ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 3, March 2017

Algorithm for Protection of Key in Private Key Cryptography

[1] Neha Tyagi, [2] Ashish Agarwal, [3] Anurag Katiyar [4] Shubham Garg [5] Shudhanshu Yadav
[1][2][3][4][5]G.L.Bajaj Institute of Technology & Management,
Greater Noida, Uttar Pradesh, India

***Abstract* - This paper is in reference with our previous paper entitled "Protection of Key in Private Key Cryptography" published by "International Journal of Advanced Research" in Feb 2017 edition... In this paper we have tried to devise an algorithm that would protect the key in transmission, as in the era of digitization, threats to information security instigate the concerned people to take proactive measures for communication between two communicating parties. Since our major focus is on the symmetric key cryptography, also called as private key cryptography, we have studied different techniques of securing a private key or shared key or secret key that are used to shield information in such systems. The different statistical data being published so far and recent phishing scam which plays with the information transfer by taking away the user's identity highlights the need to make our security measures strong enough to counter such unwanted accesses. After looking into the functioning of widely accepted protocols and thinking of introducing a few changes to enhance their functionality, we here, are going to focus mainly on application of asymmetric key cryptographic algorithm named RSA algorithm. We have already referred to suggestions by means of several research papers being published so far related to our area of interest such as N-Prime RSA, magic rectangle, etc. We have tried to present a method taking one step ahead in the available sketch and without diminishing the basic essence of the algorithm. We also refer to some examples and its application as thought of in its modified form to further support our idea.**

***Key words:*-- Cryptography, Key, Private Key, Public key, Asymmetric or Public Key Cryptography, Symmetric or Private Key Cryptography**

I. INTRODUCTION

As already mentioned in our previous analysis that the main point of concern in the application of symmetric key cryptography, hence symmetric cryptosystems i.e. the ones which are based on the principles of former, is the security of private key. Since *symmetric key cryptography* involves only one key that is used to shield the information in order to keep communication between communicating parties confidential, it is also called *private key* or *shared key cryptography*. The focus is to make communication channel i.e. path by which encrypted information travels to reach the intended receiver secure enough that no ordinary or complex attacks play with its confidentiality.

Thus, we may note that the key in private key cryptography can be protected by either of the following two methods as:-

1) Protecting the channel by applying public key encryption algorithm such as *RSA algorithm* or its modified form as discussed further and keeping the key same as before.
2) Applying modified version of RSA(different from the ones already available) on key before transmission in communication channel and keeping the channel same as before.

However, it would increase the complexity of the conventional procedure for rendering security to the key and thus the information. But it would surely be helpful as well as feasible in terms of security measures to be taken to protect user's valuable information.

The main idea behind this is to think of introducing some modifications in the conventional functioning of RSA algorithm is to apply the binary logic in accordance with mathematical techniques. That is why; we have chosen a base of numerical digit i.e. 2 to raise a number that is being obtained after computing the median of the information length by appending headers and trailers. Before moving on to introduce our modified RSA algorithm, we should have glimpse at some of the facts regarding this algorithm in its true sense. These are listed below as:-

- RSA is an acronym for Rivest-Shamir-Adleman.
- It is public key encryption algorithm.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 3, March 2017

- ♣ It was first described in 1977.
- ♣ Protocols such as SSH, OpenPGP, S/MIME and SSL/TLS depend on RSA for encryption.
- ♣ RSA signature is used for verification.
- ♣ Two prime numbers are generated using Rabin-Miller primarily test algorithm.
- ♣ The key length is expressed in terms of bits.
- ♣ The security of RSA relies on the computational difficulty of factoring large integers (computing 'e').

Now we elaborate our idea to further strengthen the communication with the application of asymmetric cryptographic algorithm namely RSA algorithm in its modified form as discussed further.

II. ALGORITHM

We may apply our modified RSA algorithm on the key that is used in private key Cryptosystem. The algorithm would have following steps.

1) Generate two prime numbers p and q such that their product is n=p*q.
2) Compute Ø (n) = (p-1)*(q-1).
3) Choose an integer e, 1<e<Ø (n), such that gcd (e, Ø (n)) =1.
4) Compute the secret exponent d, 1<d<Ø (n) such that e*d=1modØ (n).
5) The public key is (n, e) and the private key is (n,d).
6) Append a header (#$) and trailer ($#) with the plain text and then calculate median of message length. Let the median be 'k'. (This addition of header and trailer would be done by channel and will not be made public.)
7) Calculate 2^k. (While calculating 'k' the ceil function is to be used. Example:
   a. If total message length is 5 then k = ceil (5/2) = 3
   b. Similarly, if total message length is 6 then k = ceil (6/2) = 3
8) To obtain cipher text (encryption end)
   a. Calculate $C_I=P^e \bmod n$.
   b. Calculate $C_F= C_I*2^k$. This is our final cipher text.
9) To obtain plain text (decryption end)
   a. Calculate $P_I= C_F/2^k$.
   b. Calculate $P_F=P_I^d \bmod n$. This is our plain text.

- Where I stands for Initial, F for Final, P for Plain Text and C for Cipher text.

Example 1:

Let p=11, q=23, P=2 then

1) n=11*23 = 253
2) Ø(n)=10*22 = 220
3) e=3
4) d=147
5) Public Key (253,3) & Private Key (253,147).
6) P= #2#, k= ceil (5/2) = 3
7) $2^3 = 8$
8) Cipher Text (Encryption)
   a. $C_I=2^3 \bmod 253 = 8$
   b. $C_F=8*8 = 64$
9) Plain Text (Decryption)
   a. $P_I=64/8 = 8$
   b. $P_F=8^{147} \bmod 253 = 2$

Example 2:

Let p=23, q=19, P=11 then

1) n=23*19 = 437
2) Ø(n)=22*18 = 396
3) e=5
4) d=317
5) Public Key (437,5) & Private Key (437,317).
6) P= #11#, k= ceil (6/2) = 3
7) $2^3 = 8$
8) Cipher Text (Encryption)
   a. $C_I=11^5 \bmod 437 = 235$
   b. $C_F=235*8 = 1880$
9) Plain Text (Decryption)
   a. $P_I=1880/8 = 235$
   b. $P_F=235^{317} \bmod 437 = 11$

III. FUTURE SCOPE

The efficiency of any algorithm relies on its ability to withstand any possibility in terms of challenges. Even if some modifications are introduced to its basic structure, it should assimilate them without losing its ability to meet the target. That is what we have tried to do with one of the most popular asymmetric cryptographic algorithm i.e. RSA algorithm. Though it has been implemented with a set of variety of examples in terms of magnitude, still we may

look to extend it in order to meet expectations in terms of security to the information. The complexity of the algorithm in terms of space and time needs to be analysed for various length inputs and thus to be controlled for its effectiveness and efficiency. As an outcome, the confidentiality which is at the heart of encryption needs to be preserved and easy communication needs to be enforced.

IV. CONCLUSION

The modified algorithm may play a vital role in increasing the randomness and security of existing algorithm so that it prohibits the possibility of threat from various classes of suspected attacks. Attempting to search ways as to how modified algorithm can be enhanced in order to make it strong enough to counter different attacking strategies being used by the notorious people on the network. System designers need to build a system that allow for fast and secure key length algorithm upgrade. Thus area of research in this aspect comprises of many opportunities to add new features to our suggestion.

REFERENCES

1) Neha Tyagi, Ashish Agarwal, Anurag Katiyar, Shubham Garg, Shudhanshu Yadav, "Protection of Key in Private Key Cryptography" published by "International Journal of Advanced Research", Volume 5, Issue 2, Feb 2017.

2) Hardik Gandhi, Vinit Gupta, "Research on enhancing public key by the use of MRGA with RSA and N-Prime RSA" paper published by "International Journal for Innovative Research in Science & Technology", Volume 1, Issue 12, May 2015.

3) Jyotirmoy Das "A Study on Modern Cryptography and their Security Issues" published by "International Journal of Emerging Technology and Advanced Engineering", Volume 4, Issue 10, October 2014.

4) Mitali, Vijay Kumar, Arvind Sharma "A Survey on Various Cryptography Techniques" published by "International Journal of Emerging Trends & Technology in Computer Science" Volume 3, Issue 4, July-August 2014.

5) Swati Kashyap, Er. Neeraj Madan, "A Review on: Network Security and Cryptographic Algorithm" published by "International Journal of Advanced Research in Computer Science and Software Engineering" Volume 5, Issue 4, April 2015