Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 2, No. 1, February : 2023

A COMBINED MESSAGE ENCRYPTION AND DECRYPTION CRYPTOGRAPHIC ALGORITHM BASED ON AES AND RSA ALGORITHMS

Mr. R. UPENDAR RAO *M. Tech, Associate Professor, Department of ECE, NRI Institute of Technology*
K.LAKSHMI PREETHI, N.TEJASWINI, K.GEYA GEETHIKA, M.SAI SURENDRA *B. Tech, Student, Department of ECE, NRI Institute of Technology*

ABSTRACT

Cryptography is the science of information and communication security. File encryption is an easy means of securing personal or business data protection. The RSA and AES representative encryption algorithms are not capable of satisfying the criteria of file encryption reliability and security when used separately. A combined message encryption algorithm mixing of AES and RSA algorithms is recommended on this paper to overcome the above issues in order to solve file encryption performance and security problems. The Hybrid encryption will be considered a highly secure type of encryption if the public and private keys will be fully secured. The hybrid encryption is achieved through data transfer using unique session keys along with symmetrical encryption. Public key encryption was implemented for random symmetric key encryption. The recipient can use the public key encryption method to decrypt the symmetric key. Once the symmetric key is recovered, it is then used to decrypt the message. The experimental results shows that the RSA and AES combined encryption algorithm can not only encrypt files, but also provide the benefits of efficiency and protection of the algorithm.

Keywords: *AES algorithms, RSA algorithms, Hybrid encryption algorithms, File encryption, File decryption.*

I. INTRODUCTION

Throughout history, people have needed to protect their secrets. For thousands of years, people have been using codes and ciphers to protect those secrets. Back then, cryptography started off as an art; it was only studied by writers and artists. It was used as early as 1900 BCE in Ancient Egypt. During these times the Egyptians would create a code using hieroglyphics by switching the order of them and only people who knew the order could translate the message. (Cryptology) As the years went on these methods become cleverer and more involved. The Greeks contributed a lot to cryptography, including two ciphers, the Spartan Scytale and the Polybius Square. The scytale was used by the Spartan army to send messages without being detected. Two people in the army would have two pieces of wood that were equal in diameter. The messages would be written on strips of leather wrapped around the wood. These messages could only be read if the strip was wrapped around a wood of the same size. The Polybius Square was another unique technique. The Greeks used a 5 by 5 square, with sides labeled 1 through 5 on the top and the side, while the squares would be filled with the alphabet (Cryptology).

The AES algorithm has impressive results, and it is relatively simple in terms of encryption speed. It inherits the value of the speed of DES encryption and has accelerated speed. It has good encryption efficiency and is ideal for vast volumes of data being encrypted and decrypted. Compared to the DES algorithm and the 3DES algorithm, the AES algorithm is enhanced in terms of security, and its security is comparatively high, but still much lower than the RSA algorithm; In terms of key length, the AES algorithm improves the issue of inadequate DES length, which is increased from56 bits of the DES algorithm to 128/192/256 bits; In terms of resource consumption, the AEES algorithm improves. However, AES algorithm still has some shortcomings in key management,

which makes the security management and distribution of keys a little difficult, which makes it possible for AES algorithm to be cracked under certain conditions. It includes the following two aspects: (1) Since AES uses the same key in the encryption and decryption of data, it is necessary for both parties to agree on the key in advance, and to ensure that the key information cannot be obtained by the third party, otherwise the information may be cracked; (2) Each time the two parties use the AES algorithm, they use a unique key that other people do not know. This will increase the number of keys and cause a management burden. On the whole, the biggest advantage of the RSA algorithm is that it has good key management functions and security, and the security of the RSA algorithm is much higher than that of the AES algorithm. The RSA algorithm has a pair of private keys and a pair of public keys. The public key is used for encryption, and the private key is used for decryption, and the encryption key is inconsistent with the decryption key. If a certain plaintext is encrypted with a certain key, it must use the corresponding key to decrypt it, which greatly enhances its security. The security of the RSA algorithm cryptosystem depends on the difficulty of the inverse of the mathematical function of the encryption algorithm.

II. LITERATURE REVIEW

Cryptography includes two main mechanisms; Symmetric- key and Asymmetric-key cryptosystems. Symmetric key use a single pre-shared key for both encryption and decryption. The data encryption standard (DES), triple-DES(3DES), blowfish, advanced encryption standard (AES) are common examples of symmetric-key ciphers. The asymmetric cryptosystems use a pair of keys. A public key for the data encryption process and a private key is used for the decryption process. Rivest – Shamir – Adleman (RSA), El Amal, digital signature algorithm (DSA) are common examples of asymmetric ciphers. Both symmetric and asymmetric ciphers have benefits and limitations. Symmetric ciphers are fast but suffer key exchanging. Asymmetric ciphers solve the key exchange problem but slow. Practically, hybrid cryptography, which is an integration of symmetric and asymmetric ciphers, makes use of the efficiency of symmetric ciphers and the simplicity and security of asymmetric ciphers. The hybrid cryptographic approach aims to produce a more secure, better performance, and robust algorithm than applying basic ciphers individually. R. Nigoti et al., have proposed a survey on various security issues concerning cloud computing and cryptographic ciphers to achieve cloudsecurity. They have concluded that DES is easier to implement on the cloud than AES. Also, RSA and Diffie-Hellman were used in the keys generation phase that later is used with symmetric ciphers. G. Singh and Supriya, have presented a comprehensive study of the most common like RSA, DES, 3DES, and AES. Their study has concluded AES is the most efficient algorithm concerning speed, time, throughput, and avalanche effect factors. They also came up with that combination of two or more algorithms adds more security to the cloud data. R. S. Sajjan et al, have surveyed the multilevel encryption that integrates two or more ciphers and applied them to the cloud data. First, they have investigated different ciphers. At the end of their study, they developed double layers of encryption based on DES then RSA encryption ciphers. They concluded that multilevel encryption is more secure than single level models.

M. F. Mushtaq et al, have presented a comprehensive study that examined the different criteria of the most common symmetric ciphers such as DES, 3DES, Blowfish, and AES. A performance comparison in terms of encryption and decryption time, throughput, key size, memory usage, and entropy was provided. They have concluded that blowfish fit well in terms of encryption and decryption time, and AES has a better avalanche effect. A. A. Maryoosh et al, have reviewed various hybrid algorithms applied to safeguard data stored on the cloud servers. They provided a comparison between these models to emphasize the advantages and limitations of each model. M. K. Sinchana and R. M. Savithramma , have proposed a survey on cloud computing security. This study examined a set of hybrid cryptographic models and clarified their design, implementation, and advantages of each model. They come with a fact that security and efficiency are enhanced when utilizing a combination of symmetric and asymmetric ciphers. S. Chaudhary et al, have presented a

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 2, No. 1, February : 2023

comparative study between cryptographiccciphers and the hybrid approach using these ciphers. They have concluded that symmetric ciphers are more efficient than asymmetric ciphers. Hybrid cryptographic models are better in terms of security and avalanche effect.

III. PROPOSED SYSTEM

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, 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 record encryption scheme that consists of the benefits of the two algorithms based totally at the contrast among the RSA algorithm and the AES set of rules in terms of encryption and decryption time, protection, key management, and key period.

This paper absolutely utilizes the rate gain of the AES algorithm within the encryption operation and the steadiness and key management benefit of the RSA algorithm and consists of the encryption electricity of each to encrypt the code. The key need to no longer be accessed by using an insecure 0.33 celebration to make certain the security of the AES set of rules, and all events should talk the important thing earlier, in any other case the important thing may be continuously updated. In this article, after extensive notion, the AES set of rules key is used in the encryption technique of the hybrid encryption algorithm to encrypt the report records to provide cypher textual content 1, and then the RSA set of rules public key is used to encrypt cypher text 1 and the AES key to generate cypher textual content 2. The public secret's public within the RSA algorithm, and the private keys used for decryption and is non-public. Encryption with the aid of the algorithm of hybrid encryption. Since the AES key isn't always protected inside the key, public RSA encrypted records cannot be decrypted as non-public RSA secret is stored personal. The facts aren’t always encrypted. In the hybrid set of rules, mathematical operations randomly produce the public and private keys of the RSA set of rules.

3.1. Block Diagram of Proposed Model

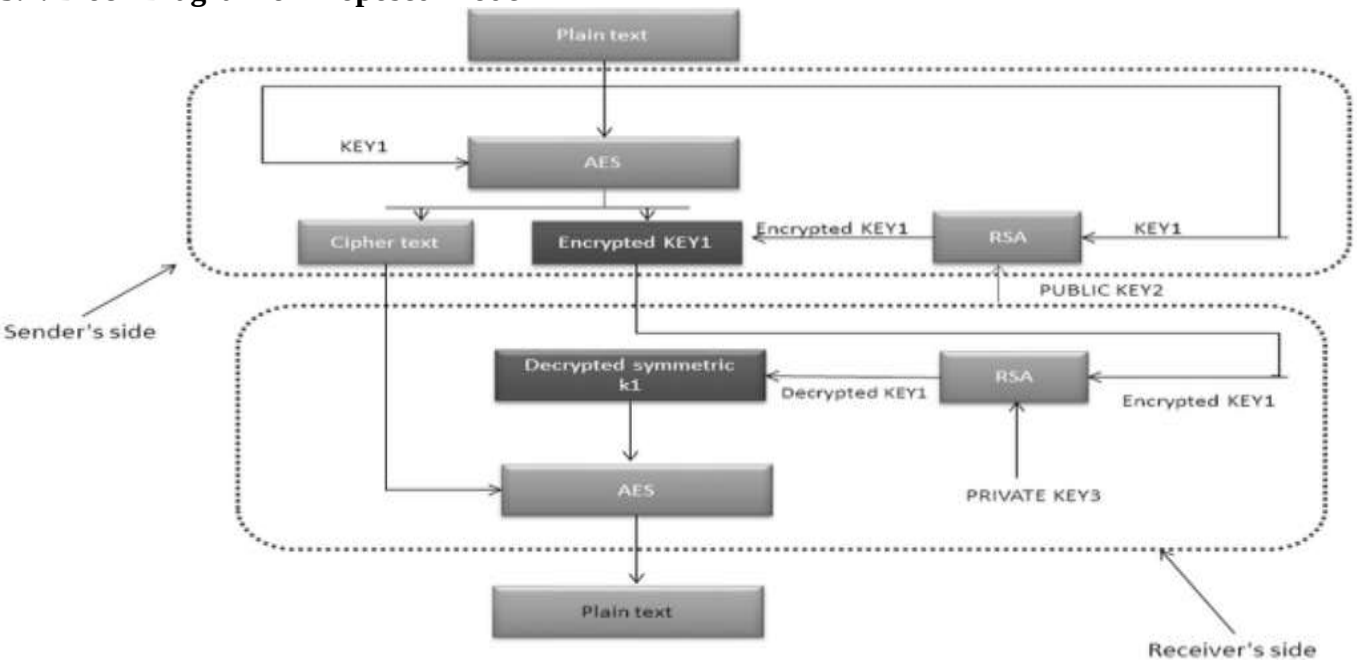

Fig 3.1 RSA &AES hybrid encryption algorithm file encryption and decryption scheme

3.2. Description of block diagram

The above block diagram describes 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. The block diagram completely utilizes 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 cipher text 2. The public key is public in the RSA algorithm, and the private key is used for decryption and is private. Since the AES key is not included in the key, public RSA encrypted data cannot 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 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 block diagram. 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. 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 in Fig-3.1.

3.3 Hybrid key generation principle

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:

1) First, two unequal large prime numbers p and q must be randomly selected.
2) Then calculate the product n of p and q, that is, $n = p \times q$.
3) Calculate Euler function $\phi(n) = (p-1)(q-1)$.
4) A positive integer e is randomly selected, and $1 < e < \phi(n)$ is made, & $\gcd(e, \phi(n)) = 1$.
5) According to the equation $ed = 1 \bmod \phi(n)$, the result of d is obtained, where $0<d<n$.
6) According to the formula PU = {e, N}, the public key of the RSA algorithm is saved, where e is a public key.
7) According to the expression PR = {d, p, q}, the private key is saved, where d is the private key.

3.4 Hybrid algorithm encryption principle

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. In this process are four simple arithmetic techniques, sub bytes, shift rows**,** mix columns and add round key.

1)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 4 byte 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 box.

2) 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.

3)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).

4)Introduce the Round Key. When converting Add Round Key, 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:

$c = m^e \bmod n$, and $0 <= m < n$-----(1)

3.5 Hybrid algorithm decryption principle

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 isused 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.

$m= c^d \bmod n$----------(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 is its own inverse.

IV. EXPERIMENTAL RESULTS

This paper suggests the implementation of file encryption and decryption by AES and RSA hybrid encryption algorithm for an effective file encryption. The hybrid algorithm is implemented using LABVIEW 2017. In this case the hybrid algorithm combination of AES and RSA is analyzed and the process of getting output is need to provide input a cipher key and a plain text and therefore we get cipher text1 this is the process at AES encryption then coming to RSA encryption here we need to provide the same cipher key (public key) at in-data and get another cipher text2 this is RSA encryption then moving to, RSA decryption we need to provided the cipher text2 and we get the output as input cipher key. AES decryption as we collected all the required, we need to provide all the data cipher key and cipher text1 therefore get the encrypted plain text very securely. The below figures shows the results of encryption and decryption of AES and RSA algorithm correspondingly.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 2, No. 1, February : 2023

4.1. AES&RSA Encryption output

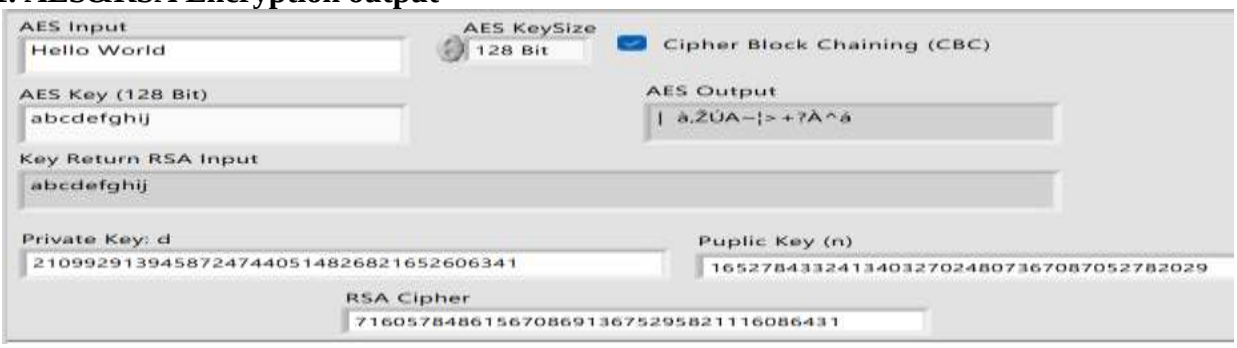

Fig-4.1 Simulation result of AES&RSA Encryption

At input side

- AES input---> Hello World
- AES Key ---> abcdefghij

At output side

- AES Cipher --> | à,ŽÚA~¦>+?À^á
- RSA Cipher --> 716057848615670869136752958211160864 31

4.2. AES &RSA Decryption Output

Fig-4.2 Simulation result of AES&RSA Decryption

At input side

- AES Cipher --> | à,ŽÚA~¦>+?À^á
- RSA Cipher --> 716057848615670869136752958211160864 31

At output side

- RSA Cipher---> Hello World
- AES output ---> abcdefghij

V. CONCLUSION

In this project the implementation of file encryption of AES and RSA hybrid encryption algorithm through the contrasting tests, it is concluded that in file encryption the hybrid encryption algorithm optimizes the performance of encryption key storage, data protection in device architecture, software-application, and other areas that can efficiently maintain file data protection.

The proposed model utilizes benefits of both symmetric and asymmetric cryptographic algorithms for providing data security to cloud user. The encryption and decryption of the main data have a single secure key, which is used for encryption and decryption. Another asymmetric key is used, to further encrypt the previous key, which provides enhanced security. Since the hybrid system gives a double layer of security, it can emerge as one of the strong and secure algorithms. Also, by using a random select key and lookup table for the RSA algorithm, we decrease the complex calculations and increase the computation speed without compromising on the randomness and efficiency of the algorithm. In future, this Hybrid system behavior can be analyzed for various inputs like video, image and audio. This proposed system supports addition and deletion of any standard

encryption algorithm to further enhance security. Hence any new algorithm can be created by replacing either one of the two or both algorithms being used. The range of applications varies from military uses to regular civilian applications.

REFERENCES

[1] Marwan Ali Albahar, Olayemi Olawumi, Keijo Haataja, Pekka Toivanen "Journal of Information Security, 9, 168-176. DOI: 10.4236/jis.2018.92012 Apr. 9, 2018.
[2] EZEKIEL Bala , AJIBOLA Aminat , and EBELOGU Christopher U" Hybrid Data Encryption And Decryption Using RSA And RC4 " International Journal of Scientific & Engineering Research Volume 10, Issue 10, October-2019 ISSN 2229-5518.
[3] Si, H., Tang, B.: The current status of RSA application and its application in file encryption. Comput. Telecom (06), 76-77+80 (2009).
[4]Zhang, W., Zhou, R., Gao, Y., Wang, J.: File encryption based on AES algorithm. Softw. Guide16(06), 180– 182 (2017).
[5]Yang, J.: Design and implementation of an AES algorithm encryption transmission system. Electron. Des. Eng.27(03), 123 – 126+131 (2019).
[6]Nedjah, A., de Macedo Mourelle, L., Wang,C.: A parallel yet pipelined architecture for efficient implementation of the advanced encryption standard algorithm on reconfigurable hardware. Int. J. Parallel Program.44(6), 1102 – 1117 (2016)
[7]Riaz, M.N., Ikram, A.: Development of a secure SMS application using advanced encryption standard (AES) on android platform. Int. J. Math. Sci. Comput.(IJMSC)4(2), 34 – 48 (2018).
[8]Vanitha M, Sakthivel R and Subha S, "highly secured high throughput VLSI architecture for AES algorithm," IEEE International Conference on Devices, Circuits and Systems, 2012, pp. 403-407.
[9] Zhang X, Parhi K K, "High-speed VLSI architectures for the AES algorithm," IEEE Transaction on Very Large Scale Integration (VLSI) Systems, vol. 12, pp. 957-967, September 2004.
[10] Hammad I, Elsankary K, Elmasry E, "High-Speed AES Encryptor With Efficient Merging Techniques," IEEE Embedded Systems Letters, vol. 2, pp. 67-71, September 2010.
[11] Daemen J, Rijmen V, The design of Rijndael: AES, the advanced Encryption Standard, Berlin, 2002, pp. 56-59.
[12] Oukili S, Bri S, "High speed efficient advanced encryption standard implementation," IEEE International Symposium on Networks, Computers and Communications, Marrakech, 2017, pp. 1-4
[13]Moumen, A., Sissaoui, H.: Images encryption method using steganographicLSB method, AES and RSA algorithm. Nonlinear Eng. Model. Appl. 6(1), 53 – 59(2017)
[14]Yang, L.T., Huang, G., Feng, J., Xu, L.:Parallel GNFS algorithm integrated with parallel block Wiedemann algorithm for RSA security in cloud computing. Inf. Sci.387,254 – 265(2016)
[15]Ye, X.: Optimization strategy of RSA algorithm. Electron. Des. Eng.25(20), 83– 85+89(2017).
[16]Qi, N.: Application of RSA algorithm in two-dimensional code anti-counter feinting technology. Nanjing University of Posts and Telecommunications (2017).
[17] D. Boneh and G. Durfee, "Cryptanalysis of RSA with private key d less than N0.292," IEEE Trans. on Information Theory, vol. 46, no. 4, pp. 1339-1349, July 2000.
[18] P. C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, Cryptology Conference on Advances in Cryptology (CRYPTO'96), London, 1996, pp. 104-113