International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 1 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT195161

Data Encryption Key Sharing Using Image Pixel Color Value

Vijay Gokul Koli, Raj Kumar Paul
Department of Computer Science & Engineering, Vedica Institute of Technology, Bhopal, India

ABSTRACT

Security is required to transmit confidential information over the network. Security is also demanding in wide range of applications. Cryptographic algorithms play a vital role in providing the data security against malicious attacks. Massage communication over internet facing problems like data security, copyright control, data size capacity, authentication etc. A new idea is to apply reversible data encoding algorithms images by wishing to remove the embedded data after data receiving with the help of image pixel color value.

Keywords: Network Security, Cryptographic Algorithms, Image Pixel, Data Encryption, Public-Key Cryptosystem, Encryption, Decryption

I. INTRODUCTION

In the field of networking, role of network security is immense. In the age of information need to keep information about every aspect of our live. These information needs to be hidden from unauthorized access (confidentiality), protected from unauthorized change (integrity), and available to an authorized entity when it is needed (availability). Hence the way of keeping the information securely is known as cryptography, which comes from a word with Greek origin, means "secret writing". Many cryptographic algorithms are developed to achieve the above said goal. The algorithms should be such that an opponent cannot defeat its purpose.

II. METHODS AND MATERIAL

A Modified RSA Encryption Technique Based on Multiple public keys

In this technique a public-key cryptosystem (RSA) using two public key and some mathematical relation. This two public keys are sent separately.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 has 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.

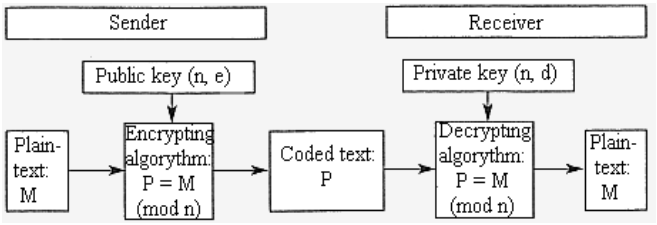

Fig 1. RSA algorithm

A new personal information protection approach based on RSA cryptosystem

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 can 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.

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

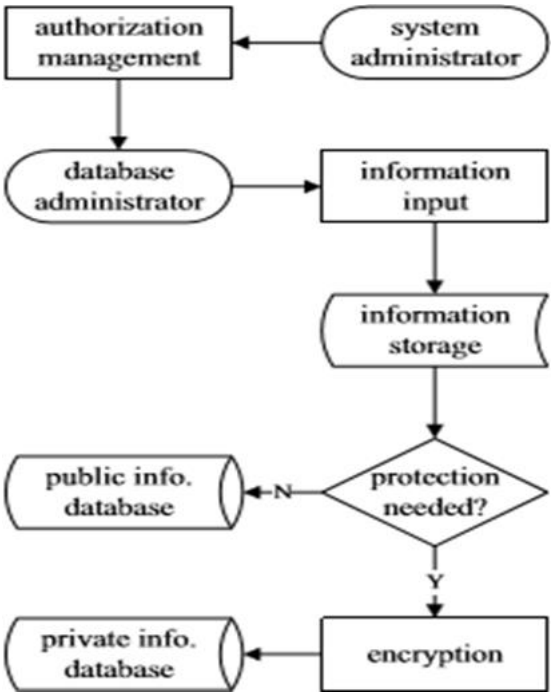

Fig. 2. The encryption approach of customers' information

Key Distribution by Using Public Key Algorithm (RSA)

Authors suggested a new model for quantum key distribution 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.

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

compromises 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.

Loop-based RSA Key Generation Algorithm using String Identity

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 has 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 can stop, and the email can be a public key. Detail explanations of i-RSA algorithm in propose algorithm section.

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.

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 is 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 Work comparison between the modified RSA and the basic RSA version introduced. Enhancement can easily be implemented on this Work. 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, RSA is more secure and it may be more stronger by applying some techniques. Here They have seen that all authors are talking about many methods but no one is talking about image pixel for security purpose. So theyF can add image pixel technique to make more powerful RSA

algorithm.

Proposed Methodology

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

after all public key and private key is generated. But before sharing public key they have to encrypt this. So that other person who doesn't belongs to my group cannot get public key.

According to the comparisons and the characteristics of RSA, it 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.

Encryption

After generating public key, before sharing to other people's sender can be 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 it doesn't need to share actual value of e. now it share E and position of that pixel in image.

Decryption

When receiver get encrypted message then if he have same image then they can be 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 wants to share public key they only share E and pixel position.

Algorithm

For both encryption and decryption algorithms are following.

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.

III. RESULT AND ANALYSIS

Figs shows front view of implementation of proposed work. It has designed using MATLAB. Here sender side "select image" button used for selecting the image. Fist text box is using for entering message that you want to send, second text box is using for giving pixel position value. And in receiver side first text box is using for giving same pixel position that has given in sender side.

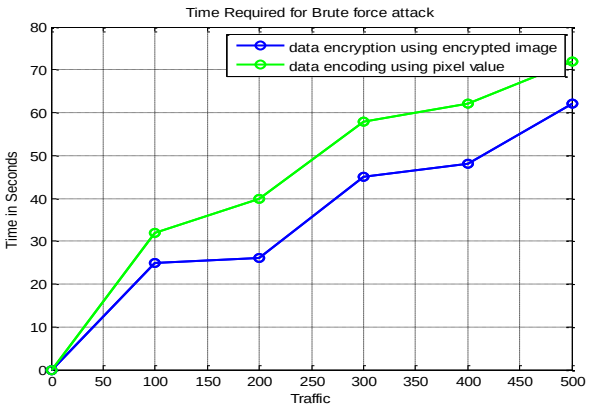

Fig. 3. Comparison of brute force attack in existing and proposed method using image pixel.

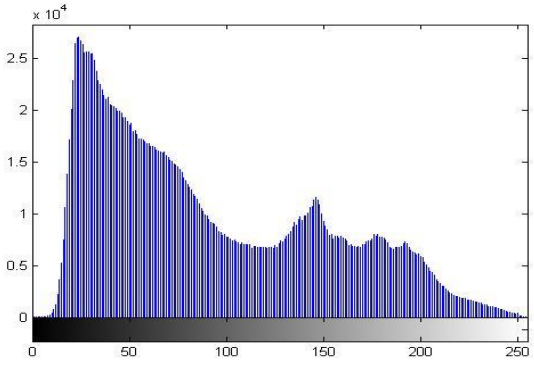

Fig. 4. Histogram of sender side image

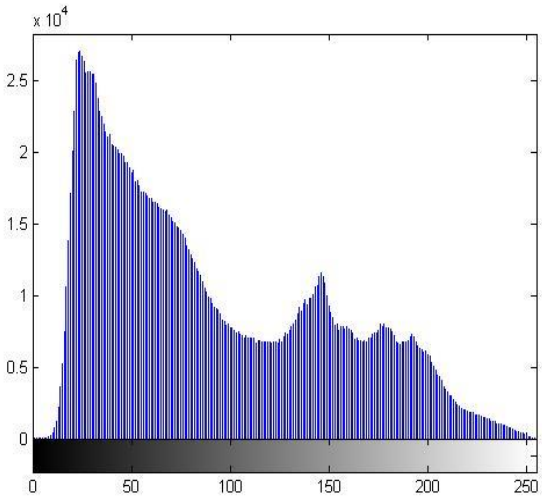

Fig. 5. Histogram of receiver side image

Here, in figs, 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

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 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. image is predefined. So after all this method is complex for attacker to getting.

V. 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]. M. Jason Hinek, Another Look at Small RSA Exponents, 2006.

[8]. B. A. Forouzan, D. Mukhopadhyay, Cryptography and Network Security, Tata McGraw-Hill, 2012.

[9]. Abdullah Darwish Imad Khaled Salah and Saleh Oqeili, Mathematical Attacks on RSA Cryptosystem, Journal of Computer Science (2006).

[10]. J. M. Pollard, A Monte Carlo Method for Factorization, BIT Numerical Mathematics (1975).

[11]. H. Riesel, Prime Numbers and Computer Methods for Factorization, Birkhauser, 1994.

[12]. William Stein, Elementary number theory. Primes, congruences, and secrets. A computational approach., New York, NY: Springer, 2009 (English).

Cite this article as :

Vijay Gokul Koli, Raj Kumar Paul, "Data Encryption Key Sharing Using Image Pixel Color Value", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 1, pp. 260-265, January-February 2019.

Available at doi : https://doi.org/10.32628/CSEIT195161

Journal URL : http://ijsrcseit.com/CSEIT195161