

**UNIVERSITI TEKNOLOGI MARA**

**TECHNICAL REPORT**

**IMPROVEMENT OF KEY EXCHANGE CRYPTOSYSTEM  
USING MATRIX WITH THREE-PASS PROTOCOL**

**PS39S18**

**ANNUUR ZAKIAH BINTI ZAINOL  
FARAH DEENA BINTI MOHAMAD FISAL  
FATIN NUR ATHIRAH BINTI MOHD RADZI**

**Bachelor of Science (Hons.) Computational Mathematics  
Faculty of Computer and Mathematical Sciences**

**DECEMBER 2018**

## **ACKNOWLEDGEMENTS**

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

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

We would like to express our gratitude to our supervisors, Miss Nur Lina Abdullah for giving us guidance support and encouragement during our study. This study cannot be done without the effort and cooperation from the group members Annuur Zakiah, Farah Deena and Fatin Nur Athirah. Last but not least, we would like to thank to our friends and families who are in one way support either mentally, orally and financially.

## TABLE OF CONTENTS

ACKNOWLEDGEMENTS.....	ii
TABLE OF CONTENTS.....	iii
LIST OF TABLES.....	v
LIST OF FIGURES.....	v
ABSTRACT.....	vi
<b>1 INTRODUCTION.....</b>	<b>1</b>
1.1 Problem statements .....	2
1.2 Objectives .....	2
1.3 Scope of study.....	3
1.4 Benefits and significance of study .....	3
<b>2 BACKGROUND OF THEORY .....</b>	<b>4</b>
2.1 Definition of Matrix .....	4
2.1.1 Square matrix.....	4
2.1.2 Transpose of matrix.....	5
2.2 Definition of Modular Arithmetic.....	5
2.2.1 Modular multiplication of matrix.....	6
2.2.2 Modular inverse.....	7
2.3 Definition RSA Cryptosystem in Choosing the Modulo .....	7
2.4 Definition of Hill Cipher .....	8
<b>3 LITERATURE REVIEW .....</b>	<b>9</b>
3.1 Public-key Exchange Cryptography .....	9
3.2 Encrypt and Decrypt Using Hill Cipher.....	9
3.3 Three-Pass Protocol Concepts in Hill Cipher.....	10
<b>4 METHODOLOGY.....</b>	<b>11</b>
4.1 The Quist-Aphetsi-Kester scheme (2012).....	12
4.1.1 The process of generating private key to public key.....	12
4.2 The Andysah Putera Utama Siahaan scheme (2016).....	14
<b>5 IMPLEMENTATIONS .....</b>	<b>15</b>
5.1 The improvement of Public Key Exchange Cryptographic Technique using Matrix .....	15

5.1.1	For establishing shared secret keys between three parties A, B and C.....	15
5.1.2	Architecture of shared secret key between three parties.....	17
5.1.3	Mathematical Explanation Using Matrix.....	18
5.2	The enhancement of proper public key generation of Three-Pass protocol concept.....	23
5.2.1	Key Agreement Algorithm.....	23
5.2.2	Architecture of public key generation in Three-Pass protocol concept.....	24
5.2.3	Mathematical explanations.....	25
<b>6</b>	<b>RESULTS AND DISCUSSIONS</b> .....	<b>29</b>
<b>7</b>	<b>CONCLUSION AND RECOMMENDATION</b> .....	<b>31</b>
	<b>APPENDIX A</b> .....	<b>32</b>
	<b>REFERENCES</b> .....	<b>35</b>

## **ABSTRACT**

These days, people need a more secure ways to share important message secretly. Public-key exchange cryptographic and encryption technique in Hill Cipher are one of the secured ways that people can use to share their message. No matter how hard to break the system, advisory always find a way to dismantle the message. Therefore, cryptosystem needs improvement from time to time. In the previous work of the research paper by Kester (2012), there are only one encryption process in public-key exchange. In this study, we concerning to increase the number of encryption in order to be difficult to break. In three-pass protocol, parties uses private encryption key to generate a cipher text. However, advisory can easily attack and obtain the private encryption key. Whereas, the private encryption and decryption key will act as a public key. Throughout this research paper, mathematical method that we use to generate public key and private key are matrix.