Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 8, August 2013, pg.219 – 223

RESEARCH ARTICLE

InKeSi-Increased Key Size Method in SRNN Public Key Cryptography Algorithm

K. Sheela[1], E. George Dharma Prakash Raj[2]
[1, 2] Department of Computer Science

[1] *Sheela.success@gmail.com*, [2] *Georgeprakashraj@yahoo.com*

Abstract— Digital signature is used to provide security to the message during transfer. The Existing SRNN (Short Range Natural Number) algorithm is used which provides high security, even though it has some problems, such as brute force attack. A new algorithm called as InKeSi (increased key size) is Proposed in this thesis in which the attack can be avoided by increasing the key size. In the proposed algorithm, the key size is increased by 512bit to 1024bit in SRNN algorithm.

Key Terms: - cryptography; Digital Signature; RSA; SRNN; Encryption; Decryption

I. INTRODUCTION

A. Cryptography

Cryptography is the Science of using mathematics to encrypt and decrypt information, store sensitive information or transmit it across insecure networks. So that it cannot be read by anyone except the intended recipient, while cryptography is the science of security. Cryptography is necessary when communicating over any untrusted medium, which includes just about *any* network, particularly the Internet. Within the context of any application-to-application communication, there are some specific security requirements, including:

- *Authentication:* The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
- *Privacy/confidentiality:* Ensuring that no one can read the message except the intended receiver.
- *Integrity:* Assuring the receiver that the received message has not been altered in any way from the original.
- *Non-repudiation:* A mechanism to prove that the sender really sent this message.

A cryptography algorithm or cipher is a mathematical function used to the encryption and decryption process. This algorithm works in combination with keys, a word or number or phrase to encrypt the plaintext. The same plaintext encrypt to different cipher text with different keys. The security of the encrypted data is entirely dependent on two things: the strength of the cryptography algorithm and secrecy of the keys. Two type of the cryptography algorithms are there one is Symmetric key algorithm and another is Asymmetric key algorithm.

Symmetric key cryptography is based on the sender and receiver of message knowing and using same secret key. The sender uses the same secret key to encrypt the message and receiver uses the same secret key to decrypt it. Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. The main problem of Symmetric key cryptography is getting the sender and receiver to agree on the same secret key without anyone else knowing it. Because all keys in Symmetric key cryptosystem must remain secret, Symmetric key cryptography often has difficulty providing secure key management, especially is open system with large number of users. To solve this problem, Diffie Hellman introduced Public key cryptosystem.

Asymmetric key cryptography algorithm is also called Public key cryptography algorithm. This algorithm uses a pair of keys for encryption and decryption. Public key encrypts the data and corresponding private key or secret key for decryption. It is computationally infeasible to deduce the private key from the public key; anyone who has a public key can encrypt the data but cannot decrypt it. Only the person who has the corresponding private key can decrypt the data. The need for the sender and receiver to share secret key via some secure channel is eliminate; all communication involved only public key, and no private key is ever transmitted or shared.

RSA implements a Public key cryptosystem, as well as digital signatures. This algorithm is based on the mathematical fact that is easy to find and multiply large prime numbers together, but it is extremely difficult to factor their product. The private and public keys in RSA are based on very large prime numbers. It is the selection and generation of the public and private key. This algorithm involves the use of two keys:

(i) A public key which may be known b anybody and can be used to encrypt message.

(ii) A private key, known only by the recipient and used to decrypt message.

SRNN algorithm is similar with RSA with some modification and included more security. This algorithm we have extremely large number that has two prime factors. In addition of this algorithm we have used to two short range natural numbers in pair of keys. This modification increases the security of the cryptosystems.

II. EXISTING WORK

In this section the 512bit SRNN algorithm is described.

Digital Signature schemes are mostly used in cryptographic protocols to provide authentication. This architecture is related with 512bit **SRNN** algorithm is similar with RSA with some modification. SRNN algorithm is also a Public key cryptography algorithm. In this algorithm we have extremely large number that has two prime factors.

In addition this we have used two short range natural numbers in pair of keys. One key (public key) for encryption and other corresponding key (private key) for decryption. This modification increases the security of the cryptosystem. So its name is short range natural number public key algorithm. Advantages of SRNN algorithm:

- The primary advantage of public key cryptography is increased security.
- It provides digital signature that cannot be repudiated.
- We can select large prime numbers for enhancement of security of keys.
- Public key cryptography may be used with secret key cryptography.

Three approaches to attacking SRNN:

- Brute force attack (size of numbers)
- Mathematical attack(modulus N)
- Timing attack(running of decryption)

A. PROBLEM STATEMENT

Digital signature schemes are mostly used in Cryptography protocols to provide authentication. 512bit SRNN (Short Range Natural Number) algorithm is designed for digital signature. This SRNN algorithm is similar to RSA algorithm with some modification. The only known way to attack is to be performed a “brute force” attack on the modulus. This attack can be easily defeated by increasing the key size.

III. PROPOSED WORK

The proposed architecture for the implementation of the digital signature scheme. The 1024bit InKeSi SRNN implementation the methodology for computing the modular exponentiation is used. This is chosen because it can achieve an appreciable decrease of covered area and sometimes increase the time-performance comparing with other methodologies.

The senders encrypt the message with Public Key of InKeSi SRNN algorithm and then the data is signed with the Private Key of InKeSi SRNN algorithm. The verification of digital signature is started after this process with the help of Public key at the recipient side. The decryption of the digital signature is done in this process which eventually results in the generation of message.

Key Generation by SRNN Algorithm:

In this module the SRNN algorithm is used with two random prime numbers of p and q of bit length equal to 1024 bytes. The random number of p and q should not be repeated so we make use of two natural numbers u and a. By using the public key and private key of the sender is created with digital signature.

Encryption process

In this the user A makes use of this public and private key creates a digital signature and sends the digital signature with the message to the user B by using the private key of user A

Decryption Process

User (B) receives Message and Signature. User (B) applies public key to the signature to create a copy of the message and extracts the message. Now user (B) compares the value of Message M with the value of M. If the two values are same, User (B) accepts the message otherwise not.

The following flowchart shows the SRNN algorithm functions**:**

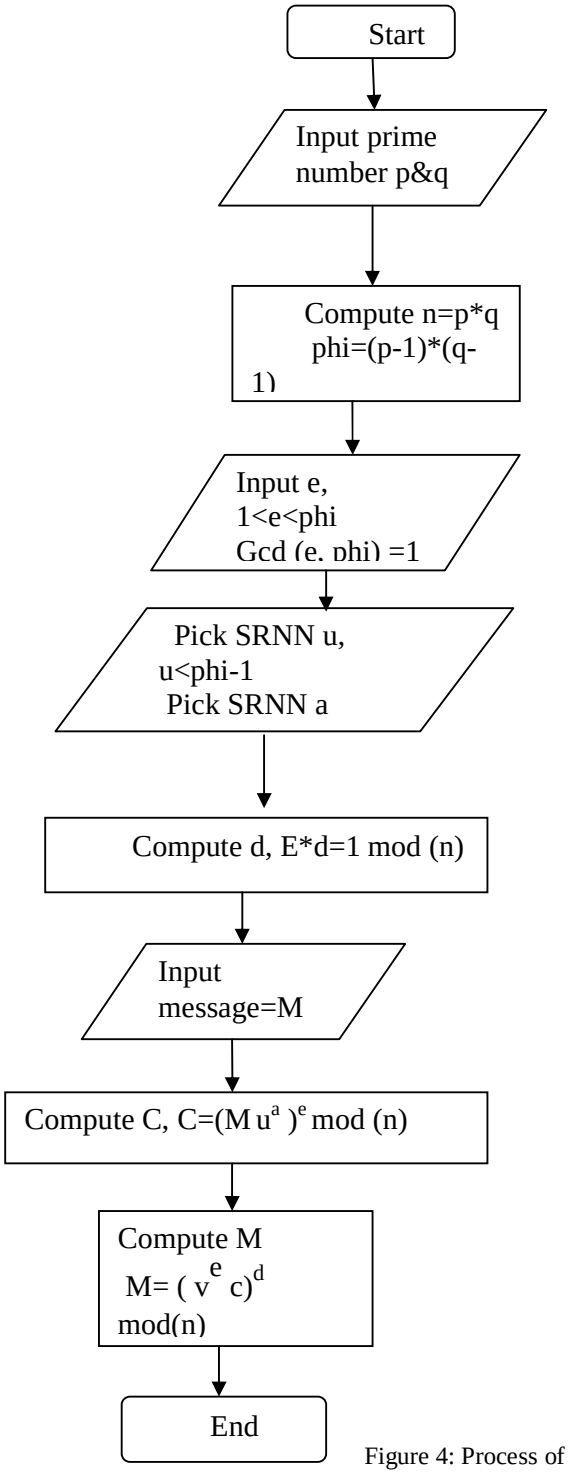

Figure 4: Process of SRNN Algorithm

Key generation Process

- Generate two large random prime p, q.
- Compute n=p*q
- Compute phi=(p-1)(q-1)
- Choose an integer e, 1<e<phi, such that gcd (e, phi)=1 compute the such that (e*d) mod phi=1
- Pick short range natural number **u** randomly such that u<phi-1
- Pick another Short range natural number **a** randomly such that phi>a>u And compute u^a
- Find d such that e*d mod ((p-1) (q-1)) =1
- Public key is (n, e, u^a)
- Private Key is (d, a, u)

P, q, phi should also be kept secret.

Encryption Process

- Obtains the recipient's public key (n, e, u^a)
- Represent the plaintext message as positive integer M
- Computes the cipher text C=(m u^a)^e mod n

Send the cipher text C to recipient.

Decryption Process

- Use Recipient private key(d, a , u)
- compute M=(v^e c)^d mod n where v= u^{phi-a} mod n
- Extracts the plaintext from the integer representative M

IV. RESULT OF INKESI SRNN

From the implementation of below figure show that the INKESI SRNN algorithm provides 100% Security than the 512bit SRNN algorithm

V. CONCLUSION

Cryptography is the Science of using mathematics to encrypt and decrypt data, store sensitive information or transmit it across insecure networks. The security of the encrypted data is entirely dependent on two things: the strength of the Cryptography algorithm and secrecy of the Key .Two types of Cryptography algorithms are there: Symmetric key & Asymmetric key.

RSA algorithm is used to two pair of keys, one for encryption and other corresponding key must be used for decryption. No other key can decrypt the message .RSA uses a variable size encryption block and a variable size key. The key-pair is derived from a very large number, *n*, that is the product of two prime numbers.

SRNN algorithm is similar with RSA with some modification. SRNN algorithm is also a Public key cryptography algorithm. In this algorithm we have extremely large number that has two prime factors. In addition this we have used two short range natural numbers in pair of keys. One key (public key) for encryption and other corresponding key (private key) for decryption. This modification increases the security of the cryptosystem. So its name is short range natural number public key algorithm.

In this thesis a new INKESI SRNN algorithm is proposed, which gives more Security strength the Existing 512bit SRNN Algorithm.

REFERENCES

[1] Mr. Hemant Kumar, Dr. Ajit singh "An Efficient Implementation of digital signature algorithm with SRNN public key Cryptography" International journal of Research Review in Engineering Science and Technology, Volume-1 Issue-1 June 2012.

[2] Sonal Sharma, Jitendra Singh Yadav, prashant Sharma "Modified RSA Public key Cryptography using Short Range Natural Number Algorithm" International Journal of Advanced Research in Computer Science and Software Engineering, Volume-2, Issue-8, August 2012.

[3] P.Saveetha ,S. Arumugam "Study on Improvement in RSA Algorithm" international journal of Computer Science and Communication Technology, Volume-3, Issue-6,7,8, 2012.

[4] Andrea Pellegrini, Valeria Bertacco, and Todd Austin "Fault Based Attack on RSA Authentication" University of Michigan.

[5] Prasant Singh Yadav, Pankaj Sharma, Dr.K.P. Yadav "Implementation of RSA Algorithm using Elliptic Curve Cryptography for Security and performance Enhancement" International Journal Of Scientific and Technology Research Volme-1, Issue-4, May 2012.

[6] Gary C. Kessler "An Overview on Cryptography" June 2010.

[7] P. Kitsos, N. Sklavos and O. Koufopavlou "An Efficient Implementation of The Digital Signature Algorithm"

[8] Yaun Xue "Public Key Cryptography and RSA Algorithm "Technical notes and papers.

[9] Carnegia Mellon Software Engineering Institute "Public Key Cryptography.

[10] R Gennaro. (2000), "RSA-Based Undeniable Signatures".

[11] National Institute of Standards and Technology (NIST), Digital Signature Standard, FIPS PUB 186-2.

