2023 IEEE 3rd International Conference on Technology, Engineering, Management for Societal impact using Marketing, Entrepreneurship and Talent (TEMSMET) | 979-8-3503-9781-9/23/$31.00 ©2023 IEEE | DOI: 10.1109/TEMSMET56707.2023.10150061

Analysis of Key Based Cryptographic Algorithms and its Applications

Nagandla Krishna Sai Keerthan
Dept of Computer Science
Amrita Vishwa Vidyapeetham
Bangalore, India
nagandla987@gmail.com

Sreekar Praneeth Marri
Dept of Computer Science
Amrita Vishwa Vidyapeetham
Bangalore, India
praneethmarri2505@gmail.com

Manju. Khanna
Dept of Computer Science
Amrita Vishwa Vidyapeetham
Bangalore, India
k_manju@blr.amrita.edu

***Abstract*—Information security is the process of safeguarding data. It safeguards its availability, privacy, and integrity. The capacity to secure data from attacks, as well as efficiency and speed are the two key features that separate one cryptography algorithm from another. Security is the most difficult issue in the present world, and the various security dangers in data security must be avoided in order to provide consumers with more privacy while still permitting high information availability and Integrity. Data encryption employing various data encryption techniques will increase the security of data transmission. This paper primarily focuses on a comparative analysis of symmetric algorithms (AES, DES, Ceaser Cipher, Stream Cipher) and asymmetric algorithms (Diffie Hellman, RSA), and also file and image encryption using symmetric algorithms.**

Keywords—AES, DES, RSA.

I. INTRODUCTION

Maintaining message confidentiality or data security is called as cryptography. It means "secret writing" in Greek. High-level encryption, on the other hand, guarantees that the information is secured so that only the approved recipients have access to it. The method Cryptography is a centuries-old technique that is continuously being researched. Examples date back to 2000 B.C., when our ancestors used “secret” hieroglyphics, with evidence that includes hidden messages and inscriptions in ancient Greece and the most popular Caesar cypher in ancient Rome.

Numerous millions of people use cryptography every day throughout the world to secure data, although most people aren't aware of it. It is regarded highly brittle, in addition to being incredibly helpful, because a single programming or specification error can ruin cryptographic systems [1]. The Internet of All (IoE) defines a system in which millions of units are connected by standard or proprietary protocols through private networks or public networks and each has sensors for measuring and assessing their status.

Encryption techniques are classified into two types: symmetric and asymmetric cryptography. In symmetric-key cryptography, both parties share the same key. The data is encrypted by the transmitter using this key and an encryption technique, and it is decrypted by the receiver using the same key and the matching decryption algorithm. Asymmetric cryptography, commonly known as public-key cryptography, is one of which uses a private key and a public key. The public key is made accessible by everyone while the private key is kept by the recipient. [2]

Asymmetric encryption algorithms that are often employed include Rivest Shamir and Adleman (RSA), Diffie-Hellman, Elliptic curve cryptography (ECC), Digital Signature Algorithm (DSA). On the other hand, the external advantages of IoT include raising societal involvement, service improvement by authorities, and bettering well-being through integrated and online health monitoring systems.

Principle behind encryption –

The converting of plain text into cypher text, which can only be decrypted by the intended recipient. —is a common example of cryptography. The name given to the process is encryption.[7]

Decryption is the procedure that transforms encrypted text into plain text.

Fig. 1. Principle behind encryption and decryption

II. LITERATURE SURVEY

[1]. This paper intends to compare the symmetric encryption algorithms especially Advanced Encryption Standard (AES) and Data Encryption Standard (DES) in terms of processing time and CPU usage in different text files. It compares Advanced Encryption Standard and Data Encryption Standard algorithms and prove that Advanced Encryption Standard has high throughput than Data Encryption Standard.

[3]. In this paper, the documents are encrypted using asymmetric RSA approach. It focuses mainly on encryption and decryption when e-mails are being sent and received. The key being generated is directly proportional to the speed and processing time. The longer the size of file the longer time it takes to encrypt the file and store it for future purpose.

979-8-3503-9781-9/23/$31.00 ©2023 IEEE

III. BASIC CONCEPTS

Let's have an overview of some basic concepts that are used in this paper.

A. ENCRYPTION

The method by which the data or information is encrypted so that the provided data can only accessed by authorised users and it can be deciphered only by authorised people is known as encryption. Technically, it is the process of converting a readable text to unreadable text, commonly known as ciphertext. The readable data appears to be random as the encryption modifies it. Encryption necessitates the employment of a cryptographic key, which is a mathematical set of values which is agreed upon by the recipient and as well as sender of an message which is encrypted. [4]

Encryption not only ensures data or data and ensure, but it also provides authentication and integrity, indicating that the source data have not been modified in any way from their original state. [5]

Fig. 2. Encryption working process

B. DECRYPTION

Decryption essentially reverses the encryption process so that the message's content can be read and understood by the recipient. As long as the recipient has the correct data encryption key, converting encrypted text to decrypted text is usually simple. This is also true when encrypting images or other types of data. [6]

The process of converting encrypted data or any other information into text that the computer can easily comprehend and as well human can read. This phrase could refer to a method that manually decrypts the data or a method of decrypting data by using the proper keys or proper codes. [7]

Fig. 3. Decryption working process

C. CLASSIFICATION

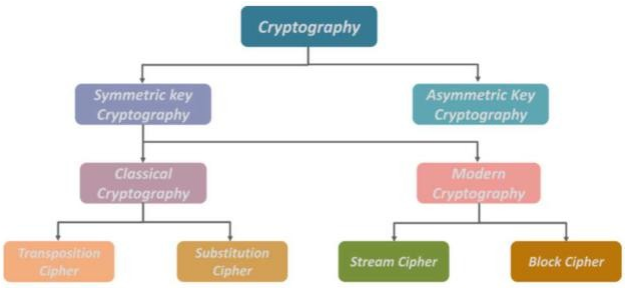

Fig. 4. Classification of cryptography

1) Symmetric Key Cryptography

- It is an encryption technology in which data or information are encrypted and decrypted by both sender and the recipient using the same shared key.[8]
- Symmetric Key Systems are simpler and faster, but the sender and recipient must securely exchange keys.
- It is also known as secret key cryptography.
- Most popular is Advanced Encryption System (AES). Symmetric algorithm is of four types:

1. Transposition Cipher - A transposition cypher is a type of encryption that involves shifting the places held by plaintext units.
2. Substitution Cipher - A substitution cypher is a type of encryption in which plaintext units are replaced with ciphertext in a predefined manner using a key.
3. Stream Cipher - It is a technique that combines plaintext digits with a pseudorandom cypher digit stream. Each plaintext digit is encrypted independently.
4. Block Cipher - It's a deterministic method that uses fixed-length groupings of bits called blocks. [9]

2) Asymmetric Key Cryptography

- Information is encrypted and decrypted using a pair of keys.
- Encoding of data is done with public key and decoding data is done with private key.
- Both public and private keys are unique.
- Only the intended user with the private key can decode the message even in case, if the public key is known to everyone.

Types of asymmetric algorithms used:

1. RSA –
   - "RSA" is a shorthand for Ron Rivest, Adi Shamir, and Leonard Adleman.
   - An RSA user generates and shares a public key consisting of two massive prime numbers and an auxiliary value.
   - The prime numbers are kept concealed. Messages can be encrypted by anyone who has access to the public key, but only those who are familiar with prime numbers can decrypt them.
2. Diffie Hellman – The secure transferring of cryptographic keys using a public channel, that was developed by Ralph Merkle and named after Martin Hellman and Whitfield Diffie.

D. IMAGE ENCRYPTION

Encrypting image confidentially with an encryption technology so that only specific users who have access to it and decipher them is known as image encryption.

The widespread usage of digital information to establish contact over the Internet and network is fast rising. As a result, technological developments in the realms of pictures, audio, and video have been tremendous. Information security has emerged as a critical concern in the realm of communication. Encryption is one approach for providing information security in communications. Image encryption is essential as part of the encryption process. The goal of picture encryption is to turn the original image into a difficult-to-detect image so that only authorised users can access the information. One technique to creating security in encryption is to employ chaos theory. There is order in disorder, according to chaotic theory. [10]

E. FILE ENCRYPTION

File encryption is done to secures files and file systems by encrypting them. The encryption is done by a unique key and the access is restricted to the keyholder. The intention is to restrict access to files saved on the disc by malevolent or unauthorized parties.

Full disc encryption, on the other hand, safeguards a complete disc or drive. However, individual files on the disc are not encrypted. For added security, use file encryption and full disc encryption simultaneously to protect both your hard drive and individual files.

Some companies encrypt important data on the cloud, but they are the exception. It can be more difficult to store encrypted files in cloud applications. IT professionals, on the other hand, believe the cloud will grow in importance, which may result in more secured file storage in cloud applications.

IV. IMPLEMENTATION

In this project, the implementation proves several symmetric and asymmetric algorithms used for encryption and compare them based on time complexities. The image encryption and file encryption are implemented using symmetric algorithmic approach.

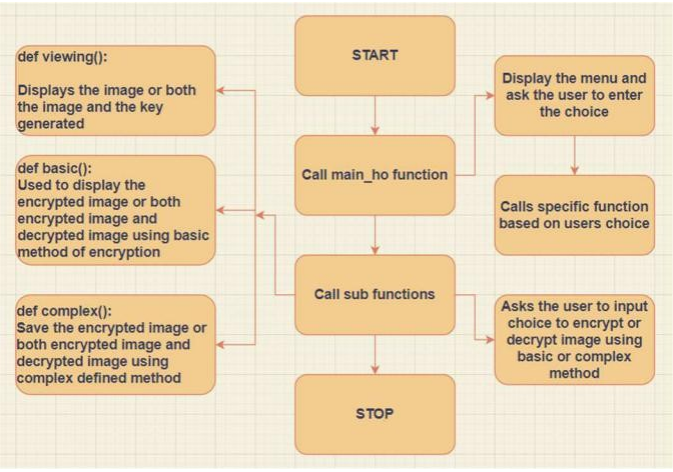

Fig. 5. Implementation of image encryption

V. RESULTS

A. Symmetric Algorithms

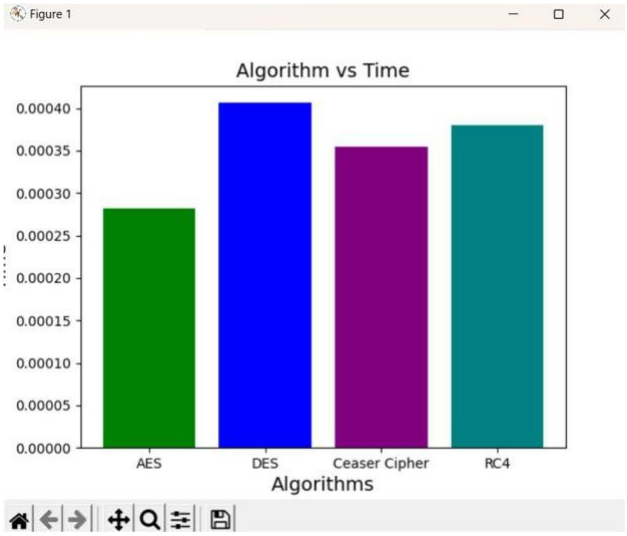

Fig. 6. Analysis of symmetric algorithms

B. Asymmetric Algorithms

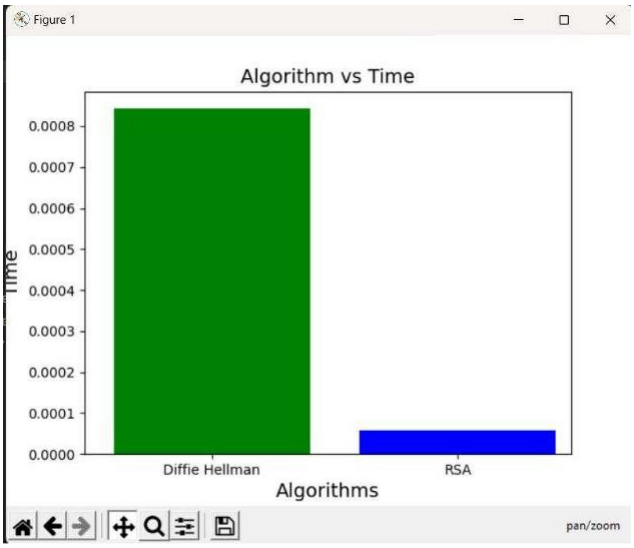

Fig. 7. Analysis of asymmetric algorithms'

C. GUI Implementation of Symmetric Encryption

Fig. 8. GUI implementation

D. Image Encryption

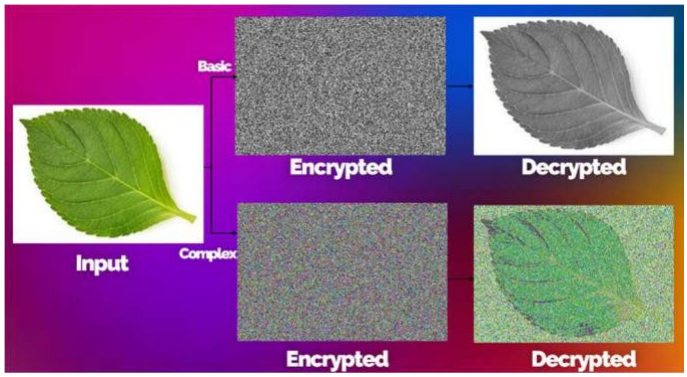

Fig. 9. Image encryption based on basic and complex methods

E. File Encryption

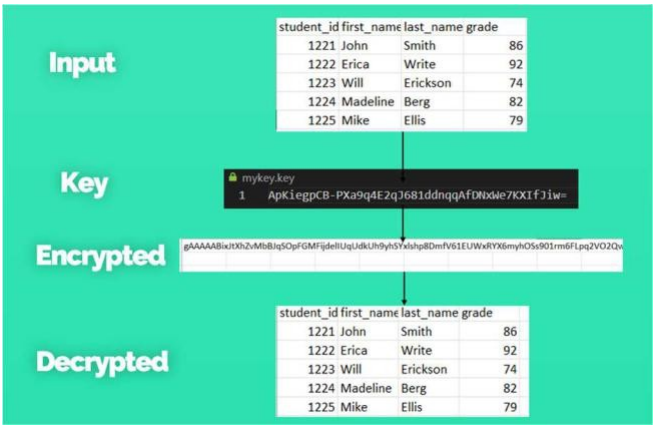

Fig. 10. File encryption procedure

VI. Conclusion

In this project, symmetric algorithms namely Advanced Encryption Standard, Data Encryption Standard, Caeser Cipher, and Stream cipher are compared and proved that Advanced Encryption Standard is better symmetric algorithm for encryption and decryption because the time complexity is less when compared to other symmetric algorithms. Coming to asymmetric algorithms, RSA and Diffie Hellman algorithms are compared and the analysis shows that RSA is highly efficient that Diffie Hellman algorithm.

The image and file encryption is implemented using symmetric algorithm as it is faster and converts the file in less time. The project also aims to compare the different approaches used for image encryption to enhance the security and the final results.

VII. References

[1] P. Bharathi, G. Annam, J. B. Kandi, V. K. Duggana and A. T., "Secure File Storage using Hybrid Cryptography," 2021 6th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2021, pp. 1-6, doi: 10.1109/ICCES51350.2021.9489026.

[2] M. Mamathashree, K. Remya and B. J. S. Kumar, "Fault analysis detection in public key cryptosystems (RSA)," 2017 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2017, pp. 0505-0508, doi: 10.1109/ICCSP.2017.8286409.

[3] M. A. D. S. Atmaja, I. N. G. A. Astawa, N. W. Wisswani, I. M. R. A. Nugroho, P. W. Sunu and I. K. Wiratama, "Document Encryption Through Asymmetric RSA Cryptography," 2020 International Conference on Applied Science and Technology (iCAST), Padang, Indonesia, 2020, pp. 46-49, doi: 10.1109/iCAST51016.2020.9557723.

[4] Mammenp, S.KN and R. Bhakthavatchalu. "Implementation of Efficient Hybrid Encryption Technique", 2022 2nd International Conference on Intelligent Technologies (CONIT), Hubli, India, 2022, pp. 1-4, doi: 10.1109/CONIT55038.2022.9048180.

[5] J. H. Cheon and J. Kim, "A Hybrid Scheme of Public-Key Encryption and Somewhat Homomorphic Encryption," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 5, pp. 1052-1063, May 2015, doi: 10.1109/TIFS.2015.2398359.

[6] V. S. Aparna, A. Rajan, I. Jairaj, B. Nandita, P. Madhusoodanan and A. A. S. Remya, "Implementation of AES Algorithm on Text and Image using MATLAB," 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2019, pp. 1279-1283, doi: 10.1109/ICOEI.2019.8862703.

[7] R. Bhatnagar and M. Kumar, "Visual Cryptography: A Literature Survey," 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2018, pp. 78-83, doi: 10.1109/ICECA.2018.8474649.

[8] P. Sridhar and R. R. Sathiya, "Crypto-watermarking for secure and robust transmission of multispectral images," 2017 International Conference on Computation of Power, Energy Information and Commuincation (ICCPEIC), Melmaruvathur, India, 2017, pp. 153-163, doi: 10.1109/ICCPEIC.2017.8290357.

[9] T. M. Zaw, M. Thant and S. V. Bezzateev, "Database Security with AES Encryption, Elliptic Curve Encryption and Signature," 2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), St. Petersburg, Russia, 2019, pp. 1-6, doi: 10.1109/WECONF.2019.8840125.

[10] B. J. S. Kumar, V. K. Roshni Raj and A. Nair, "Comparative study on AES and RSA algorithm for medical images," 2017 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2017, pp. 0501-0501, doi: 10.1109/ICSP.2017.8286408.