Volume 4, Issue 4, April 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Repeated Encryption on RSA

Anjana S. Chandran
Assistant Professor, SCMS School Of Technology And Management,
Kochi, India

Abstract— RSA algorithm is an encryption algorithm which is still used in the industry for various applications. This paper discusses on the nature of RSA algorithm when repeated encryption is done on it. It also focuses on the situation when on small repeated encryption RSA gives back the original plaintext what may be the possible cause.

Keywords— Encryption, Repeated, RSA, Algorithm

I INTRODUCTION

From the strength of the factorization problem to back it RSA remains to be one of the most powerful algorithm under public key cryptosystem. The algorithm is named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman.The main feature of the algorithm is that the key length can be variable. The longer the key the stronger the algorithm.[1] The motivation for this paper is that RSA is one of the classical approaches with a strong security , as for solving RSA problem is to factor the modulus n. If the prime factors can be recovered then an intruder can calculate the secret private key d from the public key pair (e, n). Once the private key is obtained then smoothly the decryption can be done. But until now there has not been any polynomial time algorithm for factoring large integers on a standard computer been developed.[5] The key objective of this paper is to understand the working of the RSA algorithm and to check the situation when a small number of repeated encryption on RSA gives back the same plaintext what may be the possible cause.

This paper would discuss in brief the concept of modular arithmetic in RSA and move on to the problem statement and then to the detailed analysis.

II MODULAR ARITHMETIC AND RSA

The RSA algorithmic technique is to get the value M where $C=M^e \bmod n$ where (e,n) is an RSA public key and c is RSA ciphertext.[1][2][3][5]

A. *RSA Algorithm*

RSA Key Generation Algorithm

1. Select two large random prime numbers p and q where $p \neq q$
2. Find the product n=pq
3. Calculate m= (p-1)(q-1)
4. Choose an integer e, $1<e<m$, such that gcd(e,m)=1
5. Compute d where $1<d<m$ such that $d \equiv e^{-1} \pmod m$.
6. The public key computed is (e,n)
7. The private key is (d,n)
8. The values of p,q,n should be kept secret.

Here n is modulus, e the encryption exponent and d the decryption exponent.

B. *Encryption process :*

The source sending the message to the destination does the encryption in the following way:

1. Get the destination public key (e,n)
2. Positive integer M being the message , compute the ciphertext $C=M^e \bmod n$.
3. Transmit ciphertext C to the destination

C. *Decryption process:*

At Destination the message is decrypted in the following fashion:

1. Use the private key of the destination (d,n) to compute $M=C^d \bmod n$
2. Get the plaintext from the integer representation M.

III PROBLEM STATEMENT:

Being a classic algorithm it was fascinating to peep into the working of RSA algorithm and to think over the case where when small amount of repeated encryption on RSA gives back the plaintext what may be the possible cause.[1][3][6][7][8][9][10]

IV DETAILED ANALYSIS

The problem statement can be derived as

$$C=M^e \bmod n$$
$$C_1 = C^e \bmod n$$
$$C_2 = C_1^{\ e} \bmod n$$
$$C_3 = C_2^{\ e} \bmod n$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$C_r = C_{r-1}^{\ e} \bmod n \quad , \text{where} \quad 1<r < x \quad , \text{where x is a small number.}$$

If Cn happens to be the plaintext M we can write it as

$$M = C_r = C_{r-1}^{\ e} \bmod n$$

Which can be written as $M = ((((C^e)^e)^e)^e)^{\ldots\ldots e}$

$= (C^e)^{re}$ where r is the number of times C is encrypted.

$= ((M^e)^{\ e})^{re}$ Substituting the value of C

$= (M^e)^{re}$ where r is the number of times C is encrypted

If $(C^e)^{re}$ returns the plaintext M then re happens to be the inverse of e

If re is inverse of e then both of these terms cancelled and the message can be obtained.

To avoid this the encryption key to be used in RSA should be as large as possible so that the inverse of the same is difficult to obtain if small number of repeated encryption is done.

V CONCLUSION

The confidentiality of the message M will be at a threat if it is possible for an intruder to retrieve the message with a small repeated encryption on the ciphertext . Hence always it is advised to keep the encryption key always very big integer so that its inverse is difficult to find .

References :

[1] William Stallings, Cryptography And Network Security Principles And Practises
[2] RSA Cryptography Standards, PKCS#1 , RSA Laboratories.
[3] Information Security Theory And Practise , Dhiren R. Patel,2008 Edition
[4] Cryptography And Network Security, Atul Kahate, Second Edition
[5] Cryptography and Information security, V.K. Pachghare, 2009 Edition
[6] Security in Computing Charles P.Pfleeger , Shari Lawrence Pfleeger, Third Edition
[7] Principles And Practices Of Information Security,2009
[8] Mark Stamp's Information Security,Principles and Practice,Deven N.Shah
[9] Computer Security Art And Science,Matt Bishop,2003
[10] Hunting Security Bugs,Tom Gallagher,Bryan Jeffries ,Lawrence Landaker,2006
[11] Information Security Policies,Processes and Practice,2008

