IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-3, Issue-5 E-ISSN: 2347-2693

# Encrypted RSA Public Key Sharing By Using Image Pixel Color Value

Sarika Khatarkar [1*] and Rachana Kamble[2]

[1*,2]*Department of computer science, Technocrats Institute of Technology, Bhopal, Madhya Pradesh, India*

www.ijcseonline.org

Received: Apr /25/2015 Revised: May/07/2015 Accepted: May/19/2015 Published: May/30/ 2015

***Abstract*—** RSA algorithm is extensively used in the popular implementations of Public Key Infrastructures. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. One key is used for encryption and the other corresponding key is used for decryption. No other key can decrypt the message. In this paper an approach which is more secure than original RSA algorithm has presented, which is used for digital signatures and encryption in public key cryptography. This approach eliminates the need to transfer e. because in this approach before transfer e is encrypting with any pixel color value of any image.

***Keywords*—** RSA, Public Key, Pixel color value.

## I. INTRODUCTION

For security and speed of RSA, it has some important parameters. By increasing the modulus length it plays an important role for increasing the complexity of decomposing it into its factors. That increases the length of private key and hence it will difficult to be decrypted without knowing the decryption key. Length of encrypted message proportionally changes when the message length is changed.

hence to obtained larger encrypted message, larger size chunks are selected to increase the security of the data in use[10]. An organization with suffientely deep pockets, It is possible that can build a large scale version of his circuits and effectively crack an RSA 1024 bits message in a relatively short time period, which could range any where from a number of minutes to some days[7,8]. Performance of RSA algorithm analyzed by varying that parameters with respect to time[9]. For pair of keys, we use natural numbers, in addition to existing parameters of RSA. Then after simulations of results on basis of speed and security we compare the new algorithm and RSA.

### 1.1 RSA Key Generation, Encryption, Decryption Process

The following steps are there to determine the values of e, d and n.

- Choose two very large (100+ digit) prime numbers p and q.
- Set n equal to p * q.
- Choose any large integer, e, such that

GCD (e, ((p-1) * (q-1)) = 1

- Find d such that e * d mod ((p-1)*(q-1)) = 1

The public key is the number (n, e). Although these values are publicly known, it is computationally infeasible to determine ‘d’ from ‘n’ and ‘e’ if p and q are large enough. To encrypt a message, M, with the public key, creates the cipher, C, using the equation:

C = Me mod n e: Public Key

The receiver then decrypts the cipher with the private key using the equation:

M = Cd mod n d: Private Key

Now, this might look a bit complex and, indeed, the mathematics does take a lot of computer power, given the large size of the numbers; since p and q may be 100 digits (decimal) or more, d and e will be about the same size and n may be over 200 digits.

Nevertheless, a simple example may help. In this example, the values of p, q, e and d are purposely chosen to be very small and the reader will see exactly how badly these values perform, but hopefully the algorithm will be adequately demonstrated.

## II. LITERATURE SURVEY

A. *Modified RSA Based on Multiple public keys*

Security is most important to transmit confidential data over the network, in the today’s world. In wide range of applications, Security is also demanding. For data security Cryptographic algorithms play a vital role against malicious attacks. In the most popular implementations of Public Key Infrastructures, RSA algorithm is extensively used. In this paper[1] an algorithm hsa proposed for RSA a method for implementing a public-key cryptosystem (RSA) using two public key and some mathematical relation. This two public keys are sent separately, this makes the attacker not to get much knowledge about the key and unable to decrypt the message. Two different keys are used in Public Key cryptography. One key is used for decryption & only the other corresponding key must be used for encryption. Not

 

any other key is possible to decrypt the message, even the original (i.e. the first) key can't used for encryption. Every communicating party requires pair of key for communicating with any number of other parties. It is beauty of this scheme. Once someone obtains a key pair, he can communicate with anyone else. They have done implementation of RSA algorithm efficiently using two public key pairs and using some mathematical logic rather than sending the e value directly as a public key.

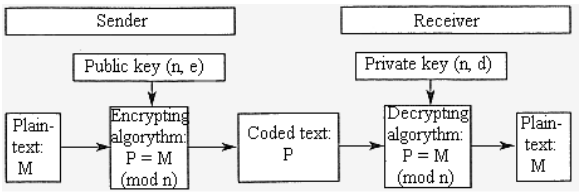


Fig 1. RSA algorithm

B. *Personal Information Protection Approach Based on RSA*

With the widespread and rapid development application of the information technology, the communication pattern has obviously changed among individuals, corporations and even nations. However, convenient network-based communication method brings not only the benefits but also some disadvantages such as individual information leak. this paper[2] introduced that, personal information can be transformed from plain text into cipher text. Customer representatives will be able to contact their clients without seeing the privacy. On the server side, the system administrator has the permission of authorization management. They devolve the authorization to database administrators and then database administrators input customers' information into the system. At the same time, sensitive information such as phone number is encrypted. On the client side, the customer representatives only see the names list.

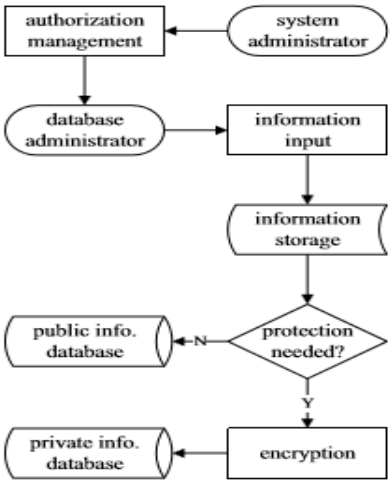


Fig 2. The encryption approach of customers information.

When operation is needed, software installed on the customer representatives' computer or cell phone will decrypt the data and send them to the call center directly without touching the representatives.

C. *Quantum Key Distribution*

Using the current computing systems classical cryptography is based on the computational difficulty to compute the secret key. Depending only on the difficulty of computational complexity does not provide enough security because finding a fast method to calculate the secret key. it will compromise the security of the systems. Law of physics is used in Quantum computing for communication. In cryptography and key distribution quantum theorems and principles are applied. In this paper[3], new model for quantum key distribution are introducing among three parties or more where there is a trusted center that providing the necessary secret information of clients to securely communicate to each other.

To compare the bases, classical channel is used by quantum key distribution protocols BB84, B92 and ERP.

D. *i-RSA algorithm*

This paper[4] propose i-RSA algorithm, that is focus on key generation algorithm. user identity is Enhancement of this algorithm. it can be used as a public key, such as email address. The key certificates are used to authenticate the user's key pair. So certificate does work as important role in secure communication but to issue the certificate is a big challenge and it also increases the overhead due to the increasing cost. For public key Previous algorithm was successful used email identity, but all type of email can't be used as a public key. So the propose i-RSA algorithm that can produces 66.6% compared to previous algorithm (46.67%) email can be a string public key. in key generation looping process is the main differences between i-RSA and previous algorithm, to get new value of p and q parameter, when value of k is equal to 1, then looping process will stop, and the email can be a public key. Detail explanations of i-RSA algorithm in propose algorithm section.

*E. Modified RSA Cryptosystem Based on Offline Storage and Prime Number*

In RSA computation is lengthy and some less secure. This paper[5] present a new algorithm to presents the modified form of new RSA algorithm in order to boost up the speed of the implementation of RSA algorithm during data exchange across the network world. In this method keys are stored offline before the process start. Thus, the speed of process increased as compared to original RSA method.

*F. Enhancing The Security Of The Rsa Cryptosystem*

This paper[6] increases the security of the RSA algorithm, this enhancement use randomized parameter to change every encrypted message block such that even if the same message is sent more than once the encrypted message block will look different. This paper suggests that how to use randomized parameters in the encrypt the data to make RSA. By this enhancement it makes the RSA semantically more secure. Means an attacker cannot distinguish two encryptions from each other, even if the attacker knows (or has chosen) the corresponding plaintexts(original message). In this paper a comparison between the modified RSA and the basic RSA version introduced. Enhancement can easily be implemented on this paper. Also other attacks are presented by this paper, also how to speed up the RSA encryption and decryption process is an important issue for the RSA implementation.

here we have seen that RSA is more secure and it may be more stronger by applying some techniques. Here we have seen that all authors are talking about many method but no one is talking about image pixel for security purpose. So we can add image pixel technique to make more powerful RSA algorithm.

## III. PROPOSED WORK

In this proposed work first of all p and q two prime number is selected then find p*q after this calculate (p-1)*(q-1). Then select e and d. after all public key and private key is generated. But before sharing public key we have to encrypt this. So that other person who doesn't belongs to my group cannot get public key.

### *A. Encryption*

After generating public key, before sharing to other people's sender will use an image that already have in receiver side. First of all select an image that already have all receivers then select any pixel color value of that image. Then add that color value with e and save in E. now we don't need to share actual value of e. now we will share E and position of that pixel in image.

### *B. Decryption*

When receiver get encrypted message then if he have same image then they will select same image and select pixel position that they have received and after all, pick color value of that pixel and minus that value from E that they have received from sender. Means anyone who want to share public key they only share E and pixel position.

### *C. Algorithm*

**Encryption**

(1) Select p and q both prime number, p is not equal to q.

(2) Calculate n = p x q.

(3) Calculate ø (n) = (p -1) x (q-1).

(4) Select integer e whose gcd (Ø (n), e) = 1; 1 < e <Ø (n).

(5) Calculate private key d = e-1 (mod Ø (n)).

(6) Public key PU = {e, n}.

(7) Private Key PR = {d, n}.

(8) Im=Load any image img.

(9) Select pixel position p_id.

(10) For(i=1; i<=P_id; i++)

{

If(i==P_id)

Px=im(p_id);

}

(11) E=Px+e.

(12) Public key to transmit = {E,P_id,n}.

(13) Message (M) Cipher text- C = M^e mod n.

**Decryption**

(1) Public key to transmit = {E,P_id,n}.

(2) For(i=1; i<=P_id; i++)

{

If(i==P_id)

Px=im(p_id);

}

(3) e=E-Px.

(4) Message M = C^e mod n.

Where M is message (Plane text), p and q are prime numbers, N is common modulus, e and d are public and private keys, p_id is a pixel position of selected image, im is a program variable which contain all pixels color values of selected image, Px is a color value of pixel position p_id for selected image.

### *D. Flow Chart*

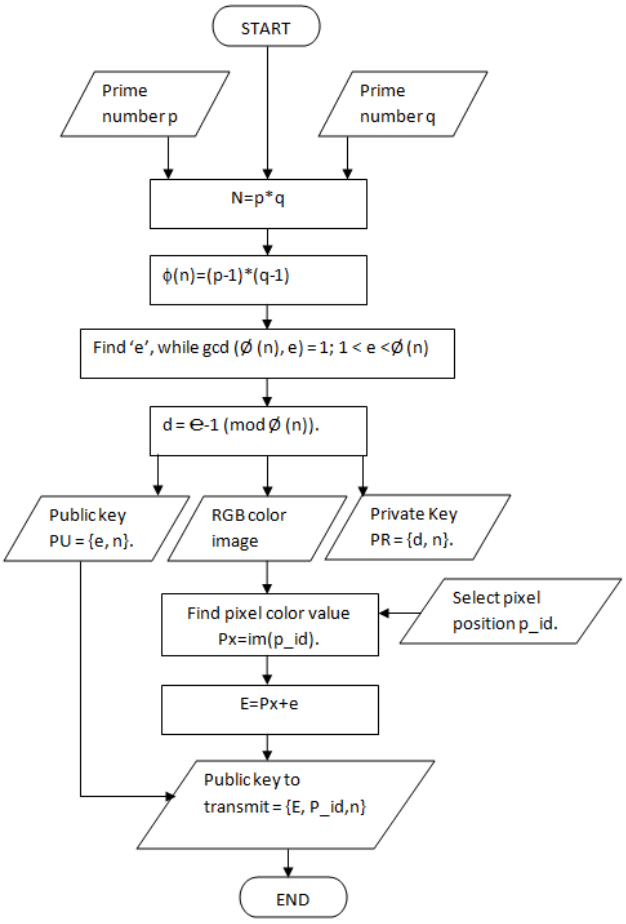


Fig. 3 flow chart

*E. Result And Analysis*

**Table 1.** Comparison of probability of attacks.

| Traffic(No. of nodes) | Probability of attacks | |
|---|---|---|
| | RSA key sharing | RSA encrypted key sharing |
| 0 | 0 | 0 |
| 100 | 0.3 | 0.20 |
| 200 | 0.32 | 0.25 |
| 300 | 0.5 | 0.29 |
| 400 | 0.55 | 0.32 |
| 500 | 0.75 | 0.33 |

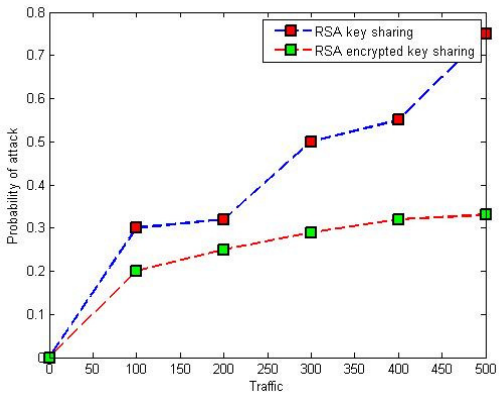


Fig 4 comparison of probability of attack in original RSA and proposed method

Fig 4 shows the probability of attack in original RSA is more than the probability if RSA using encrypted key sharing is used.

Fig 5. A sample image that is use for encryption and decryption.

Fig 5 shows a sample image that is selecting for encryption in sender side and same image is using for decryption in receiver side.

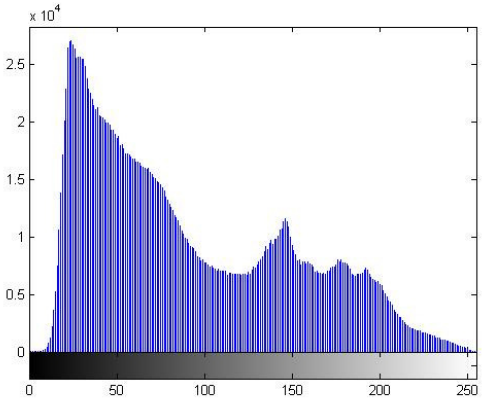


Fig 6. Histogram of sender side image

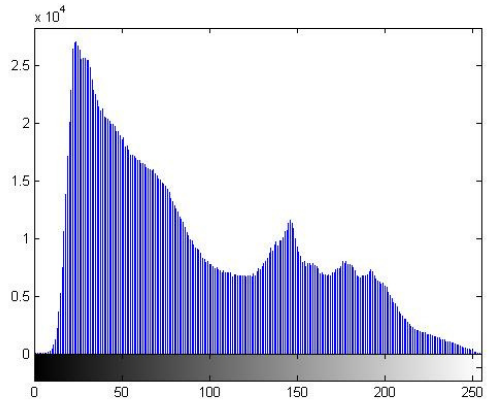


Fig 7. Histogram of receiver side image

Here, in fig 6 and fig 7, it is clearly seen that histogram of sender side image is same as histogram of receiver side image because this algorithm don't modifying image. only pixel color value is using for reference.

## IV. CONCLUSION

According to the comparisons and the characteristics of RSA, we determined to use RSA cryptography as the core algorithm for personal information protection in information system. It makes users don't have to store a mass of calculated secret keys. The information owner can easily send messages to the receiver when he got reliable public key from the receiver. This approach makes things easy, only one pair of keys is necessary.

In this work a new method has proposed for RSA public key sharing. In this method before sharing the public key, e is encrypted with any specified pixel color value of any particular image. So, it doesn't need to transfer e. because e is encrypted with any pixel color value then possibility of attack is very less as compared to without encrypted e. that's why if any attacker got shared key then they don't know what is actual value of e. it is possible if and only if he has same image. But in this method no one is sharing image. images is predefined. So after all this method is complex for attacker to getting e.

## REFERENCES

[1]. Amare Anagaw Ayele, Dr. Vuda Sreenivasarao, June 2013, "A Modified RSA Encryption Technique Based on Multiple public keys", International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 4.

[2]. Liang Wang, Yonggui Zhang, 2011, "A New Personal Information Protection Approach Based on RSA Cryptography", IEEE.

[3]. Ammar Odeh, Khaled Elleithy, Muneer Alshowkan, Eman Abdelfattah, 2013, "Quantum Key Distribution by Using Public Key Algorithm(RSA)", IEEE.

[4]. Norhidayah Muhammadi, Jasni Mohamad Zaini, Md Yazid Mohd Saman, "Loop-based RSA Key Generation Algorithm using String Identity", 13th International Conference on Control, Automation and Systems (ICCAS 2013).

[5]. Ms. Ritu Patidar, Mrs. Rupali Bhartiya, 2013, "Modified RSA Cryptosystem Based on Offline Storage and Prime Number", IEEE.

[6]Malek Jakob Kakish, "Enhancing The Security Of The Rsa Cryptosystem", Ijrras August 2011.

[7] KetuFile White Papers "Symmetric vs. Asymmetric Encryption ", a division of Midwest research corporation.

[8] RSA Laboratories : Technical Notes and Papers.

[9] A fast implementation of the RSA algorithm using the GNU MP library. By Rajorshi Biswas,Shibdas Bandyopadhyay,Anirban Banerjee, IIIT – Calcutta.

[10] Sensitivity of Changing the RSA Parameters on the Complexity and Performance of the Algorithm By Allam Mousa ;Journal of Applied Science 5 (1) :60-63,2005 ISSN 1607 – 8926.Asian Network for Scientific Information.