27, 2021, from https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware

*FIPS 197, Advanced Encryption Standard (AES) - CSRC*. (2001, November 26). Retrieved December 27, 2021, from https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf

Gantenbein, K. (2021, August 16). *How ransomware works and how to prevent it: ExtraHop*. ExtraHop. Retrieved December 27, 2021, from

https://www.extrahop.com/company/blog/2020/ransomware-explanation-and-prevention/

Jareth. (2019, December 22). *How ransomware spreads: 9 most common infection methods and how to stop them - emsisoft: Security blog*. Emsisoft. Retrieved December 27, 2021, from https://blog.emsisoft.com/en/35083/how-ransomware-spreads-9-most-common-infection-methods-and-how-to-stop-them/

*Ransomware attack statistics 2021 - Growth & Analysis*. Cognyte. (2021, August 29). Retrieved December 27, 2021, from https://www.cognyte.com/blog/ransomware_2021/

*RSA algorithm in cryptography*. GeeksforGeeks. (2021, January 5). Retrieved December 27, 2021, from https://www.geeksforgeeks.org/rsa-algorithm-cryptography/

*Ryuk - what is ryuk ransomware?* Ryuk - What is Ryuk Ransomware? (n.d.). Retrieved December 27, 2021, from https://www.malwarebytes.com/ryuk-ransomware

Techopedia. (2011, October 8). *What is removable media? - definition from Techopedia*. Techopedia.com. Retrieved December 27, 2021, from https://www.techopedia.com/definition/13731/removable-media#:~:text=Removable

TechTarget. (2021, May 14). *What is cipher block chaining?* SearchSecurity. Retrieved December 27, 2021, from https://www.techtarget.com/searchsecurity/definition/cipher-block-chaining

*The RSA algorithm. | download scientific diagram*. (n.d.). Retrieved December 27, 2021, from https://www.researchgate.net/figure/Figure-213-The-RSA-Algorithm_fig12_328828460

*What is WANNACRY/Wanacryptor? - CISA*. (n.d.). Retrieved December 27, 2021, from https://www.cisa.gov/uscert/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_WannaCry_Ransomware_S508C.pdf

Wikimedia Foundation. (2021, December 22). *Block cipher mode of Operation*. Wikipedia. Retrieved December 27, 2021, from https://en.m.wikipedia.org/wiki/Block_cipher_mode_of_operation