Volume 4, Issue 11, November 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Faster Decryption and More Secure RSA Cryptosystem

Akansha Tuteja*, Amit Shrivastava
Department of Computer Science & Engineering
RGPV University, MP, India

***Abstract*—RSA cryptosystem is the first public key cryptosystem. Cryptography is the art or science encompassing the principles and methods of transforming an intelligible message (plaintext) into one that is unintelligible (cipher text) and then retransforming that message back to its original form.** *This paper proposed an implementation of a complete and practical RSA encrypt/decrypt solution based on the study of RSA public key algorithm* **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 by a known sender and during transformation, it was not altered by third person. In our proposed cryptosystem, decryption is faster and more secure against common module attack 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*.**

***Keywords*— Public Key, private key, Data security, common module attack, encryption, decryption, prime number, Fermat's theorem.**

I. INTRODUCTION

In this age of universal electronic connectivity and communication system security issues will play crucial role. 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. Central tool for achieving system security are cryptography algorithm 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. Many paper have been proposed in this direction but they are tread off between low decryption time and are vulnerable to common module attack and low decryption exponentiation attack. 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. Cryptography is not the only means of providing information security but rather than that it is a set of techniques. 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. In public key algorithm a shared secret can be established online between communicating parties without any need for exchanging any secret data. that the security of RSA depends on large factorization. If the factorization is possible then the whole algorithm can become breakable. In this paper we have implement modified RSA algorithm which is faster decryption time than the existing RSA algorithm and Also our proposed cryptosystem is more secure against low decryption exponentiation attack and common module attack.

II. IMPLEMENTATION OF THE OUR PROPOSED RSA ALGORITHM

RSA key of length 1024 can be generated within two minutes on platform of a common PC [21]. 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 [25]. 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 [24]. 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 by a known sender and during transformation, it was not 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:

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 [21]. 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 [22]. 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 [23]. 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 [21]. The private key e is used to encrypt when we are sending any plaintext message to others.

III. SOLUTION DOMAIN

Proposed RSA implementation work is as follows:

ENCRYPTION

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

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-

- First compute
  $X1 = c^{dp} \bmod p$
  $X2 = c^{dq} \bmod q$
  Where dp = d mod p-1 &
  dq = d mod q-1
- The compute
  W = (X2 – X1) * W1 mod q
  Where W1 = p mod inverse q
- Then finally compute
  $M = c^d \bmod n = X1 + W * p$

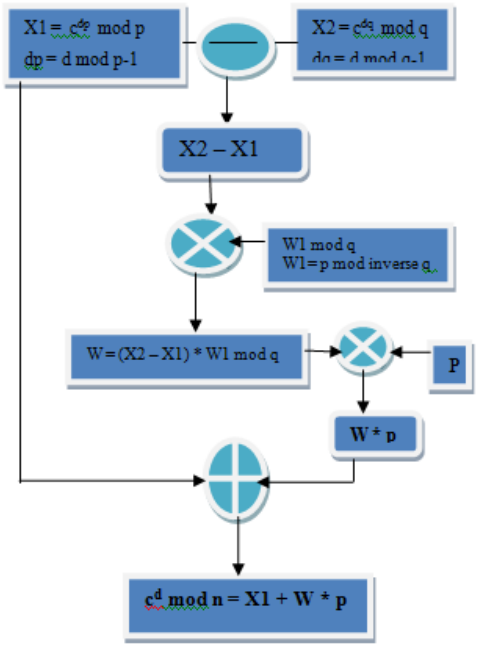

Fig 1: New Decryption scheme

IV. COMPARISON RESULTS BETWEEN CURRENT RSA AND OUR PROPOSED RSA RESULT

PERVIOUS RSA

INPUT

```
random rnd = new Random()

BigInteger m, m1, m2, m3, c, s, s1;

RSAPrivateKeybase alice = new RSAPrivateKeybase(1024, rnd, "Alice");

RSAPrivateKeybase bob = new RSAPrivateKeybase(1024, rnd, "Bob ");

start = System.currentTimeMillis();

m = new BigInteger("12345678909876543210");

System.out.println("Message m:\n" + m + "\n");

c = bob.RSAEncrypt(m);
```

RESULT(TIME)

Message m: 12345678909876543210

ALICE ENCRYPTS m FOR BOB; BOB DECRYPTS IT:

Message encrypted with Bobs public key:

188167637630517819795612199230958846243891607910851816100 0

Original message back, decrypted: 12345678909876543210

Total time ~ 141 ms

FASTER RSA

```
Input message

BigInteger m, m1, m2, m3, c, s, s1;

PrivateKeyFast alice = new PrivateKeyFast(1024, rnd, "Alice");

PrivateKeyFast bob = new PrivateKeyFast(1024, rnd, "Bob ");

m = new BigInteger("12345678909876543210");

System.out.println("Message m:\n" + m + "\n");

long startTimestamp1 = 0;

System.out.println("ALICE ENCRYPTS m FOR BOB; BOB DECRYPTS IT:");

                startTimestamp1 = System.currentTimeMillis();

c = bob.Encrypt(m);

endTimestamp1 = System.currentTimeMillis();
```

```
Message m:12345678909876543210

ALICE ENCRYPTS m FOR BOB; BOB DECRYPTS IT:

Message encrypted with Bob's public key:

188167637630517819795612199230958846243891607910851816100O

Original message back, decrypted:

12345678909876543210

Total time ~ 63 ms
```

V. CONCLUSION

In this paper, the implementation of RSA algorithm is discussed. The problems domain of pervious RSA algorithm and solution domain are also discussed. Also compare decryption time of current RSA algorithm and our proposed RSA algorithm which is more fast decrypt the input message as compare to pervious RSA cryptosystem and also secure against low decryption exponentiation attack, and common module attack. The proposed scheme improves the security and reduces decryption time for decrypting the input message.

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] 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.

[10] Nidhi Singhal1, J.P.S.Raina2, Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technology- July to Aug Issue 2011 pp177-181.

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

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

[17] 1Shashi Mehrotra Seth, 2Rajan Mishra," Comparative Analysis Of Encryption Algorithms For Data Communication", IJCST Vol. 2, Iss ue 2, June 2011 pp.192-192.

[18] Diaa Salama Abd Elminaam1, Hatem Mohamed Abdual Kader2, and Mohiy Mohamed Hadhoud2," Evaluating The Performance of Symmetric Encryption Algorithms", International Journal of Network Security, Vol.10, No.3, PP.213{219, May 2010.

[19] Diaa Salama1, Hatem Abdual Kader2, and Mohiy Hadhoud2" Wireless Network Security Still Has no Clothes", International Arab Journal of e-Technology, Vol. 2, No. 2, June 2011 pp.112-123.

[20] N.Ruangchaijatupon and P. Krishnamurthy, "Encryption and power consumption in wireless LANs-N,"The Third IEEE Workshop on Wireless LANs,

[21] Chong Fu, Zhi-liang Zhu, Sch. of Inf. Sci. & Eng., Northeastern Univ., Shenyang 110004,P.R.China. [22]William Stallings, ―Cryptography and Network Security: Principles and practices, Dorling Kindersley (india) pvt ltd., 4th edition(2009)

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

