Received Date: 11 May 2021; Accepted Date: 22 June 2021; Published Date: 30 June 2021

Review on Cryptography Techniques in Network Security

Gan Hui Ching[1*] & Mohamad Fadli Zolkipli[2]

[1]*School of Computing, Universiti Utara Malaysia; gan_hui_ching@soc.uum.edu.my*
[2]*School of Computing, Universiti Utara Malaysia; m.fadli.zolkipli@uum.edu.my*

** Corresponding author*

To cite this article (APA): Ching, G. H., & Zolkipli, M. F. (2021). Review on Cryptography Techniques in Network Security. *Journal of ICT in Education, 8*(2), 125-135. https://doi.org/10.37134/jictie.vol8.1.10.2021

To link to this article: https://doi.org/10.37134/jictie.vol8.1.10.2021

Abstract

This article's aim is to provide an overview of network security encryption technologies. This article discusses the different types of cryptographic techniques, advantages, and disadvantages of cryptography on network security. First, we will go over the different cryptographic techniques' operational characteristics. The approach entails comparing and observing the outcomes of 20 different papers. The survey's findings would demonstrate the characteristics, advantages, and disadvantages posed by cryptographic technology, allowing the general public to gain a deeper understanding of the technology.

Keywords: cryptography, network security, symmetric-key algorithms, asymmetric-key algorithms.

INTRODUCTION

With the advancement and growth of the online world, the Internet has developed into everyone's everyday life, becoming borderless and trans-international. Nowadays, anybody can use the Internet to perform everyday tasks such as learning, working, and engaging in leisure activities, among other things. Because of the Internet's globalisation and transparency, everyone can freely access and appreciate the vast tools and convenience it provides. However, this exposes network security to a variety of risks, including hacker attacks, network viruses, and the dissemination of illegal and unverified information. As a result, network security has become a major subject of debate and interest around the world.

Cryptography is used to provide security services such as anonymity, data privacy, access protection, verification, and non-repudiation. It allows you to secure confidential information by converting it to incomprehensible text, which only the approved recipient can read (Faheem et al., 2017). In cryptography, there are three categories of algorithms: symmetric techniques, asymmetric techniques, and hash functions (Hassan, Khalid, & Khanfar, 2016). Secrete key is another name for symmetric key. On both the sender and receiver sides, only one key is used. The term "public-key cryptography"

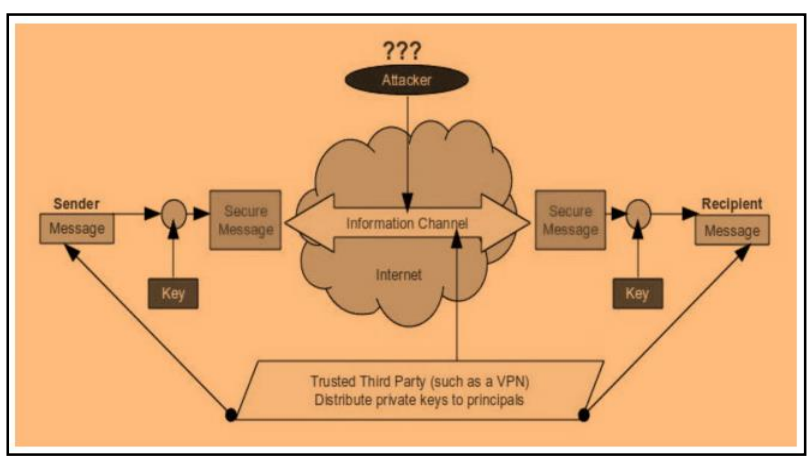
refers to asymmetric cryptography. On both the sender and receiver sides, separate keys are used (Sujatha & Ramya, 2018). In the field of cryptography, hash cryptography functions are a fundamental building block with applications ranging from message integrity and authentication to digital signatures and safe time stamping, among many others (Hossain et al., 2016).

Various encryption methods are used to improve information security. The evolution of encryption is leading to a world of an infinite number of possibilities. Since it is difficult to completely prevent hacking, we can use encryption methods to protect our sensitive data even if it is hacked (Amalraj & Jose, 2016). We will present a paper on cryptographic techniques based on some algorithm, their impact on network security, and the applications of cryptography techniques in this article. The following section is completed as follows. Section 2 introduces that literature review which related with network security and cryptography (symmetric algorithm and asymmetric algorithm). Section 3 summarizes with different types of cryptographic techniques. Section 4 explores discussion about the advantages and disadvantages of cryptography techniques on network security. Section 5 conclude this article in conclusion part and follow with acknowledgement.

LITERATURE REVIEW

Network Security

Network security oversees ensuring the security of all data sent from one device to another over the internet. Both software and hardware operations, accountability, functionality, administrative and administration, measures, characteristics, access control, information in a network, and operating procedures that secure software and hardware are referred to as network security (Sujatha & Ramya, 2018). The program should also understand the existence of confidentiality and integrity when developing network security. Confidentiality states that the non-authenticated party does not review the data, while Integrity is a certification that the information obtained by the collector has not been changed or modified after it was sent by the sender. Figure 1 shows the network security model (Sharma & Gupta, 2017).



Received Date: 11 May 2021; Accepted Date: 22 June 2021; Published Date: 30 June 2021

Figure 1: Network Security Model (Sharma & Gupta, 2017).

Cryptography

The term (cryptography) comes from the Greek terms Kryptos (secret) and graphein (writing). Cryptography can be described as the writing of confidential information or as a science or art that studies how data, information, and documents are translated into especially difficult-to-understand forms. Cryptography aims to protect data, records, and documents from being accessed by people who are not supposed to know about them (Babu, 2017). Cryptography is a method of storing and transmitting data in a special format such that only those who need it can read and process it (Tayal et al., 2017). The different kinds of cryptography that can be classified are symmetric techniques (also known as encryption of a private key) and asymmetric techniques (also known as encryption using a public key). Figure 2 shows the types of cryptography techniques (Sharma & Gupta, 2017).

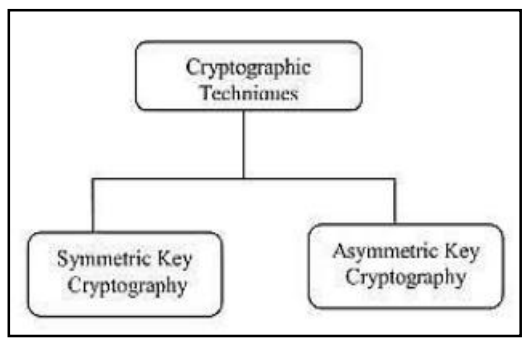


Figure 2: Types of cryptography techniques (Sharma & Gupta, 2017).

The oldest and most well-known method is symmetric algorithm. A secret key is added to the text of a message to alter the data in a certain way. It may be a number, a word, or a series of letters chosen at random. A key pair, which consists of two related keys, is used in an asymmetric algorithm. Your public key can be obtained from someone who wishes to send you a text. A second, private key is kept protected and accessible only to you (Sharma & Gupta, 2017).

a) Symmetric Algorithm

The term "symmetric algorithm" refers to encryption strategies in which the sender and recipient each have access to the same key (Sharma & Gupta, 2017). It is critical to devise a mechanism for exchanging secret keys over public networks that is both effective and safe. An asymmetric algorithm was developed to overcome the main distribution issue in symmetric algorithms (Mavroeidis, Vishi, & Jøsang, 2018). The example for symmetric algorithm which are AES, DES, 3DES, BLOWFISH and RC4 (Faheem et al., 2017; Hossain et al., 2016). Figure 3 shows the classification of symmetric algorithm (Mewada, Sharma, & Gautam, 2016).

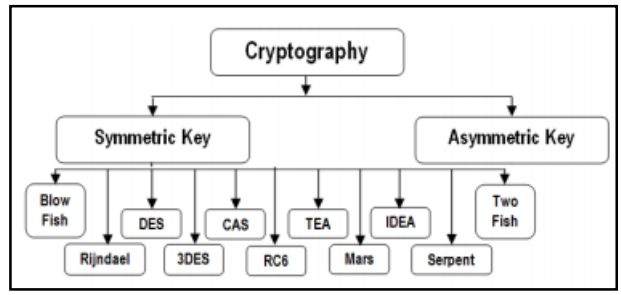


Figure 3: Classification of symmetric algorithm (Mewada, Sharma, & Gautam, 2016).

b) Asymmetric Algorithm

Asymmetric algorithms are cryptographic systems in which the sender and recipient each have access to the different key named public and private key (Mavroeidis, Vishi, & Jøsang, 2018). The plaintext is encrypted using the public key, while the unreadable text is decoded using the private key (Mohamad, Din, & Ahmad, 2021). Example for asymmetric algorithm which RSA and Diffie-Hellman (Adamovic et al., 2018; Chatzikonstantinou et al., 2016). Figure 4 shows the classification of asymmetric algorithm (Abood & Guirguis, 2018).

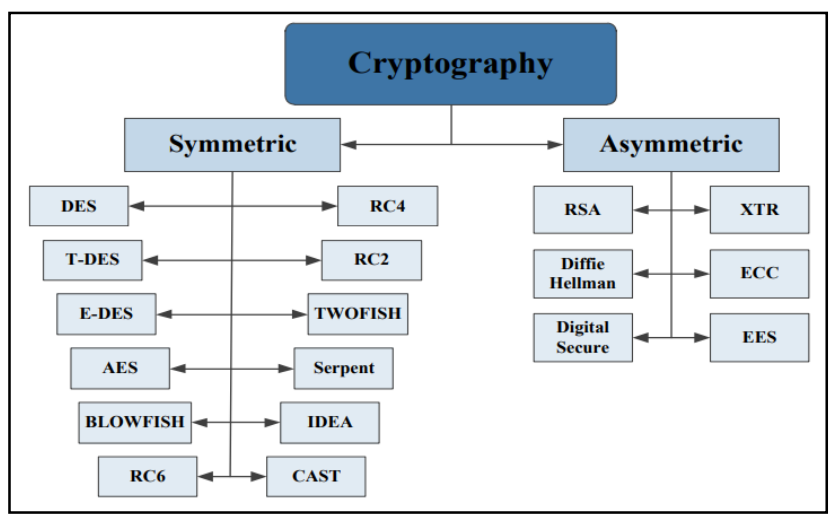


Figure 4: Classification of asymmetric algorithm (Abood & Guirguis, 2018).

TYPES OF CRYPTOGRAPHY TECHNIQUES

Cryptography techniques can be classified as symmetric algorithm and asymmetric algorithm. Table 1 shows the cryptography algorithms' characteristics (Hossain et al., 2016).

Table 1: Cryptography algorithms' characteristics (Hossain et al., 2016).

Scheme	Algorithm Type	Contributor	Key Length	Rounds	Block Size
AES	Symmetric	Rijindael	128,192, 256	10 or 12 or 14	128 bits
DES	Symmetric	IBM 75	56-bits	16	64 bits
3DES	Symmetric	IBM 78	168, 112 bits	48	64 bits
BLOWFISH	Symmetric	Bruce Schneier 93	128-448 bits	-	64 bits
RC4	Symmetric	Ronald Rivest 87	40-128-bits	-	-
RSA	Asymmetric	Rivest,Shamir, Adleman 77	1024	1	Minimum 512 bits
DSA	Asymmetric	NIST 91	-	-	-
Diffie-Hellman	Asymmetric	Diffie, Hellman 76	-	-	-
EI-Gamal	Asymmetric	Elgamal 84	-	-	-
Paillier	Asymmetric	Paillier 99	-	-	-
MD5	Hashing	Rivest 91	128	-	512 bit
MD6	Hashing	Prof. Rivest 08	-	-	-
SHA	Hashing	NIST 95	160	-	-
SHA256	Hashing	-	256	-	32 bit

Symmetric Algorithm

There are some examples for symmetric algorithm such as AES, DES and 3DES. The details will explain as below:

a) AES

The AES algorithm is a secret-key algorithm, which means that the same key is used for both encoding and decoding of files hacked (Amalraj & Jose, 2016). AES method encodes 10 rounds are needed for 128-bit keys between encryption and decryption. For 192-bit keys go 12 rounds and for 256-bit keys go 14 rounds to get the last encoded message (Abood & Guirguis, 2018). AES's characteristics include density of coding and pace through a diverse range of formats, as well as a straightforward interface and defence against all documented attacks. Figure 5 shows AES algorithm structure (Faheem et al., 2017).

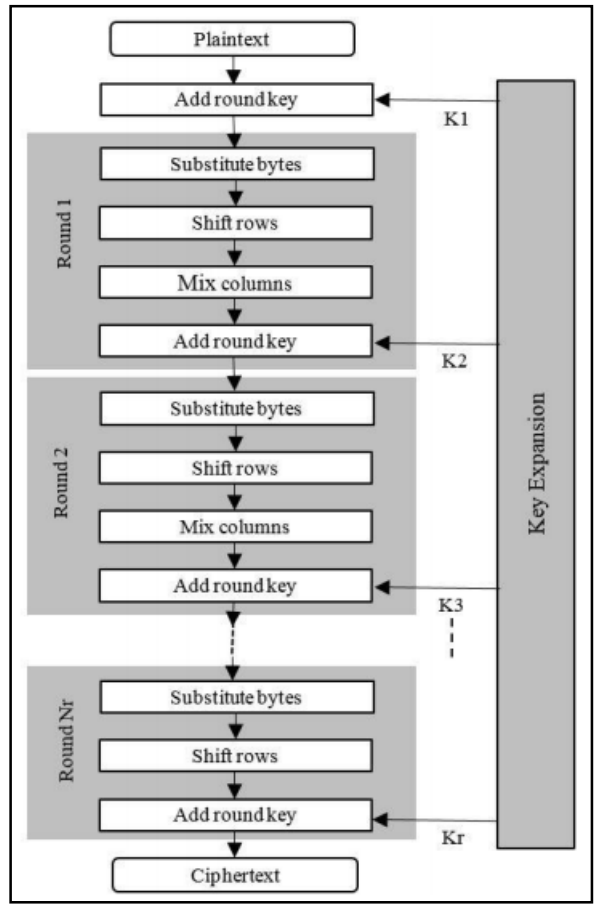


Figure 5: AES algorithm structure structure (Faheem et al., 2017).

b) DES

NIST has recommended DES as a symmetric block encryption standard. DES technique is the world's most commonly used encryption technique (Hossain et al., 2016). According to Davis R, the DES algorithm transforms a fixed length of plaintext bits into a cypher text bit sting of the same length, with each block being 64 bits long (Amalraj & Jose, 2016). Horst Fiestel was the first to implement DES to IBM in 1972. The DES algorithm's aim is to provide a strategy for securing critical financial databases (Abood & Guirguis, 2018). Figure 6 shows DES algorithm structure structure (Faheem et al., 2017).

Received Date: 11 May 2021; Accepted Date: 22 June 2021; Published Date: 30 June 2021

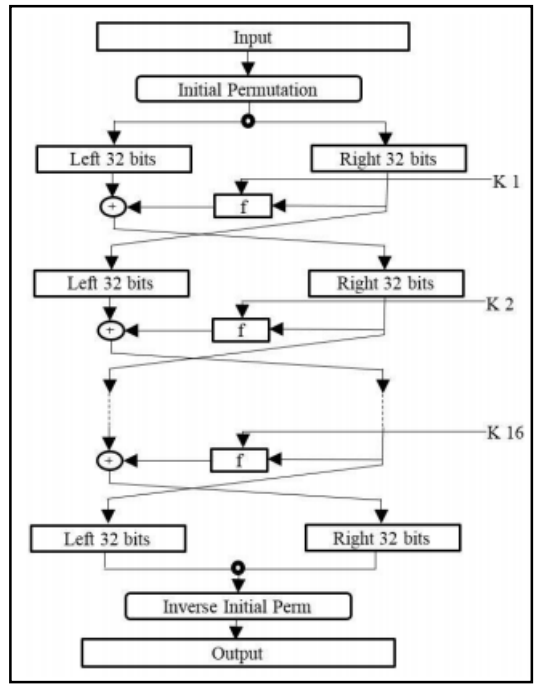


Figure 6: DES algorithm structure (Faheem et al., 2017).

c) 3DES

3DES is a symmetric-key block cypher that is like DES but has three times the degree of encryption. Consequently, compared to other block cypher methods, this method is slower. 3DES employs a 192-bit key and a block size of 64 bits (Hossain, et al., 2016; Amalraj & Jose, 2016; Abood & Guirguis, 2018). In terms of throughput, the 3DES algorithm is found to be less efficient than other algorithms (Akhil, Kumar, & Pushpa, 2017).

Asymmetric Algorithm

There are some examples for asymmetric algorithm such as RSA and Diffie-Hellman. The details will explain as below:

a) RSA

Rivest, Shamir, and Adleman invented the RSA technique. Public key and secret key are used in RSA. The public key, which is used to encrypt communications is accessible to all Messages encrypted with the public key can only be decrypted with the secret key. The RSA algorithm's keys can be generated in a lot of ways (Amalraj & Jose, 2016; Sharma & Gupta, 2017; Maqsood et al., 2017). There are a few steps for RSA algorithm which are Key Generation, Encryption and Decryption (Hossain et al., 2016). In today's world, RSA is the most common, efficient, and secure algorithm, and it's useful for network security (Hassan, Khalid, & Khanfar, 2016). Figure 7 shows RSA algorithm’s workflow (Abood & Guirguis, 2018).

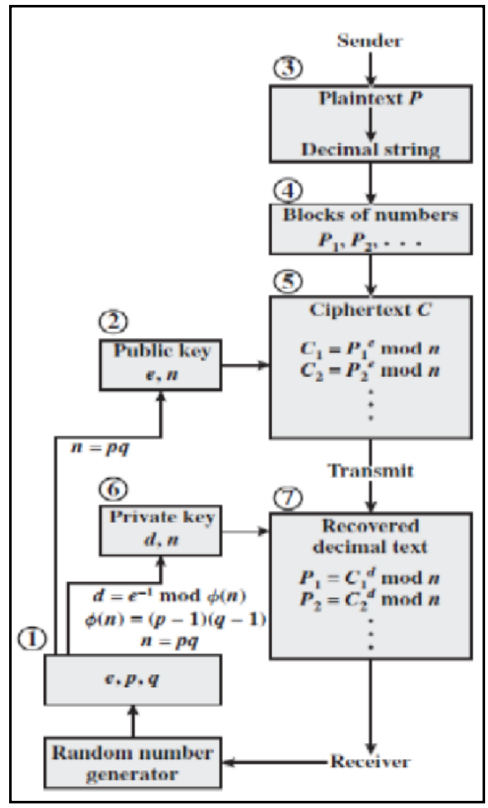


Figure 7: RSA algorithm's workflow (Abood & Guirguis, 2018).

b) Diffie-Hellman

Diffie-Hellman came up with this algorithm in 1976. The Diffie-Hellman algorithm allows two users to discover a common secret key and communicate over an insecure channel (Abood & Guirguis, 2018). Diffie-Hellman is an asymmetric cypher that employs the above property to securely transmit keys over the internet (Mavroeidis et al., 2018).

CURRENT TREND IN CRYPTOGRAPHY

Each new cryptographic standard defined and released by NIST in the academic world has taken anywhere from three to five years in the past. Transitions from two-key to three-key triple DES encryption took place from 2010 to 2015; transitions from RSA Key Transport and Digital Signature Generation and Verification using RSA1024 to RSA-2048 took place from 2010 to 2013; transitions for Key Derivation Functions took place from 2010 to 2015; and transitions from SHA-1 to SHA-256 took place from 2010 to 2013 (Connor et al., 2018).

Received Date: 11 May 2021; Accepted Date: 22 June 2021; Published Date: 30 June 2021

DISCUSSION

We will discuss the advantages and disadvantages of cryptography techniques on network security.

Advantages of Cryptography Techniques

According to the paper that found, there are some of the advantages for cryptography that can be detected. In Hassan, Khalid and Khanfar (2016) stated that the advantages for cryptography techniques are assurance of confidentiality, geographical limitations and retention and loss of data. After the information processor, the data is encrypted internally in the password storage method. The data of the consumer will be secured during this phase. This significantly decreases any legal risks that each customer and supplier may face. Besides that, information cannot be held in encrypted form during the encryption process, so any law-related knowledge would have a lower effect on customers. Customers can use cloud storage to provide and encrypt data, which can significantly reduce costs. The encryption service helps users to delete the remaining data after it has been deleted, making it more convenient for them.

Ubaidullah & Makki (2016) have summarized that the advantages of symmetric algorithms are symmetric-key cyphers could be designed to achieve high data throughput rates. Some hardware implementations can encrypt hundreds of megabytes per second, while software implementations can only get megabytes per second as throughput rates. Symmetric key cryptography can be combined to produce a more secure result. In addition, conversion is easy, and analysis is simplified. While there is a lot of knowledge about the field that needs to be understood and before the invention of the rotor machinery, the encryption of symmetric keys appears to have a large history.

Faheem et al. (2017) show that the advantages of 3DES which is one of the types of symmetric algorithm. It states that the main strength for 3DES is three times more secure with a key size of 2^{168} bits. Therefore, it provides sufficient information protection, but the disadvantage is that it takes longer to encrypt data than DES.

According to Table 1 in Mohammad, Din, & Ahmad (2021) explain that RSA is more stable and resistant to brute-force attacks. The public key is sent twice where each time separately and overwhelming contact. RSA added to the difficulty by making it highly safe and difficult to hack. In a high-security scenario, the RSA method for encryption and decryption is faster than the original algorithm for generating public and privacy keys with efficiency and readability.

Disadvantages of Cryptography Techniques

According to the paper that found, there are some of the disadvantages for cryptography that can be detected. According to Chatzikonstantinou et al. (2016), the weaknesses of cryptography can be divided into four categories: poor cryptography, weak implementations, weak keys, and weak cryptographic parameters. Weak cryptography refers to cryptographic algorithms that are used in

implementations considering the fact that their insecurity is well established. Unsafe implementations may be created by using or using cryptographic algorithms in a non-standard way or by failing to obey best practices. Weak cryptographic keys are used in situations where weak cryptographic keys are used that will be putting users' and applications' protection at risk. Weak cryptographic parameters refer to flaws caused by bad cryptographic parameter selection.

Madsood et al. (2017) explain that cryptography has a drawback in that it is only a criterion for output comparisons that encompasses common parameters. According to Praveena and Smys (2016), they state the key exchange problem with symmetric algorithms is that the two communication nodes must somehow know the mutual key before communicating safely while the time and space complexity of asymmetric algorithms is shown to be a weakness in Kapoor and Yadav (2016). Akhil, Kumar, and Pushpa (2017) also mention the limitations of symmetric algorithms, which are due to the large number of keys in a large network, necessitating the use of an unconditionally trusted TTP to properly handle it during period when keys are changed frequently. Simultaneously, the symmetric algorithm necessitates a broad key size in order to process the verification.

We will focus on symmetric and asymmetric algorithms like DES, 3DES, RSA, and Diffie-Hellman as examples. According to Mewada, Sharma, and Gautam (2016), DES is vulnerable to targeted attacks. In [5] show that 3DES need to spend much of time to solve the problem. Sharma & Gupta (2017) demonstrate that RSA encryption, a probabilistic encrypted data technique allows hackers to effectively carry out a known ciphertext threat on the cryptographic protocol. Follow with findgings from Abood & Guirguis (2018) that weakness for Diffie-Hellman is that contact takes place through it, which means it can be broken in the middle of an attack.

CONCLUSION

In conclusion, this paper determines the types of cryptography techniques, advantages and disadvantages of cryptography techniques on network security. The cryptography techniques can be divided into symmetric algorithm and asymmetric algorithm. The symmetric algorithm examples such as AES, DES, 3DES and asymmetric algorithm examples are RSA, Diffie-Hellman were discussed in the paper. All the advantages and disadvantages of symmetric algorithm and asymmetric algorithm that mentioned also will explained in this paper. In this paper, we can find that there are not the best cryptography techniques. This is because every cryptography technique has each advantages and disadvantages.

ACKNOWLEDGEMENT

The authors would like to thank to all School of Computing members who involved in this study. This study was conducted for the purpose of System and Network Security Research Project. This work was supported by Ministry of Higher Education Malaysia and Universiti Utara Malaysia.

REFERENCES

Abood, O. G., & Guirguis, S. K. (2018). A Survey on Cryptography Algorithms. *International Journal of Scientific and Research Publications (IJSRP), 8*(7), 495-516. https://doi.org/10.29322/ijsrp.8.7.2018.p7978

Adamovic, S., Sarac, M., Stamenkovic, D., & Radovanovic, D. (2018). The Importance of the Using Software Tools for Learning Modern Cryptography. *International Journal of Engineering Education, 34*(1), 256-262.

Akhil, K. M., Kumar, M. P., & Pushpa, B. R. (2017). Enhanced cloud data security using AES algorithm. Proceedings of the *2017 International Conference on Intelligent Computing and Control (I2C2)*, 2017, pp. 1-5. https://doi.org/10.1109/I2C2.2017.8321820

Amalraj, A.J., & Jose, J.R (2016). A Survey Paper on Cryptography Techniques. *International Journal of Computer Science and Mobile Computing, 5*(8), 55-59.

Babu, S.A. (2017). Modification Affine Ciphers Algorithm for Cryptography Password. *International Journal of Research in Science & Engineering, 3*(2).

Chatzikonstantinou, A., Ntantogian, C., Karopoulos, G., & Xenakis, C. (2016). Evaluation of Cryptography Usage in Android Applications. BICT'15: Proceedings of the *9th EAI International Conference on Bio-inspired Information and Communications Technologies* (formerly BIONETICS), 83-90. https://doi.org/10.4108/eai.3-12-2015.2262471

Connor, L., Dukatz, C., DiValentin, l., & Farhady, n. (2017). Cryptography in a post-quantum world", *Accenture.com, 2018. [Online]*. Available: https://www.accenture.com/us-en/insights/technology/quantum-cryptography.

Faheem, M., Jamel, S., Hassan, A., A., Z., Shafinaz, N., & Mat, M. (2017). A Survey on the Cryptographic Encryption Algorithms. *International Journal of Advanced Computer Science and Applications, 8*(11), 333-344. https://doi.org/10.14569/ijacsa.2017.081141

Hassan, N., Khalid, A., & Khanfar, K. (2016). A Survey of Cryptography Cloud Storage Techniques. *International Journal of Computer Science and Mobile Computing, 5*(2), 186-191.

Hossain, A., Hossain, B., Uddin, S., & Imtiaz, S. (2016). Performance Analysis of Different Cryptography Algorithms. *International Journal of Advanced Research in Computer Science and Software Engineering, 6*(3).

Kapoor, V., & Yadav, R. (2016). A Hybrid Cryptography Technique for Improving Network Security. *International Journal of Computer Applications, 141*(11), 25-30. https://doi.org/10.5120/ijca2016909863

Maqsood, F., Ahmed, M., Ali, M., & Shah, M.A. (2017). Cryptography: A Comparative Analysis for Modern Techniques. *International Journal of Advanced Computer Science and Applications, 8*(6). https://doi.org/10.14569/IJACSA.2017.080659

Mavroeidis, V., Vishi, K., D., M., & Jøsang, A. (2018). The Impact of Quantum Computing on Present Cryptography. *International Journal of Advanced Computer Science and Applications, 9*(3), 405-414. https://doi.org/10.14569/ijacsa.2018.090354

Mewada, S., Sharma, P., & Gautam, S. (2016). Classification of Efficient Symmetric Key Cryptography Algorithms. *International Journal of Computer Science and Information Security, 14*(2). https://doi.org/10.13140/RG.2.2.30465.66402

Mohamad, M. S. A., Din, R., & Ahmad, J. I. (2021). Research trends review on RSA scheme of asymmetric cryptography techniques. *Bulletin of Electrical Engineering and Informatics, 10*(1), 487–492. https://doi.org/10.11591/eei.v10i1.2493

Praveena, A., & Smys, S. (2016). Efficient Cryptographic approach for Data Security in Wireless Sensor Networks using MES V-II. Proceedings of the *2016 10th International Conference on Intelligent Systems and Control (ISCO)*. Coimbatore, India: IEEE. https://doi.org/10.1109/ISCO.2016.7726911

Sharma, S., & Gupta, Y. (2017). Study on Cryptography and Techniques. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2*(1), 249-252.

Sujatha, K., & Ramya, D. (2018). A Review Paper on Cryptography and Network Security. *International Journal of Pure and Applied Mathematics, 119*(17), 1279-1284.

Tayal, S., Gupta, N., Gupta, P., Goyal, D., & Goyal, M. (2017). A Review Paper on Network Security and Cryptography. *Advances in Computational Sciences and Technology, 10*(5), 763-770.

Ubaidullah, M., & Makki, Q. (2016). A review on symmetric key encryption techniques in cryptography. *International Journal of Computer Applications, 147*(10), 43-48. https://doi.org/10.5120/ijca2016911203