Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-244

Volume 3, Issue 7, July-2016

Implementation and analysis of modifications in RSA algorithm

Priyanka P. Koshti, Dr.U.S.Bhadade
E&Tc,S.S.B.T.C.E.T,Jalgaon
E&Tc,S.S.B.T.C.E.T,Jalgaon

Abstract- In asymmetric key cryptography, also called public key cryptography, two different keys (which form a key pair) are used. One key is used for encryption and only the other corresponding key must be used for decryption. No other key can decrypt the message not even the original (i.e. the first) key used for encryption. The beauty of this scheme is that every communicating party needs just a key pair for communicating with any number of other communicating parties. Once someone obtains a key pair, he/she can communicate with anyone else. "The short range natural number (SRNN) algorithm" is similar to RSA algorithm with some modifications. This modification increases the security of the cryptosystem. In this algorithm extremely large number has two prime factors (similar to RSA).Also this Technique two key pair has been used, 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. This natural numbers increases the security of cryptosystem. So its name is "Modified RSA public key cryptosystem using two key pairs".

Keywords- **Cryptography,** ***RSA, encryption, decryption, SRNN, Key pair, Key component.***

I.INTRODUCTION

1) Cryptography

Cryptography from Greek , "hidden, secret" respectively is the practice and study of techniques for secure communication in the presence of third parties (called adversaries).More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce. Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients, thereby precluding unwanted persons to do the same. Since World War I and the advent of the computer, the methods used to carry out cryptology have become increasingly complex and its application more widespread. Modern cryptography is heavily based on mathematical theory and computer science practice. Cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary [1]. It is theoretically possible to break such a system but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure; theoretical advances and faster computing technology require these solutions to be continually adapted. There exist information theoretically secure schemes that provably cannot be broken even with unlimited computing power—an example is the one-time pad—but these schemes are more difficult to implement than the best theoretically breakable but computationally secure mechanisms [1].

a. Cryptography key basics

The two components required to encrypt data are an algorithm and a key. The algorithm generally known and the key are kept secret. The key is a very large number that should be impossible to guess, and of a size that makes exhaustive search impractical. In a symmetric cryptosystem, the same key is used for encryption and decryption. In an asymmetric cryptosystem, the key used for decryption is different from the key used for encryption [2].

b. Key pair

In an asymmetric system the encryption and decryption keys are different but related. The encryption key is known as the public key and the decryption key is known as the private key. The public and private keys are known as a key pair. Where a certification authority is used, remember that it is the public key that is certified and not the private key. This may seem obvious, but it is not unknown for a user to insist on having his private key certified!

All Rights Reserved, @IJAREST-2016

c. Key component

Keys should whenever possible be distributed by electronic means, enciphered under previously established higher-level keys. There comes a point, of course when no higher-level key exists and it is necessary to establish the key manually. A common way of doing this is to split the key into several parts (components) and entrust the parts to a number of key management personnel. The idea is that none of the key parts should contain enough information to reveal anything about the key itself. Usually, the key is combined by means of the exclusive-OR operation within a secure environment. In the case of DES keys, there should be an odd number of components, each component having odd parity. Odd parity is preserved when all the components are combined. Further, each component should be accompanied by a key check value to guard against keying errors when the component is entered into the system. A key check value for the combined components should also be available as a final check when the last component is entered. A problem that occurs with depressing regularity in the real world is when it is necessary to re-enter a key from its components. This is always an emergency situation, and it is usually found that one or more of the key component holders cannot be found. For this reason it is prudent to arrange matters so that the components are distributed among the key holders in such a way that not all of them need to be present.

2) **Types of cryptography**

a. Symmetric-key cryptography

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key. Symmetric key ciphers are implemented as either block ciphers or stream ciphers. A block cipher enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a stream cipher. The data Encryption Standard (DES) and the Advanced Encryption Standard(AES) are block cipher designs which have been designated cryptography standards by the US government Despite its deprecation as an official standard, DES remains quite popular, it is used across a wide range of applications, from ATM encryption to email privacy and secure remote access. Many other block ciphers have been designed and released, either considerable variation in quality. Many have been thoroughly broken, such as FEAL.

b. Asymmetric key Cryptography

Public-key cryptography refers to a cryptographic system requiring two separate keys, one of which is secret and one of which is public. Although different, the two parts of the key pair are mathematically linked. One key locks or encrypts the plaintext, and the other unlocks or decrypts the cipher text. Neither key can perform both functions by itself. The public key may be published without compromising security, while the private key must not be revealed to anyone not authorized to read the messages. Public-key cryptography uses asymmetric key algorithms (such as RSA), and can also be referred to by the more generic term "asymmetric key cryptography." The algorithms used for public key cryptography are based on mathematical relationships that presumably have no efficient solution. Although it is computationally easy for the intended recipient to generate the public and private keys, to decrypt the message using the private key, and easy for the sender to encrypt the message using the public key, it is extremely difficult (or effectively impossible) for anyone to derive the private key, based only on their knowledge of the public key.

c. Block Cipher and Stream Cipher Cryptanalysis

Block ciphers encrypt information by breaking it down into blocks and encrypting data in each block. A block cipher encrypts data in fixed sized blocks (commonly of 64 bits). A stream cipher consists of a state machine that outputs at each state transition one bit of information. This stream of output bits is commonly called the running key. The state machine is nothing more than a pseudorandom number generator [3].

II.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.

All Rights Reserved, @IJAREST-2016

Encryption:
M is plain text data.
C=m^e mod n
Decryption:
C is received cipher text.
M= C^d mod n

III.IMPLEMENTATION

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

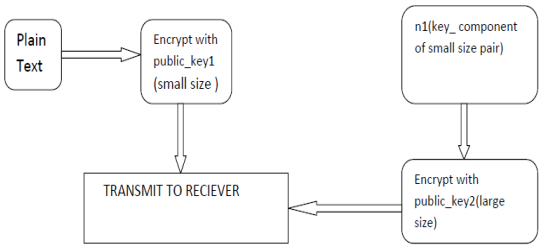

Figure 1: - At sender' end[4]

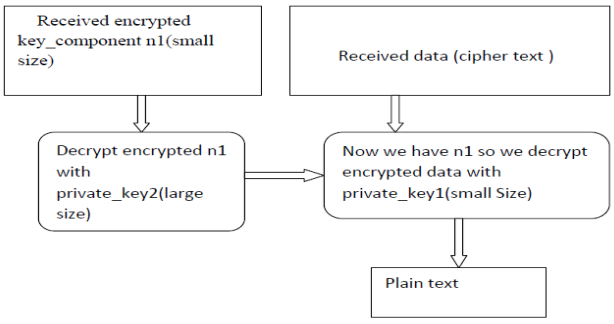

Figure 2: - At receiver's end[4]

B) Modified RSA public key cryptosystem using short range natural number algorithm:
The 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 (similar to

All Rights Reserved, @IJAREST-2016

RSA) .In addition of this we have used two short range natural numbers in pair of keys. This modification increases the security of the cryptosystem. So its name is short range natural number public key algorithm [5,6].

- SRNN Key Generation, Encryption, Decryption Process

1) Key Generation process

- Generate two large random primes, p and q, of approximately equal size such that their product n = p x q is of the required bit length, e.g. 1024 bits.
- Compute n= p x q.
- Compute phi = (p-1) (q-1).
- Choose an integer e, 1 < e < phi, such that gcd (e, phi) = 1. Compute the secret exponent d, 1<d<phi, such that (e x 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
- The public key is (n,e,u^a) and the private key is (d,a,u). The values of p, q, and phi should also be kept secret.

2) Encryption process

Sender does the following:-

- Obtains the recipient's public key (n,e,u^a)
- Represents the plaintext message as a positive integer m.
- Computes the cipher text c = (m u^a)^e mod n.
- Sends the cipher text c to recipient.

3) Decryption process

Recipient does the following:-

- Uses his private key (d, a, u) to compute m = (v^e c)^d mod n Where v= u^phi-a mod n.
- Extracts the plaintext from the integer representative m.

IV.RESULTS

RSA cryptosystem using two key pairs:

Sr.No.	File size	Encryption time(ms)	Decryption time(ms)
1	1kb	16	140
2	10 kb	62	684
3	100 kb	267	1609
4	153kb	625	15860
5	300kb	1208	27000

V. 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. We have proposed a method for implementing a public-key cryptosystem whose security rests in part on the difficulty of factoring large numbers. If the security of our method proves to be adequate, it permits secure communications to be established without the use of couriers to carry keys. The security of this system needs to be examined in more detail. In particular, the difficulty of factoring large numbers should be examined very closely. Once the method has withstood all attacks for a sufficient length of time it may be used with a reasonable amount of confidence.

All Rights Reserved, @IJAREST-2016

VI.REFREENCE

[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] Carnegie Mellon Software Engineering Institute "Public Key Cryptography".
[5] KetuFile White Papers "Symmetric vs. Asymmetric Encryption ",a division of Midwest research corporation.
[6] Sharma, Sonal, Jitendra Singh Yadav, and Prashant Sharma. "Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm." International Journal 2.8 (2012).

All Rights Reserved, @IJAREST-2016