UNIVERSITI PUTRA MALAYSIA

MODIFIED MILLER-RABIN PRIMALITY TEST ALGORITHM TO DETECT PRIME NUMBERS FOR GENERATING RSA KEYS

BALKEES MOHAMED SHEREEK

FSKTM 2016 21

MODIFIED MILLER-RABIN PRIMALITY TEST ALGORITHM TO DETECT PRIME NUMBERS FOR GENERATING RSA KEYS

By

BALKEES MOHAMED SHEREEK

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Master of Science

June 2016

`

DEDICATIONS

To My Family and Friends

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in Fulfilment of the requirement for the degree of Master of Science

MODIFIED MILLER-RABIN PRIMALITY TEST ALGORITHM TO DETECT PRIME NUMBERS FOR GENERATING RSA KEYS

By

BALKEES MOHAMED SHEREEK

June 2016

Chairman : Madam Hajah Zaiton Muda
Faculty : Computer Science and Information Technology

A prime number is a number that is only divisible by one and itself, which is essentially saying that it has no divisor. Prime numbers are important in the security field because many encryption algorithms are based on the fact that it is very easy to multiply two large prime numbers and get the result, while it is extremely computer-intensive to do the reverse. The Rivest-Shamir-Adleman algorithm (RSA) is one of the most well-known and strongest public key cryptography algorithms. The security of the RSA depends on the two prime numbers namely p and q and to generate them is an extremely time consuming process (Fu and Zhu, 2008). An efficient method for generating large random prime numbers within shortest time is thus a crucial challenge for researchers (Bahadori et al., 2010; Saveetha and Arumugam, 2012). The objective of this study is to reduce the time taken in finding prime numbers p and q for RSA.

To achieve the objective, the Miller-Rabin primality test was modified by adding few tests in the original Miller-Rabin. The prime numbers with the size of 256, 512, and 1024 bits are generated using the proposed modified algorithm. The performance of the proposed modified Miller-Rabin was analysed in terms of the time taken to detect the prime numbers and compare the time taken for generating the prime numbers using original Miller-Rabin method. The comparison between the original Miller-Rabin and the modified Miller-Rabin primality test methods show the difference of time to generate prime numbers and the modified method shown the better results. The study also reviewed previous works and the modified Miller-Rabin primality test method has shown the better results in compared to them.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk Ijazah Master Sains

ALGORITMA UJIAN KEPERDANAAN MILLER-RABIN DIUBAHSUAI UNTUK MENGESAN NOMBOR PERDANA DALAM MENJANA KUNCI-KUNCI RSA

Oleh

BALKEES MOHAMED SHEREEK

Jun 2016

Pengerusi : Hajah Zaiton Muda
Fakulti : Sains Komputer dan Teknology Maklumat

Nombor perdana adalah nombor yang hanya boleh dibahagikan dengan nombor satu dan nombor sendiri yang pada dasarnya ia adalah nombor yang tidak mempunyai pembahagi. Nombor perdana adalah penting dalam bidang keselamatan kerana banyak algoritma penyulitan adalah berdasarkan kepada fakta bahawa nombor perdana adalah sangat mudah untuk mendarab dua nombor perdana yang besar dan memperoleh hasil, manakala amat sukar untuk melakukan sebaliknya. Algoritma Rivest-Shamir-Adleman (RSA) adalah antara algoritma kriptografi kunci umum yang terkenal dan sukar untuk dicerobohi. Keselamatan RSA bergantung kepada saiz kedua-dua nombor perdana iaitu p dan q dan untuk menjananya merupakan satu proses yang memakan masa yang sangat lama (Fu dan Zhu, 2008). Satu kaedah yang berkesan untuk menjana nombor perdana rawak yang besar dalam masa yang singkat merupakan satu cabaran yang besar bagi para penyelidik (Bahadori et al., 2010; Saveetha dan Arumugam, 2012). Objektif kajian ini adalah untuk mengurangkan masa yang diambil dalam mencari nombor perdana p dan q untuk RSA.

Untuk mencapai objektif tersebut, ujian keperdanaan algoritma Miller-Rabin telah diubahsuai dengan menambah beberapa pengujian dalam algoritma Miller-Rabin yang asal. Nombor perdana dengan saiz 256, 512 dan 1024 bit telah dijana menggunakan algoritma diubahsuai yang dicadangkan. Prestasi bagi Miller-Rabin diubahsuai yang dicadangkan telah dianalisis dari segi masa yang diambil untuk mengesan nombor perdana dan membandingkan masa yang diambil untuk menjana nombor perdana menggunakan algoritma Miller-Rabin yang asal. Perbandingan ujian keperdanaan antara algoritma Miller-Rabin yang asal dan diubahsuai menunjukkan perbezaan masa untuk menjana nombor perdana dan kaedah yang diubahsuai menunjukkan keputusan yang lebih baik. Kajian juga dilakukan ke atas kerja-kerja sebelumnya dan algoritma pengujian Miller-Rabin yang diubahsuai telah menunjukkan keputusan yang lebih baik berbanding dengan mereka.

ACKNOWLEDGEMENTS

I would like to express my sincere appreciation and deepest gratitude to my supervisor Madam Zaiton Muda and my committee member Dr. Sharifah Md.Yasin for their continuous encouragement, valuable advice, and guidance throughout this research. I really appreciate the freedom they provided while I was working on my research and their openness to new ideas.

My special thanks go to my dearest friends who were always willing to help and share their ideas and knowledge even when busy with their own research. I will always treasure their friendship.

Most of all, I would like to express my sweetest appreciation to my family for their affectionate support, patience, and encouragement. Their prayers and good wishes constantly helped me to be strong, especially in difficult times. I am forever grateful and indebted to them.

I certify that a Thesis Examination Committee has met on 23 June 2016 to conduct the final examination of Balkees Mohamed Shereek on her thesis entitled "Modified Miller-Rabin Primality Test Algorithm to Detect Prime Numbers for Generating RSA Keys" in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Master of Science.

Members of the Thesis Examination Committee were as follows:

Azizol bin Hj Abdullah, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Zuriati binti Ahmad Zukarnain, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Majid Bakhtiari, PhD
Senior Lecturer
Universiti Teknologi Malaysia
Malaysia
(External Examiner)

ZULKARNAIN ZAINAL, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 23 August 2016

This thesis was submitted to the senate of University Putra Malaysia and has been accepted as fulfilment of the requirement for the Master of Science. The members of the Supervisory Committee were as follows

Zaiton Muda,PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Sharifah Md.Yasin, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

BUJANG BIN KIM HUAT, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice- Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: ___________________________ Date: ___________________________

Name and Matric No: ____________________________________

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) were adhered to.

Signature: ______________________________

Name of Chairman of Supervisory Committee: ______________________________

Signature: ______________________________

Name of Member of Supervisory Committee: ______________________________

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
AKS	Agrawal–Kayal–Saxena
BC	Before Christ
CPU	Central Processing Unit
CRT	Chinese Reminder Theorem
DES	Data Encryption Standard
EAMRSA	Encrypt Assistant Multi-Prime RSA
ECC	Elliptic Curve Cryptography
GCD	Greatest Common Divisor
GNFS	General Number Filed Sieve
IFP	Integer Factorization Problem
LFSR	Linear feedback Shift Register
MREA	Modified RSA Encryption Algorithm
PDA	Personal Digital Assistant
PKC	Public Key Cryptography
PR	Private Key
PRNG	Pseudo Random Number Generator
PU	Public Key
RNS	Residue Number System
RSA	Rivest, Adi Shamir, Leonard Adleman
SRNN	Short Range Natural Number
SQL	Structured Query Language
TRNG	True Random Number Generator
TTA	Transport Triggered Architecture

`

CHAPTER 1

INTRODUCTION

1.1 Background

A prime number is a number that is only divisible by one and itself meaning that, it has no divisor. Primes have an important role in number theory because they are the building blocks of whole numbers. The most notable practical use of prime numbers is in the area of cryptography. All integer numbers (except 0 and 1) are made up of primes resulting having to deal with them a lot in number theory or cryptography. Primes are important in the security field as the security of many encryption algorithms are based on the fact that it is very fast to multiply two large prime numbers and get the result, while it is extremely computer-intensive to do the reverse. When we have a number which is the product of two primes, finding them is extremely difficult. This problem is called prime factorization and finding an algorithm which does it faster is one of the unsolved problems of computer science. Many popular algorithms used in public-key cryptography derive from the fact that integer factorization is a "hard" problem.

However, finding large prime is very difficult, the most suitable method to select a prime number is by using a prime generating algorithm and need to conduct a prime test. A primality test is an algorithm used to determine whether the input number is prime or not. There are two main kinds of prime test algorithms, namely probabilistic prime test and the true prime test or deterministic prime test. The probable prime test is very fast and simple to conduct and is done repeatedly to achieve an accurate result. The more common probabilistic prime tests are the Fermat's little theorem, Miller-Rabin, and Solvay-Strassen test. A true prime test is considerably more accurate, but because of its time consuming calculation, it not useful in practical applications.

Cryptography the science of secret communication where the basic service involves the ability to prove data protection between participants in a particular way. It consists of two elements; that is the creation of a secret code called *cryptography* and the breaking of the secret code or *cryptanalysis*, as well as the study of mathematical techniques related to information security. Some technical terms related to cryptography are *plain text*, *cipher text*, *encryption*, and *decryption.* A message in its original form is called a *plain text* while its conversion into a particular format based on some mathematical formula is called *encryption.* A by-product of encryption is called a *cipher text* which is an unreadable format not involving any proper calculations. The conversion of cipher text into an original readable plain text format is called *decryption.*

Plain text *Encryption* → Cipher Text *Decryption* → Plain Text

Security often requires safeguarding data from unauthorized access. In the world of the Internet, since computers are connected to each other, most of them expose themselves and the communication channels that they use. Cryptography is the most powerful and common method to address this confidentiality issue (Gupta et al., 2012). It is used to encrypt the data either to be kept in a remote access storage space like cloud applications or travel through the communication channel to ensure the protection of data against illegal access. Authentication and integrity are some other crypto services. It is very difficult to authenticate a party while different parties attempt to access the information from the same system. Data integrity and non-reputation is achieved by using digital signatures to ensure that the data has not been altered since being generated by the source. A typical cryptographic system involves both an algorithm and a secret value which is referred to as the Key.

Cryptography is classified into symmetric or secret key and asymmetric or public key cryptography. In former, the key is shared between the two parties (sender and receiver) and, must be kept confidential. The encryption and decryption is done using the same key. Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are examples of secret key cryptography. In asymmetric cryptography, two keys are used, one for encryption, which is known to all, and the other for decryption which is known only to an authorized person (the receiver). The Rivest-Shamir-Adleman algorithm (RSA) is an example of an asymmetric key cryptography. The main difference between the two systems (symmetric and asymmetric) is in the way of keeping the key. One system is available to share the key (symmetric) and the other (asymmetric) does not although both systems complement each other (Sing et al., 2014)

1.2 Motivation

Today, the Internet and its applications are an important and ubiquitous part of daily life with its uses being pervasive and interconnected. Everything is available with the stroke of the keypad, and the Internet is easy to use, readily available, and facilitates the performance of faster services. All the traditional systems are changed into the internet world. Presently we cannot live nor do anything without an internet application. Whether we are aware of it or not, most of us use some kind of internet application in our daily life. Table 1.1 shows the current and earlier methods of doing selected certain activities.

Table 1.1: Traditional and Current Ways of Doing Things

Traditional Method	Current Method
Letter and Fax	Electronic Mail
Storage on Device	Data storage on remote area
Limited storage	Unlimited data storage
Crowded malls	Internet shopping
Wait in line in a queue	24-hour online banking
Using pen	Digital signature
Using the telephone	Internet voice and video call

Security is a major challenge in the IT world and cryptography technology helps to protect privacy and allows the sharing and accessing of needed information. Using proper cryptographic methods is extremely important to accomplish various communication activities. It has a wide range of applications in internet security, wireless communications, and telecommunications. The handling of sensitive data through the internet, especially in the banking and military fields, requires a high level of security, which cryptography provides.

In the cyber world, protecting data (information security) is very important. There are many ways to hack data, and the cryptosystem accepts this challenge and plays an important role in modern communications to provide secure communication. This is done on the basis of an algorithm which deals with encryption and decryption operations. Different sets of public and private key cryptography have been invented for information security at different levels. The key features of public key cryptography are that encryption and decryption are done using two different keys to help prevent some attacks from occurring because of the usage of a single key for encryption and decryption (Mahalle, 2013) .

To accomplish the various communication security goals, different cryptographic technique can be used. Moreover, such technique s are necessary for a wide range of applications such as internet applications, wireless communications, and telecommunications. Currently, the most widely used and common public key system is RSA (Zhou and Tang, 2011) which is the first public key cryptography method. It is an asymmetric cryptographic system based on number theory.

The main motivation of this work relates to:

- The importance of the internet in the present day
- There is a high probability of data information in computers being hacked. The networks transmit very sensitive data on banking, accounting, auditing and as such, it is essential to construct a security system for computer networks to protect data during transmission. In this work, the

most popular method selected to address security issues is the cryptographic algorithm RSA.

- RSA security is based on the integer factorization problem.

1.3 Problem Statement

The security of RSA is based on the Integer Factorization Problem (IFP) and this is a well-known mathematical issue (P. Sharma, 2012). The IFP can be solved by choosing large sized keys (Fu and Zhu, 2008). Two prime numbers say p and q are the backbone of RSA to ensure its security of RSA. The modulus n should be large enough, where n is the product of the prime numbers p and q. The key size determines the level of security of the algorithm, and the bigger it is the higher the level of security (Wang et al., 2013). The RSA algorithm could be easily attacked in certain considered conditions, it relies for its security on the prime numbers selection. The generation of a secure key pair which is based on finding a pair of large prime numbers is an indispensable part of RSA in creating a secure channel (Bahadori et al., 2010). The selection of large prime numbers (say p and q) can provide security where the value of p and q implicitly affects the modulus n ($n=p*q$) which is the component of the public (e,n) and private (d,n) keys (Frunza and Scripcariu, 2007).

If we generate fairly large key size numbers randomly it is much harder to predict and take more time to generate keys. But it is quite difficult to find out large prime number. The candidate (p and q) must be tested for primality in order to be useful for the generation of a RSA key pair, and the selection of the prime number is a critical step in RSA (Shams et al., 2012). However finding large primes are the most time consuming processing in RSA key generation (Lu et al., 2002) and having an efficient method to generate large random prime numbers helps to reduce the total time required to generate the key (Bahadori et al., 2010 ; Saveetha and Arumugam, 2012).

On the basis of the above discussion, we can conclude that the security of the RSA depends on the two prime numbers the generation of which is an extremely time consuming process. An efficient method for generating large random prime numbers within shortest time is thus a crucial challenge for researchers.

1.4 Research Objective

In order to obtain large sized public and private keys, the prime numbers p and q should be large enough to ensure that the module n is large enough. As such the main objective of this work is

- To reduce the time taken in finding prime numbers p and q for RSA by improving the Miller-Rabin algorithm.

1.5 Research Questions

- Does the propose algorithm reduce the key generation time?
- Does the propose algorithm overcome the time consuming issue of finding large prime numbers?

1.6 Scope

In this work the Miller-Rabin primality test which is one of the most popular primality test algorithms is modified to generate large sized prime numbers within a minimal time for the purpose of generating the key pair of an RSA. Other primality algorithms also exist such Fermat’s little theorem and the sieve of Eratosthenes. After conducting a study on the above mentioned algorithms a modified Miller Rabin primality test is proposed to achieve the objective of this research.

1.7 Research Contribution

This work points out the significant problems associated with prime number generation within a minimal time period. Large sized prime numbers have an important role in the data communication field and network security. In this work such prime numbers are used for generating keys for RSA. The use of proposed modified Miller-Rabin test can help generate large and small sized prime numbers quickly for use in any field and any system such as Elliptic Curve (ECC), which also work with prime numbers. RSA is one of the fields where the proposed modified Miller–Rabin test can be applied, and this can be used in in any mathematic works related to prime number generation.

1.8 Thesis Organization

This thesis comprises six chapters, including introductory chapter. They are:

Chapter 2: discuss crypto system, RSA and its security issues and attacks. It provides a clear picture on the importance of prime numbers, primality tests, and the different primality testing methods used to generate prime numbers. This chapter also discusses some existing works related to RSA and prime numbers.

Chapter 3: discusses the methodology of the work and the five major phases of the work, as well as the requirement analysis of the research in the first phase. An analysis of existing algorithms is included in the second phase followed by an improved algorithm in phase three. Phase four covers analysing proposed modified algorithm and the final results and documentation are on phase five.

Chapter 4: this chapter relates to the phase two of the research methodology that is analysis of existing algorithms. In this chapter the three existing algorithms namely, Sieve of Eratosthenes, Fermat's little theorem, and the Miller-Rabin are analyse to know their limitations and advantages.

Chapter 5: focus on the proposed modified method, which include the implementation of the proposed method and compare the result of the proposed method with existing methods and some previous works.

Chapter 6: The conclusion and some area for future work for this research including some enhancements are discussed.

REFERENCES

A.jasim. (2012). Design and Implement Fast Algorithm of RSA Decryption using java. *Al-Mansour Journal*, (17), 151–166.

Al Zakir Hossain, A. (2007). *Implementation of the AKS Primality Testing Algorithm* (Master's thesis). University of Asia Pacific, Dhaka, Bangladesh.

Bahadori, M., Mali, M. R., Sarbishei, O., Atarodi, M., & Sharifkhani, M. (2010). A novel approach for secure and fast generation of RSA public and private keys on SmartCard. In *NEWCAS Conference (NEWCAS), 2010 8th IEEE International* (pp. 265–268). IEEE.

Bordevic, G., & Markovic, M. (2007). On optimization of Miller-Rabin primality test on TI TMS320C54x signal processors. In *Systems, Signals and Image Processing, 2007 and 6th EURASIP Conference focused on Speech and Image Processing, Multimedia Communications and Services. 14th International Workshop on* (pp. 229–232). IEEE.

Cagrici, G. (2005). *An analysis of key generation efficiency of RSA cryptosystem in distributed environments* (Master's thesis). İzmir Institute of Technology, Izmir,Turkey.

Cohen, A. E., & Parhi, K. K. (2011). Architecture Optimizations for the RSA Public Key Cryptosystem. *Circuits and system Magazine,IEEE, 11(4)*, 24-34.

Dongjiang, L., & Yandan, W. (2012). An Optimization Algorithm of Rsa Key Generation in Embedded System. *Journal of Theoretical and Applied Information Technology*, *46*(1).

Dongjiang, L., Yandan, W., & Hong, C. (2012). The Research on Key Generation in RSA Public-Key Cryptosystem. *2012 Fourth International Conference on Computational and Information Sciences*, 578–580. doi:10.1109/ICCIS.2012.348

Frunza, M., & Scripcariu, L. (2007). Improved RSA Encryption Algorithm for Increased Security of Wireless Networks,signals,circuits and systems. In *ISSCS 2007. International Symposium on* (Vol. 2, pp. 1–4). IEEE.

Fu, C., & Zhu, Z.-L. (2008). An efficient implementation of RSA digital signature algorithm. In *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08. 4th International Conference on* (pp. 1–4). IEEE.

Garg, D., & Verma, S. (2009). Improvement over Public Key Cryptographic Algorithm Fartorsnce exprpoadsongeent information. *Advance Computing Conference, 2009. IACC 2009. IEEE International*, (March), 6–7.

Gauss, C. F. (2012). Implementation of RSA Algorithm using Elliptic Curve Algorithm for Security and Performance. *International Journal of Scientific & Technology Research*, *1*(4).

Gupta, V., Singh, G., & Gupta, R. (2012). Advance cryptography algorithm for improving data security. *International Journal of Advanced Research in*

Computer Science and Software Engineering, *2*(1).

Huang, X., & Wang, W. (2015). A Novel and Efficient Design for an RSA Cryptosystem With a Very Large Key Size. *IEEE Transactions on Circuits and Systems SYSTEMS—II: EXPRESS BRIEFS*, *62*(10), 972–976.

Hurd, J. (2003). Verification of the Miller – Rabin probabilistic primality test, *56*, 3–21. doi:10.1016/S1567-8326(02)00065-6

Jahan, I., Asif, M., & Rozario, L. J. (2015). Improved RSA cryptosystem based on the study of number theory and public key cryptosystems. *American Journal of Engineering Research*, *4*(1), 143–149.

Jaiswal, R. J. (2014). Reformed RSA algorithm based on Prime Number. *International Journal of Computer Applications (0975 – 8887)*, 23–26.

Jamgekar, R. S., & Joshi, G. S. (2013). File Encryption and Decryption Using Secure RSA. *International Journal of Emerging Science and Engineering (IJESE)*, *1*(4), 11–14.

Losetti. (2013). An Enhanced RSA Algorithm for Low Computational Devices. *International Journal Advanced Research and Innovation*, *1*, 114–118.

Lu, C., dos Santos, A. L. M., Pimentel, F. R., Santos, A. L. M., & Pimentel, F. R. (2002). Implementation of fast RSA key generation on smart cards. *Proceedings of the 2002 ACM Symposium on Applied Computing - SAC '02*, 214. doi:10.1145/508832.508837

Mahajan, S., & Easo, S. (2012). Performance Evolution of RSA and New Cryptosystem. *Nternational Journal of Emerging Technology and Advanced Engineering*, *2*(3), 279–283.

Mahalle, V. S. (2013). Enhancing Data Security in the Cloud using Security (RSA) Algorithm. *Internatonal Journal Of Computer Science And Applications*, *6*(2), 70-75.

Meelu, P., & Meelu, R. (2012). Implementation of Public Key Cryptographic System : RSA. *International Journal of Information Technology and Knowledge Management*, *5*(2), 239–242.

Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2010). *Handbook of applied cryptography*. CRC press.

Nagar, S. A., & Alshamma, S. (2012). High Speed Implementation of RSA Algorithm with Modified Keys Exchange. *Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), 2012 6th International Conference on*, 1–4.

Paar, I. C., & Pelzl, I. J. (2010). Introduction to Public-Key Cryptography. In *Understanding Cryptography* (pp. 149–171). Springer.

Pateriya, R. K., Rana, J. L., Shrivastava, S. C., & Patel, J. (2009). A Proposed Algorithm to improve security & Efficiency of SSL-TLS servers using Batch RSA decryption. *International Journal of Computer Science and Information*

Security, *3*(1), 1–5.

Pellegrini, A., Bertacco, V., & Austin, T. (2010). Fault-based attack of RSA authentication. *2010 Design, Automation & Test in Europe Conference & Exhibition (DATE 2010)*, 855–860. doi:10.1109/DATE.2010.5456933

Peng, C., & Yang, C. (2007). Design and Implementation for Integer Factorization and Primality Testing Tools with Elliptic Curve on Windows Platforms. *SCIS 2007, The Symposium on Cryptography and Information Security*.

Peng, J., & Wu, Q. (2008). Research and Implementation of RSA Algorithm in Java. *2008 International Conference on Management of E-Commerce and E-Government*, (5), 359–363. doi:10.1109/ICMECG.2008.17

M. Perrenoud (2009). *Randomized and Deterministic Primality Testing*. Retrieved fromhttp://algo.epfl.ch/_media/en/projects/bachelor_semester/randomized_and_deterministic_primality_testing.pdf

Rahman, M. M., Rokon, I. R., & Rahman, M. M. (2009). Efficient hardware implementation of RSA cryptography. *2009 3rd International Conference on Anti-Counterfeiting, Security, and Identification in Communication*, 316–319. doi:10.1109/ICASID.2009.5276895

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120–126. doi:10.1145/359340.359342

Robinson, J. (2011). *Fermat's little theorem* (Doctoral dissertation). University of Arizona, Tucson, United States.

Saveetha, P., & Arumugam, S. (2012). Study on Improvement in RSA Algorithm and its Implementation. *International Journal of Computer & Communication Technology*, (6), 975–7449.

Sayed, R. salah, Aziem, M., & Gomaa, M. ali. (2008). An Efficient Signature System using Optimized RSA Algorithm. *International Journal of Computer Science and Network Security*, *8*(12), 343.

Shams, R., Khan, F. H., Jillani, U., & Umair, M. (2012). Introducing Primality Testing Algorithm with an Implementation on 64 bits RSA Encryption Using Verilog. *SSU Res,J.Of Engg & Tech*, *2*(1), 12–17.

Sharma, P. (2012). Implementation of RSA Algorithm for Security and Performance Enhancement. *International Journal of Advances in Engineering, Science and Technology*, *2*(2), 61–65.

Sharma, S. (2012). Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm. *International Journal of Advanced Research in Computer Science and Software Engineering*, *2*(8), 134–138.

Shen, G., Liu, B., & Zheng, X. (2009). Research on Fast Implementation of RSA with Java. *Nanchang, PR China*, *8*, 186–189.

Shinde, G. N., & Fadewar, H. S. (2008). Faster RSA Algorithm for Decryption Using

Chinese Remainder Theorem. *ICCES: International Conference on Computational & Experimental Engineering and Sciences*, *5*(4), 255–261.

Singh, A., Vaish, A., & Keserwani, P. K. (2014). Information Security : Components and Techniques. *International Journal Advanced Research in Computer Science and Software Engineering*, *4*(1), 1072–1077.

Tripathi, R. (2014). International Journal of Advanced Research in Computer Science and Software Engineering Critical Analysis of RSA Public Key Cryptosystem, *4*(7), 83–87.

Tripathi, R., & Agrawal, S. (2014). Critical Analysis of RSA Public Key Cryptosystem. *International Journal of Advanced Research in Computer Science and Software Engineering*, *4*(7), 83–87.

Vishak, M., & Shankaraiah, N. (2012). Implementation of Rsa Key Generation Based on RNS Using Verilog. *International Journal of communication Network Security, (4), 1–5*.

Wang, H., Song, Z., Niu, X., & Ding, Q. (2013). Key generation Research of RSA Public Cryptosystem and Matlab Implement. In *Sensor Network Security Technology and Privacy Communication System (SNS & PCS), 2013 International Conference on* (pp. 125–129). IEEE.

Wang Hsiu. (2000). *Speed improvements for the RSA encryption method (*Doctoral dissertation, Edinburgh Napier University).

Xiang, G., & Cui, Z. (2012). The Algebra Homomorphic Encryption Scheme Based on Fermat's Little Theorem. *2012 International Conference on Communication Systems and Network Technologies*, 978–981. doi:10.1109/CSNT.2012.208

Zhou, X., & Tang, X. (2011). Research and implementation of RSA algorithm for encryption and decryption. *Proceedings of 2011 6th International Forum on Strategic Technology*, 1118–1121. doi:10.1109/IFOST.2011.6021216