International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 5 1227 - 1231

Improved Trial Division Algorithm by Lagrange's Interpolation Function

[*]Maloth Bhavsingh, [1]M. Sri Lakshmi, [2]Dr. S. Prem Kumar,[3]N. Parashuram
[1,3]Assistant Professor, Dept. of CSE, G.Pullaiah College of Engineering and Technology, Kurnool, Andhra Pradesh
[2]Prof &HOD, Dept of CSE, G Pullaiah College of Engineering and Technology, Kurnool.Andhra Pradesh.

Abstract- Nowadays data communication over the internetgrowths the security risk on the side of receiver and transmitter. To reduce risk level, cryptography technique has been used which is based on aprivate and public key in disquiet of endorsement. The process of encryption and decryption improved the capacity of data security. Asymmetric cryptography technique provides renowned RSA public key cryptography technique. The success story of RSA algorithm depends on the prime factor. For the estimation of theprime factor used various mathematical functions. In this paper,Lagrange's interpolation derivation for the estimation of aprime factoris used. The estimated prime factor is very complex and reduces the complexity of prime factor.

Keywords: - *public cryptography, RSA, factor, trial division, Lagrange's Interpolation*

*****

1. INTRODUCTION

Public key cryptography is one of the applications that are valuable in sending information via insecure channel's algorithm is a public key encryption algorithm. RSA has become most popular cryptosystem in the world because of its simplicity. According to number theory, it is easy to finds two big prime number, but the factorization of the product of two big prime numbers is very difficult task. The difficulty of computing the roots N, where N is the product of two large unknown primes, it is widely believed to be secure for large enough N. Since RSA can also be broken by factoring N, the security of RSA is often based on the integer factorization problem [1]. The integer factorization problem is a well-known topic of research within both academia and industry. It consists of finding the prime factors for any given large modulus Thereliability and security of data over the internet aremain issue. For the reliability and authentication cryptography technique is used. The cryptography techniques give the process of encryption and decryption. The process of encryption and decryption uses the symmetric and asymmetric technique. The Asymmetric technique used RSA algorithm. The Strength of RSA algorithms depends on the processing of factorization and complexity of factor. For the minimization of the complexity of factorization Lagrange's interpolation function is used to enhance the capacity of RSA factorization. Factorization is a reverse process of multiplication. It is the act of splitting an integer into a set of smaller integers (factors) which, when multiplied collected, form the original integer so it is a arduousprocess to find the factors of very large numbers. It has not been demonstrated that factoring requirement is difficult, and their residues a chance that a rapid and easy factoring method might be exposed [6]. The private key is period coupled and it is mathematically related to the corresponding public key. Hence, it is repetitively probable to attack a public-key system by originating the private key commencing the public key. For occurrence, specific Public-key cryptosystems are considered such that deriving the private key from the public key involves the attacker to factor a large number, therefore, it is computationally infeasible to implement the derivation. This is principally the significant idea of the RSA public-key cryptosystem [5]. RSA operations are secluded exponentiations of huge whole numbers with a common size of 512 to 2048 bits. RSA encryption creates a figure content C from a message M in light of a secluded exponentiation = Me mod n. Unscrambling recovers the message by computing = C^d mod n. Among the few systems that can be utilized to quicken RSA, they extraordinarily centered around those appropriate under the requirements of 8-bit gadgets.

2. RELATED WORK

In 1978, RSA developed a public key cryptosystem thatis based on the difficulty of integer factoring. The RSApublic key encryption scheme is the first example of aprovable secure public key encryption scheme againstchosen message chosen attacks [5].

 ISSN: 2321-8169
1227 - 1231

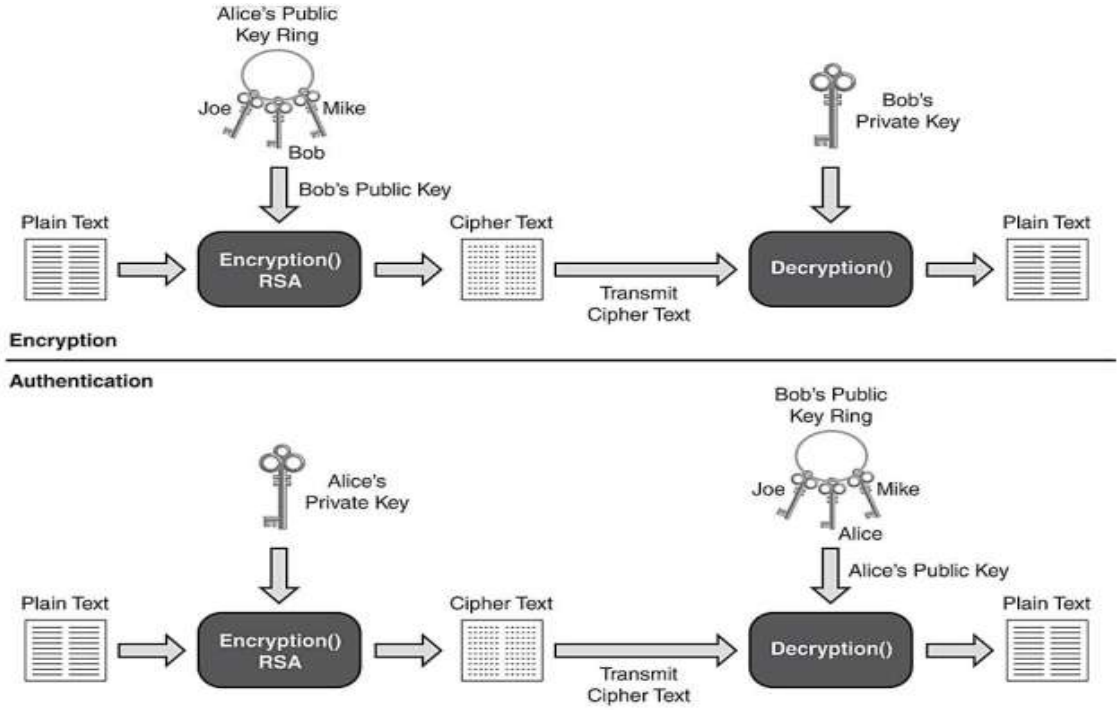

Fig 1.RSA algorithm

The RSA Algorithm is as follows [6]:

Key generation algorithm, to generate the keys entity A must do the following:

a. Randomly and secretly select two large prime numbers p and q both are prime but p! =q.

b. Compute the N = p*q.

c. Compute Euler Totient function phi (N) = (p-1) (q-1).

d. Select random integer e, 1<e<N

e. Compute the secret exponent d, 1 < d < phi, such that ed =1(mod (phi))

f. The public key is (N, e) and the private key is (N, d). Keep all the values d, p, q and phi secret. N is known as the modulus.

e is known as the public exponent or encryption exponent or just the exponent. d is known as the secret exponent or decryption exponent

An algorithm for attacking RSA scheme based on the knowing public key (e, n) work efficiently if the decryption key d is small. This algorithm divide Fermat Factorization method in two part first is, factorize number with respect floor function of square root of N, to get maximum factors that are neighbor to the (√N) , second is if don't get positive integer value of square root , then sequence between floor(√N) to N. An innovative technique has been introduced, to factorize RSA modulus N. This was established on Trial Division method and customs simple arithmetic operations for finding the factors which are nearby to √N.

3. PROBLEM STATEMENT

The generation of RSA factor is very critical task [2]. For the production of factor different mathematical functions are used.The mathematical function generates strong pairs of (P, Q). The P and Q are prime factor of given number. The main weakness static password is that if it is simple, it can be easily attacked by Trojan attacks, password attacks, or by simply guessing it. A static password is a usual way that a user authenticates when logging in to a service is needed. The password is usually a secret word or phrase picked by the user and used together with the user's username. It can be used when logging into your personal computer, an e-mail system, an online community, etc. Cloud computing security should be very secure and reliable otherwise the people confidential information will get compromised. People Still Using the same passwords to access the different accounts on the cloud which is very insecure and third party cloud computing service providers are not providing proper security about static passwords. This is the big disadvantage of the cloud computing environment because the static password can be attacked by unauthorized user and account information can be easily taken by hackers. Some problems are given below

1. Length of factor
2. Factional part of factor
3. Strength of factor
4. Prime factorization
5. Computational complexity

 ISSN: 2321-8169
1227 - 1231

4. PROPOSED METHOD AND MODEL

In this section, we will discuss the improved algorithm of RSA factor generation using the interpolation derivatives and algorithm. The interpolation derivates derived the input message regarding data and create a variable size matrix for the processing of input data of through Lagrange's interpolation and generate P and Q Prime Factor.

Lagrange Interpolation Algorithm:

1 Read x, n
2 for i=1 to (n+1) in steps of 1 do Read xi, fi endfor
//The above statement reads x_is and the corresponding values of f_is.
3 sum←0
4 **for** i=1 to (n+1) in steps of 1 do
5 prodfunc←1
6 for j=1 to (n+1) in steps of 1 do
7 If (j≠i) then
Prodfunc←prodfunc × (x-xj)/(xi-xj)
endfor
8 sum←sum+f_i× prodfunc
//sum is the value of f at x
endfor
9 Write x, sum
10 Stop

Algorithm for Lagrange's interpolation for key factor:

Input: Real Positive integer number N
Output: Factors of N
1. define the rand function for the coordinate generation of point x_1,x_2,x_3,x_4……..x_n
2. enter the positive number
3. if N<1 then goto step 2
4. Rand(N) // random point creation for coordinate system
5. Sum of point p coordinate in alternate axial
6. If P divided N then
7. Return P,N/p
8. End if

5. TESTING AND ANALYSIS

The generation and security strength of RSA key cryptography depend on the estimation of key factor value. If the key factor value is the week it is easily breakable by third party and hacker. For the enhancement of key factor, various authors used various multiplication and interpolation derivate. The Modified Trial Division Algorithm Using Lagrange's Interpolation, gives better results as compared the Trial-Division method using KNJ Factorization method. The Lagrange's Interpolation Factorization method provides efficient results with the minimum number of time. Hence it reduces the time complexity and increases the speed of the computation. The Trial-Division,KNJ, and LIF algorithm were tested on Intel core-i5 PC 2.50 GHz with 4 GB RAM under Microsoft Windows-8.1 Pro 32-bit using Dot Net. The original and modified Factorization method implementations are shown in Fig 2.

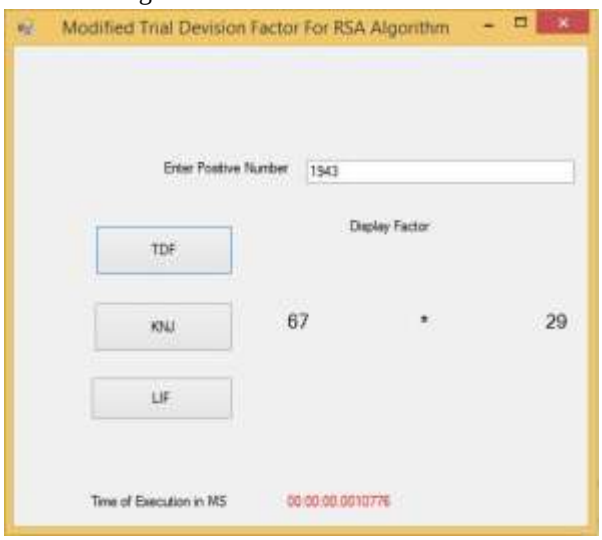

Figure 2: the TDF method button of modified trial division factor for RSA algorithm

Figure 3: KNJ method button of modified trial division factor for RSA algorithm

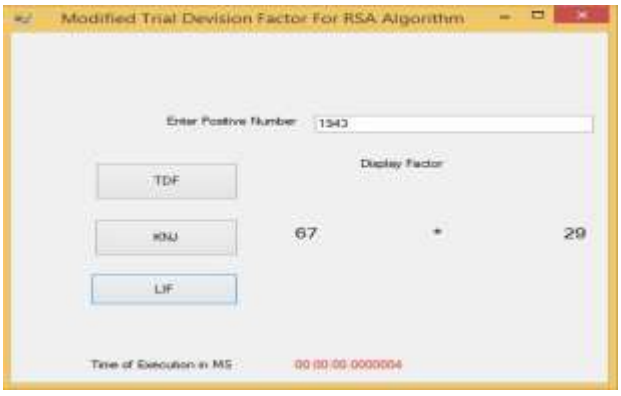

Figure 4: method button of modified trial division factor for RSA algorithm

6. RESULT

There are many factoring algorithms that are developed in the research area of RSA, but we equated and compared some of the results of this algorithm with Trial-Division and KNJ.

Table 1: Result table shows the number value of N, a factor of N and taken time using TDF, KNJ, LIF Methods in our Modified Trial Division Algorithm, using Lagrange's Interpolation Method to factorize RSA Public Key Encryption.

N	Factorization	Time Execution in TDF	Time Execution in KNJ	Time Execution in LIF
55	11*5	00.0037423	0.0041254	00.0000008
1943	67*29	00.0010952	0.0048015	00.0000008
998299	1213*823	00.0033018	0.0047859	00.0000004
85928201	9817*8753	00.0946525	0.0043368	00.0000004
1323172573	47591*27803	01.8576520	0.0047592	00.0000004

.

Even though the number of digits in N is increased; the proposed algorithm takes less time to compute the factors of N as compared to the Modified Trial Division Algorithm using KNJ Factorization method. Hence, the time execution in the Lagrange's Factorization method is very less as compare to Modified Trial Division method. Therefore Lagrange's Factorization method gives better results, increases thespeed of computation and provides anefficient way of factorization.

7. CONCLUSION AND FUTURE WORK

The proposed interpolation algorithm reduces the time complexity and space complexity in point factor interpolation. The main concept is to check only those factors which are odd, as well as those, are prime numbers. The proposed Lagrange's Interpolation Factorization algorithm works very efficiently on those factors that are nearby and very closest to √N. The Lagrange's interpolation enhanced the capacity of prime factorization of RSA algorithm. The Lagrange's interpolation used the point distribution function for the estimation of aprime number. If the distribution function length is increased, the complexity of time is also increased. The 12-digit number factor gives better prime value and minimum period. In future increase, the duration of integer and reduces the time complexity.

REFERENCES

[1] AL-Hamami AL-Ani, Technology of information security and protection systems, ISBN 978-9957-11-697-2, pp.173 - 223, Dar Wael , Jordan. 2007

[2] NidhiLal, AnuragPrakash Singh and Shishupal Kumar "Modified Trial Division Algorithm Using KNJ-Factorization Method to Factorize RSA Public Key Encryption", IEEE, 2014, Pp 1-4.

[3] Nils Gura, Arun Patel, Arvinderpal Wander, Hans Eberle and Sheueling Chang Shantz "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs", Springer, 2014, Pp 119-132.

[4] Alese, B. K., Philemon E. D. and Falaki, S. O."Comparative Analysis of Public-Key Encryption Schemes", International Journal of Engineering and Technology, 2012, Pp 1552-1568.

[5] Kamran Ali, Muhammad AsadLodhi and Ovais bin Usman "FPGA Implementation of RSA Encryption System", LUMS, 2012. Pp 2-9.

[6] Tal Malkin, Isamu Teranishi and Moti Yung "Efficient Circuit-Size Independent Public Key Encryption with KDM Security", 2013, Pp 1-20.

[7] Joppe W. Bos, J. Alex Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig and Eric Wustrow "Elliptic Curve Cryptography in Practice", Springer, 2014, Pp 157-175.

[8] Mohamed HamdyEldefrawy, Muhammad KhurramKhan and KhaledAlghathbar "A Key Agreement Algorithm with Rekeying for Wireless Sensor Networks using Public Key Cryptography", IEEE, 2010, Pp 1-6.

[9] Jesus Ayuso, Leandro Marin, Antonio J. Jara and Antonio F. G´omezSkarmeta "Optimization of Public Key Cryptography (RSA and ECC) for 16-bits Devices based on 6LoWPAN", International Workshop on the Security of the Internet of Things, 2010, Pp 1-8.

[10] Hoeteck Wee "Public Key Encryption AgainstRelated Key Attacks", NSF CAREER, 2011, Pp 1-18.

[11] Michael Hutter and Erich Wenger "Fast Multi-precision Multiplication for Public-Key Cryptography on Embedded Microprocessors", International Association for Cryptologic Research, 2011, Pp 459-474.

[12] Samuel Neves and Filipe Araujo "On the Performance of GPU Public-Key Cryptography", IEEE, 2011, Pp 133-140.

[13] DhananjayPugila, Harsh Chitrala, SalpeshLunawat and P.M.Durai Raj Vincent "An efficient encryption algorithm based on public keycryptography", IJET, 2013, Pp 3064-3067.

[14] Thomas P¨oppelmann and Tim Guneysu "Towards Practical Lattice-Based Public-Key Encryption on Reconfigurable Hardware", Springer, 2014, Pp 68-85.

[15] B.Persis Urbana Ivy and PurshotamMandiwa. Mukesh Kumar "A modified RSA cryptosystem based on 'n' prime numbers", IEEE, 2013, Pp 1-4.