RESEARCH ARTICLE

NORTH AMERICAN ACADEMIC RESEARCH (NAAR) JOURNAL
2021 MARCH, VOLUME 4, ISSUE 3, PAGES 256-267
https://doi.org/10.5281/zenodo.4661097

Join Public Key and Private Key for Encrypting Data

Md Helal Hossen[1]*, Md Monim Hasan[2], Wenjun Hu[2]

[1]Intelligent information processing technology, Huzhou University, China.

[2]School of Information Engineering, Huzhou University, China.

OPEN ACCESS

Accepted Mar 31,2021
Published Apr 03,2021

***Corresponding Author:**
Md Helal Hossen

DOI :https://doi.org/10.5281/zenodo.4661097

Pages: 256-267

Funding: Huzhou University, China

How to cite this article (APA):
Hossen M, H., Hasan, M. M., & Hu, W. (2021 Join Public Key and Private Key for Encrypting Data. *North American Academic Research, 4(3)*, 256-267. doi: https://doi.org/10.5281/zenodo.4661097

Conflicts of Interest
There are no conflicts to declare.

ABSTRACT

Data security is a major issue in the digital world. Cryptography is the most use technique for data security. Cryptography is one of the principle of protection of digital data. Encryption and decryption ensure the data confidentiality. The effectiveness of the encryption security depends on the key management, while RSA algorithm uses two keys. Public key is used to encrypt the data, this key can be used by anyone to encrypt. Private Key is used only to decrypt the data. If the private key is leaked that means the security system cannot protect any data. The Perfection of the encryption depends on the key management and the internal mathematics method of the algorithm. In this paper we propose an encryption method using AES and RSA algorithm. This encryption method can be used for cloud computing, desktop data and database data security.

Keywords—CRYPTOGRAPHY, DATA SECURITY, ENCRYPTION, DECRYPTION, CIPHER TEXT

Introduction

The modern age is almost dependent on digital technology and digital communication. At present digital data is a crucial part of our life. Now managing this on-air data and cloud storage data is a big challenge for us. So, data security is a crucial issue in computing. The methods for encrypting a message can be classified into: transposition method and mathematics encryption. The transposition method moves the characters around. Encryption is a process of converting data to conditionally unreadable format. In this process data is converted to a special format that is called cipher text. A cipher text is only accessible to the real user of the data. The "Encryption" word comes from the Greek words Krypton, this indicates something is hidden or secret. The encryption was first introduced into communication with information security and it aims make normal text into cipher text, which elaborately makes a simple information unreadable to unauthorized person. The method which uses mathematics for encryption operation is called cryptography or cryptology. It is also Greek word that is hidden/secret. Cryptography is basically used to hide documents in a methodical way so that only the legal owner can read the documents. It is a convenient method to reserve and transfer documents in secured system. Statue authorized own rescan access the Information [1] [2]. Cryptography is involved with two operations: decryption and encryption. This is a data science that scrambled data in a mathematical way that no one can

get information from the data. The intended receiver can get the real contents of data after decrypted [3] [4]. The encryption makes a meaningless format of a data, that can be readable, but it does not contain any information to the unauthorized receiver. The information will be significant when it is decoded by the legitimate decryption key. The encryption and decryption is involve with key sharing. In a symmetric cryptography key sharing is challenges. Symmetric cryptography utilizes just one key for encryption and decoding. The deviated cryptography utilizes two unique keys for encryption and unscrambling. Symmetric cryptography is quicker than Unbalanced cryptography [5] [6]. The cryptography guideline is a numerical based calculation for encryption and decoding activity [7] [8].

I. Related Works

A. Digital signature with RSA Encryption huge amount of data is waiting for the future generation. To make more convenient use of data, this data should be converted to dynamic resources [9]. It is a distributed computing environment that provides data sharing, resource sharing even hardware sharing over the internet. When resources are sharing over the internet, there is concern issue about data security. Cloud networking, including data storage, file server, backups, network traffic, host protection, has several issues. A digital signature principle with the RSA algorithm is proposed here to encrypt the data as the user transmits it over the network. A mathematical scheme for proving the validity of a digital letter or record is a digital signature or digital signature scheme. Then the software encrypt these lines by the private key those are called message digest. Finally, the software creates a digital signature. The public key is used decrypt the digital signature. For the creation of a true one-way authentication system [12], a public key cryptosystem may be used. For financial transactions, over the network and in other situations where it is necessary to detect forgery and tampering, this approach may be used.

B. RSA cryptosystem by applying the algorithm for cuckoo search optimization this calculation was intended to make smooth information alliance issues in the distributed storage by applying the Cuckoo Search Optimization calculation [10]. They scramble the information from the unapproved client utilizing the mystery key that is produced by the RSA calculation. The generated key will be shared with the sender and receiver. The cuckoo search algorithm is used to select the key. The encryption keys optimized by the cuckoo search technique, to avoid the brutal force attack. Since this method can increase the length of the private key of the algorithm, it is effective for improving safety. Besides, it performs faster than the other algorithms, thus it is efficient.

C. Modified Advanced Encryption Standard Evaluation of the AES encryption first and then use the had loop System to render an updated version. To strengthen data protection, they incorporate random disruption in creation [11]. AES algorithm uses a single key to column mix operation and key choreography that is improved in this paper. Had loop framework is basically use to calculations of the massive amounts of data. Massive data need a strong security when they are in online. Symmetric algorithm use a single key to encrypt and

decrypt the data, such as AES and DES algorithms. A symmetric encryption system can be represented as CS = M, C, K, e, d, where: m ∈M represents a plaintext message set; C = c represents a cipher text message set; K = k represents the key set; E represents the encryption mapping process, i.e. E: K×M = C; D, represents the decryption mapping process, i.e. D: K×C = M

II. Proposed model

The proposed model is structured to ensure secure communication from one point to another during the transmission of such data files (which contain sensitive information). Until transferring, data files are encrypted and then decrypted to reveal the hidden information inside them after they arrive at the destination stage. A two-stage encryption is implemented using RSA and AES encryption standards to secure and complicate the capture of information within data files as far as possible. 3 keys, one is AES key (256-bit) and a public & private RSA key pair are required in this technique. The public and private key pair must be created by the target stage, the private key must be kept in a safe location and the public key should be sent to the source side to encrypt the AES key [19].The Basic operation procedure of RSA algorithm is depicted by figure 1. The AES algorithm is depicted by figure 2

Figure 1. Encrypting file using symmetric key

Figure 1. Decrypting key and Data

A. Motivation

Symmetric encryption and asymmetric encryption are carried out using various methods. Symmetric encryption is done on streams and is therefore ideal for encrypting large quantities of data. Asymmetric encryption is achieved on a small number of bytes and is thus only suitable for small quantities of information. Symmetric cryptography use single key for encryption and decryption. Comparatively symmetric algorithm is usually very faster and its works normal with low RAM requirements like AES. But symmetric algorithm has big problem to key transportation for its single key operation. On the other hand asymmetric algorithm like RSA use two different keys for encryption and decryption. Its use public key to encrypt. So there is not risk to transport the key, but this is little bit costly compared with the symmetric key algorithm. Here we propose a method that use AES to encrypt the file and then we encrypt the AES key with RSA that make the

encryption asymmetric and effective.

B.

RSA Algorithm the RSA algorithm is an asymmetrical cryptography algorithm. Asymmetric means that there are two separate keys. This is also called public key cryptography, because one of them can be given to anybody. It is best to keep the other key confidential. It is based on the fact that it is difficult to find the factors for an integer (the factoring problem).RSA stands for Ron Rivets, Leonard Adelman and Aid Shamir, who first identified it publicly in 1978[8][14]. A RSA user creates and then publishes the product of two broad prime numbers, along with an auxiliary value, as their public key. Keeping the prime variables secret is critical. Those may use the public key to encrypt a text, however only anyone with knowledge of the main factors can decode the message successfully with the methods currently published if the public key is wide enough[15].

For the RSA algorithm, the keys are generated as follows:

1. Choose two independent p and q prime numbers. The integer p and q should be selected at random for security reasons, and should be identical in magnitude but vary in length by a few digits to make factoring more difficult. Using a primarily test, prime integers can be found effectively.
2. Compute n = pq, where n is used as a module for both public and private keys. The primary length is its length, typically expressed in bits.
3. Compute λ (n) = lcm(λ(p), λ(q)) = lcm(p − 1, q − 1), where λ is Carmichael's titian function. This value is kept private.
4. Choose an integer e such that 1 < e < λ (n) and gcd(e, λ(n)) = 1; i.e., e and λ(n) are cop rime.
5. Determine d as d ≡ (mod λ(n)).This is more clearly stated as: solve d width e ≡ 1 (mod λ(n)).e with short bit-length and small Hamming weight results in more efficient encryption –most commonly+ 1 = 65,537. However, much smaller values of e (such as 3) have been shown to be less secure in some settings[13][17].e is released as the public key exponent. d is kept as the private key exponent.

We're now presenting a summary of encryption and decryption. Suppose that the data is "M."

Transform it to a number m less than n for encryption by using the agreed-upon reversible procedure known as the padding system. Then compute the cipher text c corresponding to:

$$c = m^e \ mod \ n$$

In which c is the Encrypted data? For decryption, m can be recover from c using private key exponent d by computing

$$c^d \equiv (m^e)^d \equiv \ m \ (mod \ n)$$

For clearly understanding this process, here we give a simple example about RSA encryption and Decryption [16].

Example:

1. Choose two distinct prime number, such as $p = 47\ and\ q = 59$;
2. Compute n = pq , i.e. $n = 47 \times 59 = 2773$;
3. Compute the Carmichaels' totient function of the product as $\lambda(n) = \text{lcm}(p-1, q-1)$, i.e. $\lambda(2773) = lcm(46,56) = 2576$;
4. Choose an integer e with $1 < e < 2576$ and suppose $e = 17$
5. Compute d by the modular multiplicative inverse of e (mod λ(n)) and we have $d = 157$.

Worked example for the modular multiplicative inverse:

$$d \times e = 1\ mod\ \lambda(n)$$
$$157 \times 17 = 1\ mod\ 2576$$

The public key is (n= 2773, e=17). For a padded plaintext message m, the encryption function is $c(m) = m^{17}\ mod\ 2773$.

The private key is (n=2773, d=157). For an encrypted cipher text c, the decryption function is $m(c) = c^{157} mod\ 2773$

For instance, in order to encrypt m= 65, we calculate

$$c = 65^{17}\ mod\ 2773 = 332$$

To decrypt c= 2790, we calculate

$$m = 332^{157}\ mod\ 2773 = 65$$

Advanced Encryption Standard (AES) Algorithm AES is based on a design principle known as a substitution-permutation network, and it is fast for both software and hardware. AES is a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. In the other hand, a 32-bit multiple, with a minimum of 128 bits and a maximum of 256 bits, could be possible .AES functions on a byte matrix of 4-4 column-major order, called the state, while some Randal implementations have a greater block size and have additional columns in the state. The Advanced Encryption Standard is the symmetric encryption algorithm that is most widely used and is expected to be used today (AES) [18]. It is found to be six times quicker than triple DES, at least. As follows, the characteristics of AES are:

- Symmetric key cipher of symmetric block
- 128-bit data, 128/192/256-bit keys
- Stronger and quicker than Triple-DES
- Provide complete specification and layout information

The number of rounds in AES is unpredictable and depends upon the length of the key. AES uses 10rounds for the 128-bit keys, 12 rounds for the 192-bit keys, and 14 rounds for the 256-bit keys. In each of these rounds, a distinct 128-bit round key is used, calculated from the original AES key. The schematic of AES structure is given in figure 3 and figure 4.

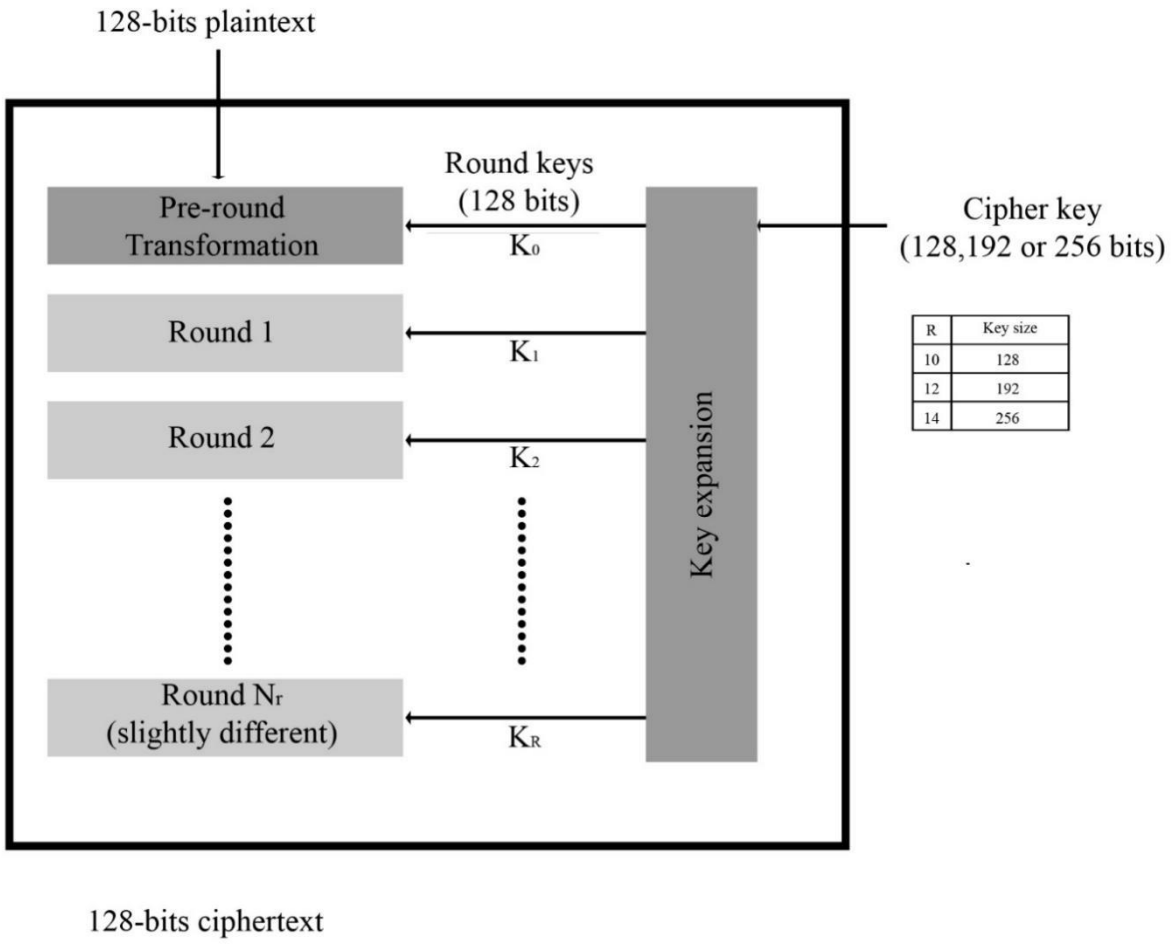

Figure 2. 128 bits AES operation

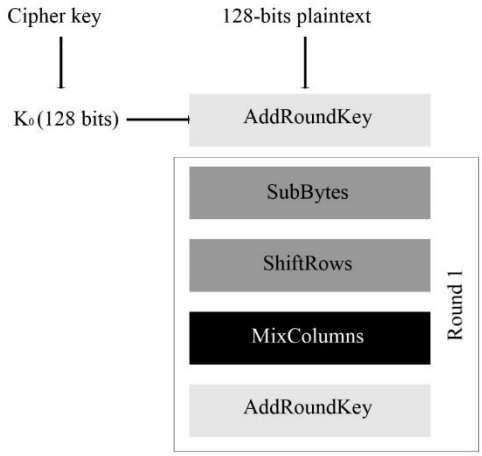

Figure 3. Encryption process

(1) Encryption Process

We are restricted to clarifying a norm round of AES encryption here. Four sub-measures comprise each round. Figure 3 shows the first round of activity. Shift Rows any of the grid's four columns is moved to one side. All 'dropping down' passages on the correct side of the column are re-embedded. The change happens as follows:

- The first row does not move,
- The second row moves one place (byte) to the left.
- The second places are pushed to the left by the third side
- The third place is moved to the left by the fourth row

(2) Decryption Process

The method of decryption of an AES cipher text is similar to the encryption procedure in reverse order. Each round consists of four processes executed in reverse order. —

- Add round key
- Blending columns
- Row change
- Substitution of bytes

D.RSA and AES Combine operation normally for file encryption, we use two types of encryption algorithms symmetric and asymmetric. In our model, we have AES symmetric algorithm and RSA asymmetric algorithm. AES algorithm is best for file encryption but AES cannot perfect security for its single key operation secured. That is why we use asymmetric RSA algorithm to encrypt the AES key. Step by step our method procedure is given below.

(1) Receiver makes a key pairs of asymmetric-key algorithm (RSA), then give the public key to sender.

(2) As data is ready to be sent, the key from AES is encrypted by public key and eventually the AES key is also encrypted by RSA private key.

(3) Using the RSA private key the data receiver decrypt the AES key and the receiver decrypt the data using AES key.

E. Solution Symmetric Encryption an extraordinary stream class called Crypto Stream, which scrambles information read into the stream, is utilized to deal with symmetric cryptography classes. Utilizing any class got from the Stream class, including File Stream, Memory Stream, and Network Stream, the Crypto Stream class might be instated. We can execute symmetric encryption on a set of stream objects using these groups. The groups of symmetric encryption given by. To encrypt and decrypt data, the NET Framework needs a key and a new initialization vector (IV). Another key and IV are naturally produced at whatever point we make another example of one of the controlled symmetric cryptographic classes utilizing the default constructor. Anybody we approve to unscramble our data should have a similar key and IV and should utilize a similar

calculation. For the most part, for every meeting, another key and IV ought to be made, and neither the key nor the IV ought to be held for ensuing meeting use. Client will typically scramble the symmetric key by utilizing lopsided encryption to hand-off a symmetric key and IV to a distant element. It is hazardous to communicate the key through an unprotected organization without scrambling it, since somebody who captures the key and IV will at that point unscramble their data.

Iv. Discussion of proposed model

Our system is almost perfect for any kind of file security of all platforms. The system has some limitation that is not remarkable. Overall the system is working fine with great data security.

Advantages

In our model we have use private key for decryption. Private Key hacking is almost impossible, because we have used every time auto generated different cop rime numbers. An auto generated manifest file contain information about the encrypted key. Private Key remain safe from the general user, because, for encrypting file, no need private key. Our system can encrypt large file and any kinds of file. This system can be used in offline data (Personal Computer), Cloud computing and web database [20].

Disadvantages

Our system is not convenient with low ram devices. To encrypting large data, this method is time-consuming. The encrypted file needs a manifest file for decrypting, losing manifest file can make some data damage.

V. Experiments

We use Microsoft .NET Cryptography library to demonstrate our system. In our application, the symmetric algorithm IV property's utilized, which's automatically set to a new random value when a new instance of one of the Symmetric Algorithm classes is created .Generate RSA Key Pair: "Generate RSA Key Pair" function apply "RSA Crypto Service Provide" to make the RSA key pairs and then the created keys are saved in a file format of XML string, which is saved into two different XML format files, "private Key. Xml" and "public Key. xml."First, we give detailed description about Encrypting File and Decrypting File.

(1) Encrypting: "Encrypt File" uses "As Crypto Service Provider" to make plain file encrypted. Encrypt is the end user of "Encrypt File". Encrypt make the one-time pad AES key and IV to encrypt file. At a time it create the signature key to calculate the file signature. Finally, it encrypts the AES key and "signature Key" using the public key (RSA Key), and saves all encrypted key information in file. This file name is manifest file. The manifest file will be use next time when the data should be decrypted.

(2) Decrypting: This process is the alternative way of the file encryption. At first it use the manifest file for gaining data from the cipher text using the RSA private key. Decryption is simply the inverse process of encryption logic. It uses decrypts cipher text. This how it got the AES key. Then it use the

AES key to finally decrypt the data. Now, we will give the working procedures and its application in real data. We Selecta file for encryption, i.e. "Test File", in which this file can be any format file. This process is shown in Figure 5.

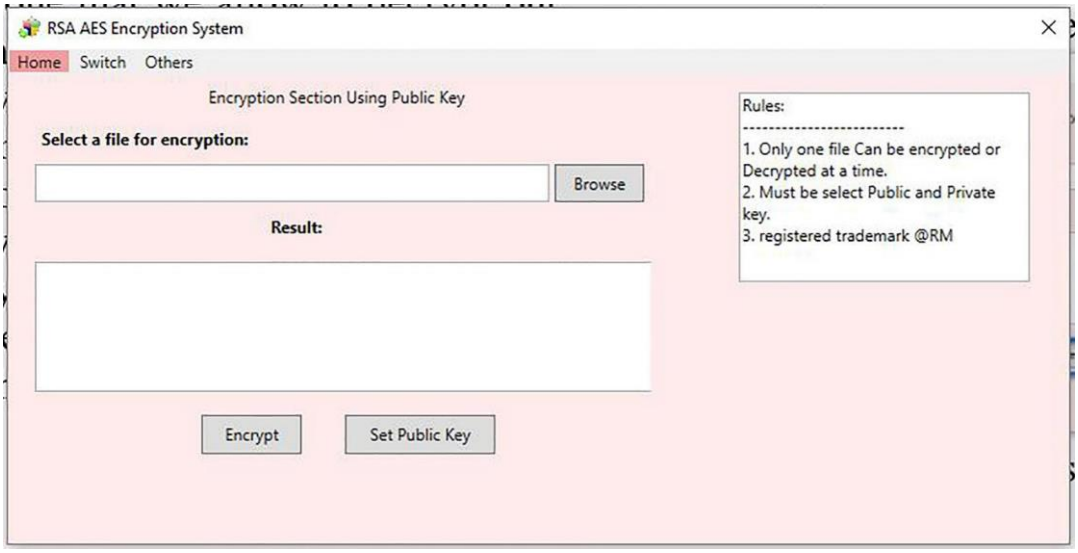

Figure 4. File selection for encryption

Then, import the public key, which is saved in an XML file. After pressing the "OK" button, the file is encrypted and saved as a file named "Test File. encrypted". Mean while, a manifest file is also saved in the same location named "Test File .manifest .xml". This process is shown in Figure 6.

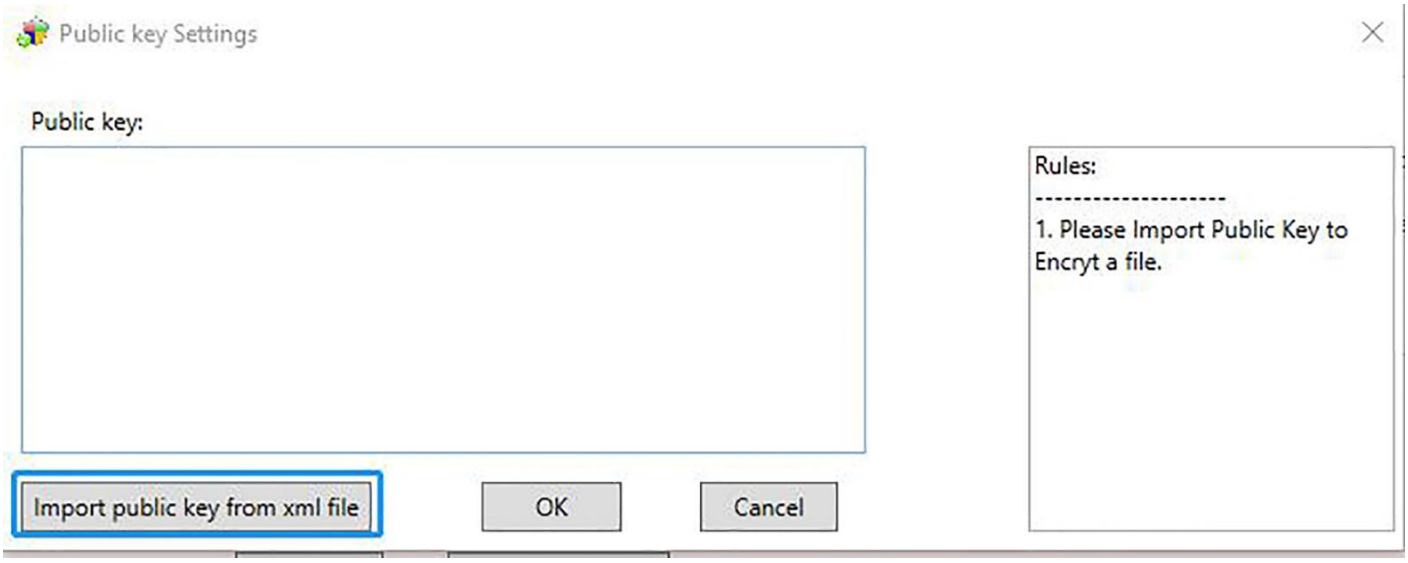

Figure 5. Importing public key from xml file

Figure 6. Importing public key from xml file to decrypt file, trigger the "switch “menu and the application will be changed to decryption mode. Now, we select the encrypted file. Use the private key and manifest file and press "Decrypt "for decryption. Then, the Decrypted file “Test File .decrypted “can be obtained. These two steps are shown in Figure 7 and Figure 8, respectively.

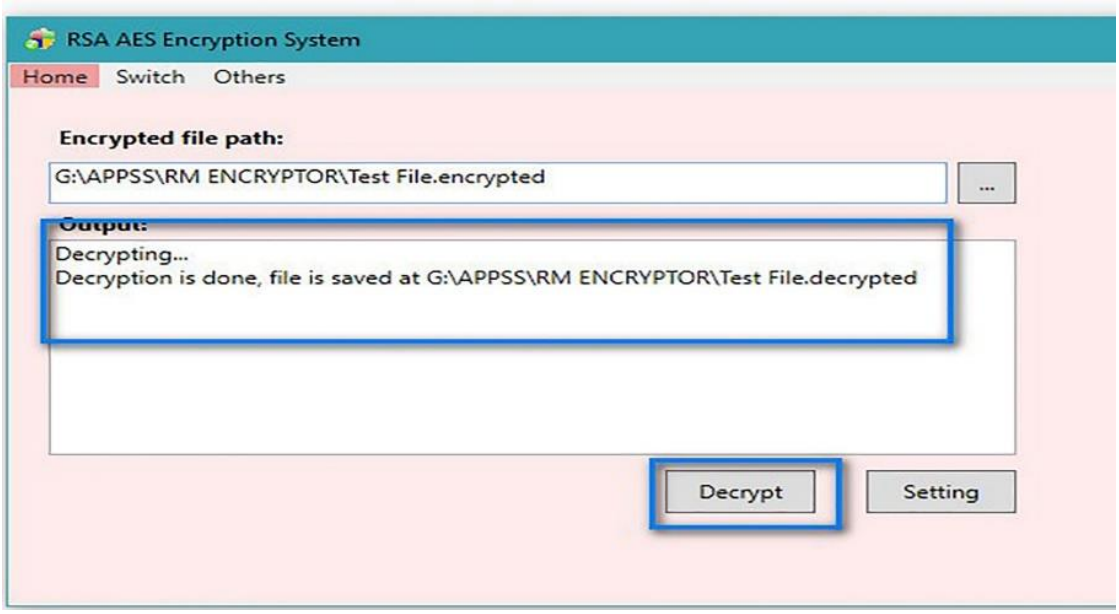

Figure 6. Selecting encrypted file

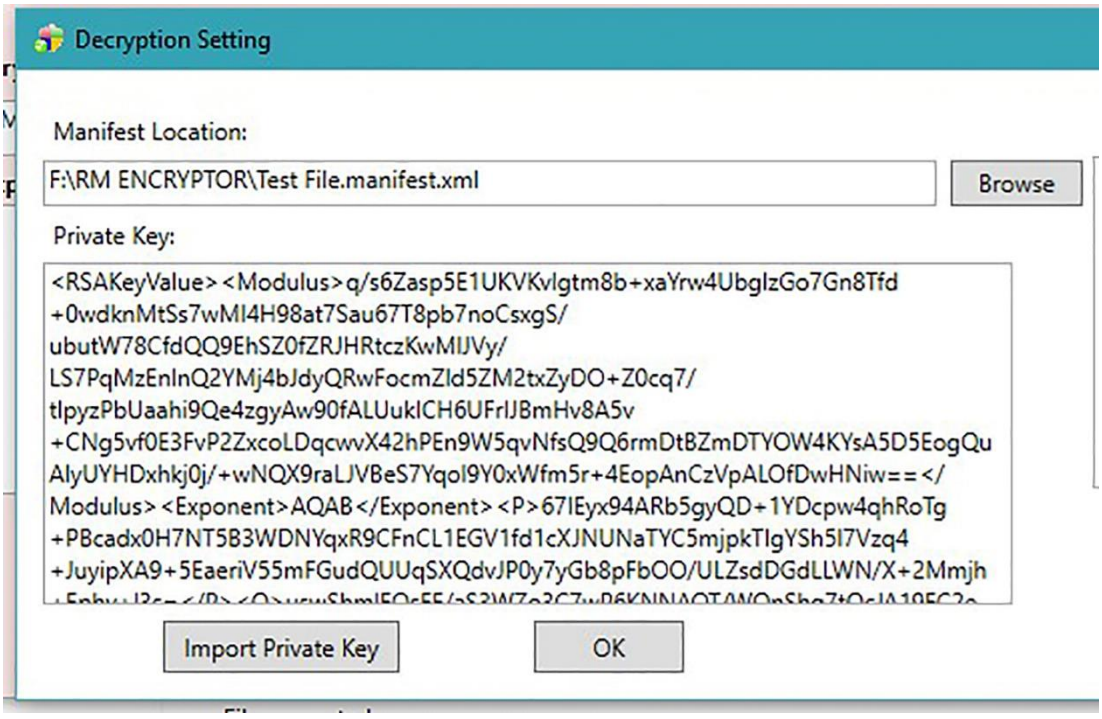

Figure 7. Import private key and decryption successfully done

Conclusion

In this paper we have analysis various algorithm. And finally we choose the RSA algorithm for data encryption. RSA is an asymmetric key algorithm. It provides high level security for encryption. Here we developed a system that secured your data in web database, desktop database, and cloud storage or anywhere

you want to store data. For available storage system, sometimes information lost the privacy. When your database is in online it can be hacked. Someone can destroy your data or they can use your data to unethical and corruption types job. Our encryption method protects your data with a great security. This encryption method will protect all kind of data in any type of database (MS SQL server, oracle, MySQL, DB2) from hacker. Corporate company, banking system, government and Non-Government Company should try this method.

References

[1] Fatma Mallouli, Aya Hellal. "A Survey on Cryptography: comparative study between RSA vs ECC Algorithms, andRSA vs El-Gamal Algorithms"6th IEEE International Conference on Cyber Security and Cloud Computing 2019

[2] Stallings, Network Security Essentials -Applications and Standards (4. ed., internat. ed.). PearsonEducation,2010.

[3] H. D. Phaneendra, "Identity-Based Cryptography and Comparison with traditional Public key Encryption : A Survey," International Journal of Computer Science and Information Technologies, vol. 5, no. 4, 2014, pp. 5521- 5525.

[4] Cai, C. and Y. Lu. "Asymmetric encryption JAVA and VC. Comput. Knowled. Technol.", 2011, pp. 4306-4307.

[5] G. C. Kessler, "An Overview of Cryptography," 2018.

[6] D. Stinson, Cryptography: Theory and Practice. CRC Press LLC, 1995.

[7] A. Kahate, Cryptography and Network Security. Mc-Graw Hill Education, 2013.

[8] V. K. Mitali and A. Sharma, "A survey on various cryptography techniques," International Journal of Emerging Trends Technology in Computer Science, vol. 3, Issue 4, July-August 2014, pp. 307-308.

[9] Uma Somani, Kanika Lakhani, Manish Mundra "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing". PDGC-2010.

[10] S. Raja shree, A. Chilambu Chelvan, M. Rajesh "An efficient RSA cryptosystem by applying cuckoo search optimization algorithm" 24 April 2018.

[11] Lin Teng, Hang Li, Shoulin Yin, and Yang Sun, "A Modied Advanced Encryption Standard for Data Security" , (VDOI: 1816-3548-2019-00016),2019.

[12] W. Diffie and M. E. Hellman, " New Directions in Cryptography," I€€€ Trans. Info. Theory, vol. IT-22, November. 1976, pp. 644-54.

[13] Dorothy E. Denning, "Digital Signatures with RSA and Other Public-key Cryptosystems " ,NSF Grant MCS80-154 84.April 1984, Vol.27, no.4.

[14] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM,February. 1978,vol. 21, no. 2, , pp. 120-126.

[15] Gary C. Kessler, "An Overview of Cryptography.Handbook on Local Area Networks",Auerbach, September. 1998.

[16] R.L. Rivest, A. Shamir, and L. Adleman "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems",September 1, 1977.

[17] Chen, C. and Z. Zhu. "Application of RSA algorithm and implementation details",2006, Comput. Eng. Sci., 9: 13-14.

[18] Daemen, Joan; Rijmen, Vincent (March 9, 2003). "AES Proposal: Rijndael". National Institute of Standards and Technology. p. 1. 5 March 2013. Retrieved 21 February 2013.

[19] M. Kumar and E. G. Dharma, "A comparative analysis of symmetric key encryption algorithm", IJARCET, vol. 3, no. 2, 2014.

[20] L. Singh and R. K. Bharti, "Comparative performance analysis of cryptographic algorithms", International journal of advanced research in computer science and software engineering (IJARCSSE), 2013, vol. 3, no. 1

Md Helal Hossen
Intelligent information processing technology
Huzhou University, China.
Email: helal.h017@gmail.com

Md Monim Hasan
School of Information Engineering
Huzhou University, China.
Email: monimcse@gmail.com

Wenjun Hu
School of Information Engineering
Huzhou University, China
hoowenjun@foxmail.com