I J C T A, 9(5), 2016, pp. 2627-2632

Customized RSA Public Key Cryptosystem Using Digital Signature of Secure Data Transfer Natural Number Algorithm

R. Mahaveerakannan* and C. Suresh Gnana Dhas**

ABSTRACT

The cryptography network security means to protect data transmission during their interconnected networks in all over the world. Cryptography network security is the important way of hiding/keeping information during transmission over a network. There are different kinds of cryptographic algorithms available to protect our data from intruders. The challenging of resource sharing on data communication in a network is its network security. The important issues of data security become critical. In this paper, we mainly focus on data encryption and decryption in a network environment using RSA algorithm. RSA is an efficient algorithm in cryptography network security. In this paper, we solvethe most security problem for data transmission in a network environment. So in this paper, a secure data transfer natural number algorithm is like to RSA algorithm with a few modifications. In this modifications much more increase the security of the cryptosystem. In this STNN algorithm, we have particularly used four prime factors (similar to RSA). In addition of this, we have used four prime factor is calculate two natural numbers in a pair of public key and private key. The two natural numbers much more increase the security of the cryptosystem.

Keyword: Encryption, Decryption, RSA, Data Secure, Digital Signature, Cryptography.

1. INTRODUCTION

Cryptography Network security is used to make secure data transmission and communication over networks. The algorithms are selected for cryptography network security should meet the conditions of authentication, confidentiality, integrity and non-repudiation. An efficient data transmission (key distribution) is an important problem in group communication. Members are joining and leaving in the groups are dynamical. They required for key updating by using encryption and decryption algorithm during the time of member join and leave the group. Many encryption algorithms are commonly available and used in cryptography network security. They can be categorized into two different types of keys: one for symmetric (private) and another one for asymmetric (public) keys encryption. In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. In Asymmetric keys are two different types of keys are used; private and public keys [1]. The public key is used for encryption and a private key is used for decryption (e.g. RSA). Public key encryption is based on mathematical functions, computationally intensive. We used asymmetric key cryptography for a key update of member join and leave in the group, the asymmetric key also called Public Key and Private Key cryptography; two different types of keys are used.

A public key is used for encryption and other corresponding private key must be used for decryption (E.g. RSA and Digital Signatures). Because users tend to use two keys: a public key, which is known

* Research Scholar, Information Technology St. Peter's University, Chennai, India, Email: mahaveerakannan10@gmail.com

** Professor and Head, Vivekananda College of Engineering for Women, Namakkal. India. Email: sureshc.me@gmail.com

to the public and private key which is known only to the user [2]. Asymmetric encryption techniques are almost 1000 times slower than Symmetric techniques because they require more computational processing power [3]. A digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature. Typically the signature is formed by taking the hash of the message and encrypting the message with the creator's private key. The signature guarantees the source and integrity of the message [4]. It depends on all bits of a transmitted message and also on a secret key but which can be checked without knowledge of the secret key. A digital signature is computed using a set of rules and a set of parameters such that the identity of the signatory and integrity of the data can be verified [9]. The encryption process is completed then decryption and verification of digital signature is started. The decryption of digital signature is done; in this process which finally results will be the generation of a message. Finally, the two messages are compared at the verification side. if the plain text (messages) are matched then the digital signature is said to be authenticated, the mismatch of the two messages show that the digital signature is said to be de-authentication of signature.

2. RELATED WORK

2.1. Network Structure

Hierarchical network structures are more centralized of secure multicast. The networks have three major parts; key server, sender, and member. The key server is responsible for accepting a new member join/leave for generating the group key and delivering them to both sender and the existing members. Sender encrypts of the contents by using a secret key which is received from the key server and distributes the encrypted content to all the group members. Authorized group members are received content of a message from a sender and also received secret keys from the key server. When new members join/leave an existing group, he/she have to send Internet Group Message Protocols (IGMP) request to his/her nearest routers to receive multicast data from the network. Also, new member requests to send a join/leave request message to the key server. Key server accepted a join/leave request message from a new member; key updating process should be started. Key server updating an individual key and group key/ re-keying must be delivering for new member and all also existing group members.

2.1.1. Using Short Range Natural Number Algorithm

Sonal Sharma, Jitendra Singh Yadav, Prashant Sharma, In this paper proposed short range natural number algorithm is related to RSA algorithm with the small number of modification. This modification increases the security of the cryptosystem. In this algorithm, we have actually a large number that has two prime factors. In addition of this, we have used two natural numbers in a pair of keys (public, private). These natural numbers increase the security of cryptosystem .so its name is "modified RSA public key cryptosystem using short range natural number algorithm". The comparison between RSA and SRNN both algorithm they found that by increasing modulus length n security increase, speed decrease and when chunk size m increases both security and speed increases. From key generation point of view SRNN, an algorithm is a bit of slower then RSA algorithm. From encryption point of view, both algorithms are working same. In a case of SRNN algorithm, only one multiplication operation is additional for each chunk calculation. So when chunk size increases we found both algorithms are giving almost same time. Decryption point of view SRNN algorithm is much slower then RSA algorithm. The overall performance we found that SRNN, algorithm is better in security but slower in speed. When modulus length is an increased speed of SRNN algorithm is decreases with respect to RSA algorithm. The Difference of SRNN and RSA with modulus length 1024 bits are approximately 5080 milliseconds whereas the difference of RSA 2048 bits and SRNN 1024 bits are milliseconds. Hence, SRNN with modulus length 1024 bits are is good balance speed and security [5].

2.1.2. Using Hybrid Cryptography Algorithm

RavishankerDhakar, Amit Kumar Gupta, Prasant Sharma In this paper presents a hybrid cryptography algorithm which is based on additive holomorphic properties called modified RSA encryption algorithm (MREA). MREA is secure as compared to RSA as it is based on factoring problem as well as decisional composite residuosity assumption which is the intractability hypothesis. This method used additive holomorphic properties means that given only the public key and the encryption of m1 and m2, one can compute the encryption of m1+m2 [6].

2.1.3. Using Subset Sum Cryptosystem

Sonal Sharma, Prashant Sharma, Ravi Shankar Dhakar In this paper presents a hybrid cryptography algorithm which is based on the factoring problem as well as Subset-Sum problem called a Modified Subset-Sum over RSA public key cryptosystem (MSSRPKC). The Subset-Sum cryptosystem (Knapsack Cryptosystem) is also an asymmetric cryptographic technique. The Merkle-Hellman system is based on the subset sum problem (a special case of the knapsack problem): given a list of numbers and a third number, which is the sum of a subset of these numbers, determine the subset. In general, this problem is known to be 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 [7].

2.1.4. Using Neighborhood-Generated Keys

RituTripathi, Sanjay Agrawal, In this paper a performance evaluation of selected symmetric and asymmetric encryption algorithms such as DES, 3DES, AES, Blowfish, RSA, and Diffie-Hellmen. The evaluation table that displays the encryption ratio is high in using the both encryption techniques. The tunability and key length are higher at the Asymmetric encryption technique .The key length is high in an asymmetric encryption algorithm to break the code is complex in RSA. In the aspect of throughput, Throughput is increased so power consumption is decreased. Throughput is high in blowfish and blowfish is less power consumption algorithm hence speed is fast in the Symmetric key encryption is viewed as good. Finally, in the symmetric key encryption techniques, the blowfish algorithm is specified as the better solution **[**8].

2.2. Existing RSA Algorithms

RSA Algorithms are using key generation, encryption, and decryption. The following steps are using public key and private key for during encryption and decryption.

1. Choose two large prime numbers p and q.
2. To calculate n equal to $p * q$
3. Compute $\varphi\ (n) = (p - 1) * (q - 1)$
4. To choose large prime number e, such that gcd $(\varphi(n), e) = 1$ is $1< e < \varphi\ (n)$.
5. Find private key $d * e \bmod \varphi(n) = 1$ using multiplicative inverses.
6. Encryption using public keys is (e, n) and
7. Decryption using private keys is (d, n).

2.2.1. Asymmetric Encryption and Decryption

Encryption: Encryption is a form of cryptosystem in which encryption and decryption are performed using the different keys—one a public key and one a private key. It is also known as public-key encryption [4] .Encryption is a well known technology for protecting sensitive data. The combination of public key and private key encryption to hide the sensitive data of users, and cipher text retrieval [10]. Encryption is the process of transfer original plain text (data) into cipher text (data). In this paper, RSA algorithm [$C = M^{e} \bmod n$] plain text (M) the power of public key e and modulus of public key natural number n. Asymmetric encryption algorithm using RSA that is different from symmetric encryption algorithms are need two types of key, one of this a public key, another one a secret key. The two of keys appear in pairs of the public key to encrypted data, only with the corresponding secret key (private key) can decrypted.

2.2.2. Decryption

Decryption is essentially the encryption algorithm run in reverse. It takes the cipher-text and the secret key and produces the original plaintext [4]. Decryption is the process of transfer cipher-text (data) into original plain text (data). In this paper, RSA algorithm [$M = C^{d} \bmod n$] after converting plain text into cipher text C, power of private key d and modulus of public key natural numbers n.

2.2.3. Digital Signature of Secure Data Transaction Natural Number Algorithm

The STNN algorithm is related with RSA Algorithm with some modification. STNN algorithm is moreover a public key cryptography algorithm. In this algorithm, we have extremely large four prime numbers $p1$, $p2$, $q1$, $q2$. In this modification is an increase the security of the cryptosystem. In this algorithm only four large prime numbers not for random selection of e. The value of e is calculate of greatest common divisor (gcd ($\varphi(n_1)$, e_1) = 1), if comes 1 the e value is true or false.

Key Generation:

1. Generate four large random primes, p_1, p_2, q_1 and q_2.
2. To compute n_1, n_2 and n_3 for example: $n_1 = p_1 * q_1$, $n_2 = p_2 * q_2$ and $n_3 = q_1 * p_2$ (for any two prime numbers)
3. To compute $\varphi(n_1) = (p_1\text{-}1)\ (q_1\text{-}1)$, $\varphi(n_2) = (p_2 - 1)\ (q_2 - 1\ )$ and $\varphi(n_3) = (q_1 - 1)\ (p_2 - 1)$
4. To calculate an integer “e_1, e_2 & e_3” value is $e_1 = n_1 \bmod \varphi(n_1)$ the remainder values is e_1, $1 < e_1 < \varphi(n_1)$, such that gcd ($\varphi(n_1)$, e_1) = 1.
5. Other two integer’s e_2 and e_3 is similar to e_1. (for example: $e_2 = (n_2 \bmod \varphi(n_2))$ and $e_3 = (n_3 \bmod \varphi(n_3))$ the new public key $s = e_2{}^{e}{}_3 \bmod n_1$.
6. Three public keys are (n, e, s).
7. Compute the secure secret key d, such that (e x d) mod $\varphi(n) = 1$. The private key is (d, g).

Encryption:

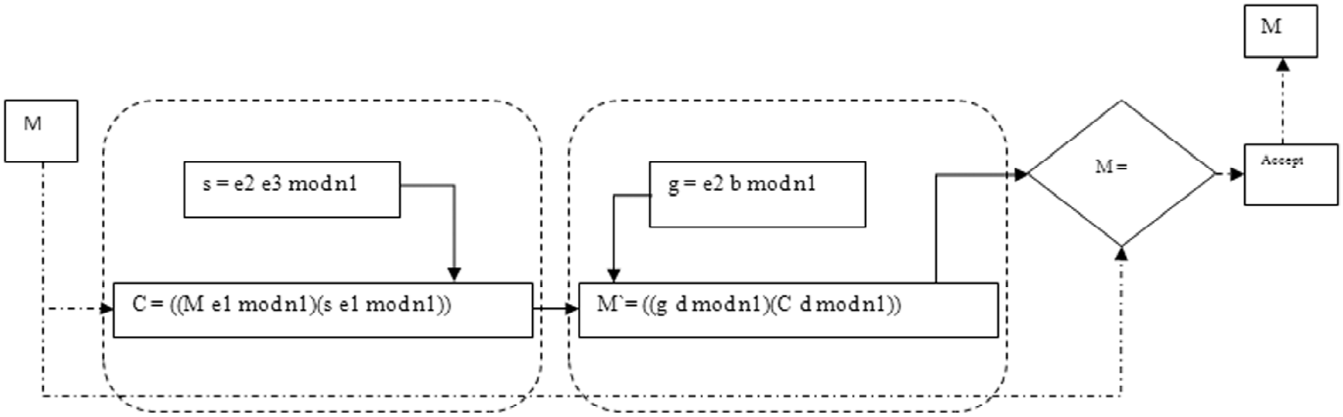
8. Encryption: user sending the plaintext (numerical or image) message as a positive integer M. To compute cipher-text

   $C = (M^{e}{}_1 \bmod n_1\ ) * (s^{e}{}_1 \bmod n_1)$.

Decryption:

9. Decryption: we received cipher-text C to compute $g = e_2^{b} \bmod n_1$.subject to $b = \varphi(n_1) - e_3$ to compute $M = (g^{d} \bmod n_1) * (C^{d} \bmod n_1)$ we received extracts the plaintext from the integer representative of M.

Table 1 shows the general comparison between RSA and STNN algorithm. In both algorithms are creating that by rising modulus length of n security increases, low-speed decrease and when chunk size m



Comparison between RSA Algorithm and STNN Algorithm

S. No	*RSA Algorithm*	*Proposed Algorithm*
1	It uses different type of key for encryption and decryption	STNN is uses different type of keys for encryption and decryption
2	It provides data security, a digital signature for authentication.	STNN also provide data security, a digital signature for authentication.
3	RSA have less security.	STNN have increase security.
4	Processing speed is fast.	Processing speed is slow.

increases both security and speed increases. From key generation STNN algorithm is a little bit slower than RSA algorithm. The both algorithms are working almost same in the process of encryption. In a case of STNN algorithm more multiplication operation for each chunk calculation. After received cyber-text then we go for decryption process in STNN algorithm is much slower then RSA algorithm. The overall performance of STNN Algorithm is more security but much slower in the speed.

CONCLUSION

In this work RSA algorithm and STNN algorithm, we proposed STNN algorithm for implementing an asymmetric key in cryptography network security. In this paper provides an analytical study of RSA, SRNN, and STNN algorithm. We have proposed public key cryptosystem is increasing security and processing speed is slow compared to RSA algorithm. In particularly we increase security for online transaction and data communication. It's difficult to identify the prime factors and natural numbers. Using STNN algorithm is added some extra processing time for encryption and decryption. The overall performance of this STNN algorithm is a secure transaction.

REFERENCE

[1] Idrizi, Florim, Dalipi, Fisnik & Rustemi, Ejup. "Analyzing the speed of combined cryptographic algorithms with secret and public key". International Journal of Engineering Research and Development, e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com Volume 8, Issue 2 (August 2013), p. 45

[2] Abdul.Mina, D.S, Kader, H.M. Abdual & Hadhoud, M.M. "Performance Analysis of Symmetric Cryptography". p. 1.

[3] Hardjono, "Security In Wireless LANS And MANS," Artech House Publishers 2005.

[4] William Stallings-Cryptography and Network Security Principles and Practice, 5th Edition-1

[5] Sonal Sharma, jitendrasinghyadav and prasant Sharma "modified RSA public key cryptosystem using short range natural number algorithm" international journal 2012.

[6] Ravishanker Dhakar, Amit Kumar Gupta, Prasant Sharma "Modified RSA Encryption Algorithm (MREA)" 2012 Second International Conference on Advanced Computing & Communication Technologies.

[7] Dhananjay Pugila, Harsh Chitrala, Salpesh Lunawat, P.M. Durai Raj Vincent "An EfficientEncryption Algorithm Based On Public Key cryptography" International Journal of Engineering and Technology (IJET), Vol. 5 No. 3 Jun-Jul 2013.

[8] Lalit Singh, R.K. Bharti, Ph.D. Comparison among different Cryptographic Algorithms using Neighborhood-Generated Keys, International Journal of Computer Applications (0975–8887) Volume 73– No. 5, July 2013.

[9] A. J. Menezes, P.C.V. Oorschot and S. A. Vanstone, Handbook of applied cryptography, CRC Press, 1996.

[10] Padmapriya, Dr. A, Subhasri, P. "Cloud Computing: Security Challenges & Encryption Practices". International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 3, Issue 3, March 2013, pp. 257.