

**Cryptography & Encryption: Behind the Magic**

Cole A. Zill

Paradise Valley Community College

ITS-240: Ethical Hacking and Network Defense

Professor Aaron Casterline

December 4<sup>th</sup>, 2023

## CRYPTOGRAPHY &amp; ENCRYPTION: BEHIND THE MAGIC

## Table of Contents

Chapter 1: Introduction.....	4
1.1 Problem Statement.....	4
1.2 History of Cryptography.....	5
Chapter 2: Cryptographic Techniques.....	8
2.1 Symmetric Cryptography.....	8
2.2 Asymmetric Cryptography.....	9
2.3 Hashing Techniques.....	11
Chapter 3: Encryption Algorithms.....	14
3.1 Symmetric Algorithms.....	14
3.2 Asymmetric Algorithms.....	16
3.2 Hashing Algorithms.....	17
Chapter 4: SaaS Encryption & Open-Source Cryptography.....	19
4.1 SaaS Encryption Methods.....	19
4.2 Open-Source Encryption Tools.....	20
Chapter 5: Methodologies and Countermeasures.....	22
5.1 Methods and Standards.....	22
5.2: Countermeasures and Risks.....	24
Conclusion.....	26
References.....	27
Appendices.....	30
List of Figures.....	33

## CRYPTOGRAPHY & ENCRYPTION: BEHIND THE MAGIC

### Abstract

As the world transitions into the inevitable digital realm, security will need to advance and develop alongside. People from all around the globe communicate, work, entertain and provide for each other all through networks, computers, and other devices. Now, more than ever, strong security and authentication is advised to ensure your business stays your business. This research aims to analyze different cryptography techniques and encryption algorithms and see how they coexist to improve and secure websites, transactions, passwords and much more. Examples of different encryption algorithms will be shown as a representation on encryption and decryption as well as key generation.

Following, further research will be done on how cryptography has evolved and how encryption and cryptography play a role in compliance standards with government and other areas of business and operations. Lastly, analyze the differences and similarities of open-source cryptography and SaaS encryption along with robust countermeasures on how to protect and understand your data during the cryptography cycle.

*Keywords:* Cryptography, Encryption, AES, DES, RSA, SHA, SSL, Symmetric, Asymmetric, Hashing, Compliance, Security.

# CRYPTOGRAPHY & ENCRYPTION: BEHIND THE MAGIC

## CHAPTER 1

### INTRODUCTION

Throughout this research, cryptography and encryption will be discussed often, and I believe it is important to establish the difference between the two. Cryptography is the science of concealing data with different techniques and algorithms, and encryption is the algorithm itself that is used mathematically by taking the plain text and creating ciphertext. With the two intertwined they can create robust cryptographic systems to protect and secure data.

#### 1.1 Problem Statement

Cryptography and encryption systems work together to protect and secure data while machines are at rest and during transmission. Many organizations and entities conduct most of their business online and need to ensure those details are secure, such as credit card information, direct messages, sensitive file transfers and so much more. Different cryptography techniques can be applied to systems that utilize secure algorithms to encrypt text and hash data to verify the integrity of that data. With so many users accessing enterprise portals or servers, the need for security must increase as well for the data at rest and the data in motion. Throughout this research, analysis of different encryption algorithms will be researched as well as cryptographic methodologies that are used to create robust systems. Cryptography is crucial as more sensitive information is stored and retrieved from online systems and servers. It is not as simple as keeping documents locked away in a vault or guarded with top notch security. Security professionals must be ruthless to maintain and protect against ongoing attacks.

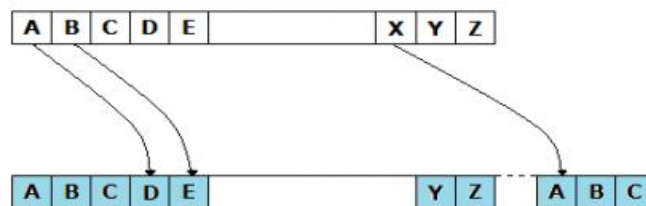
## CRYPTOGRAPHY & ENCRYPTION: BEHIND THE MAGIC

### 1.2 History of Cryptography

In the year 100 BC, Roman General Julius Caesar was busy conveying messages to his soldiers and generals during the war to defend and expand the Roman Empire. However, Caesar did not just send his orders or messages in plain text. Instead, he adopted the ‘Substitution Cipher’, better known today as the ‘Caesar Cipher’. The cipher encrypted these messages by taking the plain text character and shifting it three places in the alphabet. For example,  $A \rightarrow D$ ;  $B \rightarrow E$  (Sidhpurwala, H. 2023). This system was state of the art at the time since the encryption system itself was not known, the messages were able to be concealed to hide the true meaning. However, with modern day computing and observation it would not take long to crack the ‘Caesar Cipher’ due to its simplicity in the current day.

**Figure 1.1**

*Caesar Cipher*



*Note.* Caesar Cipher 1 (Red Hat, 2023)

Fast forward to 1918, German engineer Arther Scherbius, composed the Enigma machine for commercial use. This device had a built-in typewriter that sent electrical signals to a series of rotating disks that would obfuscate the plain text into cipher text. Not too long after this, the

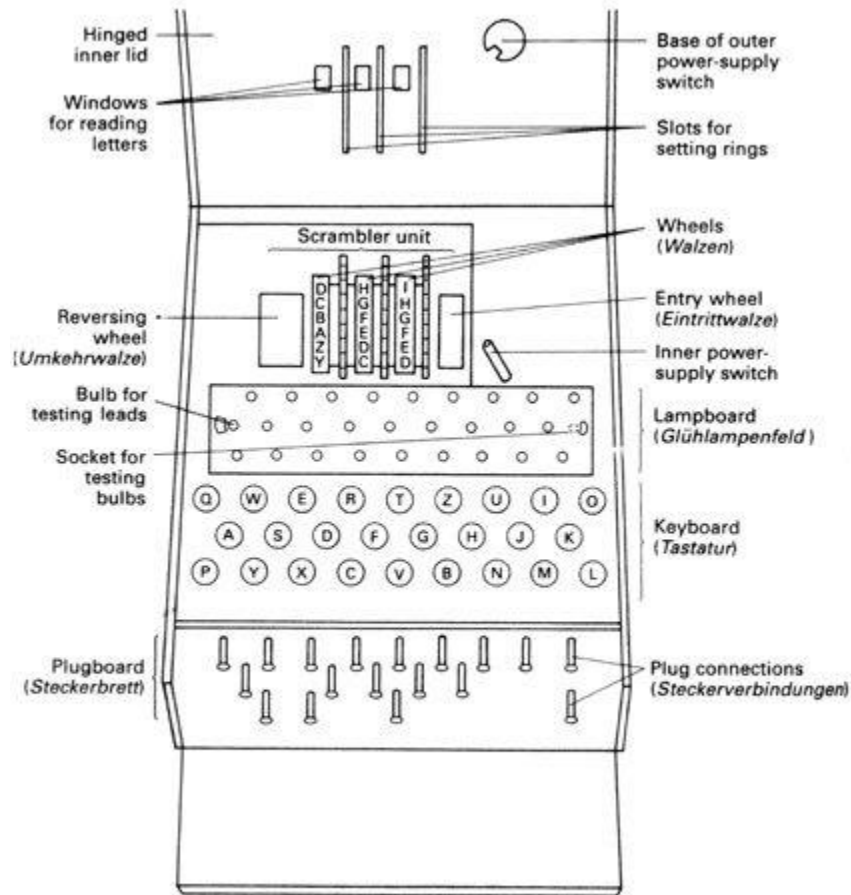
## CRYPTOGRAPHY & ENCRYPTION: BEHIND THE MAGIC

German Army heard of the invention and began using it in military communications. Before the invasion of Poland, Marian Rejewski and his Polish team had been working on a device to crack Enigma. Due to the danger in Poland at the time Rejewski and his team handed their work over to British Intelligence for further research. The British then started a group in secrecy called 'Ultra', led by Mathematician Alan M. Turing. The group worked together to crack Enigma and ultimately destroy the Nazi party as well as contribute to the success in the Pacific for the U.S and other allies. (Britannica, 2023).

## CRYPTOGRAPHY & ENCRYPTION: BEHIND THE MAGIC

**Figure 1.2**

### *Enigma Machine*



*Note.* Enigma Machine and Detailed Components (Nova | PBS, 2023)

In the world today, encryption and cryptography are used in many other sectors than just the military. Whether you are accessing your banking information via the web or communicating with your friends in a direct message, chances are your traffic and data is being encrypted. Cryptography has spread its way into society and even certain organizations must follow encryption standards when dealing with the public. As we move into the next section, we will discuss the different cryptography techniques and the evolution of encryption algorithms.

## CHAPTER 2

### CRYPTOGRAPHIC TECHNIQUES

This chapter analyzes common cryptographic techniques used to secure information. Certain techniques have evolved over time and others are combined to further protect the content. Techniques observed will cover asymmetric, symmetric, and hashing. With the use of these techniques' integrity, validation and authentication can ensure the data or communications are secure.

#### 2.1 Symmetric Cryptography

Earlier, a brief look into the Caesar Cipher was analyzed. This was one of the earlier forms of cryptography and is also a form of symmetric cryptography. Symmetric cryptography only uses one key for the encryption and decryption process. For instance, the 'key' in the Caesar Cipher was simply the knowledge of how each character in the plain text was to be converted. Back then, this system may have been secure for its time, but in modern day, if a criminal or attacker were to figure out your 'key', especially one as simple as a Caesar Cipher, it would compromise the entire system as well as no longer being able to secure its content. However, more robust symmetric cryptography techniques have developed throughout time which will be covered in the next chapter.

**Figure 2.1**



## CRYPTOGRAPHY & ENCRYPTION: BEHIND THE MAGIC

### *Symmetric Encryption*



*Note.* Visualization of Symmetric Encryption with One Key for Each Process (Wikipedia, 2023)

## 2.2 Asymmetric Cryptography

Diving into our next technique, we are focusing on asymmetric cryptography.

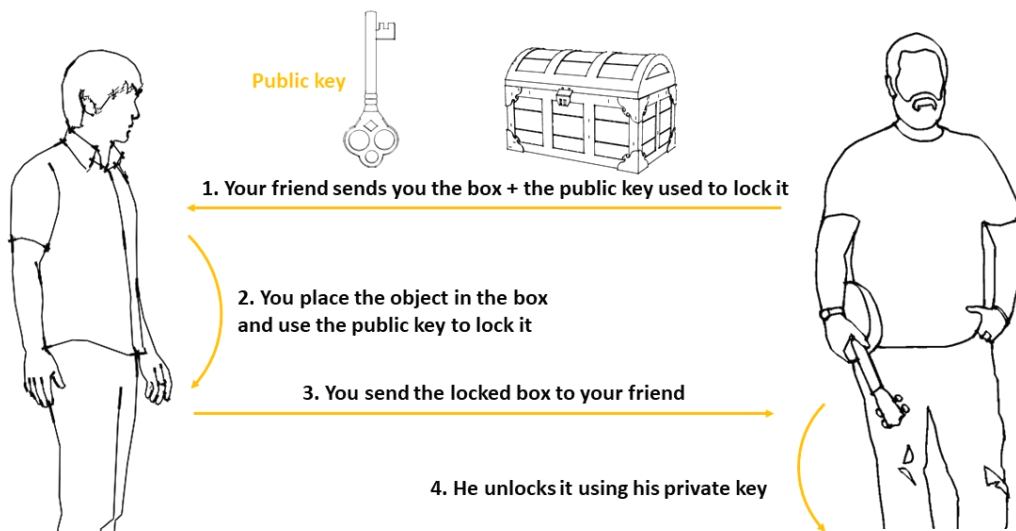
Asymmetric cryptography uses two keys for the encryption process, known as the public key and the private key. Asymmetric cryptography can also be referred to as ‘Public Key Encryption’ as the data being encrypted with the public key can only be decrypted with the private key. It helps visualize how this process is intended to work. Daniel Adetunji, a contributor to freeCodeCamp breaks down a great example of asymmetric cryptography, “Imagine you wanted to send something to your friend, but it was essential that nobody else, except your friend, could have access to that object. So, your friend buys an indestructible box so that you can place the object in it and have it sent. Your friend also sends you the key that can only be used to lock the box. Now, this box has one more special property. It has two keyholes. One keyhole to open the box, another to lock the box. Naturally, this box will also need two keys – one to open and another to lock it. As the sender of the object, all you have is the box to place the object in and a key to lock the box. Only your friend has the key that can unlock the box. The key used to lock the box is called the public key, and cannot be used to open it, as that requires the private key. If anyone

## CRYPTOGRAPHY & ENCRYPTION: BEHIND THE MAGIC

intercepted the package and made a copy of the public key, it could not be used to open the box, only to lock it. Only the person who holds the private key can open the box.” (Adentunji, D. 2023).

**Figure 2.2**

### *Asymmetric Cryptography Example*



*Note.* Visualization of the asymmetric encryption process.

Asymmetric is used when two or more individuals are involved in the exchange. Its focus is to encrypt data that is being transmitted. This is why asymmetric is paired with symmetric in TLS/SSL protocols for websites to provide security to users accessing the content.

### 2.3 Hashing Techniques

## CRYPTOGRAPHY & ENCRYPTION: BEHIND THE MAGIC

Hashing techniques have a realm of their own. Hashing functions/algorithms do not necessarily encrypt large amounts of data or protect data while it is in transit. The reason for this is that once text has been hashed, it is not possible for it to be ‘un-hashed’ into the original text. Hashing is commonly used in securing passwords in databases and file systems. For example, when you are logging into your computer, and you need to enter a password to gain access. When entering your password, the computer will take your entered password and process it through the hashing algorithm and if the hashes match (user input password hash matches the system’s stored password hash), then you are able to login. Another technique that utilizes hashing is the ability to verify the integrity of a file. For instance, let’s say someone wanted to download the latest release of the Nobara Linux Distribution. When accessing their downloads page, you are presented with a sha256sum file that can be used to verify that the file you are wanting to download, and install has not been altered or tampered with.

### Figure 2.3

*Current Release for Nobara iso (Nobara Linux, 2023)*

Current Release:

Nobara-38-GNOME-2023-08-29.iso:

sha256sum:

[7c08740b98d435970a6118ecc578e8aeb302ee0b77243d51f46532926baa9b51 Nobara-38-GNOME-2023-08-29.iso](#)

Download

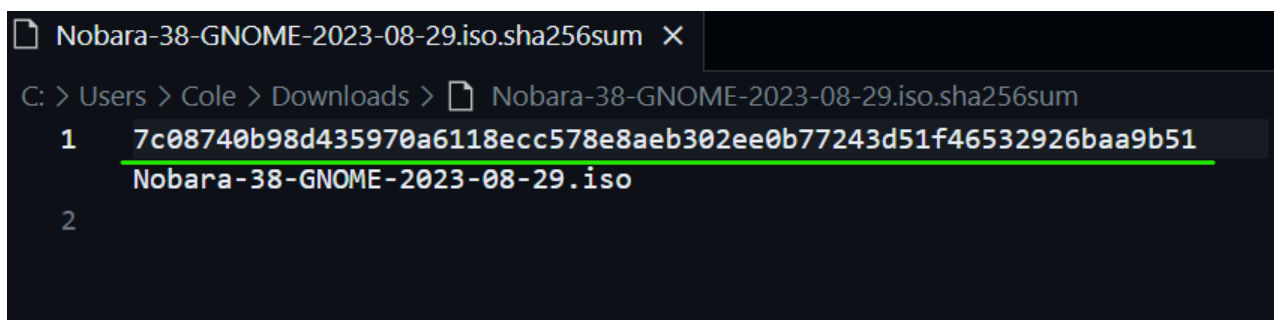
*Note.* Nobara’s sha256sum file can be viewed in the link in the image or downloaded via the link.

## CRYPTOGRAPHY & ENCRYPTION: BEHIND THE MAGIC

The user can calculate the hash of the zipped file locally (using built in hashing functions) and then compare the hashes from Nobara's website and their hash generated locally to ensure the integrity of the zipped file.

**Figure 2.4**

*Downloaded Nobara sha256sum file.*



The screenshot shows a file explorer window titled 'Nobara-38-GNOME-2023-08-29.iso.sha256sum'. The address bar shows the path 'C: > Users > Cole > Downloads > Nobara-38-GNOME-2023-08-29.iso.sha256sum'. The file content is displayed as follows:

```

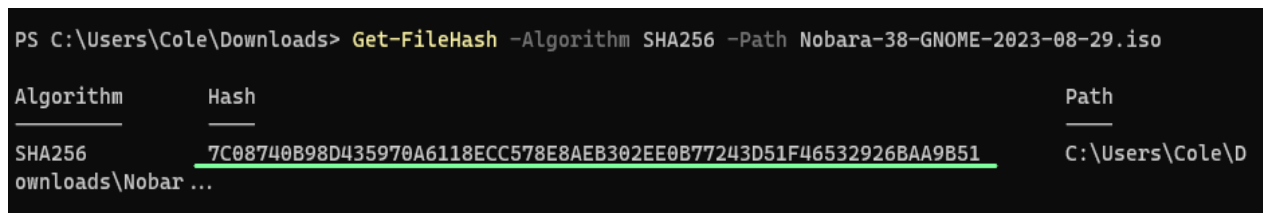
1  7c08740b98d435970a6118ecc578e8aeb302ee0b77243d51f46532926baa9b51
   Nobara-38-GNOME-2023-08-29.iso
2

```

*Note.* Downloaded sha356sum file from Nobara's official website and are presented with the underlined hash.

**Figure 2.5**

*Hashing the Zipped File Locally to Match the Hash on Nobara's Website*



The screenshot shows a Windows Command Prompt window with the following command and output:

```

PS C:\Users\Cole\Downloads> Get-FileHash -Algorithm SHA256 -Path Nobara-38-GNOME-2023-08-29.iso

```

Algorithm	Hash	Path
SHA256	<u>7C08740B98D435970A6118ECC578E8AEB302EE0B77243D51F46532926BAA9B51</u>	C:\Users\Cole\Downloads\Nobara...

*Note.* Using Windows Command Prompt, we can use the 'Get-FileHash' command to generate a hash of the targeted file. Command: 'Get-FileHash -Algorithm <algorithm to use> -Path </path/to/zipped-file>'

## CRYPTOGRAPHY & ENCRYPTION: BEHIND THE MAGIC

From the images above, we can verify that the hashes do match as we hashed the zipped file 'Nobara-38-GNOME-2023-08-29.iso' and generated the matching hash shown on Nobara's website (underlined string of numbers above the file name in Figure 2.4). The 'Get-FileHash' command is used in Windows PowerShell while passing in the hashing algorithm type from the '-Algorithm' flag and passing in the zipped file to be hashed from the '-Path' flag. SHA256, is a hashing algorithm that is pretty much the gold standard for cryptographic hashing methods, and this will be covered in more detail later in the next section.

## CHAPTER 3

## ENCRYPTION ALGORITHMS

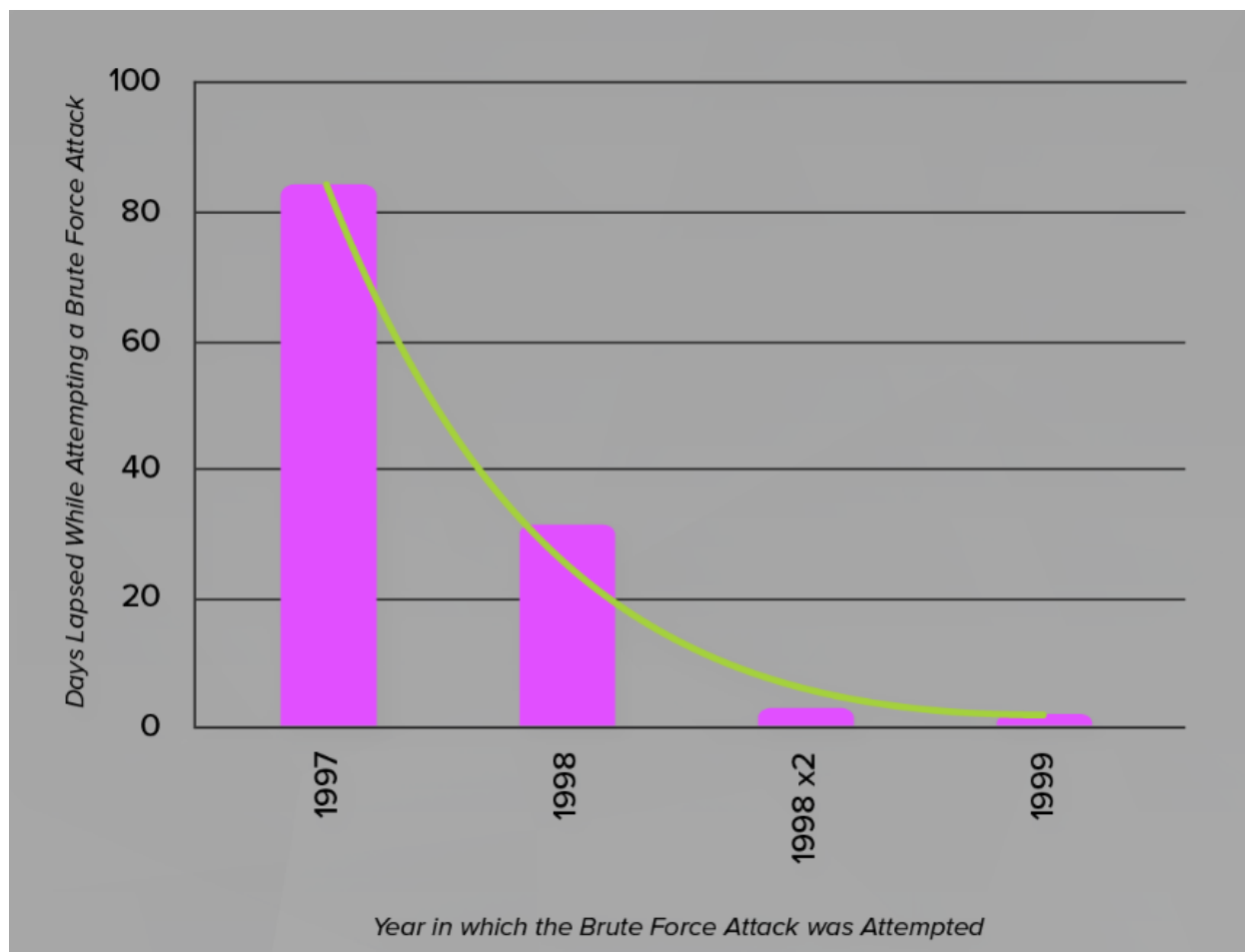
Numerous encryption algorithms have been created over time to help secure and protect data. In the previous chapter, various techniques were observed such as symmetric, asymmetric, and hashing. Throughout this chapter, research will be conducted on the algorithms like the Data Encryption Standard (DES) and Advanced Encryption Standard (AES) for symmetric encryption, the Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC) algorithm for asymmetric encryption, and the Message-Digest (MD5) and the Secure Hashing Algorithms (SHA) for hashing. With the analysis of the algorithms for each technique, a better idea of how these techniques work together to secure information can be understood.

## 3.1 Symmetric Algorithms

DES, also known as the Data Encryption Standard, was the peak of encryption technology at its time as it was the product of research from a team at IBM. In 1977 DES was announced as the new standard for encryption in the United States. DES is a symmetric block cipher that uses a 56-bit key to encrypt with an extra 8-bits added in case of errors (see Appendix A). How this algorithm encrypts its content is by taking in a fixed-length string of plaintext and converting it into a cipher text string that is the same fixed length. DES was very popular among hardware implementations for single users such as storing files or encrypting hard drives. (EC-Council, 2023, pg. 2039). However, due to inherent security issues with DES, most organizations and enterprises prefer to use alternative methods like AES to combat the vulnerabilities found in DES such as the weak key size which can be brute forced with modern computing power.

**Figure 3.1**

*Days Taken to 'Brute Force' DES Encryption*



*Note.* The image shows the decline of security in DES as brute force attacks were able to crack encryption faster as the years progressed.

Days Taken to 'Brute Force' DES Encryption (Larson, M. 2014)

(<https://info.townsendsecurity.com/hs-fs/hubfs/Brute-Force-DES.png?width=1400&name=Brute-Force-DES.png>)

## CRYPTOGRAPHY & ENCRYPTION: BEHIND THE MAGIC

Due to the security issues around DES, a new encryption standard was introduced known as the Advanced Encryption Standard (AES). AES (See Appendix B), also known as ‘Rijndael’, was chosen by the US government due to its robust algorithm. AES became the new standard in 2001 after a 3-year testing period which consisted of many competitors, but AES was the clear choice for the standard as AES can use multiple key sizes in its cryptographic methods. This allows organizations like the government to use different key lengths (128-bit, 192-bit, 256-bit) for different levels of confidentiality. For example, top secret material would require 256-bit keys due to the contents and less sensitive data/documents may only require a 128-bit key. (Bertaccini, M. 2022). To this day, the AES algorithm is widely implemented into hardware and operating systems to provide encryption methods. Microsoft’s BitLocker and Apple’s FireVault for Mac all use a version of AES encryption to provide user security. AES is still the standard for the United States and many claim it to be one of the best encryption algorithms ever developed. (Bertaccini, M. 2022)

### 3.2 Asymmetric Algorithms

Moving out of symmetric methods and venturing into more robust algorithms, a significant encryption method used for asymmetric cryptography is the Rivest-Shamir-Adleman (RSA) algorithm. EC-Council explains, “Ron Rivest, Adi Shamir, and Leonard Adleman formulated RSA, a public-key cryptosystem for Internet encryption and authentication.” (EC-Council, 2023, pg. 2100). The algorithm uses modular arithmetic and number theories to perform encryption using two large prime numbers. RSA is very popular and often referred to as an encryption standard as well. Top companies incorporate RSA into hardware and operating systems alongside AES (symmetric encryption) to provide secure cryptographic methods. RSA is also considered to be the most practical technique available for digital signatures (signing of a



## CRYPTOGRAPHY & ENCRYPTION: BEHIND THE MAGIC

message to verify it) as the scheme provides message recovery as well. (EC-Council, 2023, pg. 2100).

Elliptic Curve Cryptography (ECC) provides a more advanced and futuristic look into asymmetric encryption techniques. One of the cons with RSA is the need for very large key sizes. ECC promises to provide the same amount of security as RSA, but with smaller key sizes which would reduce overall costs and other overheads. How the algorithm works is by making use of Elliptic Curves that draw values from their variables and coefficients from finite fields. With the same quality of security and much lower costs, the US National Security Agency has already endorsed ECC and is using it for the protection of classified information with a key size of 328-bits. (Musa, S. M. 2018). For reference, “The largest ECC system to be broken to date is a 108-bit system, whereas the largest RSA system broken so far is a 512-bit system. The computational effort required to break the 108-bit ECC system was about 50 times the effort required to break the 512-bit RSA system.” (Musa, S. M. 2018).

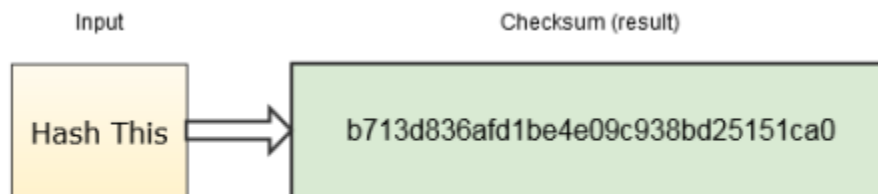
### 3.3 Hashing Algorithms

The MD5 (Message Digest 5) algorithm was a hashing function developed in 1991. For its time, MD5 was a trusted algorithm, but as time progressed security issues started to arise. This is due to the collisions found in the digest. A collision is where you take in two different inputs but generate the same hash for each of the different inputs. Author Farhad Ahmed Sagar detailed this quote on collisions found in MD5, “Den Boer and Bosselaers first found collisions in MD5 in 1993. In March 2004 a project called MD5CRK was initiated to find collision in MD5 by using a ‘Birthday Attack’. The project stopped as early as August 2004 after Xiaoyun Wang, Dengguo Feng, Xuejia Lai, and Hongbo Yu showed an analytical attack that only takes one hour on an IBM p690 cluster. For security reasons details of their method was not

published.” (Sagar, F. A. 2016).

**Figure 3.2**

*MD5 Hashing function.*



*Note.* Hexadecimal representation of input by MD5. (Sagar, F. A. 2016).

Much like AES stepping in for DES, MD5 would soon be superseded by a new hashing algorithm known as the Secure Hashing Algorithm (SHA) which is specified in the Secure Hash Standard and published as a Federal Information-Processing Standard.<sup>1</sup> Even though SHA is slower than MD5, its larger message digest makes it much more secure against brute-force collisions and inversion attacks. (EC-Council, 2023, pg. 2107). There are currently three generations of the SHA algorithm (SHA-1, SHA-2, SHA-3) and you can often find a SHA function being coupled with an asymmetric/symmetric algorithm to provide a secure cryptographic system.

---

<sup>1</sup>(FIPS PUB 180) Is the Secure Hash Standard for hashing algorithms to be used to generate message digests. (EC-Council, 2023, pg. 2107).

## CHAPTER 4

## SaaS ENCRYPTION &amp; OPEN-SOURCE CRYPTOGRAPHY

In this section, analysis of Software as a Service applications (SaaS) will be analyzed on their cryptographic methods as well as a brief look into open-source encryption tools to host encrypted data locally or via the cloud. With coverage on previous topics such techniques and algorithms, a better understanding of these methods can be observed which can lead to assurance on the methodology being adopted by leading organizations that offer SaaS as a primary product.

## 4.1 SaaS Encryption Methods

Storing files and media in the cloud or with third party companies has grown exponentially. The ease of use and mobility of these applications is a driving factor, but how well do they protect the users stored information? Let's look at Dropbox and observe the encryption methods they implement to ensure user security. According to Dropbox's official website, they currently use AES256-bit as well Secure Sockets Layer/Transport Layer to protect data between Dropbox apps and their servers. SSL/TLS creates a secure tunnel with a 128-bit or higher AES algorithm.<sup>2</sup> (Dropbox, 2023). Users can also add two-step verification to provide an extra layer of security. For the most part, Dropbox provides a robust cryptographic system to protect their users from security breaches. However, there are some things to consider before migrating to SaaS providers to manage your data. Most of these have a monthly subscription for starters. Dropbox has a starter plan for \$11.99/month, which includes one user, 2 TB of storage, file delivery up to 2 GB, and 30 days to restore files previously deleted. (Dropbox, 2023). For the everyday user, this option is great as it comes with a lot of disk space as well as extra security

---

<sup>2</sup>Secure Sockets Layer (SSL) manages the security of message transmission on the internet and Transport Layer Security (TLS), provides a secure/private connection from client to server. (EC-Council, 2023, pg. 2134).

## CRYPTOGRAPHY & ENCRYPTION: BEHIND THE MAGIC

Benefits. It all matters what the user is willing to pay for, and after analyzing Dropbox's methods and pricing, it does seem to be a suitable option for a hands-off approach or due to limited resources on the user's side.

Following, Google Drive is another top-ranking SaaS popular among the globe. Google states that Drive, Docs, Sheets, and Slides are encrypted at rest and in transit with AES256 bit encryption. Additionally, users may encrypt their data further with Workspace Client-side encryption, but to use the advanced functionality you must use a Workspace account, the administrator must enable client-side encryption, and identify verification must be completed. (Google, 2023). Google does offer up to 15 GB of storage with their base plan, and a subscription is not needed. However, you can upgrade storage with options of 100 GB for \$1.99/month, and their top personal plan being 2 TB \$9.99/month provides many affordable options for data storage while also knowing you're the contents are secure.

### 4.2 Open-Source Encryption Tools

Open-source projects are used in many enterprise applications as well as for personal use. The beauty of open-source projects is that they are free to use and completely customizable. Most open-source encryption technologies allow the user to encrypt their data locally rather than transferring documents to the cloud and relying on the SaaS encryption methods. However, users can still transfer encrypted files into the cloud with open-source tools to enhance their security further. An incredibly lightweight and easy to use tool to encrypt files securely and safely in your browser is the Hat.sh project. Hat.sh runs locally in your browser (<https://hat.sh>) and allows you to upload files and folders to be encrypted with the XChaCha20-Poly1305 symmetric algorithm.<sup>3</sup> You have the option to use a password as the key and or generate keys to be used for the

---

<sup>3</sup>The XChaCha20-Poly1305 is a symmetric authenticated cipher with associated data. It works with a 32-byte secret key and a nonce which must never be reused across encryptions performed under the same key. (PyCryptodome, 2023).

## CRYPTOGRAPHY & ENCRYPTION: BEHIND THE MAGIC

encryption and decryption process. Hat.sh can also be self-hosted in a ‘Docker’ container or with the ‘npm’ software library. (Hat.sh, 2022)

Moving out of lightweight tools, let’s investigate a project that allows you to encrypt drives on your local computer with open-source encryption. VeraCrypt is a free open-source, on-the-fly disk encryption program available for Windows, Mac OSX, and Linux. The service is based on TrueCrypt (now a part of Microsoft’s BitLocker) but has enhanced security features and a more accessible user interface. VeraCrypt comes with a great creation wizard to help guide the user through the process and right out of the box it allows you to encrypt the system partition which your OS is installed, create an encrypted file container, and or encrypt external drives like a USB flash drive. The option of being able to encrypt your system drive is a great alternative, as Windows 11 Home edition does not come with encryption features. The methods used by VeraCrypt are a symmetric algorithm for encryption at rest and hashing algorithm for integrity and validation (AES256 & SHA-512 by default). With a large variety of options and plenty of information detailing each cipher, users can also pick the encryption and hashing algorithms from a large variety of options and plenty of information detailing each cipher. (VeraCrypt, 2023).

## CHAPTER FIVE

## METHODOLOGIES &amp; COUNTERMEASURES

Whether running an enterprise security team or protecting sensitive files on a personal computer, understanding the magic of cryptography can help determine the best methods and techniques to protect and secure data. It is important to note that encryption is not a solution to all security concerns, but rather a resource to aid and advance security. Throughout this section, various methodologies and countermeasures will be suggested based on previous research which can help security professionals understand and implement safe and secure cryptographic methods.

## 5.1 Methods and Standards

Creating a cryptographic system at the enterprise level is a strategic process and when dealing with user information, organizations must adhere to the standards to maintain compliance. For a basic example, let's say we have a medical billing company that needs a cryptographic system to secure sensitive documents and payments. For a general overview, we will focus on providing encryption techniques for three areas such as data at rest, data in transit and key management. Since we are working in the medical industry, we must ensure or consider that we are following standards for the medical industry such as HIPAA (Health Insurance Portability and Accountability Act of 1996). According to cyber enthusiast, Anwita, "As per subpart 164.132 of title 45 in HIPAA, covered entities and business associates must implement a mechanism to encrypt or decrypt protected health information wherever applicable or appropriate." (Anitwa, 2023).

## CRYPTOGRAPHY & ENCRYPTION: BEHIND THE MAGIC

For data at rest, HIPPA suggests that AES128 or greater be used. We can secure the data at rest by encrypting the full drive that stores the public health information. A greatly trusted algorithm we can use for this is AES256 in CBC (Cipher Block Chaining) mode. AES256 will provide adequate security as well as following the protocols for data at rest from the National Institute of Standards and Technology. For further layer of encryption, we can add another symmetric AES128 algorithm to encrypt associated files and folders within the drive

While employees are interacting and updating the databases or customers are making payments, the data being transmitted will need to be protected as well. For this we will follow the SSL/TLS protocols. With this method we can encrypt the transmitted data with an asymmetric algorithm/public key algorithm, hashing function and a symmetric algorithm with the use of a cipher suite.<sup>4</sup> We will utilize a cipher suite in TLS 1.3 which is safer, as they do not list the authentication algorithm (servers' certificate) in the suite. Due to this, only the bulk cipher (usually for encrypting drives/symmetric) and the MAC (Message Authenticated Code) algorithm are listed: TLS\_CHACHA20\_POLY1305\_SHA256. Let's break down this cipher to understand the algorithms being used. For bulk encryption, much like Hat.sh, we are using the CHACHA20\_POLY1305 algorithm which uses a smaller key to handle faster encryption and decryption processes. Next, the SHA256 hashing algorithm is being used to verify the integrity of the data being transmitted to ensure it has not been tampered with. With this level of encryption, we can ensure that connections to transmit data will be encrypted, and the user can trust the server being accessed. (Kiprin, 2022).

---

<sup>4</sup>Borislav Kiprin, explains, "A cipher suite is a set of algorithms used to secure a connection via the TLS or SSL protocols between clients and servers. When initiating a connection, clients and servers will perform a handshake.". (Kiprin, 2022).

## CRYPTOGRAPHY & ENCRYPTION: BEHIND THE MAGIC

Lastly, we must implement a key management system. This will allow us to separate the keys from the data to provide more flexibility. There are a few options, but for this we will focus on using an open-source tool called, “HashiCorp Vault” to manage. The project allows us to easily store secrets, credentials, and certificates safely and securely. We can also implement this into a cloud provider to reduce our overhead such as “Linode” or “Azure” to host our key management system. (HashiCorp Vault, 2023). With a strong cryptographic strategy, data in all stages can be confidently protected.

### 5.2 Countermeasures and Risks

Based on the findings and research many cryptographic methodologies can be adequate for securing information. However, even with a robust system, cryptography is not a one stop shop for security. Attackers can still target systems with various cryptanalysis methods to draw a strategic plan to crack the encryption. Luckily, with previous research, extensive countermeasures can be applied to help mitigate risk. Since we implemented a few versions of symmetric algorithms, the best practice to follow would be to ensure a key size of at least 168 bits is used, and for more sensitive material a 256-bit key should be used. Also, since we are storing our key management system in the cloud, no keys should be present in our source code. Lastly, professionals can add redundant cryptosystems within the infrastructure to encrypt the data multiple times to layer security. (EC-Council, 2023, pg. 2173). Touching on our cipher suite used in the previous section, since we are using TLS 1.3, this is already a great countermeasure as the 1.3 cipher suite is much safer option as it does not showcase all the techniques or algorithms used in the suite. TLS 1.3 does not show the servers certificate, for example, 1.2 displays a cipher suite as: TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256. Where, ‘DHE’



## CRYPTOGRAPHY & ENCRYPTION: BEHIND THE MAGIC

and 'RSA' display the authentication algorithm/servers' certificate being used. Now, we look at

1.3: TLS\_AES\_128\_GCM\_SHA256, here we can see the cipher suite is much shorter than the

1.2 cipher suite and the authentication algorithm is not displayed. With limited information being displayed, attackers can find it more difficult to try and carry out an attack. (Kiprin, 2022)

## CRYPTOGRAPHY & ENCRYPTION: BEHIND THE MAGIC

### CONCLUSION

To conclude, advancements have been made in the cryptographic world with more secure algorithms and techniques. AES is the gold standard when it comes to compliance and overall security. From the analysis, we can see that most enterprise's use some form of AES to encrypt data and AES is also trusted and endorsed by the US government. Eventually, a time will come like AES taking over DES, where a new algorithm will be developed to combat with the everlasting advancement of technology. Quantum computing is also under massive research and once fully developed it could crack many asymmetric and symmetric algorithms commonly used today. However, many techniques are being developed known as quantum-safe cryptography methods to combat the concerns of quantum computing. For now, many modern cryptographic methods have withstood the test of time and continue to provide security for all. After comprehensive analysis of techniques, I hope a clearer understanding of cryptography is conveyed to help better equip professionals and consumers with the mathematical magic behind cryptography.

## References

- Adentunji, D. (2023, Apr 5). *Symmetric and Asymmetric Key Encryption – Explained in Plain English*. freeCodeCamp. <https://www.freecodecamp.org/news/encryption-explained-in-plain-english/>
- Adentunji, D. [Digital Image]. (2023, Apr 5). *Symmetric and Asymmetric Key Encryption – Explained in Plain English*. freeCodeCamp. <https://www.freecodecamp.org/news/encryption-explained-in-plain-english/>
- Anwita. (2023, May 27). *HIPAA Encryption Requirements: The Key to Protecting Patient Privacy*. Sprinto. <https://sprinto.com/blog/hipaa-encryption-requirements/#:~:text=HIPAA%20requirements%20for%20data%20at,provides%20adequate%20levels%20of%20protection.>
- Arcserve. (2023). *5 Common Encryption Algorithms and the Unbreakables of the Future*. Arcserve. <https://www.arcserve.com/blog/5-common-encryption-algorithms-and-unbreakables-future>
- Bertaccini, M. (2022). *Cryptography Algorithms: A guide to algorithms in blockchain, quantum cryptography, zero-knowledge protocols, and homomorphic encryption*. Packt Publishing
- Bokhari, M. U., & Shallal, Q. M. (2016). A Review on Symmetric Key Encryption Techniques in Cryptography. *International Journal of Computer Applications*. Vol. 147(10), 43-48. [https://www.researchgate.net/profile/Qahtan-Shallal/publication/333118027\\_A\\_Review\\_on\\_Symmetric\\_Key\\_Encryption\\_Techniques\\_in\\_Cryptography/links/5d21134a299bf1547c9ef4d0/A-Review-on-Symmetric-Key-Encryption-Techniques-in-Cryptography.pdf](https://www.researchgate.net/profile/Qahtan-Shallal/publication/333118027_A_Review_on_Symmetric_Key_Encryption_Techniques_in_Cryptography/links/5d21134a299bf1547c9ef4d0/A-Review-on-Symmetric-Key-Encryption-Techniques-in-Cryptography.pdf)

## References

Britannica. (2023, Oct 13). *Enigma German code device*. Britannica.

<https://www.britannica.com/place/Bletchley-Park>\_ Buchanan, W. J., Li, S., & Rameez, A. (2017). Lightweight Cryptography Methods. *Journal of Cyber Security Technology*. Vol. 1(3-4), 187-201. <https://doi.org/10.1080/23742917.2017.1384917>

Caesar Cipher 1 [Digital Image]. (2023). Red Hat. [https://www.redhat.com/rhdc/managed-files/caeser-cipher\\_1.png](https://www.redhat.com/rhdc/managed-files/caeser-cipher_1.png)

Dropbox. (2023, Sep 01). *How Dropbox keeps your files secure*. Dropbox.

<https://help.dropbox.com/security/how-security-works>

EC-Council (2023). Certified Ethical Hacker (CEH) Version 12 eBook w/ CyberQ Labs (Volumes 1 through 4) (2<sup>nd</sup> ed.). International Council of E-Commerce Consultants (EC Council). <https://bookshelf.vitalsource.com/books/9798885931717>

GeeksforGeeks (2023). *Data encryption standard (DES) / Set 1*. GeeksforGeeks. <https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/>

GeeksforGeeks (2023). *Round Keys for AES*. GeeksforGeeks. <https://media.geeksforgeeks.org/wp-content/uploads/20210729155115/aesfull.png>

Google (2023). Get started with encrypted files in Drive, Docs, Sheets & Slides. Google Docs Editor. <https://support.google.com/docs/answer/10519333?hl=en&co=GENIE.Platform%3Ddesktop&oco=0#zippy=%2Cadd-encryption-to-a-document>

HashiCorp Vault. (2023). *Manage secrets and protect sensitive data with Vault*. HashiCorp Vault. <https://www.vaultproject.io/>

Hat.sh. (2022). *Simple, fast, secure client-side file encryption*. Hat.sh. <https://github.com/sh-dv/hat.sh>

## CRYPTOGRAPHY &amp; ENCRYPTION: BEHIND THE MAGIC

## References

How the Enigma Works [Digital Image]. (2023). Nova | PBS.

<https://www.pbs.org/wgbh/nova/article/how-enigma-works/>

Kiprin, B. (2022, Jan 10). *What are TLS/SSL Cipher Suites and how to order them*. Crash-test security. <https://crashtest-security.com/configure-ssl-cipher-order/>

Larson, M. [Digital Image]. (2014, Sep 14). *WHAT ARE THE DIFFERENCES BETWEEN DES AND AES ENCRYPTION?* Townsend Security and Data Privacy Blog.

<https://info.townsendsecurity.com/bid/72450/what-are-the-differences-between-des-and-aes-encryption>

Musa, S. M. (2018). *Network Security and Cryptography*. Mercury Learning and Information.

Nobara Linux. [Digital Image]. (2023, Aug 29). *Download Nobara*. Nobara.

<https://nobaraproject.org/download-nobara/>

PyCryptodome (2023). *ChaCha20-Poly1305 and XChaCha20-Poly1305*. PyCryptodome.

[https://pycryptodome.readthedocs.io/en/latest/src/cipher/chacha20\\_poly1305.html](https://pycryptodome.readthedocs.io/en/latest/src/cipher/chacha20_poly1305.html)

Sagar, F. A. (2016). *Cryptographic Hashing Functions – MD5*.

<https://cs.indstate.edu/~fsagar/doc/paper.pdf>

Sidhpurwala, H. (2023, Jan 12). *A Brief History of Cryptography*. Red Hat Blog | Red Hat.

<https://www.redhat.com/en/blog/brief-history-cryptography>

Symmetric-key algorithm [Digital Image]. (2023). Wikipedia.

[https://en.wikipedia.org/wiki/Symmetric-key\\_algorithm](https://en.wikipedia.org/wiki/Symmetric-key_algorithm)

VeraCrypt. (2023). *What does VeraCrypt bring to you?* VeraCrypt.

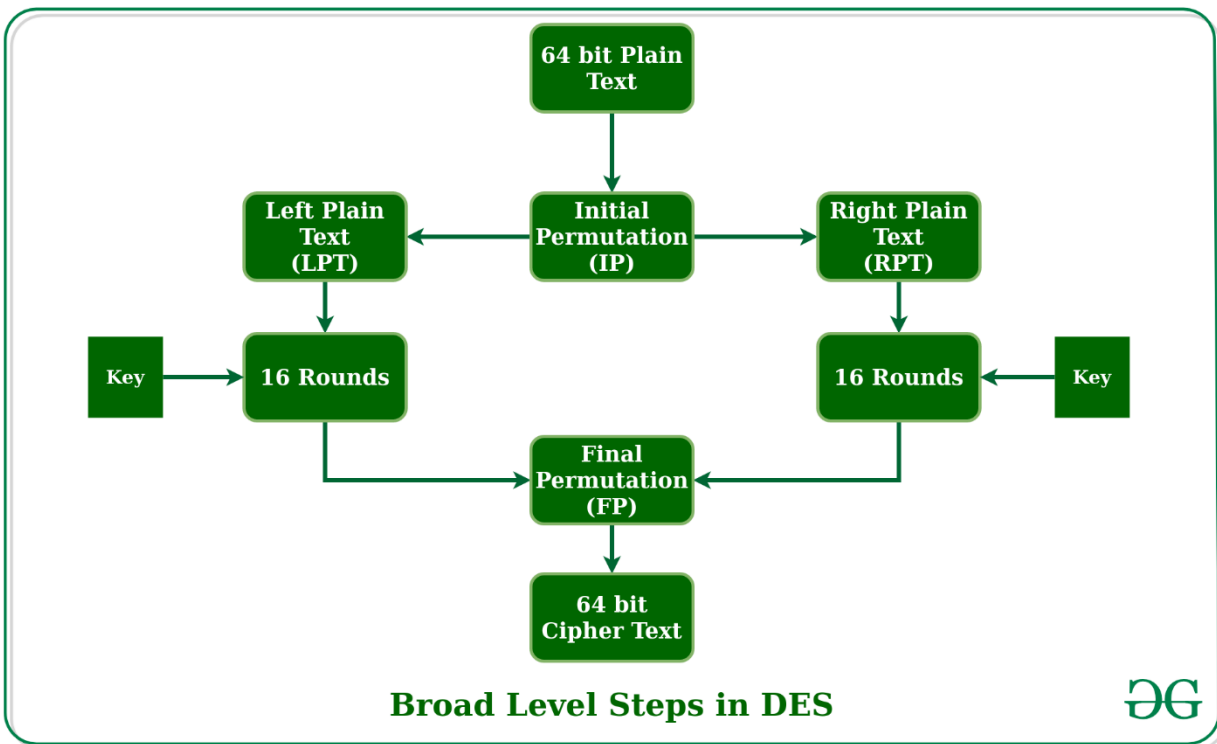
<https://www.veracrypt.fr/en/Home.html>

## Appendix A.

## DATA ENCRYPTION STANDARD (DES)

DES is a 16-round, 64-bit symmetric algorithm. The operations are performed by dividing the message, [m], into 64-bit blocks. The key is also an equal 64 bits. However, it is effectively only 56 bits (plus 8 bits for parity). With this technique, you are eventually able to check for errors. Finally, the output, (c), is 64 bits as well. (Bertaccini, M. 2022).

**Figure A1:** *Broad Level Steps in DES.*



*Note.* Visualization of the cryptographic process of the DES algorithm. (GeeksforGeeks, 2023).

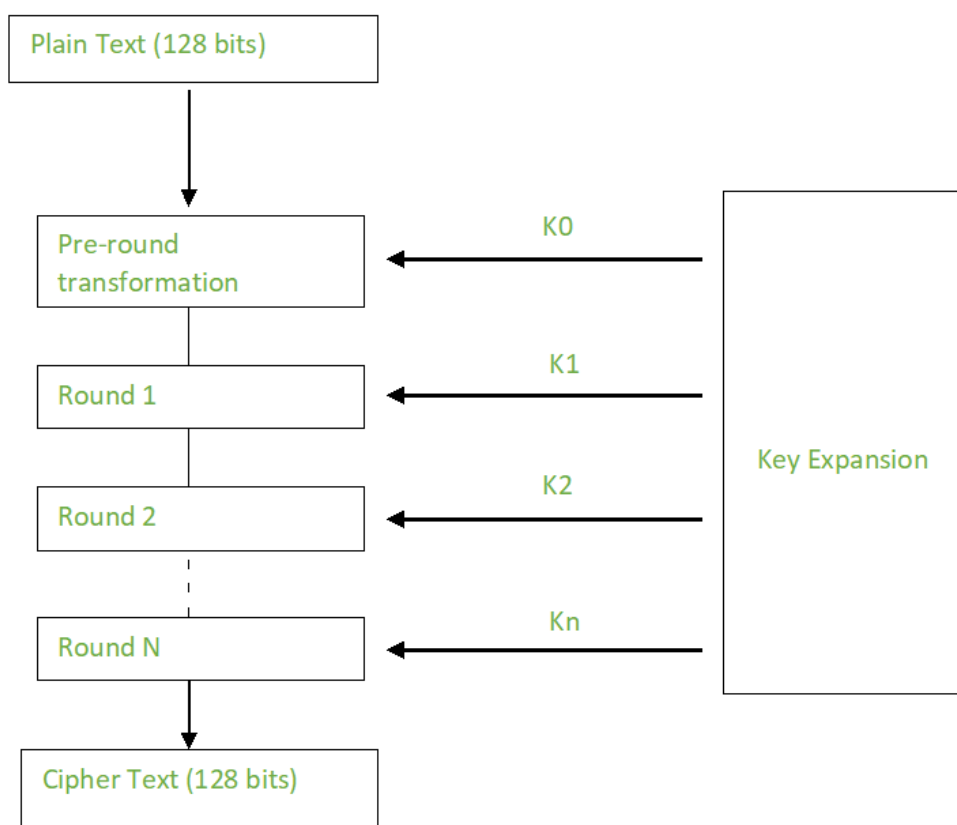
(<https://media.geeksforgeeks.org/wp-content/uploads/20200306124326/Steps-in-DES.png>).

## Appendix B

## ADVANCED ENCRYPTION STANDARD (AES)

AES is a block cipher that was created in 2001. It was the finalist amongst five contestants for the best algorithm and AES was known to be the clear winner. AES can be performed in various modes such as Cipher Block Chaining (CBC) and Cipher Feedback Block (CFB) to name a few. AES can also use different key sizes such as 128-, 192-, and 256-bit, which makes it a very robust and secure algorithm. (Bertaccini, M. 2022).

**Figure B2:** *Creation of Round Keys.*



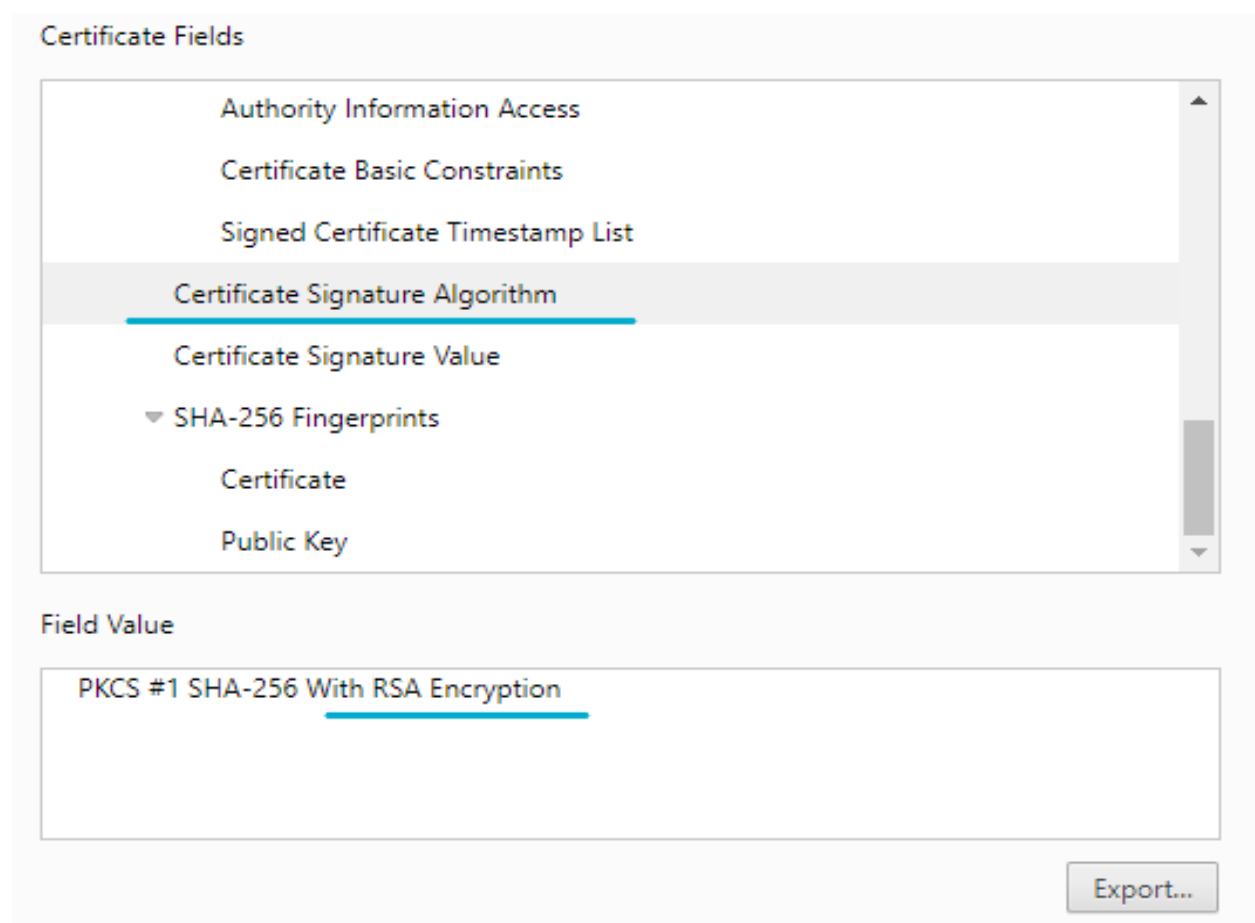
*Note.* The image shows the process of AES and visualizes the ‘Key Expansion’ for every round in the algorithm. (GeeksForGeeks, 2023). (<https://media.geeksforgeeks.org/wp-content/uploads/20210729155115/aesfull.png>)

## Appendix C

## RIVEST-SHAMIR-ADLEMAN (RSA)

RSA is an asymmetric encryption algorithm for internet functions and authentication. The RSA system is widely used in various products, platforms, and industries. It is one of the de facto encryption standards for the modern day. RSA can also be found securing operating systems as well as network interface cards on the consumer and enterprise levels. (EC-Council, 2023, pg. 2100). A great example of how to see where RSA is being used, is just to head to any https website and view the certificate details. In Figure C1, we can see the certificate algorithm for the website is ‘PKCS #1 SHA-256 With RSA Encryption.’

**Figure C1:** *Certificate information from https website*





## List of Figures

Figure 1.1: Caesar Cipher.....	5
Figure 1.2: Enigma Machine.....	7
Figure 2.1: Symmetric Encryption.....	9
Figure 2.2: Asymmetric Encryption.....	10
Figure 2.3: Current Release for Nobara ISO.....	11
Figure 2.4: Downloaded Nobara sha256sum file.....	12
Figure 2.5: Hashing the downloaded Zip file locally.....	12
Figure 3.1: Days Taken to 'Brute Force' DES.....	15
Figure 3.2: MD5 Hashing Function.....	18
Figure A1: Broad Level Steps in DES.....	30
Figure B1: Creation of Round Keys (AES).....	31
Figure C1: Certificate Information from HTTPS website.....	32