Modified RSA Cryptographic Algorithm

Anand Kulkarni, Prof Rahul Patil Department of Computer Science
Engineering, PCCOE, Pune, India(kulkarnianand147@gmail.com)

Abstract* - *The most common public key algorithm is RSA cryptosystem used for encryption and decryption. This paper suggests a new algorithm concept to present the modified form of RSA. In the proposed method we extend the number of bits in the keys to avoid some external attacks. The proposed RSA method is compared with the original RSA method by some theoretical aspects. Comparative results provide better security with proposed algorithm in some contexts.

Keywords: -RSA, cryptography, public key, private key, prime number, wiener's attack, encryption, decryption.

I. INTRODUCTION

Encryption is one of the significant means to guarantee the security of sensitive information. It not only provides the mechanisms in information confidentiality, but also functioned with digital signature, authentication, secret sub-keeping, system security etc.

RSA is the most widely used asymmetric encryption system which was invented by Ronald Rivest, Adi Shamir, and Len Adleman in the year 1977. As a public key encryption standard, the private key is kept secret, but the public key is revealed to everybody in RSA. Since its innovation, RSA is regarded as one of the most secure cryptosystems in existence.

In our modified approach we choose the values of chosen prime numbers greater than 1024 bits randomly to avoid certain attacks such as Brute force attack, Weiner's attack, etc. In proposed method, some concepts of existing RSA algorithm method are improved to provide higher security.

II. RSA ALGORITHM

RSA cryptographic algorithm is one of the most famous security algorithms which is composed of three phases- key generation, encryption, and decryption. Following is the procedure of how keys are generated in RSA cryptosystem.

RSA algorithm is asymmetric cryptography algorithm. Asymmetric means it works on two different keys mainly public key and Private Key. RSA public key cryptosystem is one of the most typical ways that most widely used for public key cryptography in encryption and digital signature standards.

A. Key Generation

(1) Select p and q both prime number, p is not equal toq.

(2) Calculate n = p * q.

(3) Calculate ø (n) = (p -1) * (q-1).

(4) Select integer e whose gcd (Ø (n), e) = 1, 1 < e < Ø(n).

(5) Calculate private key d = e^{-1} (mod Ø(n)).

(6) Public key PU = {e, n}.

(7) Private Key PR = {d, n}.

B. Encryption Procedure

Plaintext- Message (M)
Cipher text- C = M^e mod n.

C. Decryption Procedure

Cipher text- C
Plaintext- M = C^d mod n.

III. LIMITATIONS OF RSA

1 ***Speed-*** RSA cryptography takes time to compute its operation for encryption and decryption of data. Therefore, its calculations are lengthy and take lot of time. To reduce the complexity of RSA algorithm we need to modify it.

2 ***Public key must be authenticated-*** In RSA cryptography public key is used by the sender to encrypt the message. Thus, only authenticated user canparticipate in encryption procedure.

3 ***Computational Cost*** - RSA algorithm refers to an asymmetric cryptography in which two different keys are used for encryption and decryption, therefore its computational cost is high as compared to symmetric cryptography because in symmetric cryptography same secret key is for both encryption and decryption of message.

4 ***Attacks On RSA*** - There are various attacks in RSA cryptosystem such as factorization problem, low decryption exponent, common modulus, short message, cyclic attack etc. These attacks can break the security of RSA cryptography.

IV. PROPOSED METHOD

In proposed method we developed a modified RSA algorithm which is based on original RSA cryptographic algorithm. Considering these assumptions for algorithm –

a) The prime numbers P and Q is considerably large at least 1024 bits each.
b) The length of common modulus N is greater than 1024 bits.
c) The length of private key D must be large enough to avoid Weiner's attack.

We use the following equation to avoid this attack.

$$D > N^{0.25*}(0.33)$$

V. COMPARISION ANALYSIS BETWEEN RSA AND PROPOSED RSA ALGORITHM

RSA	PROPOSED RSA
In original RSA length of prime n was supposed to be up to 604 bits.	In this we take N as 1024 bits long number, thus avoiding Brute force attack.
The strength of the Euler totient function depends on the value of N. Lower the value lower is the strength.	Here as N is as long as 1024 bits, the strength of Euler totient function is good as compared to original RSA.
The public key E for e-stamps is fixed and its value is $2^{16}+1$ which is 65537.	Here E is as long as phi so any attempt to break the value of E will not be in computational terms.
As E is small, it becomes vulnerable to brute force attacks.	E is of 1024 bits so Brute force attacks are avoided.
Encryption, Decryption is fast but less secure.	Encryption, Decryption is slow but more secure.

TABLE I. Comparison Table

V. ATTACKS AVOIDED

Following are the attacks that are avoided by the proposed method.

a) Brute Force Attack - It would take 2^{1024} computations to crack the values of P, Q, D, E. Even if using modern computers are used, it would take approximately 10600 years. Therefore, this attack is avoided by expanding the number of bits.

b) Small value of E - If the value of E is taken as $2^{16}+1$ i.e., 65537 then Thus, there exists an integer k such that $k < \min(E, D)$ and $\varphi(N) = (E*D-1)/k$. This suggests a search procedure for discovering $\varphi(N)$, with the length of the list of possible values shorter than min {E, D}. Since in our proposedmethod E is of 1024 bits, the attack is avoided as it requires 2^{1024} bits to crack the value of E.

c) Weiner's attack - It is sometimes tempting to choose the private decryption exponent d small to speed up the decryption process. A small value of d always leads to a large value of e, the public encryption exponent, and thus leads to slower encryption. There are two reasons to avoid choosing a small private decryption exponent. One of them is that correspondents will be discouraged by "slow" encryption process and will most likely not communicate. The other is more ominous - it opens up the system to a fairly efficient attack and one obtains a list of equations using long division. This can be avoided by given below two methods.

i. $D > N^{0.25} * (0.33)$
ii. $E > N^{1.5}$

Since typically in our proposed algorithm N is 1024 bits, it follows that D must be at least 256 bits long to avoid this attack. This would be very grateful for low-power devices such as smartcards, where it would result in big savings.

VI. CONCLUSION

In the proposed method keys generated are of 1024 bits. Thus, the speed of the proposed method is decreased as compared to original RSA method. If an unauthorized person wants to know the value of P, Q it is difficult to get them by brute force attacks. This method will provide more security and it is reliable to use. In future some security concepts can be applied in the existing RSA algorithm for providing more efficiency and security.

VII. REFRENCES

[1] Ishwarya M, Dr. Ramesh Kumar. “Privacy Preserving Updates for Anonymous and Confidential Databases Using RSA Algorithm”, International Journal of Modern Engineering Research (IJMER) , Vol.2, Issue.5, Sep.-Oct.2012.

[2] Mandeep kaur and Manish Mahajan “Using encryption Algorithms to enhance the Data Security in Cloud Computing”, International Journal of Communication and Computer Technologies Vol.01–No.12, Issue.03, January 2013.

[3] Prof .Dr.Alaa Hussein Hamami and Ibrahem Abdallah Aldariseh, “Enhanced Method for RSA Cryptosystem Algorithm”, International Conference on Advanced Computer Science Applications and Technologies, pp.402-408, Nov2012.

[4] Sami A. Nagar and Saad Alshamma “High Speed Implementation of RSA Algorithm with Modified Keys Exchange”, 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), pp.639-642, March2012.

[5] Xin Zhou and Xiao fei Tang “Research and Implementation of RSA Algorithm for Encryption and Decryption”, The 6th International Forum on Strategic Technology, Vol.2, pp.1118-1121, Aug 2011.

[6] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Vol. 21, pp.120-126,1978.

[7] W. Stallings “Cryptography and network security”, vol. 2 prentice hall,2003.

[8] Ravi Shankar Dhakar and Amit Kumar Gupta “Modified RSA Encryption Algorithm (MREA)”, Second International Conference on Advanced Computing & Communication Technologies, pp.426- 429, Jan2012.

[9] Sonal Sharma, Prashant Sharma and Ravi Shankar Dhakar “RSA Algorithm Using Modifiesd Subset Sum Cryptosystem”, International On Computer and Communication Confrence Technology(ICCCT), pp. 457-461, Sep2011.

[10] Wuiling Ren and Zhiqian Miao, “A hybrid encryption algorithm based on DES and RSA in Bluetooth communication”, Second International Conference On Modeling, Simulation and Visualization Methods, pp. 221-225, May2010