International Journal of Advanced Technology in Engineering and Science
Vol. No.5, Issue No. 05, May 2017
www.ijates.com
ijates
ISSN 2348 - 7550

IMPLEMENTATION OF RSA ALGORITHM AND MODIFIED RSA ALGORITHM METHODS:A REVIEW

Sarika Y. Bonde[1], Prof.Dr. U. S. Bhadade[2]

[1]*Research Scholar, North Maharashtra University,* Jalgaon, (M.S) (*INDIA)*

[2]*Professor and Head of IT department, S. S. B. T. College of Engineering & Technology*
Bambhori, *Jalgaon, (M.S) (INDIA)*

ABSTRACT

Now days, security is required to transmit confidential information over the network. Security is also demanding in wide range of applications. Cryptographic algorithms play a dynamic role in providing the data security against malicious attacks. RSA encryption algorithm is Public key cryptography is also called as asymmetric key cryptography.This paper presents the literature review of methods of implementation of RSA algorithm and modified RSA algorithm.

***Keywords-Cryptography, RSA*.**

I .INTRODUCTION

To send the note from one party to another intended party securely, is the work of cryptography. The cryptographic technique is also called cryptosystem or cryptographic algorithm or encryption/decryption algorithm. The algorithms in cryptography are categorized into two classes: Symmetric and Asymmetric encryption. In symmetric encryption both the sender and receiver share the same secret key. Examples are: DES, 3DES, AES etc. In asymmetric encryption the sender and receiver use a pair of keys (one key for encryption and another for decryption). Examples are RSA, Diffie-Hellman etc.

1.1 RSA ALGORITHM

RSA algorithm is a public key encryption algorithm developed by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1978. RSA is widely used Public-Key algorithm.

The RSA algorithm involves three steps: key generation, encryption and decryption [1,2].

A) KEY GENERATION

RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted by using the private key. *e*is released as the public key exponent and *d* is kept as the private keyexponent. The steps for key generation are explained below:

i. Select p and q where $p \neq q$ and both p and q are prime numbers.
ii. Determine $n = p$ x q
iii. Compute $\varphi(n) = (p\text{-}1)$ x $(q\text{-}1)$,where φ is Euler's totient function.
iv. Choose an integer e such that gcd $(\varphi(n), e) = 1$ and $1 < e < \varphi(n)$
v. Evaluate d as $d \equiv e^{-1}$ (mod $\varphi(n)$)

vi. Public Key (PU) = {e, n}

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

B) ENCRYPTION PROCESS

The steps for encryption of message in order to get the cipher-text are explained below :

i. Obtain a plain text M such that M <n.

ii. Compute the cipher text as C = M^e mod n

C) DECRYPTION PROCESS

The steps for decryption of cipher-text in order to get the original message are explained below :

i. Get the cipher text C.

ii. Calculate the plain text as M = C^d mod n

1.2 ORGANIZATION

This paper has organized into 3 sections. Section 2 presents Literature reviewon methods of Implementation of RSA algorithm andModified RSA Algorithm. In section 3 Summary of methods of Implementation of RSA algorithm and Modified RSA Algorithm is discusses.

II. LITERATURE REVIEW ON METHODS OF IMPLEMENTATION OF RSA ALGORITHM AND MODIFIED RSA ALGORITHM

Literature review on different methods of implementation of RSA algorithm and modified RSA algorithm is done as follows:

Hanae Nozaki et al.[3] has described implementation of RSA cryptosystem using the RNS Montgomery multiplication.

Milan Markovic et al.[4] has elaborated Montgomery's modular reduction algorithm and Chinese Remainder Theorem (CRT) for RSA private key operation. Possible optimization techniques for RSA algorithm realization on assembler of Texas Instruments TMS320C54x family of signal processors are considered. Obtained results justify the use of the proposed optimization methods and also show that the TMS320C54x family of signal processors is suitable for the RSA algorithm realization.

Jean-Claude Bajard and Laurent Imbert [5] has presented a new implementation of Montgomery multiplication in RNS and have shown its efficiency toward a new full RNS implementation of RSA.

VitalyYakovyna [6] has analyzed software realization of RSA public key encryption algorithm using CryptoAPI on .NET platform.

Ying-yu Cao, Chong Fu [7] has built an integrated large integer library by using C++ and gives the implementations of Miller-Rabin, extended Euclid and Montgomery algorithms for complex numeric operations in RSA. The random RSA public and private key pair with arbitrary length can be generated effectively by using the C++ large number library design by the algorithm proposed in this paper.

Sonal Sharma et al. [8] has presents a modified version of Subset-Sum problem over RSA algorithm called RSA Algorithm using Modified Subset Sum Cryptosystem. For the simulation purpose, MSSRPKC cryptosystem is implemented as a user-friendly GUI. This GUI application is implemented using JAVA BigInteger library functions.

Sami A Nagar et al. [9] has speedup the RSA algorithm by developing a new generation keys method called RSA-Key Generations Offline and saved all keys values in tables within database. The keys are generated by a program prepared in a C # language and then save these values of the keys in the databases created by SQL Server 2008 R2.

Ravi Shankar Dhakar et al. [10] has proposed the Modified version of RSA Encryption Algorithm (MREA). MREA is is based on the factoring problem, it has an additive homomorphism cryptosystem, the encryption is computed using m_1+m_2.The simulation result of the algorithm MREA, implemented in JAVA.

B.Persis Urbana Ivy et al [11] has developed modified RSA cryptosystem based on ‘n’ prime numbers and used JAVA language to get the private key and public Key.

Yezhen Liang, GuoqiangBai[12] has implement RSA as well as RSA-CRT is proposed. The proposal requires a less amount of time and energy to prevent all types of fault attacks with the absence of the public key e by taking advantage of the characteristic of the Montgomery Ladder.

CuipingShao[13]has presented an RSA implementation with FPGA, dedicated for ion fault injection experiment. Handshake protocol between the RSA circuit and the microbeam facility of IMP is designed and verified. Aswathy B.G, Resmi R.[14]has presents two architectures for FPGA implementation of modular exponentiation algorithm based on Montgomery technique- one with parallel technique and another with maximum sequential operation . Finally these architectures are analyzed with respect to area, speed, and power using Xilinx ISE.

Abdulameer K. Hussain et al**.**[15] hasproposed a method to eliminate the redundant messages occurred in the RSA method by applying the k-nearest neighbour values of either p or q or both.

Ari ShawkatTahir [16] has proposed efficient architecture to implement an optimized 1024-bit RSA encryption/decryption algorithm for restricted system using multiply and square algorithm to process the Modular exponential for encryption and decryption. The architectures have been implemented on reconfigurable platforms FPGAs. The whole system is implemented using VHDL code targeting Spartan3 (device XC3S50, package PG208, speed -4) from Xilinx. The whole design is tested using Xilinx ISE Design Suite 12.2 tool.

Xinming Huang and Wei Wang [17] has proposed an FFT-based modular multiplication and exponentiation algorithm and its hardware architecture for RSA cryptosystem with very large key size. ASIC implementations of the 8 K/12 K-bit and 48 K-bit RSA cryptosystem are presented.

RupaliVerma [18] has presents the implementation results of RSA on FPGAs based on carry save Montgomery.

Narander Kumar, PriyankaChaudhary [19] provide a modify RSA algorithm based on the n prime numbers and bit stuffing. This technique uses n prime numbers because large prime numbers are not easily factorized and bit stuffing provide extra layer of encryption by which we provide maximum security and efficiency for data over the network. The implementation is done using Net Bean IDE 8.0 software.

AsmaChaouch [20] have evaluated three famous encryption algorithms ECC, RSA and AES in terms of encryption speed, security level, encrypted JPEG image size, key generation, time and throughput. The software application is implemented using C programming.

Somesh Kumar [21] haveimplementedthe RSA algorithm with feed forward artificial neural network using MATLAB.

III . SUMMARY OF IMPLEMENTATION OF RSA ALGORITHM AND MODIFIED RSA ALGORITHM

Modified version of RSA algorithm was developed by many researchers.The goal of this paper is to observe the different implementation methods of RSA algorithmand modified RSA algorithm, which are as shown in table 1.

Table 1: Implementation methods of RSA algorithm and modified RSA algorithm

Hardware Implementation	Software Implementation
RNS Montgomery multiplication[3,5]	.NET platform[6,19]
Texas Instruments TMS320C54x family of signal processors[4]	C++[7], C programming [9,20]
Montgomery Ladder [12]	JAVA language [8,10,11]
VLSI design using FPGA [13,14,16,18]	MATLAB [21]
VLSI design using ASIC (Application Specific Integrated Circuit)[17]	Xilinx ISE [13,14,16]

VI .CONCLUSION

In this paper different method of implementation of RSA algorithm and modified RSA algorithmhas been surveyed and conclude that TITMS320C54x signal processors,VLSI design using FPGA,VLSI design using ASIC, RNS Montgomery multiplication are suitable for hardwareimplementation of RSA algorithm. For software implementationof RSA algorithmthe platform used is .NET, C, C++, Xilinx ISE,MATLAB and JAVA.Each technique is unique, which might be used for different applications. Everyday new approach is evolving hence fast and secure RSA algorithm always work out with high rate of security.

REFERENCES

[1] Bruce Schneir, “Applied Cryptography”, 2nd edition, John Wiley & Sons, 2007.

[2] William Stallings, “Cryptography and Network Security”, Pearson Education, Fourth Edition, 2007.

[3] Hanae Nozaki, Masahiko Motoyama, Atsushi Shimbo, and Shinichi Kawamura, “Implementation of RSA Algorithm Based on RNS Montgomery Multiplication”, CHES 2001, LNCS 2162, Springer-Verlag Berlin Heidelberg 2001, pp. 364–376.

[4] Milan Markovic, TomislavUnkasevic, GoranDordevic, “RSA ALGORITHM OPTIMIZATION ON ASSEMBLER OF TI TMS320C54X SIGNAL PROCESSORS”, IEEE 11th European Signal Processing Conference, 2002 , 3-6 September 2002, pp.1-4.

[5] Jean-Claude Bajard and Laurent Imbert, “A Full RNS Implementation of RSA”, IEEE TRANSACTIONS ON COMPUTERS, VOL. 53, NO. 6, JUNE 2004, pp.- 769-774.

[6] VitalyYakovyna, DmytroFedasyuk, MaxymSeniv, OrestBilas , “The Performance Testing of RSA Algorithm Software Realization”, CADSM’2007, February 20-24, 2007, Polyana, UKRAINE,pp.-390-392.

[7] Ying-yu Cao, Chong Fu, “An Efficient Implementation of RSA Digital Signature Algorithm”, IEEE International Conference on Intelligent Computation Technology and Automation, 2008, pp.100-103

[8] Sonal Sharma, Prashant Sharma, Ravi Shankar Dhakar, “RSA Algorithm Using Modified Subset Sum Cryptosystem”, IEEE International Conference on Computer and Communication Technology(ICCCT), 2011, p.p. 457-461.

[9] Sami A. Nagar, SaadAlshamma, “High Speed Implementation of RSA Algorithm with Modified Keys Exchange”, IEEE6th International Conference on Science of Electronics, Technologies of Information and Telecommunications (SETIT), March 2012, p.p.639- 642.

[10] Ravi ShankarDhakar, Amit Kumar Gupta, Prashant Sharma, “Modified RSA Encryption Algorithm” (MREA), IEEE Second International Conference on Advanced Computing & Communication Technologies, 2012, p.p. 426-429.

[11] B. Persis Urbana Ivy, PurshotamMandiwa. Mukesh Kumar “A modified RSA cryptosystem based on ‘n’ prime numbers”, International Journal of Engineering And Computer Science, Vol.1, Issue 2, November 2012 pp. 63-66.

[12] Yezhen Liang, GuoqiangBai, “A New FA and SPA Resistant Implementation of RSA”, IEEE 3rd International Conference on Computer Science and Network Technology, Dalian, China, 2013, pp.893-897.

[13] Cuiping Shao, Huiyun Li, Xiaolong Zhang, “Cryptographic Implementation of RSA for Ion Fault Injection Attack”, IEEE Consumer Communications and Networking Conference (CCNC 2014) Special Seesion: Big Data Security and Privacy, 2014, pp.-791-794.

[14] Aswathy B.G, Resmi R, “Modified RSA Public Key Algorithm”, IEEE First International Conference on Computational Systems and Communications (ICCSC), 17-18 December 2014 , Trivandrum, pp.252-255.

[15] Abdulameer K. Hussain, “A Modified RSA Algorithm for Security Enhancement and Redundant Messages Elimination Using K-Nearest Neighbor Algorithm”,IJISET – International Journal of Innovative Science, Engineering & Technology, Vol. 2, Issue 1, January 2015.ISSN 2348 – 7968, p.p. 159-163.

[16] Ari ShawkatTahir, “Design and Implementation of RSA Algorithm using FPGA”, INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY Vol. 14, No. 12, ISSN 2277-3061,September22, 2015, pp. 6361- 6367.

[17] Xinming Huang and Wei Wang, , “A Novel and Efficient Design for an RSA Cryptosystem With a Very Large Key Size”, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—II: EXPRESS BRIEFS, VOL. 62, NO. 10, OCTOBER 2015, pp. 972-976.

[18] RupaliVerma, MaitreyeeDutta, RenuVig, “FPGA Implementation of RSA based on Carry Save Montgomery Modular Multiplication”, IEEE International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT),2016, pp.1-6

[19] Narander Kumar, PriyankaChaudhary, “Implementation of Modified RSA Cryptosystem for Data Encryption and Decryption based on n Prime number and Bit Stuffing”, International Conference on Information and Communication Technology for Competitive Strategies (ICTCS-2016), March 04-05, 2016, Udaipur, India,pp.1-6.

[20] AsmaChaouch, BelgacemBouallegue, OuniBouraoui, “Software Application for Simulation-Based AES,RSA and Elliptic-Curve Algorithms”, IEEE 2nd International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), March 21-24, 2016, Monastir, Tunisia, pp.77-82.

[21] Somesh Kumar, RajkumarGoel , “Implementation of RSA with Feed-forward NeuralNetwork using MATLAB”, International Journal of Computer Applications (0975 – 8887),Volume 148 – No.2, August 2016, pp.22-26.