ISSN:0975-9646

Implementation of Modern RSA Variants

Akansha Tuteja[1,] Amit Shrivastava[2]

[1,2]Department of Computer Science & Engineering, RGPV University
SVCE INDORE 452009, INDIA

***Abstract*—.RSA cryptosystem is the most commonly used public key cryptosystem. It is the first public key cryptosystem. The strength of this cryptosystem is based on the larger key size. There are many algorithms and variants of RSA. In RSA, encryption keys are Public, but decryption keys are not, so only the person with the correct decryption key can able convert cipher into decipher or encrypted message. The keys must be making in such a way that the decryption key may not be very easily deduced from the public encryption key. In this paper, we have proposed a implementation of some modern variants of the RSA algorithm. In our proposed cryptosystem, the encryption is faster in comparison to current RSA Cryptosystem. Also our proposed cryptosystem is more secure against low decryption exponentiation attack, because we are using a large value of d and in our proposed cryptosystem computation of the plain text from the cipher text are done by applying the Fermat's theorem.**

***Keywords*— Public Key Cryptography, RSA Variant, Data Secrecy, modular multiplication, Fermat's theorem.**

I. INTRODUCTION

In this age of universal electronic connectivity, the electronic fraud is a matter of concern. There is indeed need to store the information securely. This has led to a heightened awareness to protect data and resources from disclosure, to ensure the authenticity of data and messages, and also to protect systems from network based attacks. Cryptography plays a central role in mobile phone communications, electronic commerce, sending or receiving private emails, transaction processing, providing security to ATM cards, securing computer from unauthorized access, digital signature and also touches on many aspects of our daily lives. Cryptography consists of all the principles and methods of transforming an intelligible message called plaintext into one that is unintelligible called cipher text and then retransforming that message back to its original Form. In modern era, the cryptography is considered to be a branch of both mathematics and computer science. It is also affiliated closely with information & communication theory. Although in the past, the role of cryptography referred only to the encryption and decryption of message using secret keys. But nowadays, the cryptography is used in many areas; it is because of the digitization.

It is generally classified into two categories, the symmetric and asymmetric. The data transferred from one system to another over public network can be protected by the method of encryption. On encryption the data is encrypted or scrambled by any encryption algorithm using the key.

The user having the access to the same key can decrypt the encrypted data. Such a cryptosystem is known as private key or symmetric key cryptography. There are many standard symmetric key algorithms available. Some popular ones are as:. AES advanced encryption standard, 3DES triple data encryption standard etc. All these standard symmetric algorithms defined are proven to be highly secured and time tested. The main problem related to these algorithms is the key exchange. All the communicating parties require a shared secret key. This key is required to exchange between them to establish a secured communication. Therefore the security of the symmetric key algorithm depends on the security of the secret key. The Key size is typically hundreds of bits in length. The key size also depends on the algorithm used. The key cannot be shared online. Also when a large number of communicating parties are there, then in that case the key exchange is infeasible & very difficult too. All such problems are countered by the public key cryptography.

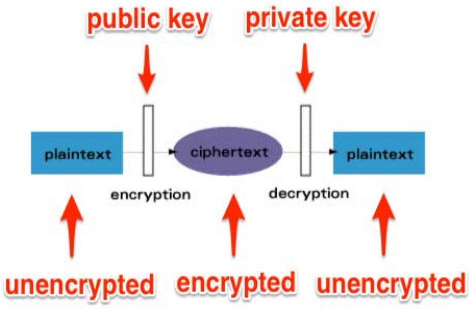

Fig. 1 public key cryptography

In public key algorithm a shared secret can be established online between communicating parties without any need for exchanging any secret data.

This paper describes the Implementation of Some Modern RSA Variants algorithm using Fermat's theorem.

II. PREVIOUS RIVEST, SHAMIR, AND ADELMAN (RSA)

RSA is the asymmetric or public key cryptography system. The security of RSA public key cryptosystem is based on the larger value of modulus. One of the main problems associated to RSA cryptosystem is factorization. The public key cryptosystem RSA is the first and most popular cryptosystem for performing encryption and decryption of data, to keep data secret, to transfer data from one location to another. Also it is known that the security of RSA depends on large factorization. If the factorization is possible then the whole algorithm can become breakable. Authors proposed a new methodology to change the original modulus with the fake modulus. Therefore if the hacker factorizes this new modulus value then he will not be able to locate the original decryption key.

Step l: In first step choose two prime numbers p and q.

Step 2: The second step toward this approach is to compute "Pe " (possible values of e) such that (p - 1) and (q - 1) are relatively prime. gcd[e, <P(n)] = 1,where 1 < Pe <<P(p. q) .

Step 3: In next step selects the value of "e " from " p^{e}" and chosen "d" such that [e. d mod <P(n)] = 1

Step 4: In this step, finds the "Se" where "Se" are special values of "Pe" which are multiplied by "n" and produce fake modulus "Fn". The new modulus "Fn" is used in place of actual modulus "n" and does the process of encryption and decryption. If the results of decryption and plaintext are matched, then the selected value that was considered "Se" will be the desired value. Similarly on other hand if the plaintext and decryption results are not matched then the selected number must be again set for Se .
If "Se " has not found go back to step 3 change the value of "e" and choose "d" then repeat step 4.

Step 5: In this step, approach computes "Fn" that is theproduct of "n" and "Se" as
Fn =n * Se Eq (1)
Where "Fn" = fake modulus value, n= product of two prime numbers p and q
Se = special value of Pe

III. Common Problems In Existing Rsa Variants

1) The main disadvantage of RSA encryption its slower speed.
2) Not secure against Weiner's attack
3) Not secure against common modulus attack

IV. The New Approach Rsa Cryptosystem

Encryption step:
The steps of the proposed work are as follows:

1. First choose random large prime integers p and q of roughly the same size but not too close to each other.
2. Calculate the product n = p×q (ordinary integer multiplication)
3. Choose a random encryption exponent e It must not has any common factor with either p-1 or q-1.
4. Compute e×d mod (p-1) × (q-1) = 1
5. Encryption Step:
   $c = m^{e} \bmod n$

Decryption step:

In this step, we will use the larger value of d. Also we will split the n in to p and q. Then we will compute the plain text by applying the Fermat's theorem as follows:

1) Compute:
$X1 = c^{dp} \bmod p$
$X2 = c^{dq} \bmod q$
Where d×p = d mod p-1
& d×q = d mod q-1
2) Compute:
W = (X2 – X1) ×W1 mod q
Where W1 = p mod inverse q
3) Then finally compute:
$M= c^{d} \bmod n = X1 + W \times p$

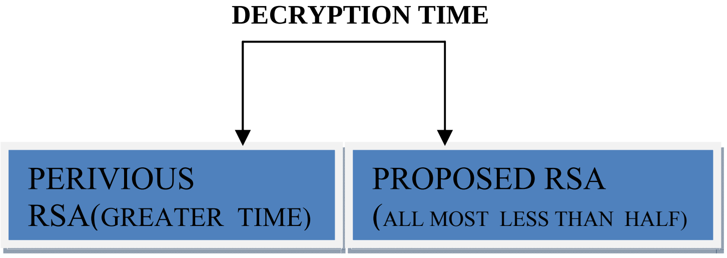
DECRYPTION TIME
PERIVIOUS RSA(GREATER TIME)
PROPOSED RSA (ALL MOST LESS THAN HALF)

Fig. 2 comparison between decryption time of pervious and proposed rsa

V. Conclusion

In this paper, the implementation of RSA cryptosystems is discussed. The problems related to pervious RSA cryptosystem are discussed. Also our proposed cryptosystem is more secure against low decryption exponentiation attack, and common module attack. The proposed scheme improves the security and it is faster in comparison to current variant of RSA cryptosystem.

References

[1] William Stallings "Network Security Essentials (Applications and Standards)", Pearson Education, 2004.
[2] National Bureau of Standards, " Data Encryption Standard," FIPS Publication 46, 1977.
[3] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.
[4] Ramesh G, Umarani. R, " Data Security In Local Area Network Based On Fast Encryption Algorithm",International Journal of Computing Communication and Information System(JCCIS) Journal Page 85-90. 2010.
[5] Diaa Salama Abdul Minaam, Hatem M. Abdual-Kader, and Mohiy Mohamed Hadhoud "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types" International Journal of Network Security, Vol.11, No.2, PP.78-87, Sept.
[6] Simar Preet Singh, and Raman Maini "COMPARISON OF DATA ENCRYPTION ALGORITHMS" International Journal of Computer Science and Communication Vol. 2, No. 1, January-June 2011, pp. 125-127
[7] Challa Narasimham, Jayaram Pradhan," EVALUATION OF PERFORMANCE CHARACTERISTICS OF CRYPTOSYSTEM USING TEXT FILES" Journal of Theoretical and Applied Information Technology,pp55-59 2008.
[8] Abdel-Karim Al Tamimi," Performance Analysis of Data Encryption Algorithms "
[9] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11, 1997.

[10] Prasithsangaree.P and Krishnamurthy.P(2003), “Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs,” in the Proceedings of the IEEE GLOBECOM 2003, pp. 1445-1449.

[11] Marwa Abd El-Wahed, Saleh Mesbah, and Amin Shoukry,” Efficiency and Security of Some Image Encryption Algorithms”, Proceedings of the World Congress on Engineering 2008 Vol I WCE 2008, July 2 - 4, 2008, London, U.K.

[12] Dr. S.A.M Rizvi1 ,Dr. Syed Zeeshan Hussain2 and Neeta Wadhwa” A Comparative Study Of Two Symmetric Encryption Algorithms Across Different Platforms”,

[13] Turki Al-Somani ,Khalid Al-Zamil “Performance Evaluation of Three Encryption/Decryption Algorithms on the SunOS and Linux Operating Systems”, Theses

[14] 1Gurjeevan Singh, 2Ashwani Kumar Singla, 3K.S. Sandha,” Through Put Analysis of Various Encryption Algorithms”, IJCST Vol. 2, Issue 3, September 2011

[15] R.Chandramouli, “Battery power-aware encryption – ACM Transactions on Information and System Security (TISSEC),’’ Vol. 9 Issue 2, May 2006.

[16] 1Shashi Mehrotra Seth, 2Rajan Mishra,” Comparative Analysis Of Encryption Algorithms For Data Communication”, IJCST Vol. 2, Issue 2, June 2011 pp.192-192.

[17] Atul Kahate ―Cryptography and Network Security‖ 3rd edition.