STUDY OF RSA ALGORITHM FOR DATA ENCRYPTION AND DECRYPTION

Mr. Pankaj Chandra
Assistant Professor. Department of Information Technology, Guru Ghasidas Vishwavidyalaya Bilaspur (C.G.)

Mr. Santosh Soni
Assistant Professor. Department of Information Technology, Guru Ghasidas Vishwavidyalaya Bilaspur (C.G.)

Abstract

There are two types of cryptography private key cryptography and public key cryptography. In Private key cryptography only single key used for encryption as well as for decryption. In Public key cryptography two different keys, one for encryption and other for decryption are used. Nobody can decrypt the encrypted message i.e. cipher text without this key pair. The following paper does the detailed study about RSA Algorithms.

Keywords: RSA Algorithm, Cryptography, Ciphers, Decryption.

1. Introduction

The Cryptography is a Greek word that means “Secret Writing”. Cryptography is a technology to hide data from Intruders on the communication channel. For Information Security many encryption algorithms are widely used. There are two types of encryption algorithms, Public (Asymmetric or Different) key encryption and Private (Symmetric or Same) key encryption. In Private key cryptography only single key used for encryption as well as for decryption. In Public key cryptography two different keys, one (Public Key) for encryption and other (Private Key) for decryption are used. RSA is a type of Public key cryptography. RSA also uses two keys, one public key for encryption and one private key for decryption. For long key size RSA works better.

2. Cryptography

The Cryptography is a Greek word that means “Secret Writing”. Cryptography is the process of transforming original message (understandable data) into not understandable data (cipher text) to secure data.

Basic Terminologies –

1. Plain Text – This is the original unencrypted message that is fed into algorithm as input.
2. Cipher Text – This is encrypted text or text after transformation.
3. Encryption Algorithm – The Encryption Algorithm transforms plain text to cipher text with the help of Encryption key.
4. Decryption Algorithm – The Decryption Algorithm Transforms Cipher text to again plain text with the help of decryption key. Decryption is reverse process of Encryption.

3. Private Key Cryptography

Symmetric key or same key of Private Key cryptography uses only one (Single) key for data encryption as well as for data decryption. Both sender and receiver should aware about the secret key to encrypt and decrypt the information in Private Key Cryptography.

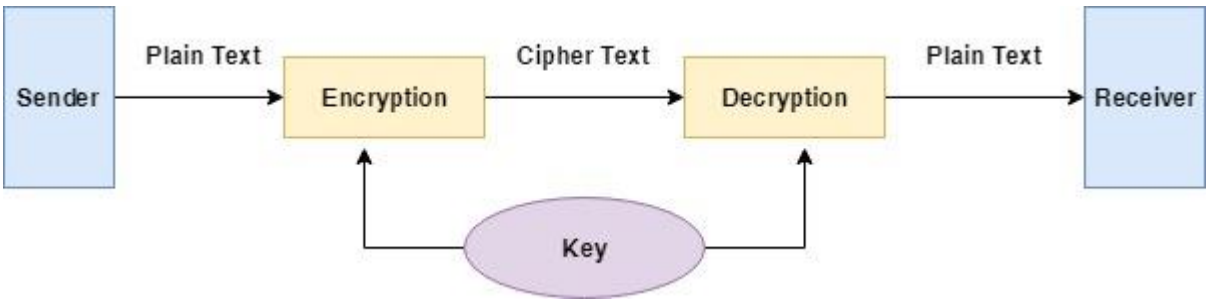

Figure 1: Private Key Cryptography

4. Public Key Cryptography

Public key or asymmetric key of different key cryptography uses two different keys, one key for encryption and other key for decryption. The key used for encryption is called the public key and the key used for decryption is called private key and should be kept secure.

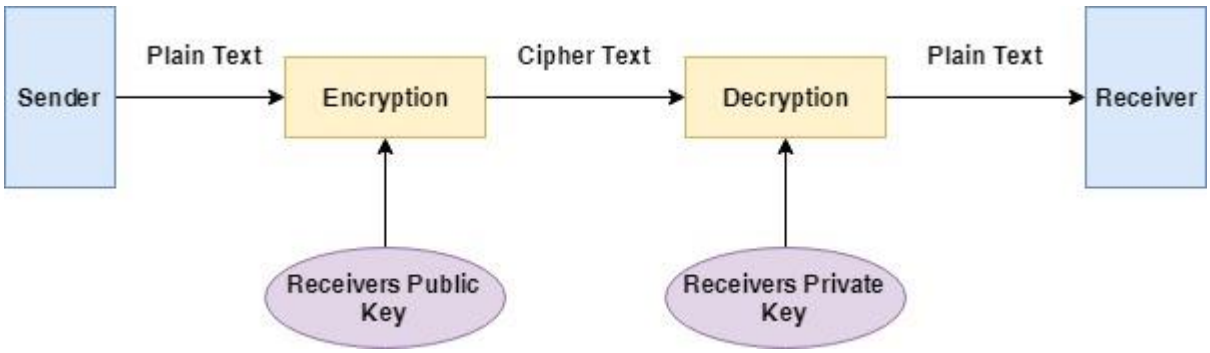

Figure 2: Public Key Cryptography

5. RSA Algorithm

RSA algorithm involves three different phases –

Phase 1 – Key Generation

Phase 2 – Encryption

Phase 3 – Decryption

5.1 - Phase 1 – Key Generation

The Key Generation Process are described below -

Step 1 – Select 2 prime numbers P and Q. (Where P is not equal to Q)

Step 2 – Calculate N by performing N = P * Q.

Step 3 – Calculate Z by performing Z = (P-1) * (Q-1).

Step 4 – Choose D such that D is relatively prime to Z

Which means GCD (D, Z) = 1

Step 5 – Determine E such that, (E*D) mod Z =1

Now Private Key is pair of numbers, Private Key = (N, D)

Public Key is also pair of numbers, Public Key = (N, E)

N is common to the Private and Public Keys and both sender and receiver know the value of N.

5.2 - Phase 2 – Encryption

The Sender uses following algorithm to encrypt the message –

Cipher Text C = M^E mod N

Where C is Cipher Text i.e. text after encryption.

M is Plain Text.

E is encryption key.

5.3 - Phase 3 – Decryption

The Receiver uses following algorithm to decrypt the message –

Plain Text M = C^D mod N

Where C is Cipher Text i.e. text after encryption.

M is Plain Text.

D is decryption key.

6. Study on RSA Algorithm using Example

6.1 - Example

Step 1 – Select 2 prime numbers P=5 and Q=11. (Where P ≠ Q)

Step 2 – Calculate N by performing N = P * Q = 5*11 = 55.

Step 3 – Calculate Z by performing Z = (P-1) * (Q-1) = (5-1)*(11-1).

Z = 4 * 10 = 40

Step 4 – Choose D such that D is relatively prime to Z

Which means GCD (D, Z) = 1

We select D = 3 so that GCD (3, 40) = 1

Step 5 – Determine E such that, (E*D) mod Z =1

(E*3) mod 40 =1

So select E = 27

Private Key is pair of numbers, Private Key = (N, D) = (55, 3)

Public Key is pair of numbers, Public Key = (N, E) = (55, 27)

6.2 - Encryption

Cipher Text C = M^E mod N

Suppose the Plain Text Value M is 2

So C = 2^{27} mod 55

C = 134217728 mod 55

C = 18

6.3 - Decryption

Plain Text M = C^D mod N

After encryption cipher text C is 18

M = 18^3 mod 55

M = 5832 mod 55

M = 2

7. Conclusion

RSA algorithm is a good algorithm. Cryptography ensures the encrypted message is securely transmitted, securely means no body can understand the received message except the authentic receiver that has the decryption key. In this paper we have analyzed the RSA algorithm and we know that public key cryptography has several advantages, in public key cryptography private keys are kept secret, which is increased the security. We analyzed RSA algorithm and we observed that if the value of exponent (i.e. E and D) is high, the security of RSA algorithm also high. so we proposed for better security in RSA algorithm select high value of exponent.

References

[1] Dr. Prerna Mahajan & Abhishek Sachdeva (2013), A Study of Encryption Algorithms AES, DES and RSA for Security, Global Journals Inc. (USA).

[2] Saranya, Vinothini, Vasumathi (2014), A Study on RSA Algorithm for Cryptography, International Journal of Computer Science and Information Technologies.

[3] M. Bahadori, M. R. Mali, O. Sarbishei, M. Atarodi and M. Sharifkhani "A novel approach for secure and fast generation of RSA public and private keys on Smartcard" NEWCAS Conference (NEWCAS), 2010 8th IEEE International, 2010, pp. 265-268.

[4] Yadav, Prasant Singh, Pankaj Sharma, and Dr KP Yadav. "Implementation of RSA algorithm using Elliptic curve algorithm for security and performance enhancement" International Journal of Scientific & Technology Research Vol 1.

[5] R. Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital Signature and Public-Key Cryptosystems, Communication of the ACM, Vol.21, No.2, 1978, pp. 120-126.

[6] Abhijit Das, C. E. (2009). Public-Key Cryptography:Theory and Practice. Mumbai: Pearson Education India.

[7] He, C. and H. Wu, 2004. Public key RSA algorithm is applied to several problems. Mod. Comput., 178: 72-74.

[8] Chen, C. and Z. Zhu, 2006. Application of RSA algorithm and implementation details. Computer Science Engineering, 9: 13-14.

[9] Buchmann, J., 2001. Einfuhrung in die Kryptographie [Introduction to Cryptography]. 2nd Edn., Springer, Berlin, Germany.

[10] William Stallings, "Cryptography and Network Security", ISBN 81-7758-011-6, Pearson Education, Third Edition