A NOVEL KEY GENERATION BASED MODIFIED RSA TECHNIQUE
FOR PERFORMING ENCRYPTION AND DECRYPTION OF DATA

1 Rahul Mishra
Dept. of Electronics and Communication Engg., SSSUTMS, Sehore.

2 Dr. Trayambak Hiwarkar
Professor and Dean Dept. of Electronics and Communication Engg., SSSUTMS, Sehore.

ABSTRACT:

The term cryptography is derived from the Greek word crypto’s. Cryptography is playing a vital role in keeping information secure. Public key cryptography or asymmetric key cryptography makes use of two keys, one is public key and another is private key for performing encryption and decryption respectively. Public key cryptography achieves confidentiality, integrity and availability. This paper presents a novel key generation technique. This paper also presents a modified RSA technique. This modified RSA method uses four variables to generate keys. Then it uses a set of prime numbers to perform encryption and decryption. The key generation time and decryption time of proposed algorithm have compared with HRSA algorithm.

Keywords: Cryptography, Cryptosystems, Public key cryptography, key generation, encryption, decryption, RSA.

[1] INTRODUCTION:

Cryptography is a Greek word for providing disguised information. It includes transformation of information (Plaintext) into some other form (Ciphertext). The main feature of cryptography is to solve the problems, which are associated with verification, integrity and privacy. A protocol is the sequence of actions, which is designed with two or more sides, through which a goal can be fulfilled. Cryptography also, is associated with the meaning of protocol. Thus, a cryptographic protocol is a protocol that deals with the use of cryptography. This protocol uses cryptographic algorithm and intends to halt attempts of thefts and invasions [1].
Figure 1 presents asymmetric key cryptography. The data is encrypted and decrypted using a pair of keys. The secret key and shared key is available at sender side as well as receiver’s side.

![Diagram of Public Key Cryptosystem]

**Figure 1: Public Key Cryptosystem**

The message is transformed into cipher text. The cipher text is transmitted from sender side to receiver side by using the internet. At receiver’s end, the cipher text is received. Then the cipher text is transformed into the original plain text by using the decryption algorithm and the key. The decryption process is exactly a reverse of encryption process.

The security services include [3]:

- Data Confidentiality
- Data Integrity
- Authentication
- Non repudiation
- Access Control

RSA [3] is most common algorithm, which includes a pair of keys to perform data confidentiality. Private Key can also be used by the sender to generate the digital signatures. Anyone who knows the public key of the sender can verify the message. If the message is intended for a particular receiver, the user applies the receiver’s public key on the message. The message is accessed by the receiver; first by applying his/her own secret key and then sender’s public key. Depending on the application, public and private key can be used in any order.

The most important part of RSA performance covers the decryption performance. Because of the security constraints, decryption exponent is usually considered to be very large of the order of the modulus size. Large size of the decryption exponent (d) lowers down the speed of decryption side. In this section, RSA variants which are based on the improvement in decryption speed are discussed. This is required in almost every case where RSA cryptosystem is used. Practical relevance of these variants lies in the signature generation (or decryption method) in heavily loaded web servers or small handheld devices, e.g. the bank customer is required to generate the signature (using his/her private key) on small device (like smart phones). The decryption method needs
to be optimized in this case by reducing the computational complexity of the decryption method. This can be achieved by reducing the bit size of the decryption exponent in the computations involved in decryption method.

[2] LITERATURE SURVEY:

In any communication system including internet, satellite and mobile, it is impossible to prevent the important or sensitive information from eavesdropping or losses when the information is broadcasted through the channel (wire or wireless). So security of information has become increasingly important for any application [6].

The protection of information for long period time is very critical in many environments. One way of implementation this protection with high activity is RSA cryptosystem. In this paper the old algorithm of RSA system is showed. And for more complexity and to increase time of attack coding. A new coefficient is \( z \) has been added to generator function \( \Phi(n) \) in additional to selected \( p \) and \( q \) which are depended in old algorithm[5].

To ensure the proper complexity of RSA algorithm, a new coefficient is \( Z \) has been added to generator function \( j(n) \) as follow:

\[
\Phi(n) = (p-1)(q-1)\times(Z \ 1)
\]

And then complete all steps of last section take \( Z \) in our consideration. It is clear that the degree of eq. becomes grater by 1 about that similar in previous section, consequentially that effects on all equations of RSA algorithm and their attacks [7].

The authors in [8] proposed a new algorithm based on RSA. The proposed algorithm was having new parameters to increase the complexity of encryption process and decryption process. The proposed method is secure in comparison to previous methods. But it is computationally very expensive. Use of many parameters in encryption and decryption process, makes it very time inefficient.

Work done in [9] presented a new modulus instead of modulus \( n \) in previous methods, \( n \) was product of 2 prime numbers. Instead of \( n \), a new variable in transmitted to receiver. It is more secure but calculation of new variable is taking a lot of time comparatively.

Another updated version of RSA was proposed by authors in [10], it uses the concept of four prime numbers instead of two. Four prime numbers were multiplied to find multiplication modulus. They also proposed a time efficient key generation process. Generation of public key and private key are dependent on new variable. They were not dependent on multiplication modulus \( n \).

Batch RSA [11] in 1989; the work was done to accomplish many decryption processes at the cost of approximately one. More than one jobs are combined to make a batch
and decryption of the complete batch is performed in a single process, thus reducing the cost of multiple decryption processes.

This variant works for small and different public exponents for the same modulus N. Decryption of the two cipher texts in Batch RSA can be done at the cost of approximately one RSA decryption. Relevance of this variant is restricted to cipher texts with only very small public exponents and where decryptions have to be handled in bulk, e.g. in banks.

MultiPrime RSA [12] was designed to enhance the decryption speed of RSA cryptosystem by taking more than two primes for the modulus. It consists of k primes \( p_1, p_2 \ldots p_k \) instead of using only two as in standard RSA. This variant is more suitable for use in resource constrained devices as it is more efficient in terms of computational speed as compared to RSA CRT.

In this variant [13] also, the purpose was to improve the decryption time of RSA algorithm. Instead of using multi-ple primes for the modulus, only two primes are used but with smaller sizes as compared to standard RSA. In the algorithm \( N = p^{b-1}q \), where \( p \) and \( q \) are \( n/b \) bits. Due to the use of only two primes MultiPower RSA is more efficient than MultiPrime RSA [12].

In [14], the public and private exponents \( (e, d) \) are generated and shared by two instances with different modulus. Sharing of the parameters by two RSA instances reduces the memory requirement by the cryptosystem.

In [15], a new version of RSA was proposed. This version makes use of four prime numbers. It has also given a new encryption key generation method. Although this key generation method is complex and taking a lot of time. In place of \( n \) they have used a single prime number \( w \) in encryption and decryption. This makes multiplication modulus weaker. Decryption time is also more.

[3] PROPOSED METHODOLOGY
The steps of proposed methodology are as follows:

**Modified RSA Key Generation:**
Algorithm is as follows:
1. Start
2. Read four prime numbers \( p, q, r \) and \( s \)
3. Calculate \( t = p \times q \times r \times s \)
4. Calculate \( \phi(w) \) as follows
   \[ \Phi(w) = (p-1) \times (q-1) \times (r-1) \times (t-1) \]

5. Generate two unique random number \( P1 \) and \( P2 \), which are not co prime to \( \phi(w) \) using random number generator

6. Calculate \( v = (2P1 + (P1 \times P2)) \mod t \)

7. Calculate public key \( e \) such that it is not co prime of \( (\phi(w) \times v) \)

8. Calculate private key \( d \) such that \( (d \times e) \mod (\phi(w) \times v) = 1 \)

9. Calculate \( n \) such that
   - \( x = \text{nextprime}(p \times q) \)
   - \( y = \text{nextprime}(r \times s) \)
   - \( n = x \times y \)

10. stop

**Modified RSA encryption algorithm:**

1. start
2. calculate \( C = M^e \mod n \), where \( C \) is cipher text, \( M \) is plain text and \( e \) is encryption key
3. stop

**Modified RSA decryption algorithm:**

1. start
2. calculate decryption as follows
   - \( dx = d \mod (x-1) \)
   - \( dy = d \mod (y-1) \)
   - \( z = y \mod\text{inverse} x \)
   - \( m1 = c^{dx} \mod x \)
   - \( m2 = c^{dy} \mod y \)
   - \( h = z \times (m1 - m2) \mod x \) (if \( (m1-m2) \) is negative then add \( q \) into it)
   - \( m = m2 + h \times y \)
3. stop

[4] RESULT ANALYSIS:

In this section, the key generation time and encryption time of modified RSA algorithm are
A NOVEL KEY GENERATION BASED MODIFIED RSA TECHNIQUE FOR PERFORMING
ENCRYPTION AND DECRYPTION OF DATA

compared with HRSA [15]. Both algorithms are implemented in java on 2.8 Ghz dual core processor with 2 GB RAM. Random numbers are generated using inbuilt java methods.

The input plain text is:
1234567890987654321012345678909876543210123456789098765432101234567890987654321012345678909876543210123456789098765432101234567890987654321012345678909876543210123456789098765432101234567890987654321012345678909876543210123456789098765432101234567890987654321012345678909876543210

The key generation time and encryption time of both the algorithms is shown below in table:

<table>
<thead>
<tr>
<th>Algorithm Name</th>
<th>Encryption Time in ms</th>
<th>Alice Key Generation Time in ms</th>
<th>Bob Key Generation Time in ms</th>
</tr>
</thead>
<tbody>
<tr>
<td>HRSA</td>
<td>187</td>
<td>5710</td>
<td>4399</td>
</tr>
<tr>
<td>Modified RSA</td>
<td>47</td>
<td>1373</td>
<td>2589</td>
</tr>
</tbody>
</table>

Table1: Result Comparison

![Time Consumed in ms](image)

Figure 2: Comparison of Alice Key Generation Time
CONCLUSION

RSA is most widely used technique for keeping data secret. This paper presented a modified version of RSA. This version contains a novel key generation technique and decryption
A NOVEL KEY GENERATION BASED MODIFIED RSA TECHNIQUE FOR PERFORMING
ENCRYPTION AND DECRYPTION OF DATA

technique. The results of proposed RSA have compare with existing versions of RSA. It is
found that key generation time of proposed RSA is less in comparison to HRSA. Decryption
time has also reduced.

References:


public key cryptosystems”, Communications of the ACM vol. 21 (2) , pp.120–126, 1978.
algorithm”, international conference on Advanced Computer Science Applications and

ENCRYPTION FOR BLOCK CIPHERS AND MULTI CODE GENERATION BASED ON
SECRET KEY, International Journal of Network Security & Its Applications (IJNSA), Vol.3,
No.6, November 2011

cryptosystem; Information Theory, IEEE Transactions on , Volume: 30 Issue: 5 , Sep 1984
Page(s): 699704


