INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN: 2278 – 0211 (Online)

Overview Of RSA And Its Enhancements

P. Gayathri Devi
Assistant Professor, Department Of Computer Science
St. Paul's College Of Arts & Science For Women, Tamil Nadu, India

Abstract:
In the today's communication development push the people to transmit their information for so many purposes using the interconnected networks. They are using the internet for credit card payments, tax returns, banking etc. In such a case network security is the very important concept because they have to protect their information from unauthorized users. So people should have to maintain the secrecy of data and also they have to authenticate the information when they transmit data through networks. So cryptography theory is useful for hiding and protecting the information. Cryptography means secret writing which is useful for se cure transmission of information from sender to receiver. Secure communication means the intruder cannot access or modify the message. There are so many cryptographic algorithms to protect our data from malicious users. In which we mainly concentrate on RSA algorithm is an asymmetric algorithm which is a public key cryptography mainly useful in network security. So this paper deals with RSA algorithm and enhancements related to RSA algorithm.

Key words: *RSA, security, cryptography, ECC, DES, DS, EAMRSA, Dual RSA. Rebalanced RSA*

1.Introduction

Initially for cryptography, symmetric key algorithms like DES, AES etc. have found. In these algorithms encryption and decryption keys are same. DES described as Data Encryption standard developed by IBM in which plaintext is encrypted in 64 bit block ciphertext. Next Triple DES was invented by Tuchman in 1979. In which three keys are used instead of two keys. That is EDE (Encrypt Decrypt Encrypt) for encryption and DED (Decrypt Encrypt Decrypt) for decryption. It gives some high security compare to normal DES. Afterwards AES (Advanced Encryption Standard) suggested by NIST in 1997 which is new cryptographic standard having some rules and many researchers have tried to achieve the AES standard. It is a symmetric block cipher and key lengths are not fixed. So the length of the key may be 128,192, and 256 bits.

Normally in symmetric crypto systems encryption and decryption keys are same. If an intruder steals the key, the total system becomes worthless. In such a case in 1976, Diffie and Hellman found a new type of cryptosystem. In which encryption and decryption keys are different, which enforces one cannot find out the decryption key from the encryption key. In this algorithm sender and receiver both has keys named as public key and private key. Here public key is known by the public but the private keys know only by that person. This is called public key cryptography (PKC). When we compare to normal encryption and decryption algorithms, PKC provides the greatest level of security when we transfer the information through the network. There are various public key cryptosystems. In which RSA is one of the public key cryptography and if we encrypt the content using RSA, no one breaks the content easily. It was published in 1977 by Ronald Rivest, Adi Shamir and Leonard Adleman [3]. It was a very popular algorithm for so many years in sending the email, online shopping and some transactions using smart cards, credit cards, ATM cards etc. [5].

2.RSA Algorithm

The RSA algorithm is a base for all networks secured public key crypto system algorithm. It is an asymmetric algorithm and it is based on some principles from number theory. RSA is a public key cryptography useful for security, identification and authorization. In this algorithm security is mainly depending on the factoring of two large prime numbers instead of using small prime numbers. So we can complicate this algorithm using key length. If key length is 1024 bits, we can achieve good security and it can be generated within two minutes. If less than 1024 bits it takes within 2 seconds [1].

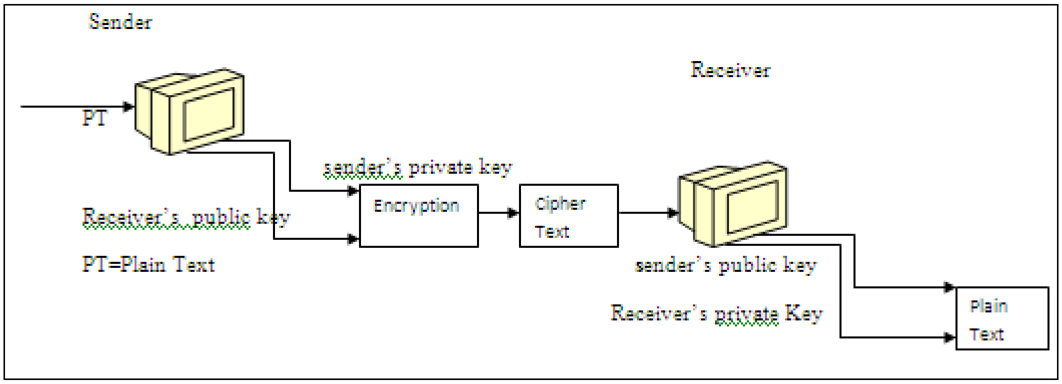

Figure 1: Basic Diagram Of RSA

2.1.Mathematical Calculation Of RSA Algorithm

Step1: Choose two large prime numbers r and s (normally in 1024 bits).
Step2: Compute t=r*s and t is the factor of two large prime numbers.
Step3: Compute Z=(r-1)*(s-1). Z can be formulated using Euler's Totient function. (It is also called Euler's phi function)

Euler's Totient Function

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

Step4: Calculate the encryption exponents e, such that 1<e< Z that is gcd(e, Z=1)
Step5: Calculate the decryption key d which is having the following equation

e*d mod Z=1.

Step6: To change plaintext into ciphertext that is for encryption use the following equation

$C=M^e$ mod t

C=Cipher Text, M=Message, e=encryption exponent, t=factor of r*s.

Step7: To change ciphertext into plaintext that is for decryption use the following formula

$M=C^e$ mod t.

(note: Here the message is divided into blocks, called P. P falls in the interval 0<P<t. Then calculate K which is a group of P. So it is the largest integer 2^k<t. so for encryption we use (e,t) is a public key and for decryption we use (d,t) is a private key.)

2.2.A Simple Example For RSA Algorithm

Step1: Choose two random prime numbers such as r**=3, s=7.**
Step2: Calculate t=r*s. so t=3*7=21. **t=21.**
Step3: Calculate Z=(r-1)*(s-1). Z=2*6=12. **Z=12.**
Step4: Choosing encryption exponent **e=11.**
Step5: Calculate the decryption key **(e*d) mod Z=1.**

After calculating Z and e, d can be found using Euclid's algorithm. So run the extended Euclid's algorithm (r-1)*(s-1) with m=2 and t=21 and calculated **d=11.**

According to the formula (11*11) mod 12 =1.

Public key is (e,n)= (11,21). Private key is (d,n)=(11,21)
Step6: Calculate the encryption key. $C=M^e$ mod t. Set **M=2.**

$C=2^{11}$ mod 21 = 2048 mod 21 = 11. So **C=11.**

Step7: Calculate the decryption key. $M=C^e$ mod t.

$M=11^{11}$ mod 21 = 285311670611 mod 21 =2.

Finally we got **M=2.**

(Note: choose e to be greater than both p-1 and q-1. d is the multiplicative inverse of e in class modulo)

2.3.Advantages Of RSA Algorithm

RSA Algorithm has so many merits such as

- RSA algorithm is a base or superior for all algorithms. Without the base of RSA, now a day's network security is worthless. Mainly it is a public key crypto system. So encryption and decryption keys are different.

- It is primarily used for network security, authentication and also for non-repudiation because RSA algorithm work with digital signature also. So the sender cannot deny the information and also receiver cannot modify the original data. It is better than hash algorithm.
- There is no need for a receiver to know the secret variables such as r,s,Z.
- This algorithm can encrypt any type of messages like letters, number, colon etc.
- The sender and receiver both have their own private keys. So nobody can steal the key even the sender cannot know the receiver's private key and receiver cannot know the sender's private key.
- If we need more security we can select very large prime numbers and we can increase the key length [6].
- It is very difficult for hackers to break the text. So it is a best secret key cryptography.

2.4.Disadvantages Of RSA Algorithm

RSA algorithm has so many advantages. Even it has some demerits also such as

- The major disadvantage is that it requires keys of at least 1024 bits for good security in encryption and also for decryption. So it is a time consuming process from the initial stage itself.
- If we choose large prime numbers, computations are also become so large. So it needs lot of memory because we have to continually refreshing the factoring power [7].
- It is a very complex algorithm because we have to choose very large prime numbers and we have to factorize, calculate it. This much complication also pushes us for alternative solution.
- In RSA algorithm, cost is very high and it needs much energy because of so many difficult calculations, modular exponentiation etc.
- RSA algorithm is not suitable for encrypting the large number of message because of its speed and also it consumes more bandwidth.
- In the modern world there are several advanced secret key encryption algorithms developed with greater speed and less memory than RSA algorithm and so many intelligent attacks are found. So RSA algorithm should have the ability to cope up.

3.Improvements Of RSA Algorithm

To overcome the disadvantages of RSA algorithm, some improvements are needed to reduce the time, memory, complexity and bandwidth. In order to achieve this there are so many algorithms have been developed. They are as follows.

3.1.Digital Signature (DS)

RSA algorithm should be useful to protect from various types of attacks such as a brute force attack (It will take all possible combinations) is partitioned into exhaustive attack and factorization attack. The second type of attack is a subtle attack (it is mainly concentrated on mathematical parameters) [2]. In such as case we can use the RSA algorithm with digital signature to get the identity of the sender, authentication and we can avoid repudiation. In digital signatures we have so many approaches such as (i) symmetric key signatures **-** In this digital signature we have a central authority and both sender and receiver should believe the central authority and they have to transmit the information through the central authority. So the central authority is responsible for all authenticated activities. 2. Public key signatures: **-** In which both sender and receiver has public and private keys. The sender can encrypt his message through receiver's public key and his private key. Then receiver can decrypt his message through sender's public key and receiver's private key.

3.2.Sieve Function

Sieve function is useful to accelerate the computations of RSA algorithm quickly and efficiently through detecting the large set of composite numbers. In RSA algorithm generating such random numbers is a time consuming process. But using sieve function we can make a trial with large number of composite numbers before we select random prime numbers. This function is useful for factoring integers within a short period of time. This function includes a set of prime numbers such that $S(U)=\{pi|2<pi\leq U,i\square N\}$ and pi is ith prime.

3.3.RSA With DES

The security of the RSA algorithm can be increased to combine the RSA algorithm with DES (Data Encryption Standard). So we combine asymmetric key algorithm (RSA) to symmetric key algorithm (DES).In DES plaintext is encrypted in blocks of 64 bits. So it gives 64 bits of cipher text and also it has 19 stages. Each stage is transformed by 56 bit key. It is very useful to transmit information via a wireless standard like wireless radios called blue tooth. We can make DES stronger using whitening method. DES encrypted the text block by block. It takes less time compared to RSA algorithm. So encryption speed is much greater than RSA algorithm. So it is well suitable for encrypting large amount of data. But RSA algorithm has the public key cryptographic feature. So in this algorithm encryption key is public but decryption key is secret and both are different keys. But in DES algorithm both encryption and decryption keys are same. So if the intruder knows the secret key, the concept is useless. So if we combine the best features of RSA and DES algorithms, we can reach the greatest level of security.

3.4.EAMRSA

EAMRSA – Encrypt Assistant Multi prime RSA cryptosystem is also very useful to improve the performance of the basic RSA algorithm by reducing modulus and private exponents. If we reduce these calculations, automatically it speeds the decryption process. EAMRSA combines the features of Multi prime RSA and RSA –S2 [14].

3.5.Elliptic Curve Algorithm

The ECC we invented by Victor Miller in 1985 and Neil Koblitz. Koyama et al find out first analogue of the RSA scheme, called KMOV scheme, based on elliptic curve. One alternative technique for public key algorithm is Elliptic Curve Algorithm (ECC) and it works better than PKC [12]. It gives high security compare to RSA and the calculative speed is increased and the complexity is reduced. ECC is having shorter key length than RSA. ECC-160 is equal to RSA-1024 and ECC-224 is equal to RSA-2028 [4]. So we need less energy even for many advanced processes such as credit card transaction, smart cards and for message transmission etc and these processes get advancement in the case of speed, memory etc.

Equation of Elliptic Curve Crypto system is $Y2=x^3+ax+b$.

3.6.Dual RSA

Dual RSA have been introduced by sun et al. In dual RSA two instances of RSA will share the same public and private key exponents. So it will reduce the memory requirements required for storing both keys because both key exponents are same. Twin RSA is also used to reduce storage requirements. Here there are two different RSA instances such as T1=r1s1, T2=r2s2. As usual we have public key (e) and private key (d). These keys should satisfy the following equations such that $ed \equiv 1 \bmod Ø\ (T1)$ and also $ed \equiv 1 \bmod Ø\ (T2)$ [9].

3.7.Message Digest

RSA algorithm used with message digests for authentication and not for secrecy. For that the sender and receiver must compute MD (P) called as one way hash function. So the sender encrypts the message after computing message digest and using his digital signature. The receiver will decrypt the message after computing message digest and using his digital signature. So Message digest mainly concentrate on authentication and this method will not encrypt the entire message and also it is useful to speed up the digital signature algorithms.

3.8.Blind Signature

In blind signature there are two different parties are involved. In this scheme one party get sign from another party who knows nothing about the message. So the message will be hidden from the signer. Eg. Anonymous voting, Anonymous e-cash etc. It can be implemented effectively using RSA Algorithm. In this scheme at first the message is blinded and sent it to the signer and signer will sign the message using normal signing algorithm. If the number of users is more, verification, computing time and storage are more. But we can manage all these things using blind signature and also malicious users cannot do anything on the original message [11].

3.9.Rebalanced RSA

Rebalanced RSA introduced by Wiener in 1990 used to give the good improvement in RSA decryption and also encryption. Normally we have to choose the small public key exponent [8]. But we should not choose the small private key exponent because it is unsafe. So here wiener is mainly discussing the weakness in the use of the private exponent. In this algorithm public exponent e is very smaller than the modulus, so automatically it will reduce the encryption costs when we are going to maintain low decryption costs. If we choose a private exponent L so that both Lr and Ls are small. So Rebalanced RSA is mainly used to balance encryption time and decryption time. It is also used to balance the cost and also the memory. Rebalanced RSA reduces the overall cost of encryption and decryption process and rebalance the difficulty of encryption and decryption. It is well suitable for many practical applications. It is just like the same calculation that is done in RSA-CRT for encryption and decryption. The only difference is that we modify this algorithm by choosing the public exponent much smaller than Z can be used [10].

3.10.IDEA Algorithm

International Data Encryption Algorithm is a block cipher invented by Xuejia Lai and James L. Massey in 1991. It is an improvement of PES (proposed Encryption standard). It is used for wide range of business applications. It gives greatest level of security compare to standard RSA and it can be learnt very easily and efficiently. This is a block cipher and each block has 64 bit plaintext and 64 bit cipher text and all controlled by a 128 bit key. In this algorithm 64 bit plaintext is divided into 16 bit sub blocks. So encryption mainly based on 16 bit numbers. This algorithm provides much speed because of block encryption and decryption [13].

4.Conclusion

In this paper we have discussed mainly about RSA and we look at a glance about some more algorithms which are alternative for public key crypto systems. Basically we have some improvements in RSA like RSA-140, RSA-155, RSA-160, RSA-576, RSA – 640, RSA-1536 and now RSA-2048. Using the RSA algorithm as a base, we can get much advancement in encryption and decryption process by many other algorithms. There are so many algorithms can be combined with RSA algorithm to improve the productivity of RSA in the consideration of time, cost etc. So we can overcome the disadvantages of RSA algorithm and we make good security analysis to raise the security level of the standard RSA in combination of other algorithms efficiently. So this advanced RSA has the capability to manage any attacks.

5.References

1. Chone Fu, Zhi-liang Zhu, Sch. Of inf. Sci. & Eng., Northeastern Univ., Shenyang 110004, P.R.China. (for 1024 bits within 2 seconds).
2. Jiezhao pen, Qi Wu, Jiangxi University of finance & Economics, Nanchang 330013, Jiangxi province, China "Research and implementation of RSA Algorithm in Java". (subtle attack)
3. R. Rivest, A. Shamir, and L. Adleman, "A Method for obtaining Digital Signatures and Public-Key Cryptosystems, "ACM Trans. OnCommunications, vol. 21, pp. 120-126, 1978. (founder of RSA in 1977)
4. Prasant Singh Yadav, Pankaj Sharma, Dr.K.P. Yadav "Implementaton of RSA Algorithm using Elliptic Curve Algorith for Security and Performance Enhancement" IJSTR, vol 1,Issue 4, May 2012.
5. William Stallings, "Cryptography and Network Security: Principles and practices, Dorling Kindersley (india) pvt let., 4th edition(2009).
6. Hongwei Si, Youlin Cai, Zhimei Cheng, "An improved RSA Algorithm based on Complex numeric operation function".
7. Atul Kahate "Cryptography and Network Security" 3rd edition.
8. Wiener M., "Cryptanalysis of short RSA secret exponents", IEEE Trans. Inform. Theory 36(1990), 553-558.
9. H.M. Sun, M.E. Wu, W.C. Ting, and M.J. Hinck, 'Dual RSA and its Security Analysis', IEEE Trans. On Information Theory, vol.53, no.8, pp. 2922-2933, August 2007.
10. H/-M. Sun, M.J. Hinek, and M.-E. Wu, On the design of Rebalanced-RSA, revised version of Centre for Applied Cryptographic Research, Technical Report CACR 2005-35, 2005 [Online]. Available:http://www.cacr.math.uwateloo.ca/techreports/2005/cacr2005-35.pdf.
11. G.Wang, Bibliography on Blind Signatures [Online]. Available: http://www.i2r.a-star,edu.sg/icsd/staff/ Guilin/bible/blind-sign.htm[ONLINE], Available.
12. Hans Eberle, Nils Gura, Sheueling Chang Shantz, Vipul Gupta, Leonard Rarick Sun Microsystems Laboratories. A Public-key Cryptographic Processor for RSA and ECC "Proceedings of the 15th IEEE International Conference on Application-Specific Systems, Architectures and Processors (ASAP'04).
13. Suying Yang*, Hongyan Piao, Li Zhang and Xiaobing Zheng, "An Improved IDEA Algorithm Based on USB Security Key" Third International Conference on Natural Computation(ICNC 2007).
14. Bio-Chaotic Stream Cipher-Based Iris Image Encryption", Alghamudi, A.S.; Ullah, H.; Mahmud, M.; Khan, M.K. Computational Science and Engineering, 2009. CSE'09. International Conference on Computational Science and Engineering.