Extension to Proposed Two – Way Improvement in RSA Encryption

Yogita
M.Tech Student, SPGOI College of Engineering, MD University, Rohtak (India).

Abstract – Data security is an essential component of an organization in order to keep the information safe from various competitors. Secured and timely transmission of data is always an important aspect for an organization. RSA is critically analyzed and key management has also been optimized. Cryptography is a technique used to avoid unauthorized access of data. Sometime, multiple keys can also be used for encryption. Strong encryption algorithms and optimized key management techniques always help in achieving confidentiality, authentication and integrity of data and reduce the overheads of the system. This paper is extension of my previous paper in which I have described new enhancement that can be considered to provide security to the RSA Algorithm. In this paper I am including experimental results along with my proposed enhancement in RSA.

Index Terms – RSA, Cryptography, Encryption.

1. INTRODUCTION

The main object of cryptography is to provide a mechanism for two (or more) people to communicate with each other without anyone else being able to read the message. Along with this Cryptography can provide many other services and they are as:

- Integrity check – this makes sure the message has not been tampered by any one in process of communications
- Authentication – this verifies the sender identity.

Initially plaintext is encrypted into cipher text; it is then decrypted back into plaintext, Cryptographic systems tend to use both an algorithm and a secret value, called the key. The requirements for the key is that it is difficult to keep develop new algorithms and also to tell the receiving party that the data is being encrypted with the new algorithm. Thus, using keys, there are no problems with everyone having the encryption / decryption system, because without the key it is very difficult to decrypt the message.

2. NEED OF CRYPTOGRAPHY

In today's world cryptography has become a necessity for all the organizations. Data security is an essential component of an organization in order to keep the information safe from various competitors. It also helps to ensure the privacy of a user from others. These days' passwords are not considered as reliable for this task because it is easy to guess passwords due to its short range. Moreover, if the range of password is small a brute force search can be applied to crack it [1]. So, as to protect our data various algorithms have been designed. It helps us to securely access bank accounts, electronic transfer of funds and many more daily life applications.

3. REVIEW OF EXISTING SCHEME

3.1. RSA – Overview

RSA is designed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978. It is one of the best known public key cryptosystems for key exchange or digital signatures or encryption of blocks of data. RSA uses a variable size encryption block and a variable size key. It is an asymmetric (public key) cryptosystem based on number theory, which is a block cipher system. It uses two prime numbers to generate the public and private keys. These two different keys are used for encryption and decryption purpose. Sender encrypts the message using Receiver public key and when the message gets transmit to receiver, then receiver can decrypt it using his own private key [2, 3]. RSA operations can be decomposed in three broad steps; key generation, encryption and decryption. RSA have many flaws in its design therefore not preferred for the commercial use. When the small values of p & q are selected for the designing of key then the encryption process becomes too weak and one can be able to decrypt the data by using random probability theory and side channel attacks. On the other hand if large p & q lengths are selected then it consumes more time and the performance gets degraded in comparison with DES. Further, the algorithm also requires of similar lengths for p & q, practically this is very tough conditions to satisfy. Padding techniques are required in such cases increases the system's overheads by taking more processing time [4].

3.2. Key Generation Procedure [5]

1. Choose two distinct large random prime numbers p & q such that $p \neq q$.
2. Compute $n = p \times q$.
3. Calculate: phi (n) = (p-1) (q-1).
4. Choose an integer e such that $1<e<\text{phi}(n)$
5. Compute d to satisfy the congruence relation $d \times e = 1 \bmod \text{phi}(n)$; d is kept as private key exponent.
6. The public key is (n, e) and the private key is (n, d). Keep all the values d, p, q and phi secret.

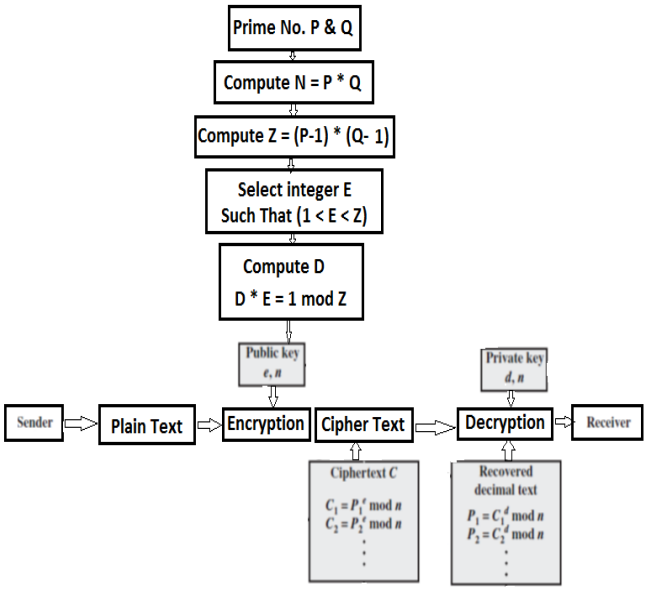

Figure 1: Block diagram for RSA

Encryption

Plain text: P < n

Cipher text: C= P^e mod n.

Decryption

Cipher text: C

Plaintext: P=C^d mod n.

4. PROPOSED RSA ALGORITHM

Here Proposed RSA Algorithm is composed of Two – Way Improvements [6] so that the attacks will have no effect on RSA Security.

In Step 1, In place of two dynamic keys I have taken a concept of using four dynamic keys by this length of key will get increase thus time requires to break down will significantly increase which makes it practically impossible to break down such length keys. Although by using such length keys lots more computing power is required but my main focus is on providing security to the data because data security at the cost of computing power is at higher preferences.

In Step 2, I have proposed a new method to provide security to the transmitted data (basically which is an encryption of encrypted data) which is in the form bite. Here a new dynamic key will be used that will rearrange the order of bits. If any how an intruder able to detect the transmission and assuming worst case that the intruder is having access to dynamic keys and algorithm. This added layer of extra encryption will provide more data security.

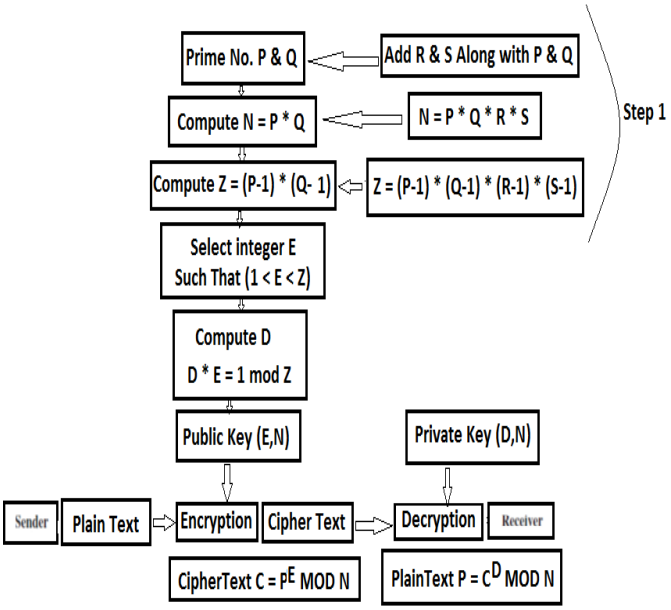

Figure 2: Step 1

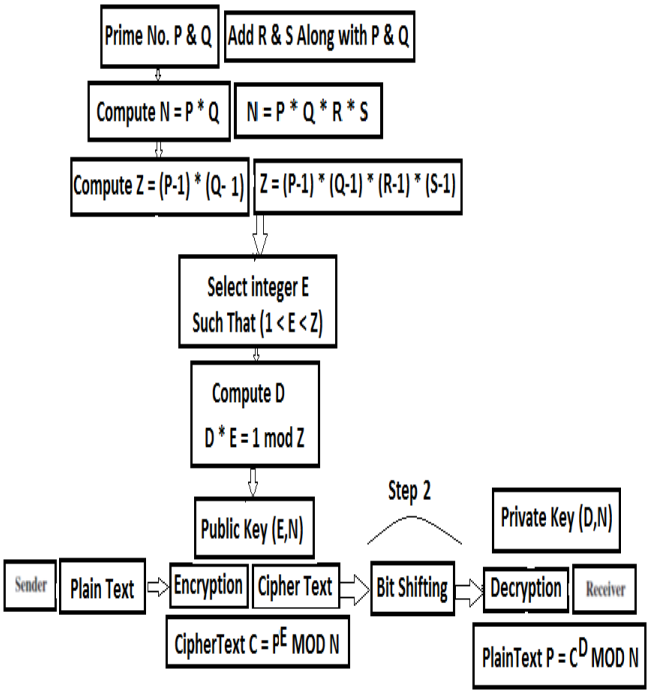

Figure 3: Step 2

5. OUTCOME OF EXISTING RSA

Public Key (E,N): 26341,43423

Private Key (D,N): 26261,43423

ds=Test Run

Encrypted message14375 25847 7551 11507 39439 42461 6188 2598

D = 26261

N = 43423

Test Run

6. OUTCOME WITH ENHANCEMENT STEP – 1

Public Key (E,N): 60211,911876279

Private Key (D,N): 70958971,911876279

ds=Test Run

Encrypted message592002894 737464476 865048939 100906988 346457383 72866268 540208835 454255682

D = 70958971

N = 911876279

Test Run

In the above outcome by increase in the number of prime number from two to four even by taking configuration as it is. The change in public and private key is significant. Public Key before change is computed out to be: "Public Key (E,N): 26341,43423" and public key after change is computed out to be "Public Key (E,N): 60211,911876279" similarly same is the case for Private Key "Private Key (D,N): 26261,43423" And "Private Key (D,N): 70958971,911876279" before and after respectively. It is very clear from the results that the new improved Step -1 enhancement to existing RSA Is of use and thus increasing security to the RSA Algorithm.

7. CONCLUSION

Test Run is conducted on existing Scheme for encryption of data using RSA and on enhancement Step -1 for encryption of data using same RSA. The results are very clear from the outcome that is represented above.

Thus I can say that the proposed new schemes provide additional security to the existing RSA encryption Algorithm.

8. FUTURE WORK

Practical Implementation of Step 2 is under process and after that details results of my research can be stated. Step 2 is to be carried out to provide a better solution to the proposed Scheme.

REFERENCES

[1] Kakkar and P. K. Bansal, "Reliable Encryption Algorithm used for Communication", M. E. Thesis, Thapar University, 2004.

[2] Aman Kumar, Dr. Sudesh Jakhar and Mr. Sunil Makkar, "Comparative Analysis between DES and RSA Algorithm's", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, pp. 386-391, July 2012.

[3] Xin Zhou and Xiaofei Tang, "Research and Implementation of RSA Algorithm for Encryption and Decryption", the 6th International Forum on Strategic Technology, pp. 1118 – 1121, 2011.

[4] Ajay Kakkar, M. L. Singh and P.K. Bansal, "Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network", International Journal of Engineering and Technology, Volume 2 No. 1, pp. 87-92, January 2012.

[5] Uma Somani, Kanika Lakhani and Manish Mundra, "Implementing Digital Signatures with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", 1st International Conference on Parallel, Distributed and Grid Computing (PDGC), pp. 211-216, 2010.

[6] Yogita, "Analysis of RSA Encryption to propose two – Step Improvement", Imperial Journal of Interdisciplinary Research (IJIR) Vol-2, Issue-6, 2016 ISSN: 2454-1362, http://www.onlinejournal.in