WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cryptography: Analysing RSA & AES for Security in Modern Communication

Aditi Sharma[1], Ganesh Kumar P.[2]

[1,2] Department of Computer Science, Bhilai Institute of Technology Raipur, Chhattisgarh, India

ABSTRACT

In the rapidly evolving digital landscape, the preservation of digital data integrity during internet transmission is a paramount concern. This paper explores security measures, focusing on hybrid cryptographic algorithms that intelligently blend symmetric and asymmetric key techniques. It meticulously examines the effectiveness of the Hybrid Cryptographic Algorithm (HCA) in comparison to established methods like AES and RSA. This thorough analysis extends to practical evaluations on three distinct machines, inclusive of two identical setups with differing CPU and memory usage. The testing encompasses various data types, ensuring a comprehensive understanding of HCA's adaptability. The study aims to uncover nuanced factors influencing encryption and decryption times, providing valuable insights into the algorithm's practical applicability.

Keywords: Hybrid Cryptography, Cryptographic Algorithms, Encryption, Decryption, Performance Analysis, Data Security, Symmetric Key Cryptography, Asymmetric Key Cryptography, AES, RSA**.**

1. INTRODUCTION

The ever-expanding digital landscape has made the safeguarding of sensitive information and the assurance of secure communication channels a paramount concern. Cryptography, serving as both an art and a science, takes a pivotal role in addressing these concerns by providing a systematic framework for encoding and decoding information. Its use extends from securing online transactions to protecting sensitive communication in various domains.

Cryptography's fundamental objective is to ensure the confidentiality, authenticity, and integrity of data. As our reliance on digital platforms for communication and transactions increases, we employ cryptographic techniques as essential tools to deter potential threats such as unauthorized access, eavesdropping, and data tampering.

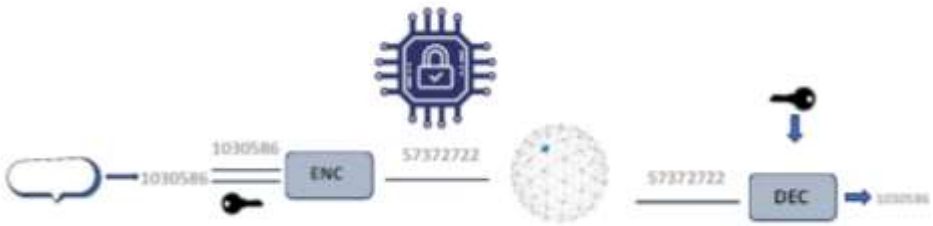


Fig 1: Basic Cryptography Model

Mathematical algorithms and cryptographic keys are the tools that cryptography utilizes to achieve its goals. These keys are the linchpin for encoding and decoding information, facilitating a secure environment for parties to communicate over potentially untrustworthy networks, like the Internet.

This introduction paves the way for a comprehensive exploration of cryptographic methodologies. It encloses both symmetric and asymmetric key algorithms, each with its unique strengths and applications. Likewise, modern cryptographic approaches, such as hybrid cryptography, are gaining prominence due to their capacity to amalgamate the benefits of both symmetric and asymmetric techniques.

As we embark on this journey through the intricate landscape of cryptography, gaining an understanding of its underlying principles becomes crucial. This understanding not only enables us to implement secure communication channels but also prepares us to face the evolving challenges posed by cyber threats. In the subsequent sections, we will plunge into the intricacies of cryptographic algorithms, their functionalities, and the pivotal role they fulfill in ensuring the security and integrity of digital information.

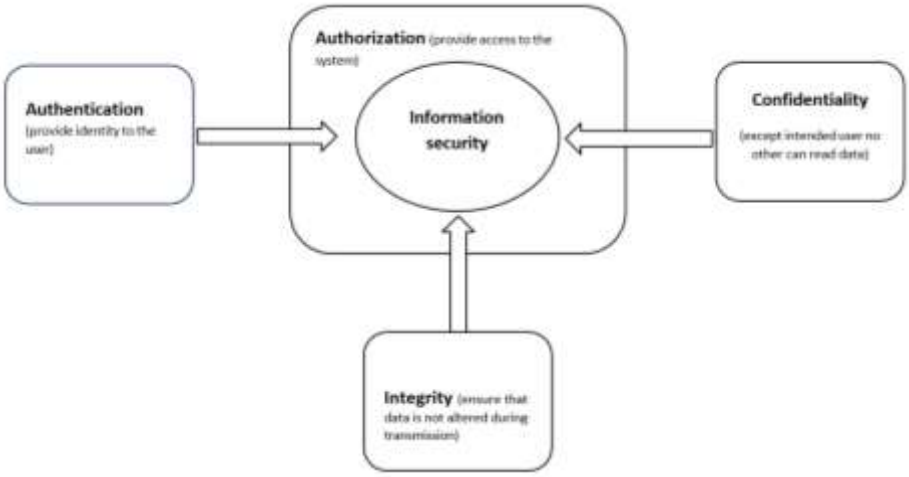


Fig 2: Principal of security

1.1 Basic terms used in cryptography

Plain Text: The original, readable data that is subject to encryption is this. It could be a message, a file, or any form of digital information.

Cipher Text: The ciphertext is the result of encryption algorithms being applied to the plaintext, resulting in an unreadable and scrambled version of the original data.

The ciphertext can be reverted to its original plaintext form by decryption, using the appropriate key.

Algorithm or cipher: It is a well-defined mathematical function that is used to encrypt or decrypt data.

Algorithm or cipher: It is a well-defined mathematical function that is used to encrypt or decrypt data.

Encryption Time: Time taken to convert plain text into cipher text.

Decryption Time: Time taken to convert cipher text into plain text.

Encryption: The fundamental concept in information security is encryption, which serve as a critical mechanism to secure data during storage, transmission, and processing. Encryption involves converting plaintext (readable data) into ciphertext (unreadable data) using mathematical algorithms and cryptographic keys. The primary objectives of encryption ensure confidentiality, integrity, and sometimes authentication.

Decryption: The process of decryption converts encrypted or ciphertext data back into its original, readable form, known as plaintext. Authorized parties must use this essential process to access and understand the information that encryption previously secured. The decryption process depends on cryptographic algorithms and keys, and its principles vary based on the type of encryption used.

2. TYPES OF CRYPTOGRAPHIC ALGORITHMS

Cryptographic algorithms have advanced over time along with the evolution of computer systems and data.

There are two categories of cryptographic algorithms that are listed below:

- Symmetric key cryptography (Secret Key)
- Asymmetric key cryptography (Public Key)

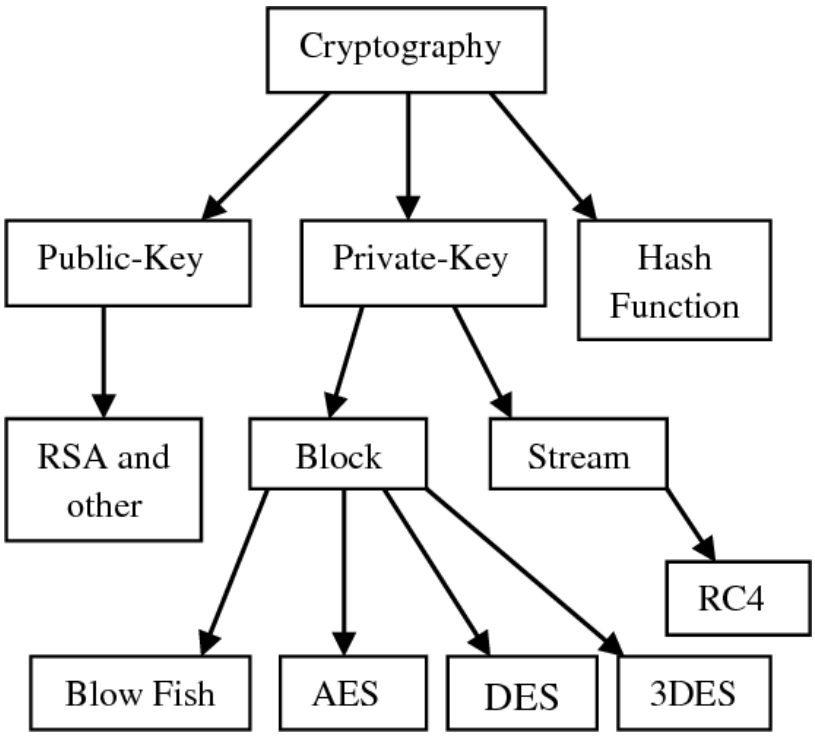


Fig 3: These two categories of algorithm are further divided into subcategories

2.1 Symmetric Key Cryptography

We also refer to it as Secret Key Cryptography/Private Key Cryptography. These types of algorithms use a single key or shared key for the encryption and decryption process, shared among both parties during the transmission. We should keep this key secret because if anyone accesses the key, they can easily decrypt the data and read or alter it. Both the sender and receiver must agree upon the key before the transmission of data. Different mechanisms are used for a key generation like the Diffie-Hellman Key Exchange/Agreement algorithm, based on some mathematical principles. AES, DES, T-DES, and Blowfish are some of the symmetric algorithms. Fig. 4 demonstrates the encryption and decryption process of symmetric algorithms

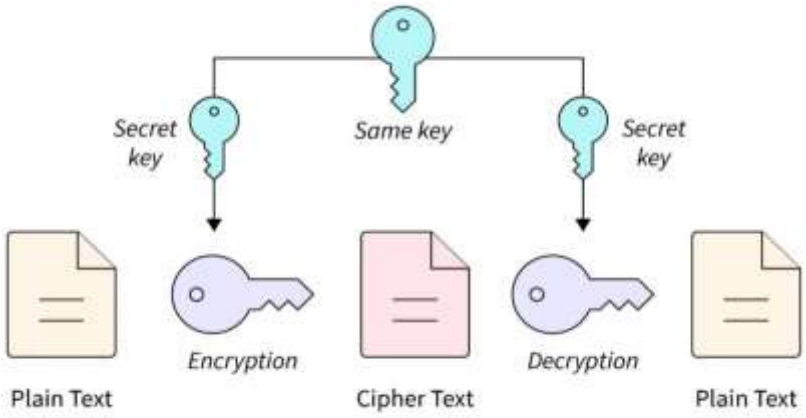


Fig 4: Symmetric Key Cryptography

2.2 Asymmetric Key Cryptography

We also know asymmetric key cryptography as Public Key Cryptography. These algorithms use two different keys to form a key pair. We use one key (known as a private key) [20] for the decryption of data and another key (known as the public key) for the encryption of data.

We announce or share a public key with everyone. Only the receiver's private key can decrypt data, not even the key used for encryption can decrypt that data.

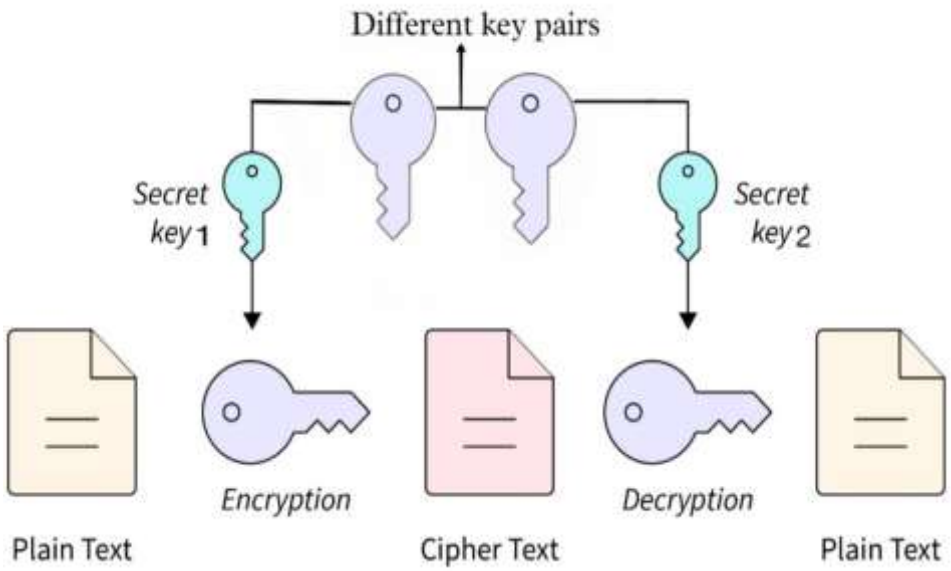


Fig 5: Asymmetric Key Cryptography

3. RSA Algorithm

The most general and broadly used public key encryption algorithm is RSA [7] [8]. Ron Rivest, Adi Shamir, and Leonard Adleman, the three inventors of the RSA algorithm, named it after themselves. They developed it in 1978. RSA operates on the mathematical fact that finding and multiplying two large prime numbers is easy, but factoring their product is an extremely difficult task. The RSA encryption and decryption process uses a private and public key based on large prime numbers. The security that the RSA algorithm provides depends on the length of the prime numbers; large prime numbers offer more security whereas small prime numbers offer less security. However, there are many faults in the design of RSA.

Algorithm:

1. Elect two large prime numbers P and Q.
2. Compute N by multiplying P and Q P * Q = N
3. Select the public key E (Encryption Key) such that it is not a factor of(P-1) and (Q-1)
4. Select the private key D (Decryption Key) such that it satisfies the following condition(D*E) mod (P-1) * (Q-1) = 1
5. For encryption, calculate cipher text (CT) from plain text (PT) PT^E mod N = CT
6. Send cipher text (CT) to receiver

For decryption calculate plain text (PT) from cipher text (CT) CT^D mod N = PT

4. AES Algorithm

The full form of AES, also known as Rijndael, is Advanced Encryption Standard. AES was not created by Joan Daemon and Vincent Rijmen but rather was invented by them. The development of AES was to overcome the weaknesses of the DES algorithm. The plaintext block size of the AES algorithm can vary from 128 to 256 bits. Three keys that can be used for encryption and decryption purposes i.e. 128 bit, 192 bit, 256 bit. The usage of 10, 12, and14 rounds is reliant on the type of key used. For instance, if a 128-bit key is used, a 10- round encryption and decryption process will be used. Similarly, a 12 -round encryption and decryption process will be used for a 192-bit key, and a 14-rounds process will be used for a 256-bit key. The encryption process begins with the "Add round key stage". In each round, 4 transformation processes occur.

Transformation or sub-bytes are generally known as substitute-byte transformation: In a sub-bytes transformation, every data bit is transformed by other data using an 8-bit substitution box, also known as a Rijndael s-box, with AES utilizing a 128-bits data blockA transformation known as Shift Row: The data bytes in three rows undergo a left cycle shift..

In the second row, a one-byte circular left shift is performed while two and three bytes left shift is performed in the third and fourth row.

A transformation referred to as Mix Column: Multiplication of every column with a stable matrix is performed at this stageAdd round key transformation: At this stage, an XOR operation is performed among the 128-bits of the current state and the 128-bits round key **Substitute byte transformation or sub-bytes:** AES uses 128-bits block of data. In sub- bytes transformation, every bit of data gets transformed by other data using 8-bit substitution box or also called as Rijndael s-box.

5. Experimental Methodology

5.1 Hybrid Encryption Scheme

The latest hybrid algorithm scheme used to encrypt files is based on the simple arithmetic methods of RSA and AES, and these two algorithms are independent of the hybrid algorithm and are not influenced by their operation. The core material of this hybrid algorithm is the encryption and decryption theory and method, including the RSA algorithm, AES algorithm,

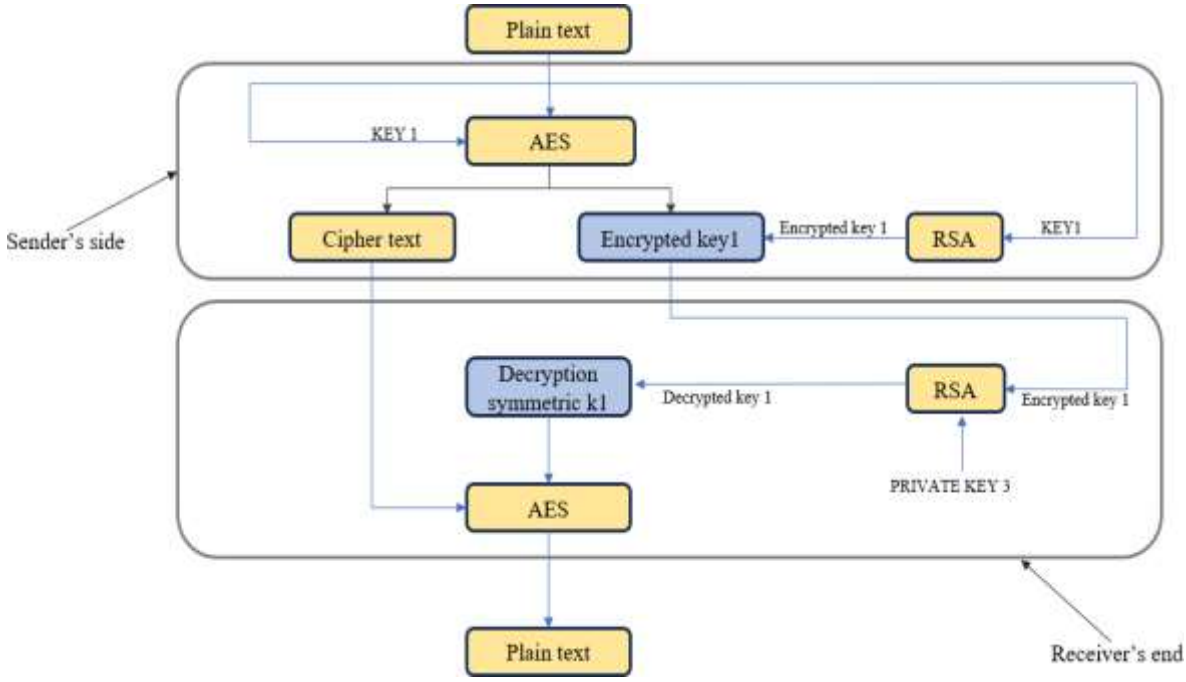


Fig 6: Hybrid Encryption Decryption flow chart and execution of algorithms.

First, this paper outlines the hybrid algorithm theory of file encryption, and then elaborates the operation principle of the hybrid algorithm method of RSA key random generation, encryption and decryption.

This paper proposes a file encryption scheme that incorporates the advantages of the two algorithms based on the contrast between the RSA algorithm and the AES algorithm in terms of encryption and decryption time, security, key management and key length. This paper completely utilises the speed advantage of the AES algorithm in the encryption operation and the stability and key management advantage of the RSA algorithm, and incorporates the encryption power of both to encrypt the code. The key should not be accessed by an insecure third party to ensure the security of the AES algorithm, and all parties should discuss the key in advance, otherwise the key can be constantly updated. In this article, after extensive thought, the AES algorithm key is used in the encryption method of the hybrid encryption algorithm to encrypt the file data to produce cypher text 1, and then the RSA algorithm public key is used to encrypt cypher text 1 and the AES key to generate cypher text 2. The public key is public in the RSA algorithm, and the private key is used for decryption and is private. Encryption by the algorithm of hybrid encryption. Since the AES key is not included in the key, public RSA encrypted data can not be decrypted as private RSA key is kept confidential. The data is not encrypted. In the hybrid algorithm, mathematical operations randomly produce the public and private keys of the RSA algorithm. Fig.3 displays the flow map of the hybrid algorithm's file encryption scheme.

As the AES key is not included in the key, it is not possible to decrypt public RSA encrypted files, as the private RSA key is held secret. It does not encrypt the files. Mathematical operations randomly generate the public and private keys of the RSA algorithm in the hybrid algorithm. The hybrid algorithm's file encryption scheme flow map is seen in Fig.3. The data length is unknown and the encryption and decryption period using the RSA algorithm is not fixed if the RSA algorithm is used to explicitly encrypt the file data in this scheme. The bigger the disc, the longer the time would take for encryption. AES is a block encryption algorithm, as stated above. After encryption, all plaintext and cypher text occur in the form of a block, and for a certain data length, the block length may only be 128 bits. In terms of encryption and decryption performance, the AES algorithm also has benefits.

Using the AES algorithm's efficient operation to encrypt the file for the first time to produce a cypher text of a defined length, and then using the RSA algorithm to encrypt the cypher text would significantly increase the efficiency of the operation and ensure the protection of clustered files. The method of decryption is the opposite of the process of encryption. In order to obtain the AES key and cypher text 1, the private key of the RSA is used to decode the encrypted cypher text 2 and, eventually, the cypher text 1 is decrypted by the AES key to obtain the plaintext. The AES and RSA hybrid encryption algorithms flow map for decrypting files is seen.

5.2 Hybrid Algorithm Key Generation

In this analysis, a key generation algorithm produces the RSA public and private keys in the hybrid algorithm randomly. The following seven steps are carried out in the process of creating the public key and the private key:

- First, two unequal large prime numbers p and q must be randomly selected.
- Then calculate the product n of p and q, that is, n = p x q.
- Calculate the Euler function ø(n) = (p-1)(q1).
- A positive integer e is randomly selected, and 1 < e < ø(n) is made, and gcd(e, ø(n)) = 1.
- According to the equation ed = 1 mod ø(n), the result of d is obtained, where 0<d
- According to the formula PU = {e, N}, the public key of the RSA algorithm is saved, where e is a public key.
- According to the expression PR = {d, p, q}, the private key is saved, where d is the private key

5.3 Hybrid Algorithm Encryption

AES and RSA two-layer encryption are used in the hybrid encryption algorithm, and the encryption process undergoes a sequence of transformations and procedures. The operations involved in the file encryption scheme of the two algorithms are listed in detail below, according to the encryption order. The processing units are clustered in the AES algorithm, and the 128bit data grouped in order will be allocated to a state matrix of 4*4. Centered on the state matrix, all transformations in the algorithm are completed. Involved in the process are four simple arithmetic techniques, Sub Bytes, Shift Rows, Mix Columns and Add Round Key. Bytes Sub. Sub Bytes, also known as s-box permutation, is the only non-linear byte transformation in an AES algorithm encryption round, and each byte in the state is determined independently using the substitute table. The Sub Bytes mapping approach is to take the high 4byte bits as the row value of the matrix and the low 4 byte bits as the column value and take the unit as the output with the column value as the index from the corresponding location in the s box. Rows Shift. Each row is cyclically moved to the left in the forward Shift Rows by a row number offset, that is, the ith row of the state matrix is shifted left by I bytes Mix Columns. Mix Columns transform operates on each column in state and treats each column as a fourth degree polynomial. The addition and multiplication of Mix Columns operation are both defined on the finite field on GF(28).

Introduce the Round Key. When converting Add RoundKey, the value obtained is the 128- bit State xor by bit and the 128-bit key. When encrypting the AES key with an RSA algorithm, the plain text is divided into groups, and the binary values of each group m are all less than n, where n is the product of the large prime numbers p and q, e is a random positive integer, and the cypher text c generated can be obtained from the following formula c = me mod n, and 0 <= m < n… (1)

5.6 Hybrid Algorithm Decryption

In the hybrid algorithm, the private key of the RSA algorithm is used to decode the cypher text encrypted by the public RSA key in the first layer, and then the AES key is used to decrypt the cypher text and get the plaintext. As RSA decryption is used, the encrypted cypher text c is decrypted and transformed, and the plain text m is obtained by the following calculation[12]. m = cd mod n (2) Where d is calculated by the key generation algorithm, where n is the product of the large prime numbers p and q. In the decryption process of the AES algorithm, Sub Bytes, Shift Rows and Mix-Columns are the inverse operations of the encryption process, but in Add Round Key, the inverse operation is the same as the forward transformation because the xor operation

6. Experimental result and analysis

Java Programming Language (ECLIPSE IDE) is used by the analysis section of this research to realize and compile algorithm using Windows 10 operating system. All types of files, whether text file, image file, video file etc with different size, can be encrypted. The encryption and decryption of any size of file requires AES and RSA Keys according to the proposed algorithm. The file that is to be encrypted and decrypted is required to be imported by the user from any location in the computer. After the file is imported, the encrypted file name with .enc extension will be set by the user in the space provided, as shown in the figure below. If the file selected for encryption was successfully encrypted using the provided keys and saved in the project folder, it is decrypted using the code below when the need for decryption arises. The keys must be used and the file should be selected from the project folder for the file to be decrypted, as it is automatically saved there. The fig. below show

the results of files encrypted using AES, RSA and the proposed algorithm with different size and format; the result analysis is based on the time parameter to determine the proposed algorithm's speed.

Output :-

Fig 7: Browsing File

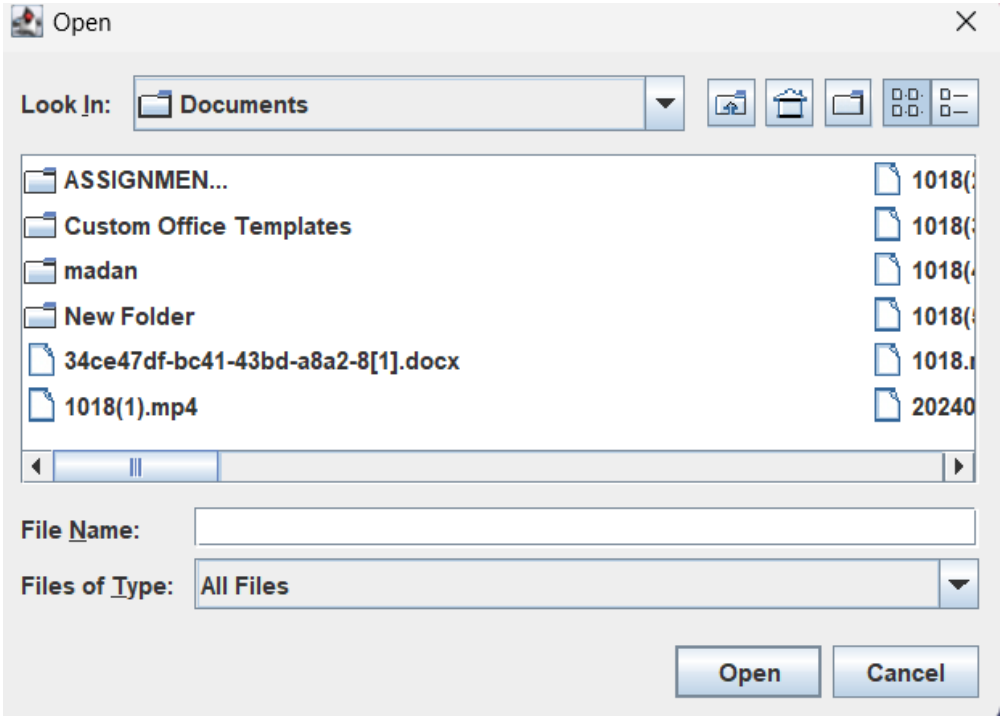


Fig 8: Selecting File

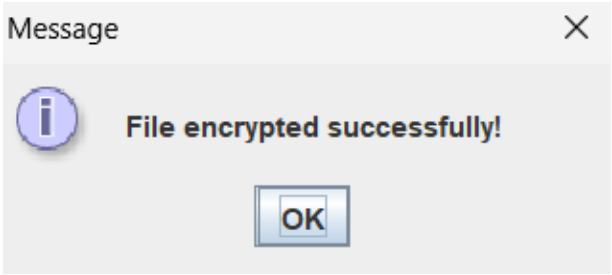
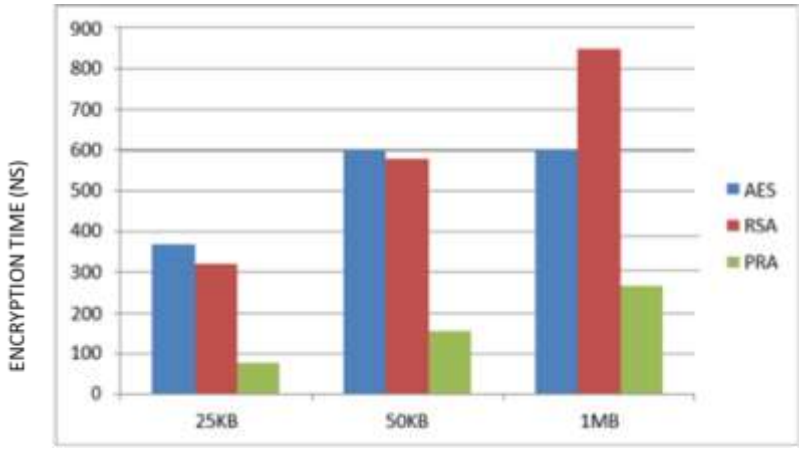


Fig 9: Encryption Completed

Fig 10: Browsing file for decryption

Fig 11: File decrypted



Key size

Fig 12: Algorithm Comparison & result

Symmetric and Asymmetric encryption algorithms are analyzed in this research. According to the study, each algorithm offers its own benefits to different needs. Asymmetric Encryption provides better security but is unable to handle large file, while AES is fast and feasible to use but has a key management problem. Symmetric Encryption offers a better speed than that of public key encryption. The strength of each algorithm depends on key management, key size, type of cryptography, number of keys, etc.

The analysis result in encryption of the RSA algorithm shows that it has a higher security level but only handles small file size and requires a lot of time and power. The AES algorithm can handle a large file size but has a key management problem, making it less secure.

The proposed encryption algorithm is highly secured, according to the security level consideration, due to the double key used for encryption and decryption. It can handle large volumes of data in a very limited time and with less power consumption compared to the RSA algorithm. Thus, the proposed algorithm has a higher possibility of maximum accuracy than that of AES and RSA algorithms.

Conclusion and future work

The technique of file encryption and decryption using only RSA algorithm is described as being somewhat involved with some difficulties due to the very low limit of data that RSA encryption can handle because of the high power consumption during encryption and decryption. The solution to these problems, enabling the encryption of larger quantities of data, is suggested to be the use of a symmetric type of algorithm such as AES for encryption, and an asymmetric type of algorithm like RSA for encrypting the AES encrypted file. The problem of key movement in a symmetric encryption algorithm and the problem of high power consumption of asymmetric encryption algorithm are suggested to have been solved by the new algorithm that combines the features of two algorithms. Furthermore, it is reported that the research is able to successfully encrypt and decrypt the particular size of file and

calculate the time elapse for encryption and decryption. It is also noted that there may still be some deficiencies in the study, such as the possibility of data tampering and forgery when the double key is cracked. These will be the subjects of future research.

Reference

Abu-Faraj, M.; Al-Hyari, A.; Alqadi, Z. A Complex Matrix Private Key to Enhance the Security Level of Image Cryptography. Symmetry 2022, 14, 664.

A. Muhammad Abdullah and A. Muhamad Abdullah, "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data Call for papers View project Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data View project Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt," no. June, 2022

S. A. Ahmad, "Computing : A Review," 2020 15th Int. Conf. Electron. Comput. Comput., no. Icecco, pp. 1–6, 2020.

T.Saravanan, Dr. S.Venkatesh Kumar, "A Review Paper on Cryptography-Science of Secure Communication," International Journal of Computer Science Trends and Technology (IJCST) – Volume 6 Issue 4, Jul-Aug 2018

S. S. Thapar and H. Sarangal, "A Study of Data Threats and the Role of Cryptography Algorithms," IEEE 9th Annu. Inf. Technol. Electron. Mob. Commun. Conf. IEMCON, pp. 819–824, doi: 10.1109/IEMCON.2018.8614943.

R. Banerjee, A. K. Chattopadhyay, A. Nag, and K. Bose, "A nobel cryptosystem for group data sharing in cloud storage," 2019 IEEE 9th Annu. Comput. Commun. Work. Conf. CCWC 2019, pp. 728–731, 2019, doi: 10.1109/CCWC.2019.8666561

S. Omer, A. Faroog, M. Koko, A. Babiker, and N. Mustafa, "Comparison of Various Encryption Algorithms and Techniques for improving secured data Communication," *IOSR*

J. Comput. Eng. Ver. III, vol. 17, no. 1, pp. 2278–661, doi: 10.9790/0661-17136269

A. M. Qadir and N. Varol, "A Review Paper on Cryptography," 2019 7th International Symposium on Digital Forensics and Security (ISDFS) Barcelos, Portugal, 2019, pp. 1-6, DOI: