International Journal of Scientific Research in Computer Science, Engineering and Information Technology

Three Prime RSA Algorithm Using Randomly Generated Prime Sequence Cryptosystem

Pooja Devi[1], Naveen Tyagi[2], Parul Saharavat[3]

[1]M.Tech Scholer J.P.I.E.T, Meerut, Uttar Pradesh, India

[2]Department of computer science J.P.I.E.T, Meerut, Uttar Pradesh, India

[3]Department of computer science D.N. Polytechnique, Meerut, Uttar Pradesh, India

ABSTRACT

Existing RSA cryptosystem is not in used due to the fact that it is very slow in process and also having the problem of Brute force and factorization attack. Hence these factors can degrade the performance of the RSA cryptosystem. Therefore a concept is needed which can overcome these entire factor. Hence we proposed algorithm we use the hybrid combination of the subset sum problem and modified RSA cryptosystem. In this work, we are going to enhance the security of the RSA algorithm. Here we are using three prime numbers in place of two and also adding super increasing sequence for the key generation process. If Attacker wants to break proposed systems then one has to factor the modulus into its primes as well as find the secret set A. If modified RSA, which is based on single module is broken in time x and subset sum algorithm is broken in time y then the time required to break this proposed algorithm is x*y. Therefore the security of our proposed system is increased as compared to RSA algorithm.

Keywords: Asymmetric key Cryptography Sub-set Sum cryptography, RSA cryptosystem, Security.

I. INTRODUCTION

Cryptography, a word with Greek origins, means "secret writing. " However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks. There are two types of cryptography techniques:

a. Symmetric key cryptography
b. Asymmetric key cryptography

There are few problems with asymmetric key cryptography because it is very slow in process and in terms of security like brute force and factorization attack. At this time asymmetric key cryptography is used only for encrypt and decrypt the keys not the entire message. On the other hand symmetric key cryptography is very fast (i.e.1000 times) as compared to asymmetric key cryptography. Hence symmetric key cryptography is used for encrypt and decrypt the entire message.

RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard, who first publicly described it in 1978. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret.

a. Security of RSA algorithm:

In the RSA cryptosystem there are problem of brute-force attack, factorization attack and mathematical attack. In RSA if one can factor modulus into its prime numbers then the private key is also detected and hence the security of the cryptosystem is broken.

b. Sub-Set- Sum cryptography:

The subset sum problem is an important problem in complexity theory and cryptography. The problem is this: given a set of integers, does the sum of some non-empty subset equal exactly zero. For example, given the set {−7, −3, −2, 5, 8}, the answer is yes because the subset {−3, −2, 5} sums to zero.

The problem is NP-Complete [6]. There are two problems commonly known as the subset sum problem. The first is the problem of finding what subset of a list of integers has a given sum, which is an integer relation problem. The second subset sum problem is the problem of finding a set of n distinct positive real numbers with as large collection as possible of subsets with the same sum [4]. The subset sum problem is a good introduction to the NP-complete class of problems.

The Subset-Sum cryptosystem (Knapsack Cryptosystem) is also an asymmetric cryptographic technique. This system is based on the subset sum problem (a special case of the knapsack problem): An instance of the Subset Sum problem is a pair (S, t), where S = {x_1, x_2... x_n} is a set of positive integers and t (the target) is a positive integer.

The decision problem asks for a subset of S whose sum is as large as possible, but not larger than t. This problem is NP complete. However, if the set of numbers (called the knapsack) is super increasing, that is, each element of the set is greater than the sum of all the numbers before it; the problem is easy and solvable in polynomial time with a simple greedy algorithm. A knapsack cipher algorithm is based on the NP-complete knapsack-packing problem. This cipher encodes a plain text message as a solution to a series of knapsack problems. A block of plain text equal in length to the number of items in the collection selects the items in the knapsack.

II. RELATED WORK

The objective of this proposed work is to produce an algorithm to enhance the security of the RSA algorithm. For enhancement of the RSA algorithm, here three prime numbers are used to provide the edge to the security to the RSA cryptosystem. After the problem statement of the RSA cryptosystem, there are two factors comes: Slow speed, Problem of factorization and brute force attack. This work is done in the direction of security i.e. cryptanalysis to overcome the problem of brute force and factorization. We are not working in the direction of speed up the system. In the proposed algorithm we are using the hybrid combination of subset sum cryptosystem and RSA cryptosystem.

In RSA algorithm only encryption key "e " is used to encrypt and decryption key "d " is used to decrypt the message. In this proposed work we are using encryption key with secret set A for the encryption and decryption key with the secret set A for decryption. The concept of three prime numbers has been introduced to provide edge to the security of the RSA cryptosystem. We are implementing this work using MatLab programming language.

III. RSA ALGORITHM

RSA consist of three steps:

[1]. Key Generation Process
[2]. Encryption Process
[3]. Decryption Process

Key Generation Process

1. Select p , q where p and q both prime , p is not equal to q.
2. Calculate n = p xq
3. Calculate $\phi(n) = (p-1) \times (q-1)$
4. Select integer e whose gcd $(\phi(n), e) = 1$; $1 < e < \phi(n)$

5. Calculate d, $d = e^{-1} \pmod{\phi(n)}$
6. Public key: PU = {e, n}
7. Private key: PR = {d, n}

Encryption Process

Plain text : $M < n$

Cipher text: $C = M^e \bmod n$

Decryption Process

Cipher text: C

Plain text: $M = C^d \bmod n$.

IV. PROPOSED TRIPLE PRIME RSA ALGORITHM USING SUBSET SUM CRYPTOGRAPHY

Algorithm 1: Key Generation Process

Input: Three prime numbers and Super increasing sequence

K= key

A = Super Increasing Set

Output: Public Key (B, n, e) , Private Key (A, M, W, n, d)

Begin

Step1. Input the value of three prime p, q and z.

Step2. Compute the product of two prime p, q and z.

Step3. Compute $\Phi = (p-1) \times (q-1) \times (z-1)$.

Step4. Choose an integer e, satisfying $1 < e < \Phi$, such that $\gcd(e, \Phi) = 1$.

Step5 Compute the secret exponent d, $1 < d < \Phi$, such that $e \times d \equiv 1 \pmod{\Phi}$.

Step6 Choose a super increasing set $A = (a_1, \ldots, a_n)$.

Step7 Choose an integer M with $M > SUM_{i=1 \ldots n}(ai)$. M is called the modulus.

Step8 Choose a multiplier W such that gcd (M, W) = 1 and 1 <= W < M This choice of W guarantees an inverse element U: $UW = 1 \pmod{M}$.

Step9 To get the components b_i of the public key B, perform $b_i = a_i{*}W \bmod M$, I = 1 ... n.

End

Algorithm 2 Encryption

Input: input file to be encrypted

K= key

Output: Encrypted file

Begin

Step1. Input the message that is to be encrypted.

Step2. Generate the ASCII code of the message.

Step3. Apply the public key B to the original message and generate the intermediate cipher text C i.e. $C = b_1 p_1 + b_2 p_2 + \ldots + b_n p_n$.

Step4. Compute the cipher Text $C_1 = C^e \bmod n$.

Step5. After finding the cipher text C_1 we send it to the transmission channel. **End**

Algorithm 2 Decryption

Input: input file to be decrypted (Cipher text)

K= key

Output: Original Message

Begin

Step1. Apply the private key "d " on the cipher text and take the modulo "n ".

$$m_1 = C_1^d \bmod n.$$

Step2. Compute $c' = Um_1 \bmod M = W^{-1}C \bmod M$.

Step3. Solve the (A, c) by the following algorithm.

For i = n downto 1

If $c \geq a_i$ then $x_i = 1$ and $c = c - a_i$

Else $x_i = 0$

If $s \neq 0$ then return (no solution)

Else return $(x_1, x_2, \ldots, x_n)$

Because A is super increasing, (A, c') is easily solvable. Let $X = (x_1, x_2, \ldots, x_n)$ be the resulting vector and $p_i = x_i$ and $p = (p_1, p_2, \ldots, p_n)$ is the plaintext

End

V. PROPOSED ARCHITECTURE:

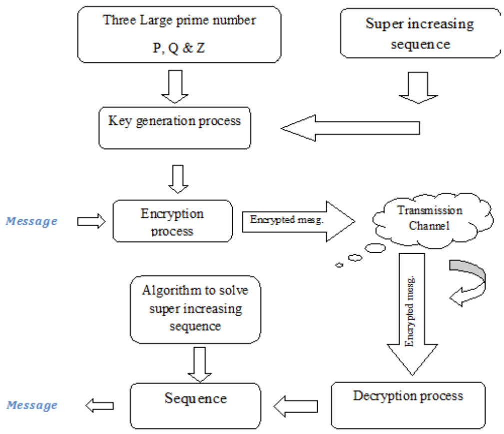

Figure 5.1: Schematic diagram of proposed method

VI. SIMULATION RESULTS

All the implementation work is done on the MatLab platform:

Results:

Table 1.1 Input message with their execution time

S. No.	Input message	Execution Time (in sec.)
1.	Vishal	0.061682
2.	vishal ja	0.087501
3.	vishal jayaswal	0.130932
4.	vishal jayaswal mtech	0.181511
5.	vishal jayaswal mtech student	0.232388

VII. CONCLUSION

This modification improves the security of RSA. If Attackers wants to break our proposed systems then he has to factor the modulus into its primes as well as find the secret set A. If RSA which is based on single module, is broken in time x and subset sum algorithm is broken in time y then the time required to break this proposed algorithm is x*y. Hence the security of our proposed system is increased as compare to RSA algorithm.

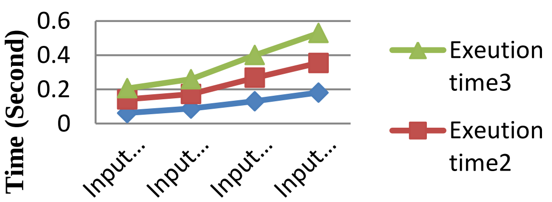

Figure1.1. Graph between input message and execution time in second

```
Implementation of Modified RSA Algorithm using Sub-Set-Sum cryptosystem

Enter the value of p: 11

Enter the value of q: 13

Enter the value of z: 17
```

Figure 1.2. Passing input value in the program during execution on MatLab

```
The value of (N) is: 143
The public key (e) is: 7
The value of (Phi) is: 120
The private key (d)is: 103
The super increasing sequence (s)is: 2    7   19   37   76
The selected modulus (m)is: 151
The multiplier (w)is: 2
The inverse element (u)is: 151
The component of public key (b)is: 4   14   38   74    1
Elapsed time is 0.091007 seconds.

Enter the message:
```

Figure 1.3. Display intermediate value by the program during execution on MatLab

```
The public key (e) is: 7
The value of (Phi) is: 120
The private key (d)is: 103
The super increasing sequence (s)is: 2    7   19   37   76
The selected modulus (m)is: 151
The multiplier (w)is: 2
The inverse element (u)is: 151
The component of public key (b)is: 4   14   38   74    1
Elapsed time is 0.091007 seconds.

Enter the message: india
ASCII Code of the entered Message:
   105   110   100   105    97

Cipher Text of the entered Message:
   118    33   100   118    59

Decrypted ASCII of Message:
   105   110   100   105    97

Decrypted Message is: india
Elapsed time is 0.088410 seconds.
fx >>
```

Figure 1.4. Output of the program

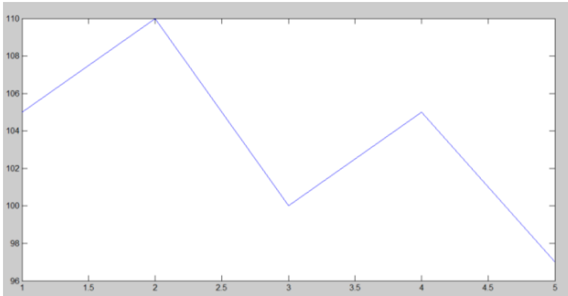

Figure 1.5. ASCII Code of the entered Message

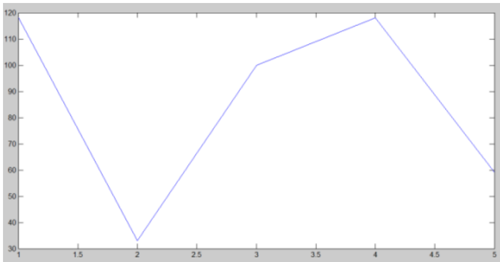

Figure 1.6. Cipher Text of the entered Message

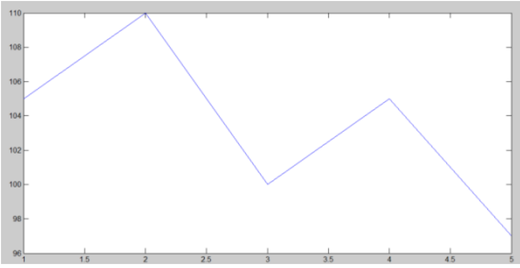

Figure 1.7. Decrypted ASCII of Message

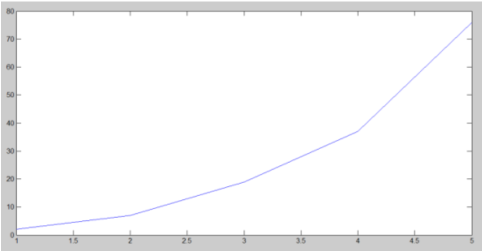

Figure 1.8. super increasing sequence

VIII. REFERENCES

[1]. Digital signature scheme with message recovery using knapsack-based ECC International journal of network security, Vol.12, No.1, jan 2011. R. Rajaram Ramasamy and M. Amutha prabakar.

[2]. Knapsack based ECC Encrytion and Decryption. International journal of network security, Vol.12, No.1, jan 2011.R.Rajaram Ramasamy and M. Amutha prabakar.

[3]. An Efficient Signature System Using Optimized RSA Algorithm IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, December 2008 Prof. MOUSTAFA ABD EL-AZIEM, Dr. MOHAMMAD ALI GOMAA.

[4]. IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, December 2008, "An Efficient Signature System Using Optimized RSA Algorithm ".

[5]. T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, July 1985.W.Diffie and M. Hellman. "New Directions in Cryptography ". IEEE transactions on Information Theory. IT-22(1978).472-492.

[6]. R. C. Merkle and M. E. Hellman, "Hiding information and signatures in trapdoor knapsacks, "IEEE Trans. Inf. Theory, IT- 24(5), pp.525-530, 1978.

[7]. Shamir, A. 1984. A polynomial-time algorithm for breaking the basic Merkle - Hellman cryptosystem; Information Theory, IEEE Transactions on , Volume: 30 Issue: 5 , Sep 1984 Page(s): 699 –704

[8]. Diffie, W.; Hellman, M.1976. New directions in cryptography; Information Theory, IEEE Transactions on , Volume: 22 Issue: 6 , Nov 1976 Page(s): 644 –654

[9]. M. E. Hellman and E.D. Karnin, 1983 "The Largest Super-Increasing Subset of a Random Set, "IEEE Trans. on Info. Theory, Vol. IT-29, January 1983, pp.

[10]. R. Rajaram Ramasamy and M. Amutha Prabakar 2011. Digital Signature Scheme with Message Recovery Using Knapsack-based ECC, International Journal of Network Security, Vol.12, No.1, PP.7 - 12, Jan. 2011

[11]. M. E. Hellman, "An Overview of Public Key Cryptography, "IEEE Communications Society Magazine, Vol. 16, Nov. 1978, pp.24-32 (Invited Paper).

[12]. W. Diffie and M. E. Hellman, "Privacy and Authentication: An Introduction to Cryptography, "Proceedings of the IEEE, Vol. 67, March 1979.