

TABLE OF CONTENTS

CONTENTS	PAGE
Declaration	ii
Abstract	iii
Acknowledgement	iv
Table of Contents	v
List of Figures	ix
List of Tables	x
CHAPTER 1 INTRODUCTION	1
1.1 Project Overview	1
1.2 Project Objective	2
1.3 Project Scope	2
1.4 Significance of Study	3
1.5 Dissertation Organization	4
CHAPTER 2 LITERATURE REVIEW	6
2.1 Introduction	6
2.2 Cryptography	7
2.3 Cryptanalysis	9
2.4 Substitution Ciphers and Transposition Ciphers	10
2.4.1 Substitution Cipher	11
2.4.2 Transposition Cipher	12
2.5 Cryptographic Systems	12
2.5.1 Symmetric Encryption	13
2.5.2 Asymmetric Encryption	14
2.5.3 Comparison of Symmetric Cryptography and Asymmetric Cryptography	16
2.6 Data Encryption Standard (DES)	18
2.6.1 DES Overview	19
2.6.2 Problems of DES	23

2.6.3 Cryptanalysis of DES	27
2.7 Review of Other Block Cipher	30
2.7.1 FEAL	31
2.7.2 IDEA	32
2.7.3 RC5	33
2.8 Multiple Encryption	34
2.8.1 Double Encryption	35
2.8.2 Triple Encryption	36
2.8.3 Meet-in-the-middle Attacks on Multiple Encryption	38
2.9 Conclusion	39
CHAPTER 3 ANALYSIS ON BLOCK CIPHER	42
3.1 Introduction	42
3.2 Substitution Layer	42
3.2.1 S-Box Properties	43
3.2.2 Types of S-Boxes	48
3.3 Diffusion Layer	51
3.3.1 Analysis on Permutation	52
3.3.2 Analysis on Linear Transformation	53
3.4 Key Schedule	56
3.4.1 Related-Key Cryptanalysis	56
3.4.2 Other Key Schedule Attacks	58
3.4.3 Requirements for Strong Key Schedule	60
3.5 Common Block Cipher Structures	61
3.5.1 SP Network	62
3.5.2 Feistel Network	63
3.5.3 Analysis on Block Cipher Structures	65
3.6 Conclusion	66
CHAPTER 4 DESIGN OF BLOCK CIPHER	69
4.1 Introduction	69
4.2 Design Principles	70
4.3 Overview of Block Cipher Structure	73
4.3.1 The Round Transformation	74

4.3.2 Substitution Layer, γ	76
4.3.3 Round Key Addition, σ	76
4.3.4 Linear Transformation, π	77
4.3.5 Key Schedule, ϕ	78
4.3.6 The Cipher	79
4.3.7 The Inverse Cipher	79
4.4 Design Strategy	80
4.4.1 The Cipher Structure	81
4.4.2 Substitution Layer	85
4.4.3 Round Key Addition	86
4.4.4 Linear Transformation	87
4.4.5 Key Scheduling	92
4.5 Conclusion	94
CHAPTER 5 TESTING AND RESULTS	96
5.1 Introduction	96
5.2 Testing	96
5.2.1 Testing Differential Characteristics	96
5.2.2 Testing Cyclic Properties	98
5.2.3 Testing Nonlinearity	98
5.2.4 Involution	100
5.2.5 Avalanche Criterion and Completeness	101
5.3 Test Results	101
5.3.1 Differential Characteristics	102
5.3.2 Cyclic Properties	102
5.3.3 Nonlinearity	103
5.3.4 Involution	103
5.3.5 Avalanche Criterion and Completeness	105
5.4 Summary of Test Results	106
CHAPTER 6 CONCLUSION AND FUTURE ENHANCEMENT	108
6.1 Overview	108
6.2 Achievements	109

6.4 Future Enhancement	112
6.5 Conclusion	113
REFERENCES	114

LIST OF FIGURES

FIGURE		PAGE
Figure 2.1	Basic Cryptosystem	8
Figure 2.2	DES Input-Output	19
Figure 2.3	DES	20
Figure 2.4	DES inner f function	21
Figure 2.5	Double Encryption	35
Figure 2.6	Triple Encryption	36
Figure 3.1	S-Boxes and P-Box Interconnection	52
Figure 3.2	S-Boxes and PHT Interconnection	54
Figure 3.3	Substitution-Permutation (SP) Network	62
Figure 4.1	Basic Building Block	73
Figure 4.2	The Round Transformation	75
Figure 4.3	Mixer	77
Figure 4.4	Encryption	83
Figure 4.5	Decryption	83
Figure 4.6	New S-Box	87
Figure 4.7	Connections between S-Boxes and Mixer	88
Figure 4.8	Interconnection of Mixers	91

LIST OF TABLES

TABLE		PAGE
Table 2.1	Types of Attacks on Encrypted Messages	10
Table 2.2	DES Modes of Operation	23
Table 2.3	DES Weak Keys	25
Table 2.4	DES Semi-weak Key Pairs	26
Table 3.1	Number of Rounds Required to Satisfy Completeness Property	55
Table 5.1	Maximum Differential Distribution Table Entry and DP_{\max}	102
Table 5.2	Cyclic Properties	102
Table 5.3	Nonlinearity	103
Table 5.4	Avalanche Effect	105