IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

Performance Enhancement in Public key Cryptosystems for Security using RSA Algorithm

Ajay Pal Singh[1], Parvez Rahi[2]

Assistant Professor, Department of Information Technology, REC Bijnor, Bijnor, India [1, 2]

Abstract: This paper introduces the concept and implementation of RSA algorithm for security purpose and to enhance the performance of software system using this algorithm. In this article we have done study about RSA algorithm. This study includes what is RSA algorithm and why they are used in the field of Cryptography & Network Security. After doing several works on this topic we came to conclude that RSA algorithm is important to Network Security because they are the components (i.e. Encryption & Decryption key) which interact with the Security system. Without them the system will be useless as RSA are used to fire a particular Encryption & Decryption keys process because of which Security system is build. Here we are dealing with general problem in which we have a particular Security system event of a software system and our objective is to secure that system into a software security because without software security system cannot be secure any things in this world. Here we are discuss with attacks made against the underlying structure of the RSA algorithm, which exploit weaknesses in the choice of values for the encryption and decryption keys, and their relation to the RSA modulus N.

Keywords: Digital Signature, PKC, Encryption, Decryption.

I. INTRODUCTION

The RSA cryptosystem was first published more than 25 years ago by Ronald Rivest, Adi Shamir and Leonard Adleman in 1977. It has been widely used for many years on the internet for security and authentication in many applications including credit card payments, email and remote login sessions [2]. A cryptosystem is simply an algorithm which converts the input data (known as plaintext) into something unrecognizable (known as cipher text) and converts the unrecognizable data back to its original form. The conversion of plaintext to cipher text is described as encryption, the reverse application is decrypted. Mathematics is the Queen of sciences, and arithmetic is the Queen of mathematics." For encryption, the sender uses the encryption key (or encryption exponent), denoted e, and the RSA modulus N. This pair of values is called the public key pair, (N, e). The receiver uses the private key pair (N, d) consisting of the decryption key (or decryption exponent) d and the same RSA modulus N, to decrypt the message. The public key is so called because it is made publicly available, allowing anyone to encrypt a message. Only the intended recipient knows the value of the private key and can therefore decrypt the message. Public key cryptosystems have many advantages over private key systems, where often the encryption key is the same as the decryption key. This means that the sender of a message must somehow securely communicate this key to the intended recipient. Often it is also required that two functions are used, one to encrypt and one to decrypt. When we compare RSA Algorithm with Hash algorithm, the private for the purpose to generate digital signature in RSA system only stores in user's computer, it is more secure than Hash algorithm, but while compare with DSA Algorithm RSA can either be used for data decryption or digital signature, which is most widely used in RSA system and it is more secure than Hash algorithm it gives the guarantee for RSA security [1]. The rest of paper is organized as below section. We have the following related work and current scenario as given in section-3.

II. RELATED WORK & PROPOSED SCENARIO

RSA key of length 1024 can be generated within two minutes on platform of a common PC [1]. On the other hand, encryption/decryption operation on data less than 1024 bits can be done within two seconds. So we can say that the actual efficiency of RSA based system is improved. It gives the guarantees for the point of implementation high security RSA algorithm using long key length on the platform of any PC not a particular PC [8].

There may be various known attacks to break the security of RSA algorithm, "Brute force attack", which is a special kind of attack who does not care of any special parameters. However it is as also partitioned into two categories: Exhaustive attack & Factorization attack. Second type of attack is "Subtle attack" who aims at the mathematic feature of some parameters [7].

We use RSA algorithm for digital signature point of view. A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. If any digital signature is valid then it gives a recipient reason to give trust that the message was created altered by third person. Now consider two employees A & B. A have some public data taken from its own cloud. Suppose there are two employees A & B of different enterprises. A wants to send some message to B, then there are following steps:

DOI 10.17148/IJARCCE.2016.51176

- A takes a document from cloud, which B wants.
- Using Hash function this message is transferred into message digest form.
- A's software then encrypts the message digest with his private key ie. Digital signature.
- Using RSA, A will encrypt with B's public key & B will decrypt it with his private key and A's public key for verification of signature [1].

If we have to modify (or develop an algorithm) in an Encryption key (E) and Decryption key (D) such that all the functioning should be depends upon the Digital Signature as a software system. Then we have obtaining results would be very optimal/optimum as well as secrecy and authentic.

To calculate encryption and decryption key using RSA algorithm is very complex so if we discover some such type of algorithm so that these calculations become easy. If this idea become successful then the time complexity of algorithm can be reduced as a result processing becomes faster and there is quite difficult job to break key for hackers and crackers.

RSA have various security issues and general considerations based on mathematical calculations.RSA is the best algorithm for security purpose but it's key length is too large so to decrypt any message there is too much wastage of time and energy. So if some concept of ECC may be added then it will give better response for security as well as complexity point of view because ECC is strongest concept having higher security level than RSA and it is easy to use. Due to the recent development in field of factoring of large prime, the key length for secure RSA has increased. The increment in the length can increase the security of the RSA Cryptography, but it requires extra communicational, computational cost [2].

When we calculate multiplicative inverse of an element in GF (p) for small values of p, it is very easy. But when we calculate it for larger numbers then RSA becomes very complex so Euclid's algorithm can be extended for this purpose. Large key size have two effects: regular increase in computing power and continuing refinement of factoring power [3].

Cyber crime's can be felt when we use internet and cloud computing offers a tempting target for many reasons. There are some providers such as Google and Amazon which having existing infrastructures to detect and survive a cyber attack. If a cyber criminal can identify the provider whose vulnerabilities are the easiest to exploit, then it is a highly visible target [Uma Somani et.al].

The security of RSA algorithm depends on the size of prime number, for security purpose we select a very large prime number n, and we have some efficient methods to divide it. The calculation of private key e, similarly d can't be calculated from n and e. The attack is difficulty equivalence to the division of the product of two very large prime numbers say p, q, however the RSA having the higher security [1]. The private key e is used to encrypt when we are sending any plaintext message to others.

III. ATTACKS ON RSA ALGORITHM

There are following two types of attacks which are often found when we are using RSA algorithm:

Brute force attack: In Brute force attack, there is no need any special type of parameters. Brute force attack is again classified in following two categories [7]:

(1) Exhaustive attack
(2) Factorization attack

Exhaustive attack is used to traverse all possible values of the decryption key (d), and it tries all possible combination of 1s in d till the attacker finds the correct value of decryption key d. Whenever any attacker finds the value d then he can easily decrypts the message which was sent by sender to receiver. The Factorization attack factorizes the modules of RSA and gets the valve of prime numbers (p, q). The quadratic sieve and special number sieve are the two most widely used methods at present time.

Subtle attack: Subtle attack is a special type of attack which aims at the mathematical feature of some parameters. These parameters are given as below:

(1) Attack by multiplication of small prime numbers: if there is no big prime factors in p+1 or p-1 or q+1 or q-1 then this type of attack is possible. The attacker can calculate the modular power by multiplication of the chain of the small prime numbers one by one as the exponent; one can get the value of p and q cleverly.
(2) Square attack: If the value of the prime numbers p, q is so close to each other then this type of attack can be possible. The attacker can get the real value of p, q by calculating the value √n.
(3) Iteration attack: This is a special type of attack in which attacker calculates the modular power again and again in the process of encryption to find out the original message i.e. Plaintext.
(4) Low private exponent attack: In this attack the attacker uses the continued fraction and can get the approximate plain text message. The Wiener attack and Boneh-Durfee can be possible in this type of attack [12].

IV. CURRENT SCENARIO

The process latest several months during which **Rivest** proposed approaches, **Adleman** attacked them and Shamir recalls doing some of each. In cryptography, **RSA** is an algorithm for public-key cryptography which was given by Rivest, Shamir and Adleman.

According to Mathematically

The RSA algorithm is based on the mathematical part that is easy to find and multiple two large prime numbers together, but it is extremely difficult to factor their product. There are some important steps are involved in a RSA algorithm to solve a problem as given below:

Step 1: Assume two large prime numbers p & q.
Step 2: Compute:

$$\mathbf{N = p*q}$$

DOI 10.17148/IJARCCE.2016.51176

Where N is the factor of two large prime number

Step 3: Select an Encryption key (E) such that it is not a factor of (p-1)*(q-1)

i.e. Ø(n)= (p-1)*(q-1)

for calculating encryption exponents E, should be 1< E < Ø(n) such that

gcd(E, Ø(n)=1

The main purpose of calculating gcd is that E & Ø(n) should be relative prime. Where Ø (n) is the Euler Totient Function & E is the Encryption Key.

Step 4: Select the Decryption key (D), which satisfy the Equation

D*E mod (p-1)*(q-1) = 1

Step 5: For Encryption:

Cipher Text= (Plain Text)^E mod N

CT = (PT)^E mod N

Or

CT=M^E mod N

Step 6: For Decryption:

Plain Text= (Cipher Text)^E mod N

PT= (CT)^E mod N

V. SECURITY OF RSA OR STRENGTH OF RSA

1. Selection of large prime number(p, q):

The main feature of RSA algorithm is the selection of large prime number (p, q) because it is logical that fraction of large number is always typical and any users or force attackers could not be able to find the capable numbers, timely to force attack is shortly non-feasible.

Example: p = 5, q = 3

N= p*q
= 5*3
= 15
= 1*15 = 15*1 = 3*5 = 5*3

2. Selection of Encryption Key(E):

Selection of large of large prime fraction always create impact during the selection of Encryption key, if the factor is high then the estimation of Encryption is infeasible.

Example:

If p=7, q=17 must not be a factor of (p-1)*(q-1)

i.e. (7-1)*(17-1) = 6*16
= 96
= 2*2*2*2*2*3

So, E can be 5, 7, 11…

3. Selection of Decryption Key(D):

Selection of large factors always create an effect on the Decryption key, there may be an inversely relation.

(E*D) mod (p-1)*(q-1) =1

D α 1/ [(E) (p) (q)]

Some important points as given below:

- According to Euler's Totient Function :

1. Ø (1) = 0
2. Ø (p) = p – 1 {if p is prime number}
3. Ø (m*n) = Ø (m)* Ø (n)
   {if m and n is relative prime number}
4. Ø (p^e) = p^e – p^{e-1} {if p is a prime number}

- There is no need for a user to know his secret parameters p, q and Ø (n).
- The plain text or message (M) has the form of one or more positive integer M<N.
- Any user can use his private key to authenticate the communication.
- RSA cryptosystem provides the facility of digital signature scheme.
- The message consists of letters, numbers and special characters (i.e. stop, colon, space etc.). Each character is represented by its own arrangement of Eight bits (o & 1).
- The most of the hardware & software products and standards that use public key technique for Encryption, Decryption etc. are based on RSA cryptosystem.

VI. MY OBSERVATIONS ON RSA ALGORITHM

After studying the work on RSA algorithm done by several researchers. We observed the following advantages:

The Elliptic Curve Cryptography (ECC) is the public key primitive that is increasingly important as to RSA. Another advantage of ECC is that it having shorter key length than RSA. For example, ECC-160 is similar to RSA-1024, and ECC-224 is similar to RSA-2028. So we can say that ECC having shorter key length than RSA[1].

There are some advantages of RSA Algorithm:

- Primary advantage of Public key Cryptography is increased security and convinces.
- Second, it provides digital signature that can't be repudiated. For example, Kerberos secret-key authentication system involves central database that keeps copies of secret key.
- Public key authentication prevents the type of repudiation and each user has its own responsibility for protecting his own private key.
- We can select large prime numbers for enhancement of security of keys.
- Public key cryptography may be used with secret key cryptography.

However the RSA Algorithm having some disadvantages also, which are given below [9]:

- The main demerit of PKC is its speed during encryption of its given plaintext. In modern cryptosystem there are several secret-key encryption algorithm that having faster speed in comparison to public key encryption methods.
- PKC may be vulnerable to impersonation if private keys of user are not available. If there is an attack on certification authority then it will allow an adversary chooses a public key certificate from the compromised authority.

PKC is not a replacement of secret key cryptography but it is not the supplement to sure it. First, use of public key technique was for secure key exchange that is one its primary function. ECC has evolved from a fringe activity to a major challenger to the popular RSA.ECC having some major advantages over traditional system such as increased speed, less memory, as well as smaller key size.

Finally, we can say that it having less memory, less power, as well as less storage capacity than other systems makes it possible to implement cryptography in many specific platforms such as wireless-devices, laptop computers and smart cards. So use such situations where efficiency is one of the important factors [9]. The Elliptic Curve Cryptography (ECC) is the public key primitive that is increasingly important as to RSA.

VII. CONCLUSION & FUTURE WORK

From the above study it is advent that RSA algorithm has the same importance as of the system in the Cryptography over network security. Since RSA are used to be provides the authentication & privacy to whole system. But it is fully depends upon the two large prime numbers, Encryption & Decryption key. Always keep you mind its mathematical calculation are very difficult and lengthy.
Since its publication, a vast amount of research has been completed on inverting the RSA function, and many clever attacks have been found. Although the attacks detailed within this paper could be devastating in the appropriate conditions, the true benefit of this research should be to highlight the need for proper implementation of RSA, preventing the use of these attacks. Thus we see that, employed correctly, RSA is still a valid security measure for digital data. The attacks outlined in this paper have exploited weaknesses in the underlying Structure of the RSA function. We have considered private exponent attacks, from which we have discovered that a low private exponent should never be used, and low public exponent attacks. These are not the only classes of attacks which have proven successful. There have also been a great number of attacks focused upon the implementation itself. Brute force attack and subtle attack are most common known attacks occur in RSA algorithm [8]. These attacks exemplify the need to focus not only upon the underlying mathematical structure of RSA, but on more practical concerns, such as time considerations and random faults.

Future work

We observed some results as well as some conclusions about RSA Algorithm which having some merits as well as some demerits because neither algorithm is sufficient for modern cryptosystem for security point of view. Another advantage of ECC is that it having shorter key length than RSA. The Elliptic Curve Cryptography (ECC) is the public key primitive that is increasingly important as to RSA. We know that ECC-160 is similar to RSA-1024 and ECC-224 is similar to RSA-2028, so we can observe that ECC having key length 160 bit having same level of security as RSA having 1024 bit key. We observed that ECC having shorter key length than RSA for same level of security. So in future we can develop such type of RSA cryptosystem having key management similar to ECC. Security of RSA depends on the fact that there is no known factoring algorithm for any particular number. Suppose there is a public number n, prime numbers p and q are its factors. We knew p, q, then given public value e, one can easily compute the secret key, d. So, as RSA heads towards its 30th year of successful use, having provoked the Discovery of many insightful results, it will be interesting to see what further research might uncover in this area.

REFERENCES

[1]. Chong Fu, Zhi-liang Zhu, Sch. of Inf. Sci. & Eng., Northeastern Univ., Shenyang 110004,P.R.China.
[2]. William Stallings, “Cryptography and Network Security: Principles and practices, Dorling Kindersley (india) pvt ltd., 4th edition(2009).
[3]. Atul Kahate “Cryptography and Network Security” 3rd edition.
[4]. Behrouz A Forouzan ,”Data Communications and Networking” “4th edition”.
[5]. Xianhong Zhang. Theory and techniques og digital signature. Beijing: Mechanic Industries press, 2003.
[6]. JavaResearch org. Advanced J2SE. Beijing: Mechanic Industry Press. 2004.
[7]. Jiezhao peng, Qi Wu, Jiangxi University of finance & Economics, Nanchang 330013,Jiangxi province,China “Research and implementation of RSA Algorithm in Java”.
[8]. Hongwei Si,Youlin Cai, Zhimei Cheng, “An improved RSA algorithm based on Complex numeric operation function”.
[9]. http://www.rsa.com/rsalabs/node.asp?id=2167
[10]. http://www.scribd.com/doc/55154238/31/DISADVANTAGES-OF-RSA
[11] http://www.tcpdump.org/#documentation
[12] Xianhong Zhang. The theory and techniques of digital signature. Beijing: Mechanical Industry Press, 2003.

BIOGRAPHIES

Ajay Pal Singh He received his B.E. degree in Information technology in 2006 from I. E.T. Agra University, Agra UP, India. He has completed M.Tech. in CSE from KNIT Sultanpur, His research interests are Software Engineering, Cryptography &Network Security, Automata Theory and Text mining and C Language. He is presently working as a HOD in IT Department in Rajkiya Engineering College Bijnor, India.

Parvez Rahi has completed his M.TECH in Computer Science Engineering from Govind Ballabh Pant Engineering College Pauri Garhwal and received degree of B.TECH in Computer Science Engineering from Tulas Institute Dehradun, Uttarakhand, India. in 2010.He is currently working in Rajkiya Engineering College Bijnor, Uttar Pardesh, India. His area of research is Computer Networks, Data Mining, Image- Processing.

DOI 10.17148/IJARCCE.2016.51176