ISSN:0975-9646

Modified RSA Public Key Cryptosystem Using Two Key Pairs

Jainul Abudin[#1], Sanjay Kumar Keot[*2], Geetanjali Malakar[*3], Nita Moni Borah[*4] Mustafizur Rahman[*5]

[#1] *Assistant Professor, Department of Computer Science Engineering, Regional Institute of Science & Technology, Meghalaya.*

[*2 *3 *4 *5] *B-Tech students, Department of Computer Science Engineering, Regional Institute of Science & Technology, Meghalaya.*

Abstract. The proposed technique is used to provide maximum security for data over the network and minimize time consumption in encryption and decryption. In this technique we used two key pair, one small size key pair for data encryption and one large size key pair to encrypt key component(n=p*q) of small size key pair. In proposed system every communicating party needs just two key pairs for communicating with any number of other communicating parties. Once someone obtains key pairs, he /she can communicate with anyone else. RSA is a well known public key cryptography algorithm and was one of the first great advances in public key cryptography.

Index Terms— Cryptography, Key pair, key-component(n), prime numbers,encryption, decryption, RSA Cryptosystem.

INTRODUCTION:

Cryptography is a process which is associated with scrambling plaintext (ordinary text, or clear text) into cipher text (a process called encryption), then back again to plain text (known as decryption). The key feature of asymmetric cryptography system is encryption and decryption procedure are done with two different keys - public key and private key. Private Key cannot be derived with help of public key that provides much strength to security of cryptography.

Symmetric-key cryptography is based on the sender and receiver of messages knowing and using the same secret key. The sender uses the secret key to encrypt the message and the receiver uses the same secret key to decrypt it. 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 a symmetric key cryptosystem must remain secret, symmetric key cryptography often has difficulty providing secure key management, especially in open systems with a large number of users. To solve this problem, Diffie and Hellman introduced a new approach to cryptography and, in effect, challenged cryptologists to come up with a cryptographic algorithm that met the requirements for public-key systems . Public-key cryptography is used where each user has a pair of keys, one called the public key and the other private key. Each user's public key is published while the private key is kept secret and thereby the need for the sender and the receiver to share secret information (key) is eliminated.

RSA ALGORITHM:

Rivest, Adi Shamir and Leonard Adleman are the developer of the RSA cryptosystem of MIT in 1997.it was described in 1978. The Rivest-Shamir-Adleman (RSA) cryptosystem is one of the best known public_key cryptosystems for key exchange or digital signatures or encryption of blocks of data. Some of the famous security system which is composed of three faces: such as prime Key generation, Encryption and Decryption phase. 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 chosen according to special rules; these primes may be 100 or more digits in length each, yielding an n with roughly twice as many digits as the prime factors.

RSA algorithm:

1. Select two different prime numbers p and q
   For security aim, the integer's p and q must be large.
2. Calculate n=p*q
   n will be used as the module for public key and private key and n is also known as key_component.
3. Calculate f(n)=(q-1)(p-1),
   Where f is a function of Euler's
4. Select an integer e such that 1<e<f(n) and GCD (e, f(n))=1;
   e and f(n) are co prime.
5. Determine d:
   d is multiplicative inverse of e mod (f(n)) (e * d) mod f (n) = 1 d is the private key.

Encryption:

M is plain text data.

$C=m^e \bmod n$

Decryption:

C is received cipher text.

$M= C^d \bmod n$

PROPOSED RSA CRYPTOSYSTEM USING TWO KEY PAIRS:

In RSA algorithm if take large size key then its take more time in encryption and decryption operation and if we select small size key then security is compromised. Since

RSA is block cipher so for each block of data we need to perform same operation and hence more time is required.
In the proposed approach we generate two different key pair one of small size(public_key1,private_key1,n1) and one of very large size (public_key2,private_key2,n2) using same existing RSA key generation algorithm.

Encryption:

Step1. Encrypt data with public key of small size key(public_key1)
Step2. Encrypt n1 of small key pair with public key(public_key2) of large key pair.
Step3. Transmit results of step 2 n step3 to receiver.

Decryption:

Step1. First decrypt n1 with private_key2.
Step2. Now we have n1, so we can decrypt encrypt data with private_key1**.**

Advantage of proposed system on existing system:

1. Proposed System is less time consuming then existing system with same label of security.
2. Proposed system is more efficient for large data file then existing.
3. Proposed system is more secure then existing system.

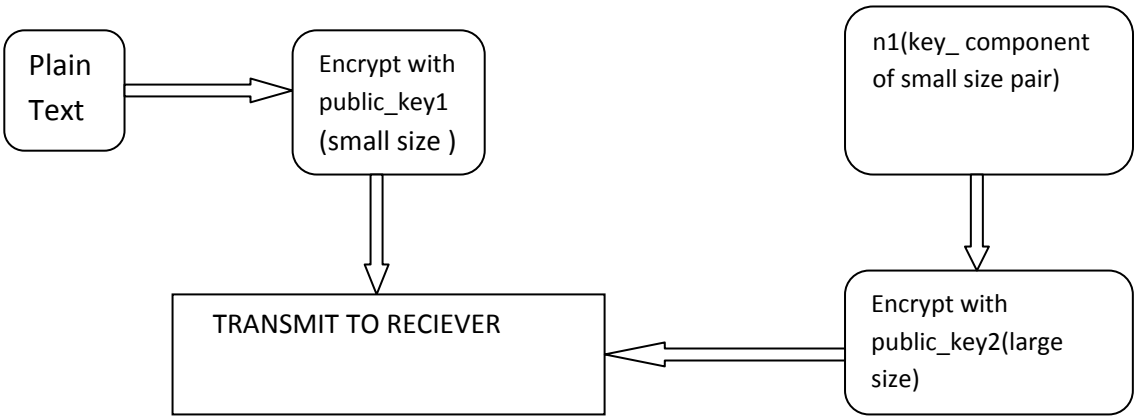

Figure 1: - At sender' end

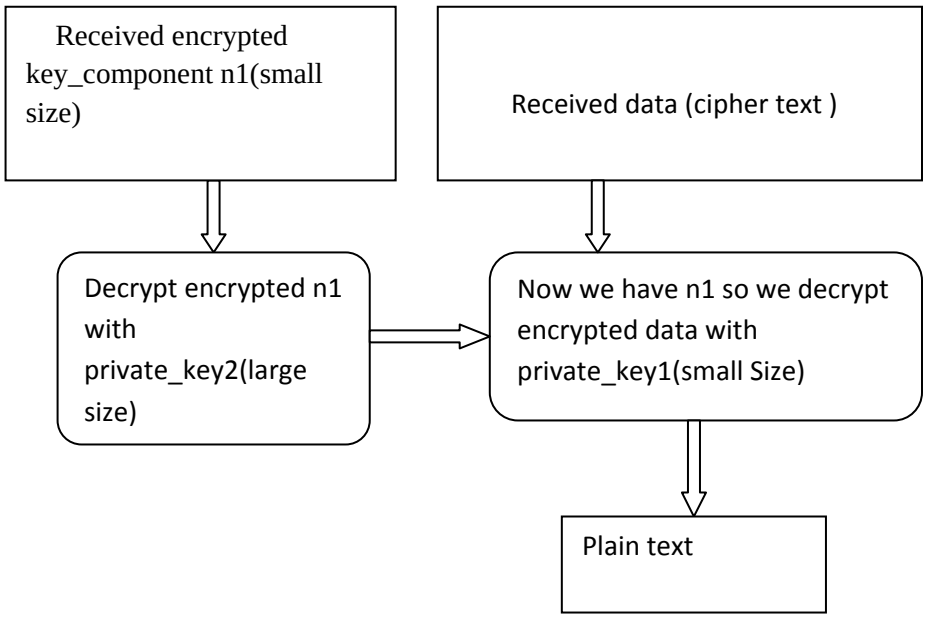

Figure 2: - At receiver's end

SIMULATION RESULTS

Since RSA is a block cipher, and a block = 64 bit. Let RSA 2048 bits system take X1 time duration to encrypt and Y1 time duration to decrypt one block and RSA 1024 bits system takes X2 time duration to encrypt and Y2 time duration to decrypt.

In existing system 2000 data block take 2000X1 time duration in encryption and 2000Y1 time duration in decryption using RSA 2048 bits system.

Let existing system be "A", and proposed system be "B".

Total time required in A = 2000X1 + 2000Y1.

Now in proposed system, 2000 data block takes 2000X2 time duration in encryption and 2000Y2 time duration in decryption by RSA 1024 system.

Total time required for data block = 2000X2 + 2000Y2

Time required to encrypt key_component(n1) of small key by large public key(2048) =16X1 and

time required to decrypt key_component(n1) of small key by large private key(2048) =16Y1.

Total time duration required in B = 2000X2 + 2000Y2 + 16X1 + 16Y1.

The table below shows the sample RSA encrypt/decrypt timing in milliseconds [6].

Processor	MHz	1024-RSAd	1024-RSAe	2048-RSAd	2048-RSAe
Ultra SPARC II	450	32.1	1.7	205.5	6.1
Strong ARM	200	188.7	10.8	1273.8	39.1

Table 1 . Sample RSA encrypt/decrypt timings (in milliseconds).

Now in case of Ultra SPARC II

Total time required in existing system by large key(2048 bits) = 2000*6.1 + 2000*205.5 = 423200 milliseconds.

Total time required in proposed system using two key pairs (Small key 1024 bits, Large key 2048bits) = 2000*1.7 + 2000*32.1 + 16*6.1 + 16*205.5 = 70985 milliseconds.

Now in case of Strong ARM

Total time required in existing system by large key(2048 bits) = 2000*39.1 + 2000*1273.8 = 2625800 milliseconds.

Total time required in proposed system using two key pairs (Small key 1024 bits, large key 2048 bits) = 2000*10.8 + 2000*188.7 + 16*39.1 + 16*1273.8 = 420006.4 milliseconds.

The table below shows the total time duration in milliseconds for encryption and decryption of 2000 blocks of data where one block is equal to 64 bits.

PROCESSOR TYPE	EXISTING SYSTEM(ES)	PROPOSED SYSTEM(PS)
ULTRA SPAR-II	423200 ms	70985ms
STRONG ARM	2625800 ms	420006.4ms

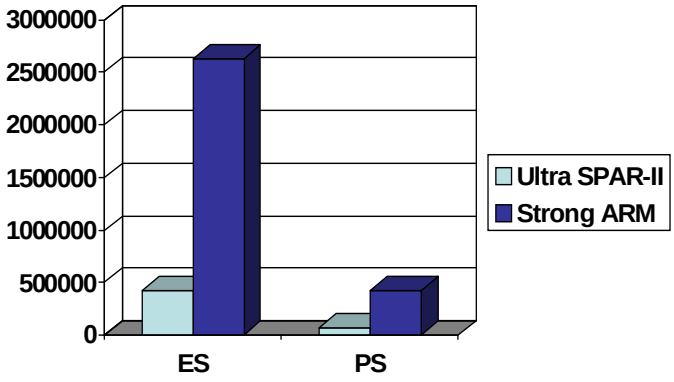

Figure 3:- Bar chart to graphically compare time consumption between existing RSA system and proposed system.

CONCLUSION:

In this paper we used two key pair, one small size key pair for data encryption and one large size key for encrypt key component (n=p*q, where p & q are chosen prime numbers) of small size key pair since small n is weakness of existing RSA cryptosystem and large n lead to more time consume in encryption and decryption . In which encryption and decryption are performed in less time compared to existing system. The proposed system is designed to improved efficiency of existing RSA cryptosystem.

REFERENCES:

1. Cryptography and network security, William Stallings
2. Atul Kahate , Cryptography and Network Security , Tata McGraw-Hill Publishing Company Limited.
3. R . L. Rivest, A. Shamir and L. Adleman, "On Digital Signatures and Public Key Cryptosystems", Technical Memo 82, Laboratory for Computer Science, Massachusetts Institute of Technology, April 1970
4. http://mathworld.wolfram.com/RSAEncryption.html
5. http://en.wikipedia.org/wiki/RSA
6. The advantages of Elliptic Curve Cryptography for wireless security, Kristin Lauter, Microsoft Corporation, IEEE Wireless Communication, February 2004.