International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 2 Issue 1 January 2015

Secure RSA Cryptosystem Algorithm Implementation

Monti Pal
SVITS, Indore
Montipal1@gmail.com

Abstract: RSA cryptosystem is that the most ordinarily used public key cryptosystem. It's the primary public key cryptosystem. The strength of this cryptosystem relies on the larger key size. There are several algorithms and variants of RSA. In RSA, encryption keys are Public, however cryptography keys aren't, thus only the person with the right decryption key will in a position convert cipher into decipher or encrypted message. The keys should be creating in such the way that the decryption key might not be terribly simply deduced from the general public encryption key. During this paper, we've projected an implementation of some trendy variants of the RSA algorithm. In our projected cryptosystem, the decryption is quicker as compared to current RSA Cryptosystem and conjointly secure against common module attack. Also our projected cryptosystem is safer against low decryption involution attack, as a result of we tend to area unit employing a massive worth of d and in our projected cryptosystem computation of the cipher text from the plain text are done by applying the Fermat's theorem.

Keywords: decryption, encryption, cipher text, public key cryptosystem, plain text.

1. Introduction

In this age of universal electronic connectivity, the electronic fraud may be a matter of concern. There's so have to be compelled to store the knowledge securely. This has led to a heightened awareness to shield information and resources from revelation, to make sure the believability of information and messages, and additionally to shield systems from network primarily based attacks. Cryptography plays a central role in mobile phone communications, electronic commerce, causation or receiving personal emails, group action process, providing security to ATM cards, securing computer from unauthorized access, digital signature and additionally touches on several aspects of our daily lives. Cryptography consists of all the principles and strategies of remodeling an intelligible message known as plaintext into one that's unintelligible known as cipher text and so retransforming that message back to its original type. In era, the cryptography is taken into account to be a branch of each arithmetic and engineering science. It's additionally attached closely with info& subject field. Though within the past, the role of cryptography referred solely to the encoding and decryption of message exploitation secret keys. But these days, the cryptography is employed in several areas; it's because of the digitization. It's typically classified into two classes, the centrosymmetric and asymmetric. the info transferred from one system to a different over public network may be protected by the tactic of encryption. On encryption the info is encrypted or disorganized by any cryptography rule victimization the key. The user having the

access to an equivalent key will rewrite the encrypted knowledge. Such a cryptosystem is thought as non-public key or centrosymmetric key cryptography. There are several normal centrosymmetric key algorithms offered. Some common ones are as: AES advanced encryption normal, 3DES triple encoding normal etc. of these normal centrosymmetric algorithm outlined are proved to be extremely secured and time tested. The most drawbacks associated with these algorithms are that the key exchange. All the communicating parties need a shared secret key. This secret's needed to exchange between them to ascertain a secured communication. thus the protection of the radial key rule depends on the protection of the key key. The Key size is often many bits long. The key size additionally depends on the rule used. The key can't be shared on-line. Additionally once an oversized range of communicating parties is there, then in this case the key exchange is unworkable & terribly tough too. All such issues are countered by the general public key cryptography. Publicly key algorithms a shared secret will be established on-line between communicating parties with none want for exchanging any secret information.

This paper describes the Implementation of Some modern RSA rule victimization Fermat's the Orem that safer and quicker.

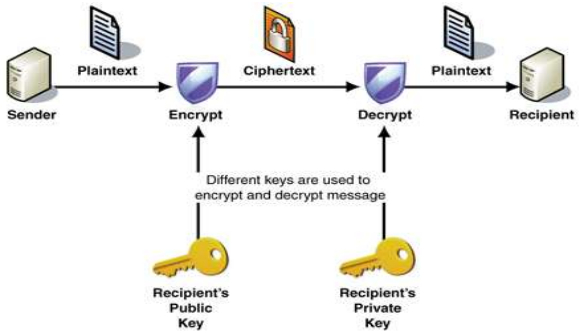

Fig. 1 public key cryptography

2. The New RSA Algorithm

The work worn out focuses on the matter of the way to prevent the quick RSA signature and decoding computation with residue number representation system speedup from a hardware fault cryptology during a extremely reliable and economical approach. It's a acknowledge proven fact that the CRT-based speedup for RSA signature has been wide used. However it's a break that a hardware fault cryptanalysis will whole break the RSA system by factorization the general public modulus. Several solutions exist to counter this drawback. However we've got determined that only a few of those existing solutions are each sound and economical. Experimental results have shown that the distended modulus approach projected by Shamir is superior to the approach of employing easy verification operate once other physical cryptanalysis. The projected work relies on the ideas of fault infective cathode-ray tube computation and fault infective cathode-ray tuberecombination.RSA is that the uneven or public key cryptography system. The security of RSA public key cryptosystem is predicated on the larger value of modulus. One in all the

most drawbacks associated to RSA cryptosystem is factorization. The authors [4] planned a replacement special purpose formula to perform factorization. This algorithm is compared with trial division algorithm TDM. The experimental results prove that the proposed algorithms runtime depends on the distinction of things and is independent of size of the modulus. Therefore it's more practical whenever factors are close to one another & in this specific case it outperforms the TDM. Giraud planned a replacement measure scheme supported the construct of Montgomery Ladder exponentiation. The proposed formula performs two standard multiplications for every little bit of exponent. Whereas the sq. and multiply formula that performs on the average 1.5 modular multiplications per little bit of the exponent. Thus the proposed technique is quicker. The authors of proposed an enhance algorithmic program for the RSA cryptosystem. This new proposed cryptosystem uses a 3rd prime quantity in scheming the value of n. this extra third prime quantity will increase the factor complexness of n. it'll give a lot of security to the RSA. The public key cryptosystem RSA is that the 1st and most well-liked cryptosystem for performing encryption and decryption of information, to stay information secret, to transfer information from one location to a different. Conjointly its best-known that the safety of RSA depends on giant factorization. If the factorization is feasible then the complete algorithmic program will become breakable. Authors planned a brand new methodology to vary the first modulus with the faux modulus. Thus if the hacker factorizes this new modulus value then he won't be ready to find the first decryption key.

However there are some Common issues in Existing RSA cryptosystem.

- The main disadvantage of RSA encryption its slower speed.
- Not secure against low decryption exponent attack
- Not secure against weiner's attack
- Not secure against common modulus attack
- Not secure against illustrious plaintext attack

2.1 The Proposed Work is as Follows:

2.1.1 Encryption Algorithm:

Step1: First select random large prime integers a and b of roughly the same size but not too close to each other.

Step 2: Calculate the product n = a*b (Ordinary integer multiplication)

Step 3: Choose a random *encryption exponent* e. It must not have any common factor with either a-1 or b-1.

Step 4: Compute ed mod (a-1) * (b-1) = 1

Step 5: Encryption Step:

$c = m^e \bmod n$ where c= cipher text

2.1.2 Decryption Algorithm:

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

Step 1: First compute X1 = cda mod a

Step 2: X2 = cdb mod b

Where da = d mod a-1 & db = d mod b-1

Step 3: Compute W = (X2 – X1) * W1 mod b

Where W1 = a mod inverse b

Step 4: Then finally compute

M= cd mod n = X1 + W * a

2.1.3 Result Of Existing and Proposed RSA Algorithm

Table 1: Result comparison

RSA	INPUT	OUTPUT	CALCULATION TIME
Existing	010101	000103060 7060301	Total time ~ 68 ms
Proposed	010101	000103060 7060301	Total time ~ 24 ms)

3. Conclusions

In this paper, the implementation of proposed rsa cryptosystems is mentioned. The issue associated with permeable RSA cryptosystem is mentioned. Conjointly our propose decryption is safer against low decryption exponentiation attack, and customary module attack. The proposed method improves the safety and decryption is quicker as compared to current variant of RSA cryptosystem.

References

[1] Kun Ma, Han Liang, and Kaijie Wu, Member, IEEE, "Homomorphism Property-Based Concurrent Error Detection of RSA: A Countermeasure to Fault Attack", IEEE TRANSACTIONS ON COMPUTERS, VOL. 61, NO. 7, JULY 2012

[2] Sung-Ming Yen, Seungjoo Kim, Seongan Lim, and Sang-Jae Moon,"RSA Speedup with Chinese Remainder Theorem Immune against Hardware Fault Cryptanalysis"IEEE TRANSACTIONS ON COMPUTERS, VOL. 52, NO. 4, APRIL 2003

[3] Prashant Sharma, "Modified Integer Factorization Algorithm using V-Factor Method", 2012 Second International Conference on Advanced Computing & Communication Technologies, IEEE 2012

[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] 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

[6] William Stallings "Network Security Essentials (Applications and Standards)", Pearson Education, 2004

[7] National Bureau of Standards, "Data Encryption Standard," FIPS Publication 46, 1977.

[8] 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.

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

[12] 1Shashi Mehrotra Seth, 2Rajan Mishra," Comparative Analysis of Encryption Algorithms

for Data Communication", IJCST Vol. 2, Issue 2, June 2011 pp.192-192.

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

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

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

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

[17] 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.

[18] Abdel-Karim Al Tamimi," Performance Analysis of Data Encryption Algorithms.