IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 6, June 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 6, June 2021||

DOI:10.15680/IJIRSET.2021.1006087

File Splitter and Merger Secured Using Cryptographic Algorithm

Pranav Choudhari[1], Kaustubh Kanakdande[2], Vishal Bichkule[3], Prof. Snehal Patil[4]

UG Student, Dept. of Computer Engineering, BSIOTR, Pune University, Pune, India[1]

UG Student, Dept. of Computer Engineering, BSIOTR, Pune University, Pune, India[2]

UG Student, Dept. of Computer Engineering, BSIOTR, Pune University, Pune, India [3]

Assistant Professor, Dept. of Computer Engineering, BSIOTR, Pune University, Pune, India [4]

ABSTRACT: Cryptographic technique is one of the principals means to protect information security. Not only has it to ensure the information confidential, but also provides digital signature, authentication, secret sub-storage, system security and other functions. Therefore, the encryption and decryption solution can ensure the confidentiality of the information, as well as the integrity of information and certainty, to prevent information from tampering, forgery and counterfeiting. Encryption and decryption algorithm's security depends on the algorithm while the internal structure of the rigor of mathematics, it also depends on the key confidentiality. Key in the encryption algorithm has a pivotal position, once the key was leaked, it means that anyone can be in the encryption system to encrypt and decrypt information, it means the encryption algorithm is useless. Therefore, what kind of data you choose to be a key, how to distribute the private key, and how to save both data transmission keys are very important issues in the encryption and decryption algorithm.

KEYWORDS: Cryptography; Encryption; Decryption; RSA Algorithm, AES Algorithm.

I. INTRODUCTION

Encryption is one of the principals means to grantee the security of sensitive information. It not only provides the mechanisms in information confidentiality, but also functioned with digital signature, authentication, secret sub-keeping, system security and etc. Therefore, the purpose of adopting encryption techniques is to ensure the information's confidentiality, integrity and certainty, prevent information from tampering, forgery and counterfeiting [1]. At present, the best known and most widely used public key system is RSA, which was first proposed in paper "A method for obtaining digital signatures and public-key cryptosystems" by RL Rivest et al. in 1978. It is an asymmetric (public key) cryptosystem based on number theory, which is a block cipher system. Its security is based on the difficulty of the large number prime factorization, which is a well-known mathematical problem that has no effective solution [2]. RSA public key cryptosystem is one of the most typical ways that most widely used for public key cryptography in encryption and digital signature standards.

File packing and unpacking is a fundamental concept in many aspects of computer science, as it is involved in many applications Even if you don't actually feel, a lot of operations inside the computer is happened. This project is used to perform packing and unpacking activity for multiple types of files for security purpose we using cryptographic algorithm for encryption and decryption of data present in file.

II. RELATED WORK

In [2] this paper they give encryption parameter and classified the types of encryption techniques. The parameter of encryption included key length, encryption ratio and speed are discussed with the help of algorithm and also placed security issue. In [3], In this paper they discussed different file features e.g., data type, data size and key size. For these features they analyzed different symmetric key algorithm. They also discussed different algorithms like AES, DES, Triple DES, RCZ, and these algorithms behave different at encryption time.

In [5], these papers different types of algorithms based on cryptography is discussed. This algorithm provides security information and all are different types. In [4], this paper a survey has done. This survey is about existing work.in this survey work on different techniques of encryption has discuses. Each technique has its own advantages

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 6, June 2021||

DOI:10.15680/IJIRSET.2021.1006087

and disadvantages. Each technique is useful for different application. Basically, all the techniques discussed in that survey is useful for real time encryption. The AES technique is most popular in term of throughput, speed and time.

While in [6], a study is done in which both symmetric and asymmetric are briefly described, and also a comparison between these two algorithms is done in this study. After comparison it is clear that symmetric algorithm is better in term of rapidity as well as power although asymmetric is improved in term of tenability. $^{Ee = s}$ Algorithm in key symmetric encryption is originated improved in term of rate, safety and implementation while RSA algorithm is better in asymmetric key encryption in term of speed and security.

III. METHODOLOGY

This project is used to perform packing and unpacking activity for multiple types of files for security purpose we using cryptographic algorithm for encryption and decryption of data present in file. In a File system, data security plays a major role Encryption is the method of transforming the original texted message into an unknown form. Decryption is the method to transform the encrypted data into the original form.
The purpose of this study was to pack the multiple files into single packed file by encrypting original data and when we unpack the file create new files by decrypting the data. This project is used to perform packing and unpacking activity for multiple types of files. In case of Packing (Merger) activity me maintain one file which contains metadata and data of multiple files from specified directory. In case of Unpacking (Splitter) activity we extract all data from packed files and according to its metadata we create all files. In this project we have to use Java as Front end as well as Backend for platform independency. So, this project used object-oriented programming with the Java2 Standard Edition (J2SE) programming language.

In the regard of symmetric key encryption, we always use same key among the encryption as well decryption techniques. The main benefit of this algorithm is low computing power and its works very fast during the encryption process. This algorithm divides in two modes such as blocks ciphers and stream cipher. In the regard of block cipher all data would be dividing in the form of chunks or blocks. Data based in size of block and key would be provided for the encrypting the data. Stream cipher, data divide in the bit such as 0101010101 and randomized after the encryption rule will be applied. Symmetric is faster than the asymmetric algorithm. Figure no.1. Clarify the symmetric and asymmetric algorithms. Asymmetric key encryption is a technique, by this method different keys could be used for the encryption techniques and as well as decryption process. Here First key set is public. Second, we kept as a private. These both keys are similarly we able to call “public key encryption”.

Let’s take an example: If we want to publish first key as an encryption then the system communication as a private from the public in regard of unlocking user’s keys. Second condition, if we going to publish one unlock key decryption, after this our system would be perform as id-based verification for the purpose of documents lock by the dealer of that private key. This kind of public keys techniques very important because they can be used for over shifting encrypted keys or could be data secure, when both of users they don’t have such opportunity for the purpose of agreement secret key in the regard of private key.

Brief Introduction on RSA and Public-key Cryptography:

The key feature of public-key cryptosystem is that the encryption and decryption procedure are done with two different keys - public key and private key, and the private key cannot be derived from the public key, that enables the publication of the encryption key without the risk of leaking the secrets The most significant approach of public key cryptography algorithm is RSA, which can resist almost all the known passwords attacks so far. RSA algorithm, which is named after the inventors, is the first algorithm that can be used both for data encryption and digital signatures RSA algorithm's security depends on the difficulty of decomposition of large numbers. In the algorithm, two large prime numbers are used for constructing the public key and the private-key. It is estimated that the difficulty of guessing the plaintext from signal key and the cipher text equals to that decomposition of the product of two large prime numbers. RSA algorithm has been used as a possible authentication method in ISAKMP / Oakley framework. Diffie-Hellman key exchange algorithm is a key component of the framework. In the beginning of a key agreement session, participants communicate by using Diffie- Hellman algorithm and create shared keys which will be used for key agreement protocol of follow- up steps. In practice, in order to achieve the optimal efficiency, the symmetric key algorithms and public key cryptography algorithms are always combined together. That is using a symmetric key cryptosystem to encrypt the confidential information needed to be sent, while using the RSA asymmetric key cryptosystem to send the DES key. This takes advantages of both the two

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 6, June 2021||

DOI:10.15680/IJIRSET.2021.1006087

kinds of cryptography, namely, high-speed DES and RSA key management mechanism which is of convenience and security

The Process of RSA:

RSA cryptosystem uses the mode n, the smallest nonnegative complete the remaining lines of operation, where n is the product of two different primes p and q. RSA algorithm is described as following:

1. Randomly generates two primes P and Q of length / 2 bit;
2. Calculate the public key public Key=P*Q; (public Key's length is k-bit)
3. Generate a random encryption key keyE, 2<=keyE<=<D(n)-I, where GCD (keyE, <D(n)) =I;

   This is the necessary and sufficient conditions for solvability of the decryption key keyE *

   keyD mod

<D(n)=I, <D(n) is known as the Euler function of n, the value is <D(n)= (P- 1) *(Q-l)

4. Calculate the decryptionkey, keyD=keyE- l mod (n), keyE-l is inverse for the decryption key keyD. The formula of the original equation is keyE
   * keyD mod <D(n)=1

Now, the public key, encryption key and decryption key are all created.

Then, the process of encryption of the plaintext and decryption of ciphertext is as follows:

1. Encryption: C = MkeyE mod public Key; where Mis plaintext, C is ciphertext.
2. Decryption: M = CkeyD mod public Key; in which M plaintext, C is cipherte

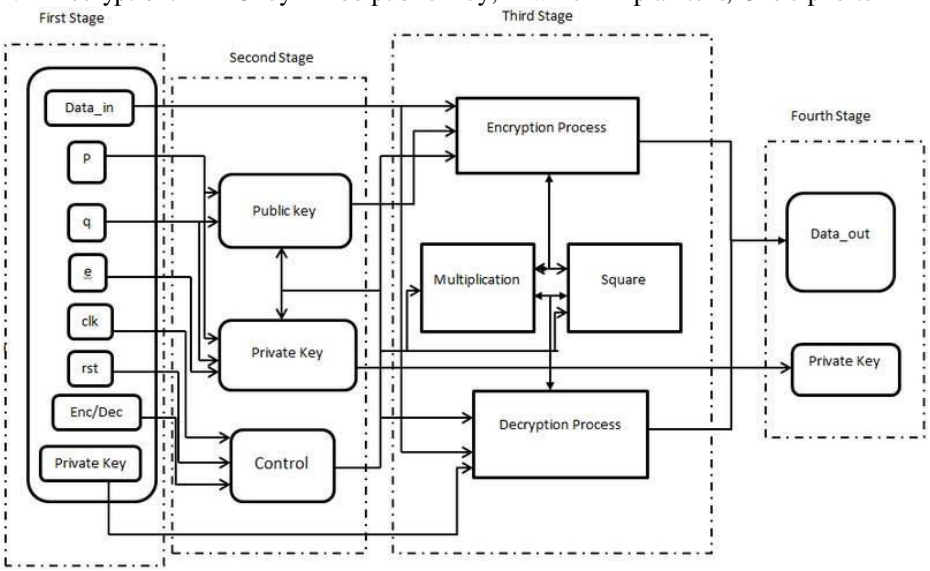

Figure 1: Block Diagram of RSA Encryption and Decryption

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 6, June 2021||

DOI:10.15680/IJIRSET.2021.1006087

Table 1: Performance analysis between some Symmetric and Asymmetric algorithms

Parameter	DES	3DES	AES	RSA
Key Used	Same key used for encryption and decryption	Same key used for encryption and decryption	Same key used for encryption and decryption	Different key used for encryption and decryption
Throughput	Lower than AES	Lower than AES	Lower than Blowfish	Low
Encryption Ratio	High	Moderate	High	High
Tunability	No	No	No	Yes
Power Consumption	Higher than AES	Higher than AES	Higher than Blowfish	High
Key Length	56 Bits	112 to 168 Bits	128, 192 or 256 Bits	>1024 Bit
Speed	Fast	Fast	Fast	Fast
Security Against Attack	Brute Force Attack	Brute Force Chosen-Plaintext, Known Plaintext	ıosen- Plain, Known Plaintext	Timings Attacks

IV. CONCLUSION

The encryption and decryption solution can ensure the confidentiality of the information, as well as the integrity of information and certainty, to prevent information from tampering, forgery and counterfeiting. Encryption and decryption algorithm's security depends on the algorithm while the internal structure of the rigor of mathematics, it also depends on the key confidentiality. In summary, this issue of the RSA encryption and decryption keys, RSA algorithm, the new use of the RSA and other issues to study and make some new programs, future work should be in the new RSA cryptographic algorithms and a wide range of applications continue to research.

REFERENCES

1. Jawahar Thakur, Nagesh Kumar, “DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis”, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 1, Issue 2, December 2011.
2. AL. Jeeva, Dr.V. Palanisamy, K. Kanagaram, “CO MPARATIV E ANALYSIS OF PERFORMANCE EFFICIENCY AND SECURITY MEASURES OF
3. SOME ENCRYPTION”, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622, Vol. 2, Issue 3, May-Jun 2012.
4. Ranjeet Masram, Vivek Shahare, Jibi Abraham, Rajni Moona, “ANALYSIS AND COMPARISON OF SYMMETRIC KEY CRYPTOGRAPHIC ALGORITHMS BASED ON VARIOUS FILE FEATURES”, International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.4, July 2014.
5. E. Surya C. Diviya, “A Survey on Symmetric Key Encryption Algorithms”, E Surya et al, International Journal of Computer Science & Communication Networks, Vol 2(4), 475-477.
6. Gurpreet Kaur, Manish Mahajan, “Evaluation and Comparison of Symmetric key algorithms”, International Journal of Science, Engineering and Technology Research (IJSETR), Volume 2, Issue 10, October 2013.
7. Gurvinder Singh Sandhu, Vinay Verma, “Comparing Popular Symmetric Key Algorithms Using Various Performance Metrics”, International Journal of Advance Research in Computer Science and Management Studies, Volume 1, Issue 7, December 2013

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details