UNIVERSITI TEKNOLOGI MARA

TECHNICAL REPORT

MODIFIED MULTI-PRIME RSA USING DISCRIMINANT OF A QUADRATIC AND CHINESE REMAINDER THEOREM

(NUR FATIMAH BINTI KABULANTO) – (2016352065)

(FARAH AINA BINTI ABDUL RAZAK) – (2016726017)

Report submitted in partial fulfillment of the requirement
For the degree of
Bachelor of Science (Hons.)(Computational Mathematics)
Faculty of Computer and Mathematical Sciences

DECEMBER 2018

Table of Contents

ACKNOWLEDGEMENTS iii

ABSTRACT iv

CHAPTER ONE 1

1.0 INTRODUCTION 1

1.1 Objective 2

1.2 Problem statement 2

1.3 Scope 2

1.4 Benefit 3

1.5 Significance 3

CHAPTER TWO 4

2.0 BACKGROUND THEORY AND LITERATURE REVIEW 4

CHAPTER THREE 6

3.0 METHODOLOGY 6

3.1 The Mathematical Primitives 6

3.1.1 Fundamental Theorem of Arithmetic 6

3.1.2 Euclidean Theorem 6

3.1.3 Fermat's Little Theorem 8

3.1.4 Euler's Theorem 8

3.1.5 Chinese Remainder Theorem 9

3.2 RSA Algorithm 10

3.2.1 Key Generation 10

3.2.2 Encryption Algorithm 11

3.2.3 Decryption Algorithm 11

3.3 Proposed model by Kamardan, Aminudin, Che-Him, Sufahani, Khalid, Roslan (2018) ... 12

3.3.1 Key Generation Operation 12
3.3.2 Encryption Operation 13
3.3.3 Decryption Operation 13
CHAPTER FOUR 14
4.0 IMPLEMENTATION 14
4.1 Proposed Model 14
4.1.1 Key Generation Operation 14
4.1.2 Encryption Operation 15
4.1.3 Decryption Operation 15
4.2 FLOWCHART OF PROPOSED MODEL 17
Figure 1 17
4.3 EXAMPLE OF PROPOSED MODEL 18
4.3.1 Key generation 18
4.3.2 Encryption Process 19
4.3.3 Decryption Process 19
CHAPTER FIVE 20
5.0 RESULTS AND DISCUSSION 20
Table 2. 20
6.0 CONCLUSION AND RECOMMENDATION 22
REFERENCES 23

ACKNOWLEDGEMENTS

IN THE NAME OF ALLAH, THE MOST GRACIOUS, THE MOST MERCIFUL

Firstly, we are grateful to Allah S.W.T for giving our strength to complete this project successfully.

We would like to express our deep gratitude to our supervisor, Nur Lina binti Abdullah, whose contribution in stimulating suggestions and encouragement helped us to coordinate our project especially in writing this report and who gave the permission to use all required equipment and the necessary materials to complete the report. Special thanks go to my teammate who give cooperation to assemble the parts and gave suggestion about the project and to our family, friends and for those who helped us in our task and have patiently extended all sorts of help for accomplishing this project. Last but not the least, we wants appreciates the guidance given by panels especially in our project presentation that has improved our presentation skills thanks to their comment and advice.

ABSTRACT

RSA is one public key Cryptosystem to secure information and communication from third parties and it can be factor by user authentication. In order to achieving security from unwanted users, the message will encode to make it unreadable format. RSA Cryptosystem is generally utilized in the popular implementation of public key Cryptosystem. In RSA Cryptosystem there are two completely different keys are generated, one key's utilized in encryption data and other corresponding key's utilized for decryption data. Many innovative ideas for RSA Cryptosystem have been presented for the past two decades, and many corresponding problems remain to be resolved. Therefore, in this study we introduce a modified RSA Cryptosystem using a hybrid of discriminant quadratic and Chinese Remainder Theorem. The securities of these models are based on the difficulties of solving multiple hard problems simultaneously. The newly algorithm will not only increase the security of system but also has high correct ability. Therefore, we implied this new formula to improve the weakness of RSA Cryptosystem in decryption and make the security of system to be more advanced.