A survey on encryption techniques using Pixel Color Value

Vijay Gokul Koli[#1], Raj Kumar Paul[#2]
[#1,#2]*Department of Computer Science & Engineering, VIT, RKDF University, Bhopal, India*
[1]viju.koli5@gmail.com
[2]rajkumar.rkp@gmail.com

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.One of the most common public key algorithms in use for secure transaction is the RSA. Hence the goal to design an efficient architecture for RSA becomes more relevant. For high secure application they need to develop new algorithm to compute such mathematical operations which are involved in cryptographic algorithm.Thispaper explores the history of RSA and the method.

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)[7], 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.

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 [5] 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 anyoneelse. They have done implementation of RSA algorithm efficiently using two public key pairs and using some mathematical logic rather than sending thee value directly as a public key.

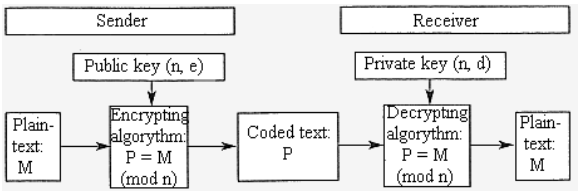

Fig 1. RSA algorithm

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 [8] 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.

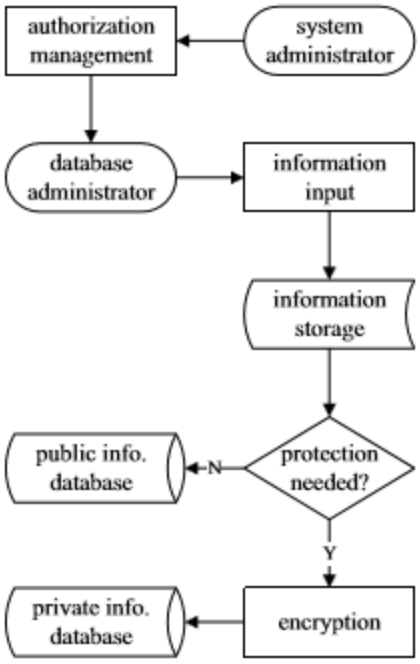

Fig. 2. Theencryption approach of customers' information

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 provideenough 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[1], 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 theemail 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[3] 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[2] increases the security of the RSA algorithm, this enhancement use randomized parameter to changeevery encrypted message block such that even if the same message is sent more than once theencrypted message block is look different. This paper suggests that how to use randomized parameters in theencrypt 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.

Table 1. Comparision of Algorithms with their attributes.

Author Name	Year	Advantages	Limitation
Malek Jakob Kakish	**2011**	This enhancement use randomized parameter to changeevery encrypted message block such that even if the same message is sent more than once theencrypted message block is look different.	Speed up in encryption and decryption process is an important issue for this algorithm.
Liang Wang	**2011**	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.	Algorithms is not so good in terms of complexity
Ammar Odeh	**2013**	Law of physics is used in Quantum computing for communication. In cryptography and key distribution quantum theorems and principles are applied. 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.	Trusted center is required, that may be intruder and may be hacked by some malicious software**.**
Amare Anagaw Ayele	**2013**	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 anyoneelse.	Algorithms is not so good in terms of complexity.

CONCLUSION

In Data communication, encryption algorithm plays an important role. Thisresearch work surveyed theexisting encryption techniques. According to the comparisons and the characteristics of RSA, it is determined to use RSA cryptography as the core algorithm for personal information protection in information system. The information owner can easily send messages to the receiver when he got reliable public key from the receiver. But this survey shows that none of the algorithms are there that have images as a security part. So it may be possible that if image will be used as a security part than it will be beneficial and new technique.

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).