RES MILITARIS
REVUE EUROPEENNE D ETUDES EUROPEAN JOURNAL OF MILITARY STUDIES
Social Science Journal

Survey of different cryptography methods

By

Sarah H. Mnkash
Al Salam University College, Department of Criminal Evidence/Iraq
Email: Sarah.H.Mnkash@alsalam.edu.iq

Abstract

The current state of encryption algorithms will be discussed in this session, with a focus on private key block ciphers, which are frequently employed for link and bulk data encryption. We started by reviewing some of the more well-known and intriguing algorithms currently in use. This essay primarily examines the various encryption methods now in use and does a comparative analysis of them all as part of a literature review. Attempt a thorough experimental investigation of several implementations of the available encryption methods. also emphasizes information encryption methods and image encryption methods. This paper analyzes the security concerns with the performance parameters utilized in encryption operations.

Keywords: cryptography, Encryption method, Survey, Encryption Algorithm.

1. Introduction

The manner that individuals communicate data has been substantially impacted by the networking technologies' quick development. Because of this, hackers may duplicate the data and distribute it again. The information must therefore be safeguarded while it is being sent. Social security numbers, credit card numbers, and financial transactions are a few instances of sensitive data that needs to be protected. There are many different encryption technologies available to stop information theft. With a focus on wireless security, today's wireless communication significantly relies on encryption to safeguard data transfer online. Various encryption techniques are used to protect the secret data from being used without authorization. Encryption is one of the most widely used techniques for strengthening information security.

2. Basic Terms Used in Cryptography

1) Plain Text

Plain Text is the definition of the initial message that the sender desires to convey to the recipient. The actual message that needs to be sent to the other end is given a particular term in cryptography called Plain text [1].

2) Cipher Text

Cipher text is a term used to describe a message that no one can understand or a message that has no purpose. Prior to transmission of the real communication, cryptography transforms the original message into an unreadable message [2].

3) Encryption

Encryption is the process of changing Plain Text into Cipher Text. With the help of cryptography, private messages can be sent via an unsafe channel. A key and an encryption algorithm are needed for the encryption process. The method that has been employed in encryption is referred to as an encryption algorithm. Encryption happens on the sender's end [3].

4) Decryption

Decryption is the term for the opposite of encryption. Cipher Text is transformed into Plain Text throughout this process. Decryption is a method that cryptography employs to recover the original communication from an unreadable message at the receiving end (Cipher Text). A key and a decryption algorithm are needed for the decryption process. The process that has been employed in decryption is referred to as a decryption algorithm. The encryption and decryption algorithms are typically the same [4].

5) Key

A key might be a particular symbol or a text with numbers or letters in them. The Key is utilized both when the Cipher Text is being decrypted and when the Plain Text is being encrypted. The choice of key in cryptography is crucial since it directly affects the security of the encryption technique. Figure 1 depicts the encryption algorithm [5].

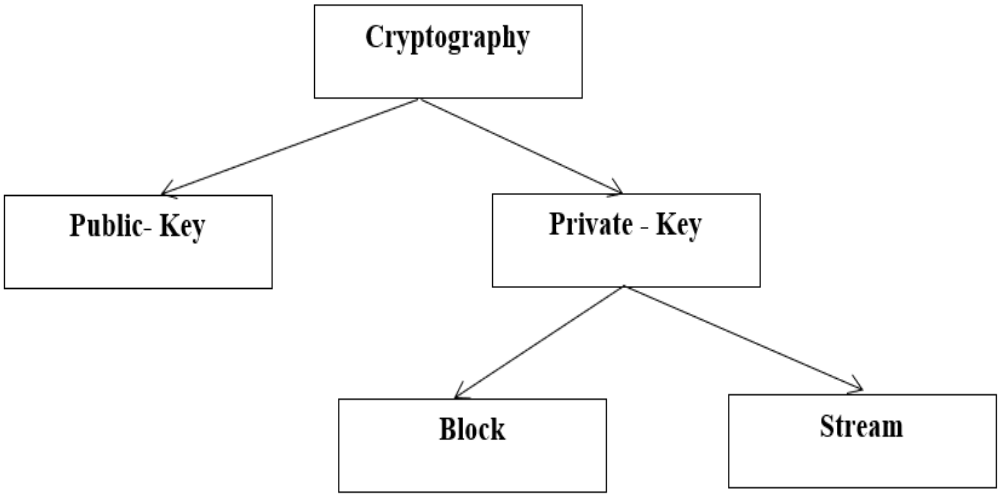

Fig.1 Encryption algorithm

3. Classification of Cryptography

Symmetric and asymmetric key encryption are the two basic categories into which encryption methods can be divided.

6) Symmetric-Key cryptography

In symmetric cryptography, the key used for encryption and decryption is the same key. Therefore, the key distribution must be done before the information is transmitted. Since the characteristics of the key, such as the key length, etc., directly affects the security of symmetric cryptography, the key is crucial. Many symmetric key algorithms exist, including DES [6]. Figure 2 illustrates symmetric-key cryptography.

7) Asymmetric-Key cryptography

Customers can transmit securely without any secret keys being granted in advance thanks to public fundamental protocols. In this arrangement, the party giving approval generates a leading pair (pk, sk). Using a public key pk, the message is encoded, and a private key is used to decode it. Asymmetric key algorithms include RSA [7], among others. Asymmetric-Key cryptography is depicted in Figure 3.

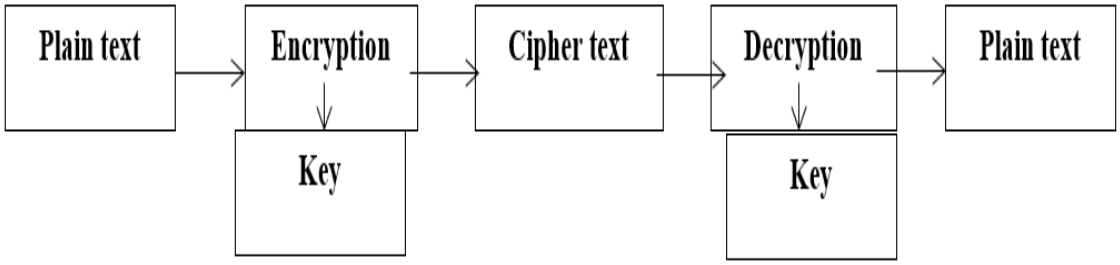

Fig.2 *Symmetric-Key cryptography*

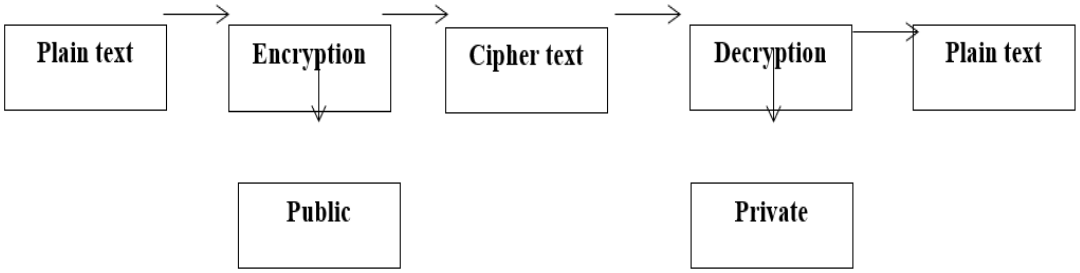

Fig.3 *A Symmetric-Key cryptography*

8) Cryptography security services

9) At that time, the following parts should be taken into consideration for data security [8].

1) Privacy.

2) Verification.

3) Data Reliability.

4) Message transfer between parties is ensured by the method.

5) Data's rights to access.

6) Availability

5. Literature review

The most prevalent algorithm implementation for both software and hardware technologies is discussed and examined in this article. Processing speed, throughput, power consumption, packet size, and data kinds are the characteristics taken into account.

Mutnuru et al. [8] A novel selective encryption-based security method that will protect data transmission even in networks without authentication. A security system based on selective encryption will also reduce the amount of time required for the encryption process, increasing efficiency. With the use of the DCT transform and the Number Puzzle approach, the image data being broadcast over a network is discriminated before being selectively encrypted to prevent unauthorized access. They talked about the advantages of numeric puzzle-based encryption over classical encryption for multimedia data security and integrity.

Sowmiya et al. [9] newly suggested algorithm Compared to previous algorithms and

the triple data encryption standard, this approach is safer and supports higher key sizes. Both in terms of hardware and software, AES is faster. They must submit a request in order to download a file from another branch. The admin will then process the request and provide the key to their email address. To transmit emails using transport layer security, we utilize Simple Mail Transfer Protocol as the mail transfer agent and port number 587. The user can receive the file after it has been decrypted using this key. This system is perfect for handling the massive amounts of data handled nowadays because of its improved efficiency, effective storage and transfer, speedy processing, and unbreakable security.

Purnama et al. [10] They altered the Caesar cipher technique, which results in encryption text that can be deciphered. If the cipher text can be read, cryptanalysis will not be suspicious of it. The Caesar cipher is modified by splitting the alphabet into two halves, substituting the vocals with the alphabet as well, and switching the consonant alphabet for a consonantal alphabet. Although some alphabet consonants are not changed, this is because Indonesian texts rarely use the alphabet on a regular basis. They managed to extract encrypted text that can be read, which prevented the cryptanalyst from being suspicious of the message and refraining from attempting to decipher the content.

Manasrah et al [11] Through the use of two private keys that are connected to the character positions (i.e., odd and even), they proposed an improved Caesar cipher method. One public key that will be sent to the recipient has the two private keys mapped onto it. The final findings demonstrate that a cryptanalysis attack on the new cryptosystem is unavoidable. The encryption text's size is also decreased, saving memory space. Utilizing binary matrices that are formed and shared by the two communication parties, it is demonstrated that the public key generation procedure is a one-way function.

Alexandru et al [12]. They looked at the issue of how to construct a Linear Quadratic Gaussian (LQG) controller on a distributed system while protecting the privacy of the measurements, state estimations, control inputs, and system model. The component sub-systems and actuator contract a cloud controller to handle the LQG calculation while encrypting their signals and matrices. Labeled homomorphic encryption is the method utilized, and it enables the evaluation of degree-2 polynomials on encrypted data by giving each piece of data a special label and making advantage of the actuator's knowledge of the external calculation. In the encrypted data, they wrote the state estimate update and control computation as multivariate polynomials and proposed an addition to the Labeled Homomorphic Encryption scheme that allows the evaluation of low-degree polynomials on encrypted data (Aydin, 2020).

Loyka et al [13]. They bring forth a homomorphic computation strategy that makes use of the ASCII data representation and the affine cipher. This is the first application of affine ciphers in homomorphic computing, to the best of the authors' knowledge. Both string operations (encrypted string search and concatenation) and arithmetic operations are supported by the scheme (encrypted integer addition and subtraction). In order to improve security, one of the suggested homomorphism's design objectives is to treat string and integer data equally.

Nassar et al [14]. They examined Paillier's encryption and its use for safe online voting and privacy-preserving compute outsourcing. With Python serving as the interface language and quick GMP C-routines doing the arithmetic operations, we propose a new implementation of Paillier's cryptosystem (Bakan, 2020; Bezwan, 2021).

Chakarov et al [15]. They put forth an algorithm that assesses the effectiveness of completely homomorphic implementations of arbitrary computer programs using the statistical

data acquired along with our mathematical model.

6. Conclusion

In the modern world, data security has taken on a significant role as a result of the regular transmission of digital goods via public networks for communication. The literature on encryption techniques has been reviewed in this paper. To improve the effectiveness of the encryption methods and to guarantee the security procedures, those encryption approaches have been thoroughly investigated and analyzed. In conclusion, real-time encryption can benefit from all of the strategies. Each technique is distinct in its own manner and may be appropriate for a variety of applications. Fast and safe conventional encryption techniques will always function with a high rate of security since new encryption techniques are constantly developed.

Reference

Sharma, D. K., Singh, N. C., Noola, D. A., Doss, A. N., & Sivakumar, J. (2022). A review on various cryptographic techniques & algorithms. Materials Today: Proceedings, 51, 104-109.

Ahn, J., Kwon, H. Y., Ahn, B., Park, K., Kim, T., Lee, M. K., ... & Chung, J. (2022). Toward Quantum Secured Distributed Energy Resources: Adoption of Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD). Energies, 15(3), 714.

Aydin, S. (2020). A Survey of the Roots and History of Kurdish Alevism: What are the Divergences and Convergences between Kurdish Alevi Groups in Turkey? *Kurdish Studies*, *8*(1), 17-42. https://doi.org/10.33182/ks.v8i1.551

Bakan, R. (2020). Socio-spatial dynamics of contentious politics: A case of urban warfare in the Kurdish region of Turkey. *Kurdish Studies*, *8*(2), 245-270. https://doi.org/10.33182/ks.v8i2.491

Zolfaghari, B., & Koshiba, T. (2022). The Dichotomy of Neural Networks and Cryptography: War and Peace. Applied System Innovation, 5(4), 61.

Kiya, H., Maung, A. P. M., Kinoshita, Y., Imaizumi, S., & Shiota, S. (2022). An overview of compressible and learnable image transformation with secret key and its applications. APSIPA Transactions on Signal and Information Processing, 11(1).

Zolfaghari, B., & Koshiba, T. (2022). Chaotic Image Encryption: State-of-the-Art, Ecosystem, and Future Roadmap. Applied System Innovation, 5(3), 57.

Bezwan, N. (2021). The state and violence in Kurdistan: A conceptual framework. *Kurdish Studies*, *9*(1), 11-36. https://doi.org/10.33182/ks.v9i1.582

Maniyath, S. R., & Thanikaiselvan, V. (2020). An efficient image encryption using deep neural network and chaotic map. Microprocessors and Microsystems, 77, 103134.

Orman, H. (2014). Recent parables in cryptography. IEEE Internet Computing, 18(1), 82-86.

Mutnuru, S., Sah, S. K., & Kumar, S. P. (2020). Selective encryption of image by number maze technique. Int. J. Cryptogr. Inf. Secur, 10(2), 1-10.

Sowmiya, M., Subeksha, S., Vanmathi, T., & Vidhupriya, P. (2020). INFORMATION SHARING ACROSS ORGANIZATION USING SYMMETRIC KEY ENCRYPTION.

Purnama, B., & Rohayani, A. H. (2015). A new modified caesar cipher cryptography method with legibleciphertext from a message to be encrypted. Procedia Computer Science, 59, 195-204.

Manasrah, A. M., & Al-Din, B. N. (2016). Mapping private keys into one public key using binary matrices and masonic cipher: Caesar cipher as a case study. Security and Communication Networks, 9(11), 1450-1461.

Alexandru, A. B., & Pappas, G. J. (2019, April). Encrypted LQG using labeled homomorphic encryption. In Proceedings of the 10th ACM/IEEE international conference on cyber-physical systems (pp. 129-140).

Loyka, K., Zhou, H., & Khatri, S. P. (2018, May). A Homomorphic Encryption Scheme Based on Affine Transforms. In Proceedings of the 2018 on Great Lakes Symposium on VLSI (pp. 51-56).

Nassar, M., Erradi, A., & Malluhi, Q. M. (2015, October). Paillier's encryption: Implementation and cloud applications. In 2015 International Conference on Applied Research in Computer Science and Engineering (ICAR) (pp. 1-5). IEEE.

Chakarov, D., & Papazov, Y. (2019, June). Evaluation of the complexity of fully homomorphic encryption schemes in implementations of programs. In Proceedings of the 20th International Conference on Computer Systems and Technologies (pp. 62-67).