

CONTENTS

APPROVAL PAGE	ii
STATEMENT.....	iii
PREFACE.....	v
CONTENTS.....	vi
LIST OF TABLES	ix
LIST OF FIGURES	x
ABSTRACT	xi
 INTRODUCTION.....	 1
1.1 Research Background.....	1
1.2 Research Problem	3
1.3 Research Scope	3
1.4 Research Objective.....	3
1.5 Research Advantages	4
 LITERATURE REVIEW.....	 5
 THEORETICAL BASIS	 13
3.1 Digital Signature Algorithm (DSA)	13
3.2 Elliptic Curve Cryptography	16
3.3 Elliptic Curve Digital Signature Algorithm (ECDSA)	20
3.3.1 Key generation:	21
3.3.2 Signature generation.....	22
3.3.3 Signature verification.....	23
3.4 Rivest Shamir Adleman (RSA) Algorithm	23
3.4.1 Key Generation	26
3.4.2 Encryption and Signing.....	27
3.4.3 Decryption and Verifying.....	28
3.5 Evaluation	29
 RESEARCH METHODOLOGY	 30
4.1 Literature Study.....	30
4.2 Data Acquisition	31
4.3 Elliptic Curve Digital Signature Algorithm (ECDSA)	31

4.3.1	<i>Generating Key Scheme</i>	32
4.3.2	<i>Signing Generation Scheme</i>	32
4.3.3	<i>Verification Signature Scheme</i>	33
4.4	RSA Analysis	34
4.4.1	<i>Key Generation</i>	34
4.4.2	<i>Encryption and Signing</i>	35
4.4.3	<i>Decryption and Verifying</i>	35
	IMPLEMENTATION	36
5.1	<i>Specification of Hardware and Software</i>	36
5.2	<i>Implementation of Data</i>	37
5.3	Elliptic Curve Digital Signature Algorithm	37
5.3.1	<i>Logging and String</i>	37
5.3.2	<i>Type of ECC Curve and Hash</i>	37
5.3.3	<i>OpenSSL</i>	38
5.3.4	<i>Time Variable</i>	38
5.3.5	<i>Implementation of ECDSA</i>	39
5.3.6	<i>Result</i>	40
5.4	RSA	40
5.4.1	<i>Logging and String</i>	41
5.4.2	<i>RSA Parameters</i>	41
5.4.3	<i>OpenSSL and RSA Padding</i>	41
5.4.4	<i>Time Variable</i>	42
5.4.5	<i>Implementation of RSA</i>	42
5.4.6	<i>Verifying Data</i>	43
5.4.7	<i>Result</i>	43
	RESULT AND DISCUSSION	45
6.1	<i>Comparation of Models</i>	45
6.2	<i>Evaluation of ECDSA</i>	46
6.3	<i>Evaluation of RSA</i>	47
6.4	<i>Comparison of Result</i>	48
6.5	<i>Evaluation of Comparison</i>	50

CONCLUSION AND SUGGESTION	53
7.1 Conclusions.....	53
7.2 Suggestion.....	53
REFERENCES.....	54
ATTACHMENT.....	56

LIST OF TABLES

Table 2.1 Comparison with Previous Works	7
Table 3.1 List of Hash Algorithm	15
Table 3.2 SHA Table Differentiation	16
Table 3.3 ECC Component	17
Table 3.4 Key Sizes for Equivalent Levels (in bits).....	18
Table 3.5 Computation Times of Curve when using ECDH Algorithm.....	19
Table 3.6 Key Generation Scheme Equation	21
Table 3.7 Signature Generation Scheme Equation	22
Table 3.8 Signature Verification Scheme Equation	23
Table 3.9 RSA Equation	25
Table 3.10 Key Generation Scheme Equation	27
Table 3.11 Encryption and Signing Scheme Equation.....	28
Table 3.12 Verifying Scheme Equation	28
Table 6.1 Method Differentiation	46
Table 6.2 ECDSA Run.....	48
Table 6.3 RSA Run	48

LIST OF FIGURES

Figure 3.1 ECC Operations	18
Figure 4.1 Flowchart of Proposed Scheme	30
Figure 4.2 ECDSA Signing Generation Scheme	32
Figure 4.3 ECDSA Verification Scheme	33
Figure 4.4 RSA Method Scheme	34
Figure 5.1 Logging and String Function	37
Figure 5.2 EC Curve and Hash Function	38
Figure 5.3 Open SSL Backend Function.....	38
Figure 5.4 Setting Time Variable Function	38
Figure 5.5 Implementation of Elliptic Curve Digital Signature.....	39
Figure 5.6 Verifying Function	39
Figure 5.7 Showing Result Function.....	40
Figure 5.8 Logging and String Function	41
Figure 5.9 RSA Parameters.....	41
Figure 5.10 Open SSL backend and RSA Padding Funcion.....	42
Figure 5.11 Setting Variable	42
Figure 5.12 Open file Function	42
Figure 5.13 Import Private Key and Public Key	43
Figure 5.14 Verifying Function	43
Figure 5.15 Showing Result.....	44
Figure 6.1 CPU and Memory Status While Running Code	45
Figure 6.2 Result of ECDSA 1st Run	47
Figure 6.3 Result of RSA 1st Run.....	47
Figure 6.4 All Method Comparison First Run	49
Figure 6.5 All Method Comparison Second Run.....	49
Figure 6.6 All Method Comparison Third Run.....	50
Figure 6.7 All Method Comparison Average Runtime After 3 Run.....	50