ISSN No. 0976-5697

Volume 2, No. 5, Sept-Oct 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

An Enhanced RSA Public key Cryptographic Algorithm

Ravindra Babu Kallam*
HOD, Computer Science Engineering
Aizza College of Engineering & Technology, JNTUH
Mancherial, AP, India
rb_kallam@yahoo.com

Dr. S. Udaya Kumar
Principal
MVSR Engineering College
Hyderabad, AP, India
uksusarla@regiffmail.com

Dr.A. Vinaya Babu
Director, Admissions
Jawaharlal Nehru Technological University
Hyderabad, AP, India
avb1222@gmail.com

V.Shravan Kumar
Computer Science Engineering
AZCET, JNTUH
Mancherial, AP, India
vemula.vsk@gmail.c

Abstract: In this paper we illustrate the importance of cryptography, symmetric and asymmetric cryptographic algorithms. Significance of RSA algorithm its merits and demerits were discussed. Finally we have proposed an enhanced and efficient RSA algorithm which is more secure and stronger then the existing RSA algorithm.

Keywords: Algorithm; Security; Cipher; public key cryptography; asymmetric key; symmetric key, RSA;

I. INTRODUCTION

Cryptography is the method which is used to convert a comprehensible message into an incomprehensible message and for reconverting the secret form into the intelligible message by a direct reversal of the steps used in the original process [1]. In the history of cryptography up to 1975, all cryptosystems required the sender and the receiver to agree before hand on the same key, a key that had to rigorously protect from exposure to the adversary.

The cryptographic algorithms in which we use the same key for encryption and decryption are named as symmetric, single key or conventional encryption algorithms[3]. Because secrecy always depends on the key rather then the algorithm, distribution of the key is major concern in these schemes[13]. In 1976, Martine Hellman, a professor at Stanford University, introduced the concept of public key cryptography in which we use two different keys and either one can be used for encryption and the other for decryption. This scheme is called asymmetric key cryptography.

In August 1977 the RSA public key cryptosystem [2] was introduced in Martin Gardner's column on Mathematical Games in Scientific American. The RSA cryptosystem has survived over thirty three years of study by cryptanalyst [3] in the public sector, but there are also dimensions in the basic concepts of RSA cryptosystems which are yet to be disclosed in order to make RSA more efficient and secure in implementation prospective.

To meet the current requirement in the field of cryptography and network security, it is obligatory to update the existing algorithms [6] or invent the new cryptographic algorithms [4][5]. Because the RSA has massive market in the filed of cryptography and network security we thought to up date the RSA to make it stronger and potential one [3]. In the next sections we will explain the existing algorithm with demerits and proposed algorithm with the merits.

II. EXISTING RSA ALGORITHM

RSA is the well known public key cryptosystem which is based on mathematical functions rather than on simple operations on bit patterns. It is block cipher in which plain text and the cipher text are the integers between 0 and n-1 for some n. It begins by selecting two prime numbers, p and q and calculating their product n, which is the modulus for encryption and decryption. The algorithm of Rivest, Shamir and Adelman (RSA) crypto system is as follows:

Each user has to generate Private/ Public key pair…

a. Choose two un-equal prime numbers (p &q);
   These numbers should be as large as possible.
b. Calculate n = p * q.
c. Ø (n) = (p - 1) * (q - 1).
d. Select integer e, gcd(ø(n),e)=1; 1<e<ø(n)
e. Calculate d de mod ø(n)= 1
f. Public key PU={e,n}
g. Private key PR={d,n}
h. Encryption:
   Plain text M < n
   Cipher text: $C = M^e \bmod n$, where $0 \le M < n$
i. Decryption:
   Cipher text: C
   Plain text $M = C^d \bmod n$

The weakness of the mentioned algorithm is to factorize (n) which is the product of two unequal primes (p & q).

In his research Aboud and AL-Fayoumi [7] tried analysis the algorithm reversely. Coppersmith [8] introduced a new type of attacks on RSA which capacitate a passive adversary to recover such message from the corresponding cipher text. This attack is of practical importance since many public key encryption schemes have been proposed which require the encryption of polynomial related messages.

Hastad [9] made an attack on RSA with small key by sending an encryption of more than $e(e+1)/2$ linearly related messages of the type ($a_i * m + b_i$), where a_i and b_i are known; allowing an adversary to decrypt the messages provided that the Modulus n_i satisfy $n_i > 2^{(e+1)(e+2)/4} * (e+1)^{(e+1)}$.

Wiener [10] proposed an attack hinges about find the *d* value directly with special case of *d*, the RSA secret exponent *d* is chosen to be small compared to the RSA modulus *N*. A well-known attack on RSA with low secret-exponent *d* was given by Wiener about 15 years ago.

In the recent past Prof. Alaa invented a new method[12], and mentioned that he can break the RSA in 953 milliseconds of length 'n' with 180 digits, where n is the product of two unequal prime numbers. Many more scientists were working day and night to break the RSA in fewer times.

Number of researchers was functioning to find the composite numbers of value (n) but failed in process. But the weakness of RSA still remains the same [11].

Hence we proposed a new method of RSA by altering the previous technique to make it more difficult in finding the private key by increasing the scale of the algorithm.

III. PROPOSED RSA ALGORITHM

To strengthen and to endure from the attacks we have improved the existing algorithm by altering the p and q.

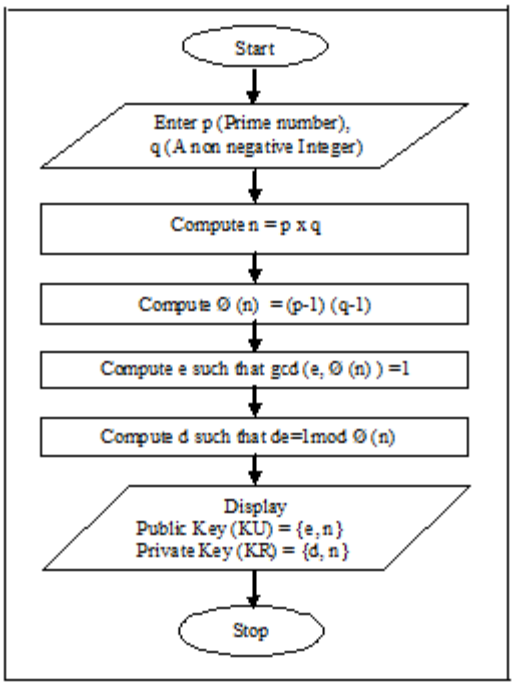

Figure 1. Flow chart of the proposed algorithm

Instead of two unequal prime numbers in this we have considered p as a prime number and q as a non-negative integer. The sequence of seeps in the algorithm is shown in the figure 1. The enhanced algorithm is explained below with an example:

Considered p=5 (prime number) and
q=12 (non negative integer)

Step1: Compute n=p x q = 5 x 12 = 60.
Step2: Compute Ø (n) = (p-1) x (q-1) = 4 x 11 = 44.
Step3: Compute *e* such that *gcd (e, Ø (n)) = 1*.
gcd (3, 44) = 1, hence e=3;
Step4: Compute d such that *de = 1mod Ø (n),*
We have calculated the value of 'd' using the Extended Euclidean algorithm as mentioned below.

a. 44 = 14 * 3 + 2 (44 in multiple of 3 + constant which is 2)
b. 2 = 44 – 14 * 3 (2 in terms of 44 and 3)
c. 3 = 2 *1 + 1 = 1 * (44 -14 * 3) + 1
d. or 1 = 15 * 3 – 44 (1 in terms of 44 and 3)
e. Hence:
3 = 2 + 1 or 1 = 3-2 = (44 -14 * 3) – (15* 3 – 44) = 2* 44 – 3*29
f. So, 1==2*44–3*29
g. Coefficient of 3 = - 29 mod 44 = 44-29 = 15
d= 15

With this the Public Key (KU) = {e, n} = {3, 60}
Private Key (KR) = {d, n} = {15, 60}

IV. TESTING

Considered one of the above keys for the encryption of plain text M=12 and it is observed that the generated cipher text C=48. We have used the remaining key for decrypting the cipher text in to plain text. It is noticed that the algorithm is working properly as shown below:

Encryption:
$C = M^e \bmod n$;
Consider M=12;
$C = 12^3 \bmod 60 = 1728 \bmod 60 = 48$
C = 48
Decryption:
$M = C^d \bmod n$;
$M = 48^{15} \bmod 60 = 12$
M = 12

V. RESULTS

Using our enhanced RSA algorithm it is confirmed that, we can comfortably generate private and public keys and either can be used for encryption and decryption.

It is also noticed that, by using one prime number and the one non negative integer, we have more choice for selecting a pair (p, q) and hence it takes more time to break the enhanced RSA by previous methods of cryptanalytic attacks.

VI. CONCLUSION

Importance of cryptography is explained, mainly focused on the strength of the existing RSA algorithm and the available attacks on it. To strengthen the algorithm we have enhanced the existing RSA and explained its execution with example.

VII. ACKNOWLEDGMENT

The first author like to thank our Aizza engineering college Principal and Mgt, for providing all the facilities to complete

the task. We also like to thank IJARCS for allowing us to use its template.

VIII. REFERENCES

[1] R.L.Rivest, Shamir and Adleman," A Method of Obtaining Digital Signatures and Public Key Cryptosystems Laboratory for Computer Science, MIT Cambridge, 1978, Original RSA papers@ http://people.csail.mit.edu/rivest/Rsapaper.pdf, p 6-8.

[2] Gupta, "RSA Operation with Performance Tuning" ICNICT11,978-93-81126-21-1,P- 631-635.

[3] Ravindra babu, Udayakumar, " A Survey on Cryptography and Steganography Methods for Infromation Security", IJCA, 0975-8887, Vol 12, No-2, Nov2010.

[4] Ravindra, Udaya and Vinaya babu, " A Variable Length Block Cipher Generation Using Modern Play Color Cipher Algorithm withAlphanumeric key and Iterative Functions" ICNICT11, 978-93-81126-21-1, P-288-296.

[5] Udaya Kumar,Ravindra babu and Vinaya babu, "A Modern Play Color Cipher Involving Dynamic Permuted key with Iterative and Modular Arithmatic Functions", IJARCS, 0976-5697, Vol 2, No.3, May-June 2011.

[6] Ravindra Babu, Udaya and Vinaya Babu," A Contemporary Poly Alphabetic Cipher using Comprehensive Vigenere Table", WCSIT, 2221-0741, Vol 1, No 4, 167-171, 2011.

[7] Aboud, AL-Fayoumi; "Efficient Method for Breaking RSA Scheme"; Ubiquitous Computing and Communication Journal, vol. 4,no.2 , p:15-20, 2008.

[8] Coppersmith, D. "Attack on the Cryptographic Scheme", Advances in Cryptology–CRYPTO '94, Springer-Verlag, LNCS 839, pp.294-307, 1994.

[9] Hastad, J. "On Using RSA with low exponent in a public key Network", Advances in Cryptology –CRYPTO '85, Springer-Velag LNCS 218, pp. 403-408, 1986.

[10] Nguyen, H. Number Theory and the RSA Public Key Cryptosystem. http://cdn.bitbucket.org/mvngu/numtheory-crypto/downloads/numtheory-crypto.pdf. Accessed on 25/9/2009.

[11] Denning, D., F. Ayoub , " Cryptographic techniques and network security", IEEE proceedings, Vol 131, 684-694,Dec 1984.

[12] Alaa H Al Hamami, "a fast approch for breaking RSA cryptosystem", wcsit, Vol 1, No 6, 260-263, 2011.

[13] Stalling, " Cryptography and network security", Fourth edition, LPE, 81-7758-774-9.