AES AND RSA-BASED HYBRID ALGORITHMS FOR MESSAGE ENCRYPTION & DECRYPTION

Mr. Abhishek Guru

Department of Computer Science and engineering, Kalinga University, Naya Raipur, India

Dr Asha Ambhaikar

Department of Computer Science and IT, Kalinga University, Naya Raipur, India

Abstract— 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 hybrid encryption algorithm mixing AES and RSA algorithms is suggested in this paper to overcome the above issues in order to solve file encryption performance and security problems. The experimental results suggest that the RSA and AES hybrid 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

With the advent of the mobile Internet, electronic records have steadily reached the lives of people, and they are widely used because of their ease of alteration and fast transition. In digital files, there are also many security threats, such as relying on disc encryption tools, insufficient data encryption, and breaking encrypted files by brute force. When important information is leaked, it can pose a significant security threat to people, companies and even national security.

This paper focuses on the standard symmetric encryption algorithm of the AES representative algorithm and the asymmetric encryption algorithm of the RSA algorithm. Many researchers have considered it as a hot subject in the study of the encryption of these two encryption algorithms. Si and Tang showed the use of the RSA file encryption algorithm and suggested that small files could be encrypted by the RSA algorithm[1]. Although the key management benefits of RSA are completely exploited by this method, the encryption of large files has not been solved by the problem that the speed of the RSA algorithm is not efficient. In order to simplify file encryption and solve the problem of grouping data from the data to be processed, Zhang et al. used the 'Cipher text misappropriation' in the AES algorithm but did not recognize the security of the AES algorithm, which could still be broken under certain conditions[2]. While the AES algorithm and the RSA algorithm have been commonly used in the field of file encryption, in terms of encryption security and encryption effectiveness, there are still some concerns.

Based on the latest RSA and AES algorithms used in file encryption alone in the implementation of certain issues, this paper makes full use of AES encryption speed, high security RSA and powerful key management features, introduces a blend of AES encryption algorithm and RSA encryption algorithm, and applies it to file encryption. In this analysis, the Netbeans environment was used to simulate the Java language algorithm, and the benefits of this hybrid algorithm have been checked in the performance of encrypted data.

II. Overview of AES and RSA Algorithms

Overview of AES Algorithm

The AES (Advanced Encryption Standard) algorithm is the abbreviation of the standard algorithm for advanced data encryption [3], which is an algorithm for symmetric key encryption. The AES algorithm is a block algorithm for encryption that is used to supplement the DES algorithm. The AES algorithm uses 128-bit, 192-bit, and 256-bit keys of varying lengths[4], but its block length may only be 128-bit, and normally 128-bit keys[5] are used. The same key is used in the AES algorithm encryption and decryption process, and the process of grouping and encryption is as seen in Fig.1

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

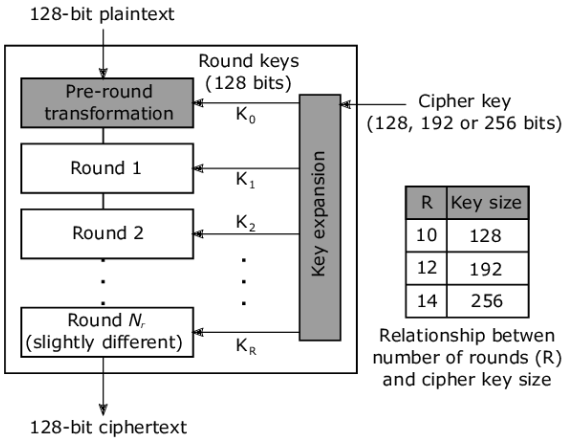


Fig. 1. AES algorithm grouping and encryption diagram

The AES algorithm has impressive results. The AES algorithm 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[6] 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[7], which is increased from 56 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.

RSA Algorithm Overview

RSA public key encryption algorithm, is the most influential public key encryption algorithm. It is an encryption algorithm based on large integer factorization [8], and is also an asymmetric encryption algorithm. The keys of the RSA algorithm appear in pairs, and the encryption of the data is done by the private key and the public key. The public key is public, can be known by anyone, is used to encrypt data and verify the signature; the private key decrypts and signs the data.

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. It is called the difficulty of the factorization of large numbers [9]. RSA algorithm keys are powers of large Numbers, the longer the key length, the more difficult to crack.

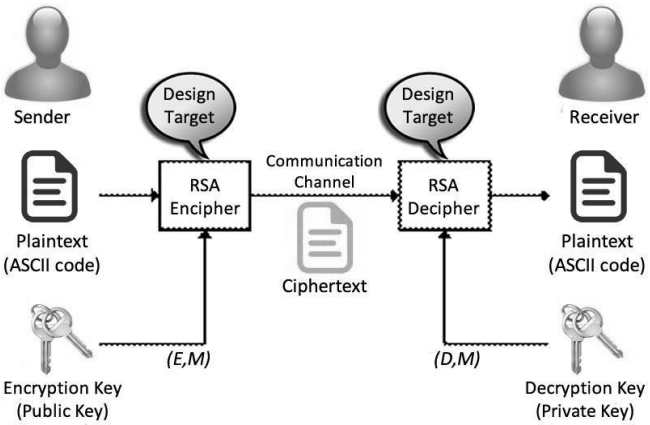


Fig. 2. RSA algorithm and encryption diagram

Although it has high security, RSA algorithm has many shortcomings in performance. RSA algorithm is based on large Numbers, which leads to slow operation speed and low efficiency. It is only suitable for encryption of a small amount of data. Most of the researches on RSA algorithm focus on prime factorization in mathematical attack.

III. A Hybrid Encryption Scheme for AES and RSA

The latest hybrid algorithm scheme used to encrypt files is based on the simple arithmetic methods of RSA and

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

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.

Hybrid Algorithm Encryption File Theory Overview

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.

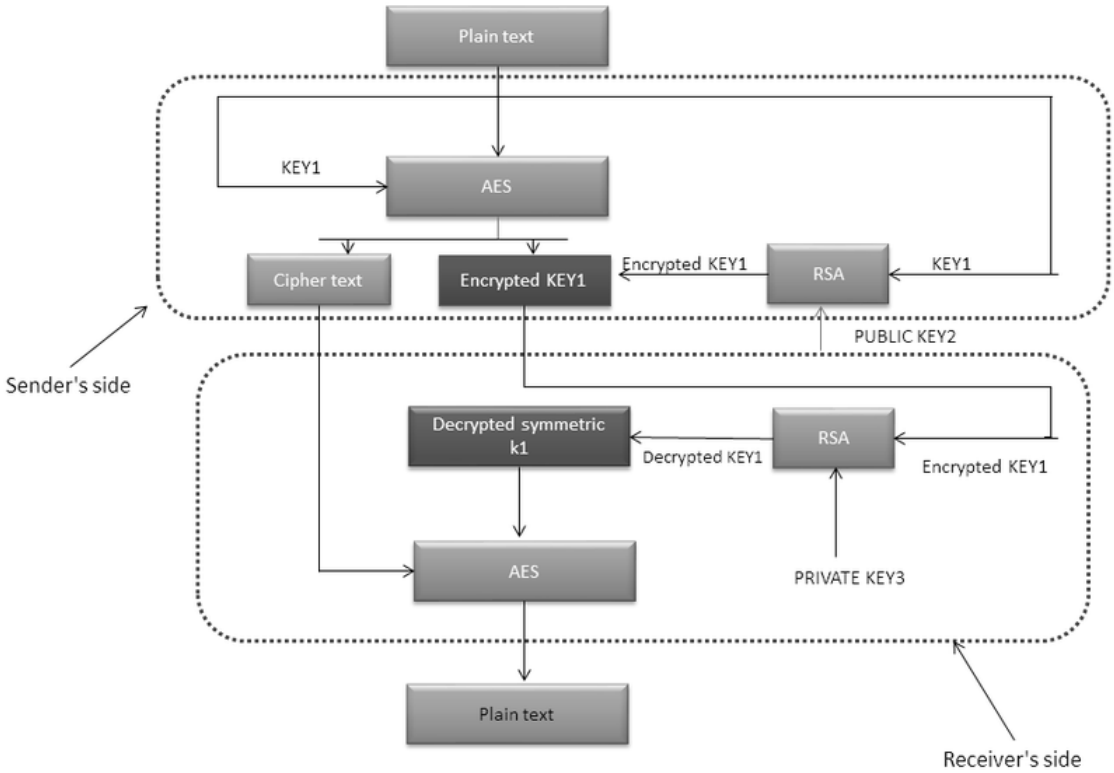


Fig. 3.RSA and AES hybrid encryption algorithm file encryption and decryption scheme

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

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

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 in Fig.3.

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:

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 x q.
3) Calculate the Euler function ø(n) = (p-1)(q-1).
4) A positive integer e is randomly selected, and 1 < e < ø(n) is made, and gcd(e, ø(n)) = 1.
5) According to the equation ed = 1 mod ø(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 [10].

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 128 bit 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, SubBytes, ShiftRows, MixColumns and AddRoundKey.

1) BytesSub. SubBytes, 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 SubBytes 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 s-box.
2) RowsShift. Each row is cyclically moved to the left in the forward ShiftRows by a row number offset, that is, the ith row of the state matrix is shifted left by I bytes[11].MixColumns. MixColumns transform operates on each column in state and treats each column as a fourth degree polynomial. The addition and multiplication of MixColumns operation are both defined on the finite field on GF(28).
3) 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[12]:

$$c = m^e \bmod n, \text{ and } 0 <= m < n \quad (1)$$

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 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].

$$m = c^d \bmod n \quad (2)$$

Where d is

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

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, SubBytes, ShiftRows and Mix-Columns are the inverse operations of the encryption process, but in Add RoundKey, the inverse operation is the same as the forward transformation because the xor operation is its own inverse.

IV. Experiment and Result Analysis

This research uses the Java language to execute the algorithm, and the Netbeans compilation tool is used under the Windows 10 operating system support. The files used in the experiment are all 1–50 MB files with the."txt" filename.

Since there are huge files in this experiment, the method of memory file mapping is used to increase performance, minimise the number of disc accesses, and regular access to large file data. This is because the IO read/write file process copies the data, copies the contents of the file from the hard disc to the buffer in the kernel space, and then copies the data to the user space, creating two copies of the data; in the memory mapping, the actual data copy is rendered during the missed page interrupt. The direct mapping relationship between the file and the user's space would actually copy the file from the hard disc to the user's space, and only one data copy will be made.

In this experiment, the same batch of files was encrypted and decrypted using three algorithms. In order to make the experimental results more reliable, the formula used to combine the results of several runs is used and the value with a significant error is omitted. Based on the results, the RSA algorithm, the AES algorithm and the hybrid algorithm are compared and the variations in encryption and decryption time are evaluated. Among them, in various file sizes, the scheduling of the three is as shown in Table 1.

Table 1. Hybrid algorithm encryption time and size of RSA and Blowfish.

Plaintext size (KB)	Plaintext size (Byte)	RSA+Blowfish Encryption Time (nanoseconds)	RSA+Blowfish Encryption File size (KB)	RSA+Blowfish Decryption Time (nanoseconds)
32	32710	9047797	59355	1881211
64	65420	12203366	118428	2189046
128	130840	13555651	237417	5057937
256	261680	14240434	477370	9345405
512	523360	29886045	951418	18116046
1024	1048460	40855251	1898922	25666278
2048	2096920	43979084	3813804	44415486
4096	4193840	63542269	7624638	54848853

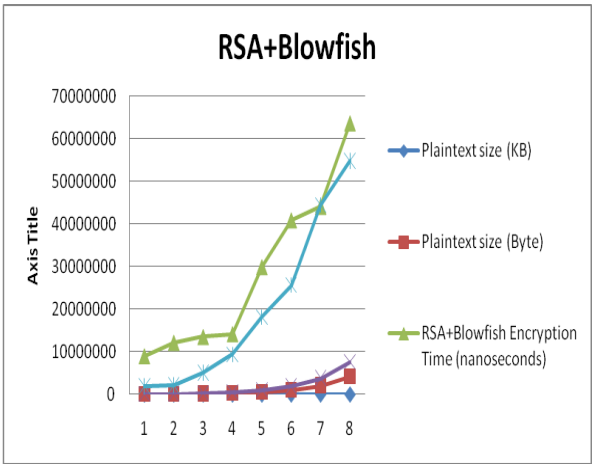


Fig. 4. Hybrid algorithm encryption time and size of RSA and Blowfish.

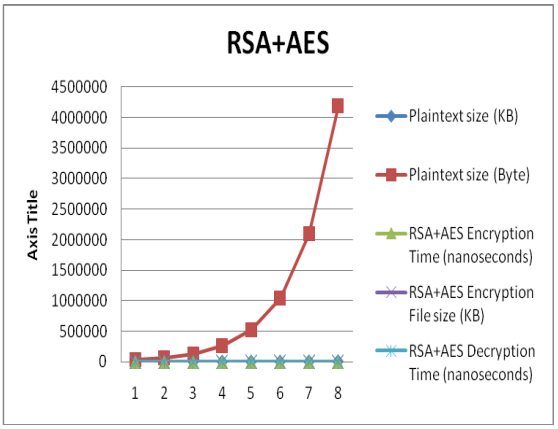
According to the above table, the encryption time map of the three is analyzed, as shown in Fig.4.

Test the encryption time of the three, and analyze the experimental results: As the file size increases, the execution time of the RSA algorithm increases almost linearly; The encryption time of AES increases with the file, and the growth rate is slow;

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Table 2. Hybrid algorithm decryption time and size of RSA and AES

Plaintext size (KB)	Plaintext size (Byte)	RSA+AES Encryption Time (nanoseconds)	RSA+AES Encryption File size (KB)	RSA+AES Decryption Time (nanoseconds)
32	32710	120	31	140
64	65420	126	64	131
128	130840	127	128	159
256	261680	133	256	143
512	523360	138	512	173
1024	1048460	145	1024	171
2048	2096920	146	2048	199
4096	4193840	188	4096	222



The encryption time of the RSA and AES combination encryption algorithm is similar to the AES algorithm. When the file size is 1.19 MB, the performance of the hybrid algorithm is 8.9 times that of the RSA algorithm, but when the file size is 50 MB, the efficiency has been increased 75.5 times, and the efficiency continues to increase as the file size increases. The decryption schedule of the three algorithms is shown in Table 2. The decryption time maps of the three algorithms are evaluated using the data of the above decryption schedule, as seen in Fig.5.

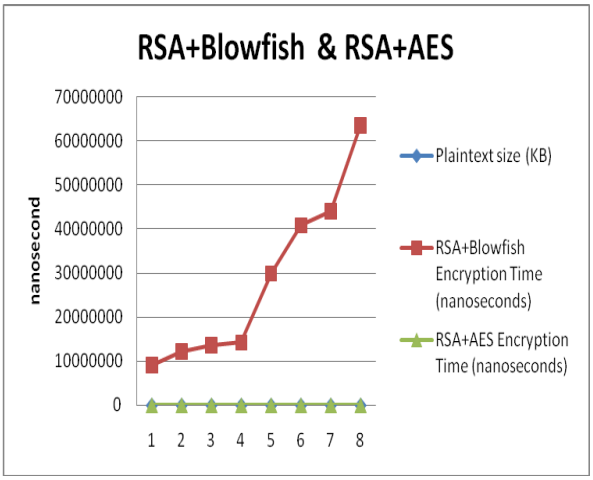


Fig. 5. Competition of RSA-Blowfish & RSA-AES

Using experimental research, the decryption time of the RSA algorithm and the AES algorithm increases with an increase in file size. The RSA algorithm has increased dramatically, almost linear development, and the AES algorithm has increased marginally. The decryption time of the hybrid encryption algorithm is stable close to a certain value, close to the AES algorithm. Compared to the RSA algorithm, the improvement in decryption performance has a noticeable impact on large files. The decryption performance of the hybrid encryption algorithm is 50 MB while the file size is 50 MB. It has grown by almost 25 times and is on a rising trend. Through contrasting encryption and decryption above, the hybrid algorithm greatly increases encryption performance relative to the RSA algorithm while encrypting and decrypting broad data. Owing to the use of dual-layer encryption, the decryption complexity is intensified as the file is decrypted, and the hybrid algorithm optimises the dilemma that the AES algorithm key is leaked and the authentication is ineffective.

V. Conclusion

This paper suggests the implementation of file encryption of the AES and RSA hybrid encryption algorithm, presents the fundamental concepts of AES and RSA algorithms, and analyses their advantages and drawbacks. Through contrasting tests, it is concluded that in file encryption, the hybrid encryption algorithm optimises the performance of encryption, key storage and data protection. In device architecture, software application, and other areas that can efficiently maintain file data protection, the application of the hybrid algorithm suggested in this paper can be used. In this analysis, however, there are still some shortcomings, such as the inability to avoid replay attacks in the

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

file encryption process, and data tampering and forgery when the double key is cracked, which will be more refined in future testing.

Reference:

[1] Si, H., Tang, B.: The current status of RSA application and its application infile encryption.Comput. Telecom (06), 76–77+80 (2009).

[2] Zhang, W., Zhou, R., Gao, Y., Wang, J.: File encryption based on AES algorithm. Softw.Guide16(06), 180–182 (2017).

[3] Yang, J.: Design and implementation of an AES algorithm encryption transmission system.Electron. Des. Eng.27(03), 123–126+131 (2019).

[4] Nedjah, A., de Macedo Mourelle, L., Wang, C.: A parallel yet pipelined architecture forefficient implementation of the advanced encryption standard algorithm on reconfigurablehardware. Int. J. Parallel Program.44(6), 1102–1117 (2016)

[5] Riaz, M.N., Ikram, A.: Development of a secure SMS application using advanced encryptionstandard (AES) on android platform. Int. J. Math. Sci. Comput. (IJMSC)4(2), 34–48 (2018).

[6] Moumen, A., Sissaoui, H.: Images encryption method using steganographic LSB method,AES and RSA algorithm. Nonlinear Eng. Model. Appl.6(1), 53–59 (2017)

[7] You, Y.: Design and implementation of combined encryption algorithm based on AES andRSA in DOA. Chengdu University of Technology (2018).

[8] Yang, L.T., Huang, G., Feng, J., Xu, L.: Parallel GNFS algorithm integrated with parallelblock Wiedemann algorithm for RSA security in cloud computing. Inf. Sci.387, 254–265(2016)

[9] Ye, X.: Optimization strategy of RSA algorithm. Electron. Des. Eng.25(20), 83–85+89(2017).

[10] Qi, N.: Application of RSA algorithm in two-dimensional code anti-counterfeitingtechnology. Nanjing University of Posts and Telecommunications (2017).

[11] Leng, F., Xu, J., Pei, S.: Network information security method based on RSA fusion AESalgorithm. J. Huaqiao Univ. (Nat. Sci.)38(01), 117–120 (2017).

[12] Wan, Z.: Public key encryption scheme based on QI hyperchaos and its FPGAimplementation. Tianjin Polytechnic University (2018).

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731