Journal of Artificial Intelligence, Machine Learning and Neural Network
ISSN:2799-1172
Vol: 02, No. 04, June-July 2022
http://journal.hmjournals.com/index.php/JAIMLNN
DOI: https://doi.org/10.55529/jaimlnn.24.26.32

A Proposed Approach for the Key Generation in Cryptography to Enrich the Data Confidentiality While Sharing Data over the Network

Eeva N. Kapopara[1], Dr. Prashant P. Pittalia[2*]

[1]Ph.D. Scholar Department of Computer science and technology Sardar Patel University, Vallabh Vidyanagar, Gujarat, India
[2]Associate Professor Department of Computer science and technology Sardar Patel University, Vallabh Vidyanagar, Gujarat, India*

Email: [1]kapopara.eeva@gmail.com
Corresponding Email: [2]prashantppittalia@yahoo.com*

Received: 22 February 2022 **Accepted:** 08 May 2022 **Published:** 10 July 2022

Abstract - Data sharing over network has been threat in the digital world. To provide the security to the data being passed over the network various system has been defined. Most widely used systems are cryptography and steganography. Cryptography is the art of converting the data to some another format which will not be understandable by the intruders. The most important phase while sharing data over network using cryptography is the key generation and key distribution. General cryptography techniques either uses public key or uses public and private key both. The major focus of the propose method is not to commute keys with the data being shared over network. Proposed approach defines a method which will get feedback from the receiver and system will identify whether the receiver is undeniable or not. If the receiver is undeniable then only the data will be decrypted to the original to the original format. In this paper we have surveyed many traditional algorithms related to symmetric key and asymmetric key cryptography. Many mathematical operations are being applied to generate the complex keys to ensure security. This approach defines the complexity with almost no mathematical complexity and using no traditional approach for the key generation which are widely known.

Keywords: Cryptography, Symmetric Key, Asymmetric Key, Public Key, Private Key, Encryption, Decryption

1. INTRODUCTION

Cryptography is an art to encrypt and decrypt data. Cryptography term is derived from Greek word “Krypto”, means hidden. Cryptography allows to store and transmit sensitive and

Journal of Artificial Intelligence, Machine Learning and Neural Network
ISSN:2799-1172
Vol: 02, No. 04, June-July 2022
http://journal.hmjournals.com/index.php/JAIMLNN
DOI: https://doi.org/10.55529/jaimlnn.24.26.32

confidential data across insecure channel. Cryptography is related to two terms: cryptology and cryptanalysis. Cryptology is creation and solution of the encoding. Cryptanalysis is technique to break the codes which is not intended for person as a recipient.
The basic terminologies used in cryptography are described below.

Plaintext: The original message or data to be passed on network that is fed into the algorithm as input is called plaintext. Plain text serves as an input for an encryption process, and the output for a decryption process.

Encryption algorithm: The encryption algorithm implements various substitutions, transformations and many other techniques on the plaintext. Encryption converts the plaintext into cipher text.

Ciphertext: Ciphertext is the encrypted form of the plaintext. It is the encoded text produced as outcome of encryption process. Structure and complexity of encoded text depends upon the plaintext and the key.

Decryption: Conversion of encoded text into original text is known as decryption. Decryption algorithm follows the same steps as encryption process but in reverse order. It takes the ciphertext as an input and applies the key and produces the original plaintext which was intended for a recipient.

Key: Key is a string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa. The security and efficiency of the algorithm is generally depended on the key. Thus, a key can be a set of digits, a set of characters or a combination of digits and characters that the algorithm uses to perform encryption and decryption.

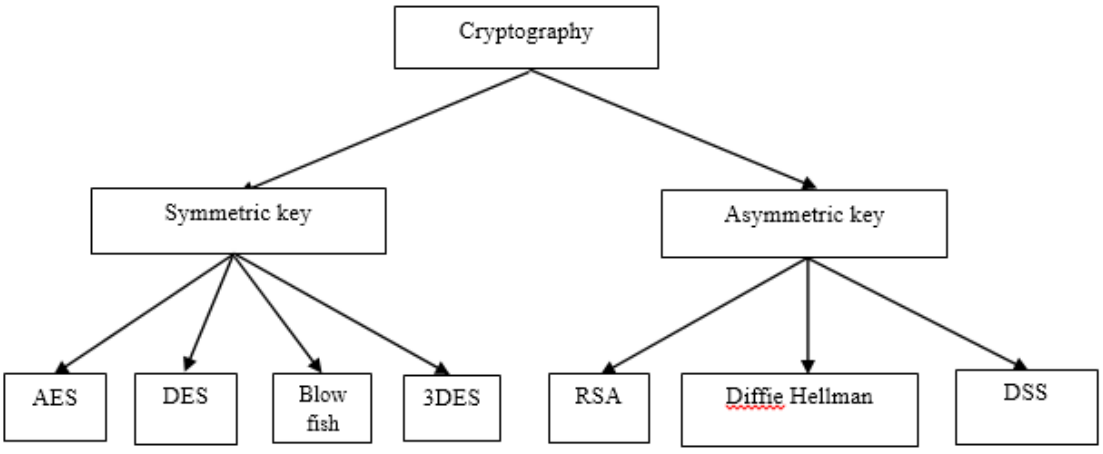

Figure 1 Classification of cryptographic algorithm

Journal of Artificial Intelligence, Machine Learning and Neural Network
ISSN:2799-1172
Vol: 02, No. 04, June-July 2022
http://journal.hmjournals.com/index.php/JAIMLNN
DOI: https://doi.org/10.55529/jaimlnn.24.26.32

This paper focuses on the key factor of the cryptosystem. There is a lock and key concept for a house to keep the things in safe. Same way cryptographic key is the same set of bits to secure the data. Key can be a number, string of characters or it can be the combination of numbers and characters. It may be in binary, decimal or hexadecimal form. It is used to encrypt the plain text and decrypt the cipher text. Key works with the cryptographic algorithms and known as transformation parameters of the cryptographic algorithms. Keys can be either symmetric or asymmetric.

A. Symmetric key cryptography

An algorithm using same key for encryption and decryption is know as symmetric key cryptography [2]. Symmetric key cryptography is also known as shared key, secret key, single key, one key and private key cryptography. Symmetric key cryptography is categorized in two categories: Stream cipher and block cipher.

Stream cipher: It is defined to work on one bit, byte or a computer word at a time. It uses feedback structure because of which key changes repeatedly.

Block cipher: It is defined to work on one block of fixed sized at a time using the same key on each block. Block cipher can be operated in different mode like Electronic Codebook (ECB) mode, Cipher Block Chaining (CBC) mode, Cipher Feedback (CFB) mode, Output Feedback (OFB) mode.

Advance Encryption Standard (AES), Data Encryption Standard (DES), Blow Fish etc. are the examples if Symmetric key cryptography.

Advantages:

These algorithms are efficient.
These algorithms take less time to encrypt and decrypt the data.

Disadvantages:

In this number of keys required is too large. Sharing secret key between sender and receiver is the biggest and important issue.

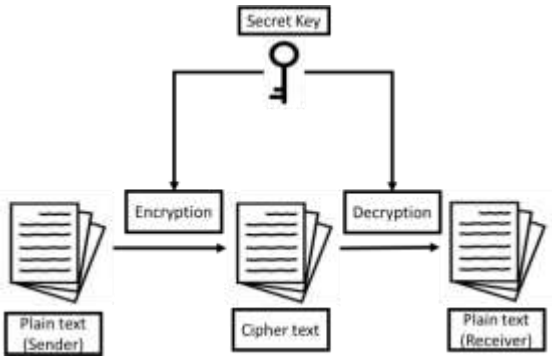

Figure 2 Symmetric Key Cryptography

Journal of Artificial Intelligence, Machine Learning and Neural Network
ISSN:2799-1172
Vol: 02, No. 04, June-July 2022
http://journal.hmjournals.com/index.php/JAIMLNN
DOI: https://doi.org/10.55529/jaimlnn.24.26.32

B. Asymmetric key cryptography

An algorithm using different key for encryption and decryption is known as asymmetric key cryptography [1]. It is also known as public key cryptography. In this technique data is encrypted using public key and decrypted using private key of recipient. This kind of technique is used in email security, web security, etc.

Digital Signature Standard (DSS), Rivest Shamir Adelman (RSA), etc. are the examples of asymmetric key cryptography.

Advantages:
These algorithms detect tempering.
This type of cryptography allows message authentication.

Disadvantages:
In this public key are not authenticated.
In this technique loss of private key is irreparable.

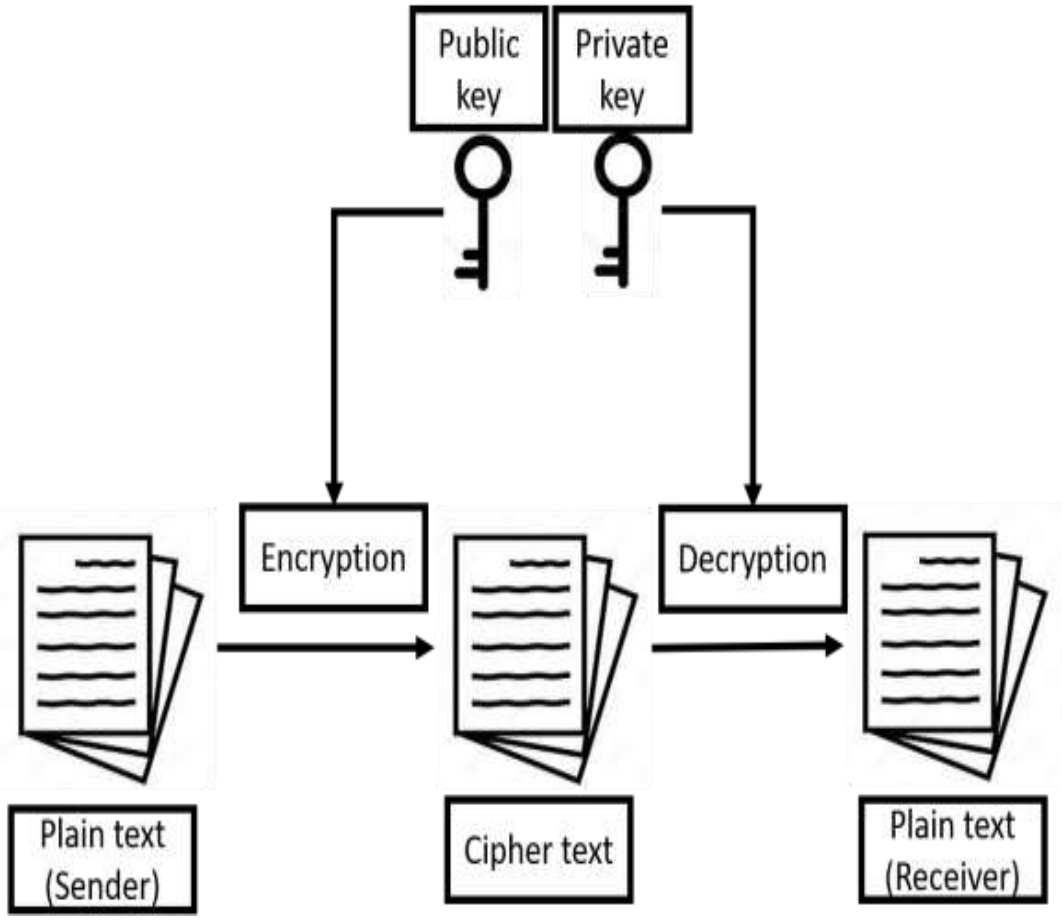

Figure 3 Asymmetric Key Cryptography

Journal of Artificial Intelligence, Machine Learning and Neural Network
ISSN:2799-1172
Vol: 02, No. 04, June-July 2022
http://journal.hmjournals.com/index.php/JAIMLNN
DOI: https://doi.org/10.55529/jaimlnn.24.26.32

I. Comparison of symmetric key and asymmetric key cryptography

Characteristics	Symmetric key cryptography	Asymmetric key cryptography
Age of technology	Old technique	New Technique
Key for encryption/ decryption	Uses same key for both encryption and decryption	Uses public key for encryption and private key for decryption
Speed	Takes less time	Takes much time
Key arrangement / exchange	A big challenge	Not an issue
Size of resulting encrypted text	Generally same as or less than the original text size	More than the original text size
Usage	Mainly used for confidentiality	Web security, digital signatures, email security
Example	AES, DES, 3DES, etc.	DSS, RSA, etc.

Table 1 Comparison of Symmetric and Asymmetric key cryptography [6]

II. Structure of the proposed method

This paper proposes a new approach having symmetric key approach but having a new kind of implementation of key. All the existing techniques usually implement key sharing over network and which creates a big risk of losing confidentiality. This paper introduces a concept of key repository. Key repository can be called a database for key. The key will be stored well in advance before the data transmission take place.
When the sender wants to encrypt and send data to specific user, sender has to pass through the verification stage. Same process will be followed for receiver as well. Before decrypting cipher text receiver has to give identity that whether it is intended receiver or not.

Key repository concept will store the senders' detail with the intended receivers' detail and a key for both sender and receiver.

When sender encrypt the plain text, he/she has to provide a receiver's detail and key for that intended receiver. So, it will be verified that the sender is original or not. Once sender has sent the cipher text receiver has to give identity. If receiver fails to give the correct key for the sender from which the cipher text is received then cipher text will not be received. So, no intruder can directly decrypt the message.

Challenge in this proposed concept is the security of the key repository. Key repository will be password protected so that no unauthenticated person has access.

2. CONCLUSION

The main objective of this paper is to introduce an easy and more secure way for the small-scale institutions and organisations. One may have comparison of various algorithms to know

Journal of Artificial Intelligence, Machine Learning and Neural Network
ISSN:2799-1172
Vol: 02, No. 04, June-July 2022
http://journal.hmjournals.com/index.php/JAIMLNN
DOI: https://doi.org/10.55529/jaimlnn.24.26.32

and introduce something new but no algorithm is less important, all having its own technique, importance and usage. This paper also shown that the existing algorithms have different key concepts and difference key exchange mechanisms but the proposed methodology seems very easy and secure than the existing as it provides the verification before encryption and decryption both.

3. REFERENCES

1. Chandra, S., Paira, S., Alam, S. S., & Sanyal, G. (2014, November). A comparative survey of symmetric and asymmetric key cryptography. In 2014 international conference on electronics, communication and computational engineering (ICECCE) (pp. 83- 93). IEEE.
2. Gunasundari, T., & Elangovan, K. (2014). A comparative survey on symmetric key encryption algorithms. International Journal of Computer Science and Mobile Applications, 2(2), 78-83.
3. Gautam, A. K., & Kumar, R. (2021). A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks. SN Applied Sciences, 3(1), 1-27.
4. Santoso, P. P., Rilvani, E., Trisnawan, A. B., Adiyarta, K., Napitupulu, D., Sutabri, T., & Rahim, R. (2018, September). Systematic literature review: comparison study of symmetric key and asymmetric key algorithm. In IOP Conference Series: Materials Science and Engineering (Vol. 420, No. 1, p. 012111). IOP Publishing.
5. Alenezi, M. N., Alabdulrazzaq, H., & Mohammad, N. Q. (2020). Symmetric encryption algorithms: Review and evaluation study. International Journal of Communication Networks and Information Security, 12(2), 256-272.
6. Kapoor, J., & Thakur, D. (2022). Analysis of Symmetric and Asymmetric Key Algorithms. In ICT Analysis and Applications (pp. 133- 143). Springer, Singapore.
7. Xu, H., Thakur, K., Kamruzzaman, A. S., & Ali, M. L. (2021, April). Applications of Cryptography in Database: A Review. In 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS) (pp. 1-6). IEEE.
8. Mandal, K. K., Chatterjee, S., Chakraborty, A., Mondal, S., & Samanta, S. (2020). Applying Encryption Algorithm on Text Steganography Based on Number System. In Computational Advancement in Communication Circuits and Systems (pp. 255-266). Springer, Singapore.
9. Kumar, R., & Singh, N. (2020). A Survey Based on Enhanced the Security of Image Using the Combined Techniques of Steganography and Cryptography. Available at SSRN 3563571.
10. Murtaza, A., Pirzada, S. J. H., & Jianwei, L. (2019, January). A new symmetric key encryption algorithm with higher performance. In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET) (pp. 1-7). IEEE.
11. Khari, M., Garg, A. K., Gandomi, A. H., Gupta, R., Patan, R., & Balusamy, B. (2019). Securing data in Internet of Things (IoT) using cryptography and steganography techniques. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 50(1), 73-80.

Journal of Artificial Intelligence, Machine Learning and Neural Network
ISSN:2799-1172
Vol: 02, No. 04, June-July 2022
http://journal.hmjournals.com/index.php/JAIMLNN
DOI: https://doi.org/10.55529/jaimlnn.24.26.32

12. Taleby Ahvanooey, M., Li, Q., Hou, J., Rajput, R., & Chen, Y. (2019). Modern text hiding, text steganalysis, and applications: a comparative analysis. Entropy, 21(4), 355.
13. Taha, M. S., Rahim, M. S. M., Lafta, S. A., Hashim, M. M., & Alzuabidi, H. M. (2019, May). Combination of steganography and cryptography: A short survey. In IOP conference series: materials science and engineering (Vol. 518, No. 5, p. 052003). IOP Publishing.
14. Shetty, V. S., Anusha, R., MJ, D. K., & Hegde, P. (2020, February). A survey on performance analysis of block cipher algorithms. In 2020 International Conference on Inventive Computation Technologies (ICICT) (pp. 167- 174). IEEE.
15. Sharma, Rakesh, Poonam Jindal, and Brahmjit Singh. "Study and analysis of key generation techniques in internet of things." Journal of Discrete Mathematical Sciences and Cryptography 23.2 (2020): 373-383.