

# Contents

<b>Declaration of Authorship</b>	<b>ii</b>
<b>Abstract</b>	<b>iii</b>
<b>Acknowledgements</b>	<b>v</b>
<b>Contents</b>	<b>vi</b>
<b>List of Figures</b>	<b>ix</b>
<b>List of Tables</b>	<b>x</b>
<b>Abbreviations</b>	<b>xi</b>
<b>Symbols</b>	<b>xii</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Statement of the Problem . . . . .	2
1.2 Contribution of Thesis . . . . .	3
1.3 Organization of the Thesis . . . . .	4
<b>2 Foundation</b>	<b>6</b>
2.1 Mathematical Preliminaries . . . . .	7
2.2 Encryption . . . . .	8
2.2.1 Symmetric Key Encryption . . . . .	9
2.2.2 Symmetric Keys Distribution Challenges . . . . .	10
2.2.3 Public Key Encryption . . . . .	10
2.3 RSA and Rabin Algorithms . . . . .	12
2.3.1 RSA Algorithm . . . . .	12
2.3.2 Rabin Algorithm . . . . .	14
2.3.3 RSA Versus Rabin Algorithms . . . . .	18
2.4 Chapter Summary . . . . .	19
<b>3 Known Attacks on RSA and Mitigation Approaches</b>	<b>20</b>
3.1 Attacks Against RSA . . . . .	20
3.1.1 Common Modulus (CMA) . . . . .	21

3.1.2	Known Plaintext Attack (KPA)	22
3.1.3	Chosen-Plaintext Attack (CPA)	22
3.1.4	Timing Attack (TA)	23
3.1.5	Frequency of Block Attack (FOB)	23
3.2	Proposed Approaches for Preventing RSA Attacks	24
3.2.1	Dice Approach	25
3.2.2	Dice Approach Follower	26
3.2.3	Hungry Mouse Approach	26
3.3	Limitations of the Proposed Approaches for Solving RSA Attacks	27
3.4	Chapter Summary	28
<b>4</b>	<b>Enhanced RSA Cryptosystem (Yamen Cryptosystem)</b>	<b>29</b>
4.1	Yamen Cryptosystem Components	29
4.1.1	Huffman Coding in Enhance RSA (Yamen Cryptosystem)	30
Header File:		33
Binary File:		33
4.1.2	Random Component in Yamen Cryptosystem	34
4.2	Design Model and Implementation of Yamen Cryptosystem	37
4.2.1	New Design Model for Yamen Cryptosystem	37
4.2.2	Implementation of Yamen Cryptosystem	39
4.3	Reduced Space Results	42
4.4	Speeding Up Yamen Cryptosystem	43
4.5	Chapter Summary	44
<b>5</b>	<b>Performance of Yamen Cryptosystem</b>	<b>45</b>
5.1	Overview of Experiment Setup	45
5.2	Results Analysis	46
5.2.1	Security Issue	46
5.2.2	Execution Time Issue	52
5.2.3	Space Issue	58
5.3	Yamen Cryptosystem Comparing with the Basic RSA	59
5.4	Chapter Summary	60
<b>6</b>	<b>Summary and Outlook</b>	<b>61</b>
6.1	Summarization of Yamen Characteristics Against RSA Attacks and Other Proposed Approaches	62
6.2	Difficulties and Obstacles	64
6.3	Recommendations	65
6.4	Outlook	65
<b>A</b>	<b>Snapshots for Yamen Cryptosystem Processes</b>	<b>66</b>
A.1	Encryption Process: Educational View	66
A.2	Encryption Process : Business View	68
<b>B</b>	<b>Experiments : Details Tables And Charts To Show That Yamen Cryptosystem Is Faster Than RSA.</b>	<b>70</b>

**Bibliography**