Application of Encryption Techniques towards the Networking & Communication Sector

IT19029146 - Eranda H.P.D
BSc (Hons) in IT Specialising in Cyber Security
Department of Computer Systems Engineering
Faculty of Computing
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka
dilshan0627@gmail.com

IT19040936 - S. M. Rathnayaka
BSc (Hons) in IT Specialising in Cyber Security
Department of Computer Systems Engineering
Faculty of Computing
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka
samadhimadushani98@gmail.com

IT19029214 - J. C. Hapuarachchi
BSc (Hons) in IT Specialising in Cyber Security
Department of Computer Systems Engineering
Faculty of Computing
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka
jayanichamodhi11@gmail.com

IT18220902 - Mandhanayaka D. D
BSc (Hons) in IT Specialising in Cyber Security
Department of Computer Systems Engineering
Faculty of Computing
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka
dilshandhananjaya@gmail.com

***Abstract*—With the massive development of new technology, today we all are living in a modern technological era. However as a side effect of this technological renaissance, the amount of cyber crimes have risen up drastically. Those cyber attacks have impacted the Networking & Communication sector in a more catastrophic manner than ever before. So in this mini-research paper, the main focus is set on studying practical aspect of using various encryption techniques in order to protect the networking & communication sector from various cyber attacks.**

In this particular mini-research paper, first we are going to take a holistic view of the entire networking & communication sector and different threats towards it. Then, we are going to explain about the significance of the encryption in network & communication sector. In here, we are explaining on how the data is transferred over the networks & various threats that are related with it. In order to explain certain incidents, we have used several referencing materials as well. Under the Methodology section, we have comprehensively explained about the Symmetric Encryption & the Asymmetric Encryption. Furthermore, we have compared and contrasted the main highlighting differences between those 2 different encryption techniques. At the end of this mini-research paper, we have provided the necessary references according to the IEEE standards.

***Index Terms*—Threats, Vulnerabilities, Safeguards, Risk Appetite, Confidentiality. Integrity, Non-Repudiation, Authenticity, End-to-End Encryption, Symmetric Cipher, Asymmetric Cipher, Steganography.**

I. Introduction

With the rapid development of the modern technology, today we all are living in a more advanced technological era. As we all know, currently the whole world is experiencing a massive pandemic situation which is Covid-19. As a result of that, most of the companies in worldwide have decided to force their employees to follow the “work-from-home” concept. However, with the massive popularity & the adaptation of the “work-from-home” concept, the number of cyber security related incidents have risen up in a more catastrophic manner.

When compared with other industry fields, the Networking & Communication sector has always been a target of the cyber criminals since from the very beginning. However with the current technological improvement, the cyber attackers are capable of getting their hands on various hacking related tools very easily. So, this particular situation has impacted the networking & communication sector immensely. According to M. Kaelin in [1], a particular network or a communication system can never be made immune to cyber attacks. The only solution that is left for the security engineers is reducing the risk level up to their specific risk appetite.

In order to comply with the current security standards & protocols, various kinds of cryptographic algorithms are used specially when transferring electronic data over the internet. Using cryptographic techniques have become a vital necessity in network & communication sector since it ensures the confidentiality. integrity, non-repudiation & authenticity of the data that is being transferred. Encryption, Hashing, Digital Certificates, Steganography are considered as some of the major examples for fundamental cryptographic techniques. According to Simplilearn in [2], Encryption is considered as the most common & the most effective fundamental cryptographic technique among all the other cyber security safeguards.

According to Simplilearn in [2], data encryption is the process of converting data from human-readable format to non-readable format. As it was mentioned previously, the main goal of data encryption is to preserve the CIA triad of the data. When it comes the data encryption, mainly there are 2 types of data encryption techniques.

- **Symmetric Encryption**
- **Asymmetric Encryption**

When it comes to the encryption, mainly there are 5 major encryption algorithms that are being commonly used in the modern cyber security community.

- **Advanced Encryption Standard (AES)**
- **Triple DES (Data Encryption Standard)**
- **RSA**
- **Blowfish**
- **Twofish**

In most of the case scenarios, encryption is more commonly used in the communication sector in order to prevent a third party from listening or intercepting the data that is being transferred over the network. Due to the massive amount of cyber threats towards the communication sector, most of the organizations are moving towards the much more secure **end-to-end encryption** mechanism. According to the Team Kaspersky in [3], organizations like Zoom and Whatsapp have already implemented this particular technique for their respective applications. End-to-end encryption ensures the confidentiality & integrity of the messages by making the data undecryptable by anyone other than the recipient. So, all those various encryption techniques & examples prove the vital necessity of the encryption in the network & communication sector.

II. Review of Literature

The **encryption method** is considered to be the **most secure cryptographic technique** when to comes to the data security. Kamaljit Lakhtaria noted in his research paper [4], that national security agencies and large financial institutions have long used cryptography and encryption to protect their sensitive data. Today encryption is used in a significant range of industries as well as a growing number of applications and platforms. Simply put, encryption have emerged as the most popular technology in the IT security; The question now is whether IT companies are ready to face this transformation and lay the foundation for their future needs.

According to Jyothi, V. in [5], network **encryption is used to protect the network and data transmission over a wireless network.** Data security is one of the most important features of wireless network data transfer. Network security includes the security of the terminal system as well as the entire network system. According to the Research paper "Analysis of Encryption for Network Security" [5], As the world shifts to the digital world, network security is a key issue. Network Security provides security for admin managed data. Enhancing communication technology requires secure communication that must be met by various encryption technologies, such as **encryption, digital signatures, watermarking, steganography, and other applications.**

It is unfair to underestimate the importance of encryption technology in networking and communication, especially in protecting our public and private networks. Emails, medical records, private company information, data on personal purchase patterns, legal documents, credit history and transactions, and government and regulatory agency databases are all protected. Protecting this data is essential for peace of mind when transmitting commercial and personal information [6]. To keep data safe, it is important to encrypt data as a means of translating data into another format or another language that provides the highest level of security. As mentioned above over the network, many organizations today use different data encryption methods to secure data transmission. According to the "research paper Encryption and Its Importance to Device Networkin", the U.S. government has mandated that all organizations have a certification system to protect data transmissions.

Encryption plays a key role in network security as well as communication. Symmetric key and public key encryption methods have long been used to encrypt sensitive information. With the advancement of technology various algorithms and encryption technologies can be seen. As the risk to information increases over time, more advanced encryption methods will have to be used in the future. There are still people who are not aware of the importance of encryption. It is therefore essential to teach the importance of security and encryption methods for the information. According to Milton Kazmeyer in [7], third parties can spy on your communications and track your online discussions and activities because the Internet provides many opportunities to engage with friends, coworkers, and even total strangers. Using encryption technologies can help keep your communication secure, whether you're sharing sensitive talks with a friend or making critical business arrangements with a customer. It can be seen that **many messaging applications used in the business world and personal life use end-to-end encryption mechanism to secure communication.** It is very much obvious, the demand for encryption is growing. There for with the increasing use of encryption technology in the future, we can expect better security for networking and communication.

III. Methodology

According to M. Rouse in [8], encryption is simply a method that can be used to convert some information into a text that is not understandable and will hide the true meaning of the information. When encryption and decryption both come together it is known as **cryptography**. Unencrypted data is known as **plain text** and encrypted data is known as **cipher text**. When performing encryption and decryption a set of steps are followed. These steps are known as Encryption Algorithms or Ciphers. The ciphers have a variable which is a key. According to the number of keys used the encryption mechanisms can be categorised as either **Symmetric Cipher or Asymmetric Cipher**. Symmetric cipher uses a single

key when performing encryption and decryption while Asymmetric cipher uses two keys as public key and private key.
According to J. Sanders in [9], encryption helps to achieve secure communication. It can protect data either when data is in transit or data is stored. When an unauthorized person gets hold of data in transit, if the data is encrypted then the malicious person need to find the key as well as the algorithm used to understand what the data really means.

Encryption helps to secure data in transit by providing various security requirements such as;

- **Confidentiality**
  - An unauthorized person will not be able to understand the content within the data.
- **Authentication**
  - The receiver can verify whether the sender he is expecting have sent the data.
- **Integrity**
  - Proves that the message is not altered while transferring.
- **Non-Repudiation**
  - The sender cannot deny that he/she sent the message.

A. Symmetric Cipher

This is the cipher in which the **same key is used for encryption as well as decryption.** These kinds of ciphers are mainly used for message encryption. These are faster than asymmetric ciphers. The sender who encrypts the data should send the key to the receiver who decrypts the message. According to R. Riley in [10], to send keys asymmetric ciphers were used, the sender encrypts the message with the key and data won't be understood by anyone who do not have access to the key. When the person who have the key gets the message, he/she will decrypt the message by reversing the algorithm and using the key. *(Fig. 1.)*

Examples of Symmetric Ciphers are as following.

- **DES (Data Encryption Standard)**
- **3DES (Triple Data Encryption Standard)**
- **AES (Advanced Encryption Standard)**

Most widely used symmetric cipher is **AES**. The algorithm used in DES is secure enough even to use in present days. But a problem arose with the key length. **DES have a key length of 54 bits which can easily be brute forced.** As a solution for these problems **3DES** and **AES** got developed.

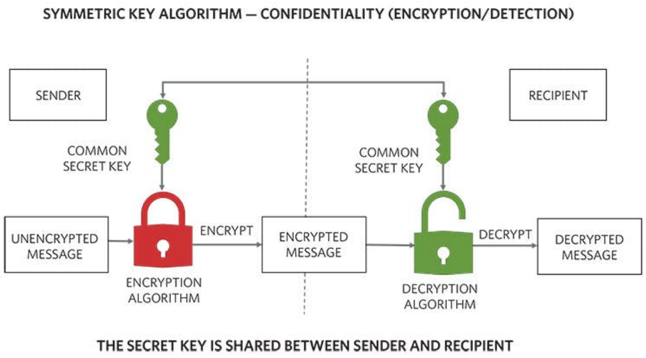

Fig. 1. Functionality of Symmetric Encryption

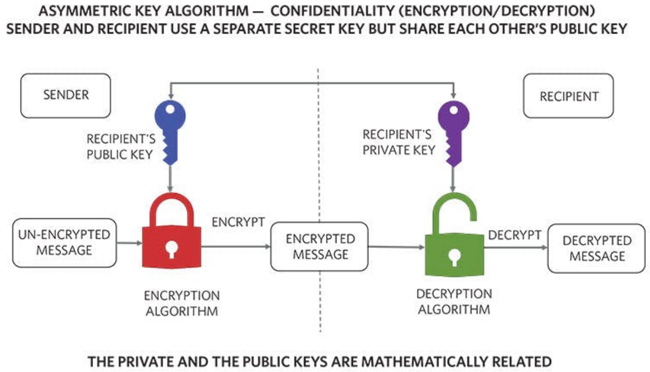
ASYMMETRIC KEY ALGORITHM — CONFIDENTIALITY (ENCRYPTION/DECRYPTION)
SENDER AND RECIPIENT USE A SEPARATE SECRET KEY BUT SHARE EACH OTHER'S PUBLIC KEY
SENDER
RECIPIENT
RECIPIENT'S PUBLIC KEY
RECIPIENT'S PRIVATE KEY
UN-ENCRYPTED MESSAGE
ENCRYPT
ENCRYPTED MESSAGE
DECRYPT
DECRYPTED MESSAGE
ENCRYPTION ALGORITHM
DECRYPTION ALGORITHM
THE PRIVATE AND THE PUBLIC KEYS ARE MATHEMATICALLY RELATED

Fig. 2. Functionality of Asymmetric Encryption

B. Asymmetric Cipher

This is the cipher in which **two keys are used for encryption and decryption.** There are 2 keys as **public key** and **Private key.** Both keys can be used for encryption as well as decryption. This kind of ciphers are mainly used for key exchange and digital signatures. If a message is encrypted by a private key, then the message should decrypted by his/her public key. If the message gets encrypted by a public key the message should be decrypted by his/her private key. *(Fig. 2.)*

Examples of Asymmetric Ciphers are as following.

- **RSA (Rivest Shamir Adleman)**
- **DSA (Digital Signature Algorithm)**
- **ECC (Elliptical Curve Cryptography)**

Although most of the times, both the Symmetric & Asymmetric Encryption do the same tasks at the end, they are not identical at all. Let's compare and contrast the main highlighting differences between the Symmetric Encryption & Asymmetric Encryption.(TABLE 1)

Security Service / Feature	Symmetric	Asymmetric
Confidentiality	Yes	Yes
Integrity	Yes	Yes
Non-Repudiation	Yes	Yes
Authentication	Yes	Yes
Speed	Fast	Slow
Complexity	Easy	Hard
Key Sizes (In Bits)	128, 192, 256	256, 1024, 2048

TABLE I
CRYPTOGRAPHIC ALGORITHM COMPARISON

IV. CONCLUSION

With the rapid growth of various cyber threats, network security has become a major issue. To protect data at transit, encryption can be considered as the most effective mechanism. With the development of technology and IT, new encryption mechanisms were developed. According to J. Sanders in [9], in the past, ancient people relied on symmetric ciphers, but with the development of digital communication, new and advanced encryption mechanisms got developed such as Asymmetric encryption. Symmetric Ciphers were very much effective to encrypt data before sending it to a receiver, but the problem was how to exchange the secret value which is the key. A secured communication channel was required to transfer the key from sender to receiver. As a solution for this, asymmetric encryption was introduced. To exchange the keys asymmetric ciphers were used and it is used in digital signatures as well. Digital signatures play an important role when it comes to communication.

AES is the most widely used asymmetric cipher. Though DES algorithm was secure enough, the key length of DES became a problem with the increasing computational power. It can easily be understood that encryption is an effective security mechanism that can be used for communication as well as for network security. Though many encryption mechanisms were introduced still there are people who do not understand the importance of encryption and what encryption can really provide. General public and the organizations should understand the importance of encryption and the security mechanisms that encryption provides to secure data. Encryption can be used to provide, Confidentiality, Integrity, Authentication and Non-repudiation. By using both symmetric ciphers and Asymmetric ciphers, communication security and network security will be increased. If proper encryption mechanisms are used, an unauthorized person will not be able to intercept a communication and understand the data that is transmitted. If an unauthorized person was unable to understand the communication, this will prevent an attacker from getting access to the network by stealing user credentials and other important information. No matter what kind of data is transmitted, either it is just a small communication between two parties or communicating very confidential information. The communication happened between any parties should not be accessed or understood by any unauthorized people.

Most of the organizations have started using encryption to protect their networks as well as the means of communications. It is a known fact that in the present day most of the messaging applications use end-to-end encryption. This clearly proves that people are becoming more aware about encryption and the importance of encryption. Though encryption mechanisms like DES was insecure, there are encryption mechanisms such as AES that can provide the required security that is enough for the present-day technologies. Also, the improved versions of DES such as 3DES is adequate enough to secure the communications and networks from unauthorized people.

ACKNOWLEDGMENT

As the 3rd year 2nd semester Cyber Security undergraduates at SLIIT, under the module IE3082 - Cryptography, we were asked to write a mini-research paper on **"The application of cryptographic techniques to a well-defined area within the computer science or any other engineering discipline"**. Furthermore mentioned, we were given the freedom to choose an appropriate field of industry and a specific cryptographic technique as per our desire. After having several discussion rounds with our group members, we have unanimously decided to choose **"Networking & Communication"** as our target field of industry and **"Encryption"** as our fundamental cryptographic technique. So I would like to make this an opportunity to thank our lecturer in charge Mr. Kavinga Yapa for giving us this wonderful opportunity to enhance our knowledge on various cryptographic techniques and its real-world applications.

REFERENCES

[1] M. Kaelin,"An absolutely secure network is not possible, but the risk can be managed" TechRepublic, Jun. 08, 2007. https://www.techrepublic.com/article/an-absolutely-secure-network-is-not-possible-but-the-risk-can-be-managed/ (accessed Sep. 30, 2021).

[2] simplilearn, "The Most Effective Data Encryption Techniques" Simplilearn.com, Mar. 26, 2020. https://www.simplilearn.com/data-encryption-methods-article (accessed Sep. 30, 2021).

[3] Kaspersky Team,"What end-to-end encryption is, and why you need it" Kaspersky.com, Sep. 11, 2020. https://www.kaspersky.com/blog/what-is-end-to-end-encryption/37011/ (accessed Sep. 30, 2021).

[4] Lakhtaria, Kamaljit. (2011). "Protecting Computer Network with Encryption Technique: A Study. 381-390. 10.1007/978-3-642-20998-7_47" (accessed Sep. 30, 2021).

[5] Jyothi, V. & Prasad, Dr & Mojjada, Dr. (2020). "Analysis of Cryptography Encryption for Network Security. IOP Conference Series: Materials Science and Engineering". 981. 022028. 10.1088/1757-899X/981/2/022028 (accessed Sep. 30, 2021).

[6] Lantronix, Inc., "Encryption and Its Importance to Device Networking," 2006. Accessed: Sep. 30, 2021. [Online]. Available: https://www.lantronix.com/wp-content/uploads/pdf/Encryption-and-Device-Networking_WP.pdf.

[7] M. Kazmeyer, "Types of Encrypted Communication," Chron.com, 2012. https://smallbusiness.chron.com/types-encrypted-communication-52746.html (accessed Sep. 30, 2021).

[8] M. Rouse,"What is encryption? Definition from WhatIs.com," SearchSecurity, 2019. https://searchsecurity.techtarget.com/definition/encryption (accessed Sep. 30, 2021).

[9] J. Sanders, "Encrypting communication: Why it's critical to do it well," TechRepublic, Jan. 08, 2018. https://www.techrepublic.com/article/encrypting-communication-how-and-why-to-do-it-well/ (accessed Sep. 30, 2021).

[10] R. Riley, "What is a Symmetric Cipher? — Security Encyclopedia," HYPR, Sep. 16, 2020. https://www.hypr.com/symmetric-cipher/ (accessed Sep. 30, 2021).