

STUDY AND DEVELOPMENT OF RIJNDAEL ENCRYPTION SYSTEM



By

M MUZAMMIL KHAN

Supervised by

Dr M A KHAN

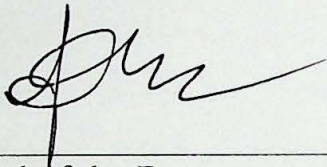
BAHRIA INSTITUTE OF MANAGEMENT & COMPUTER SCIENCES

BAHRIA UNIVERSITY ISLAMABAD 2000-2002

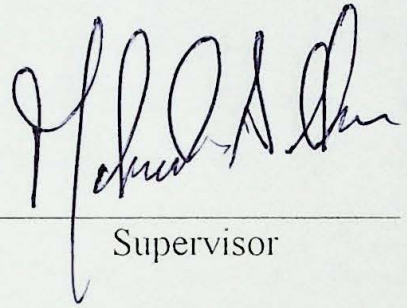
CERTIFICATE

We accept the work contained in this report as a conforming to the required standard for the partial fulfillment of the degree of MCS (Networking).

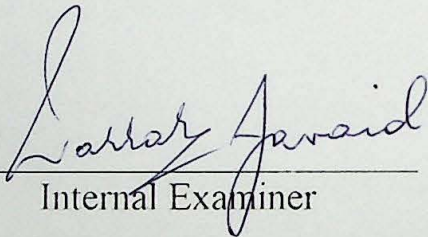
Khan in partial fulfillment of Degree of MCS



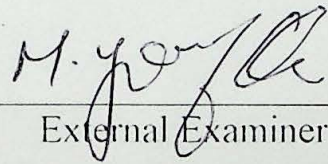
Head of the Department



Supervisor



Internal Examiner



External Examiner

Abstract

A dissertation submitted to Bahria University Islamabad by M Muzammil Khan in partial fulfillment of Degree of MCS.

My present project deals with selection, study and development of an appropriate Encryption System for Pakistan Navy. First Chapter provides general introduction of Naval Intranet and an overview of Encryption Systems, Chapter 2 outlines the selection procedure adopted by National Institute of Standards and Technology (NIST) for selection of Advance Encryption Standard (AES) to be used by US Govt. Rijndael Encryption System presented by Joan Daemen and Vincent Rijmen has been selected as AES for use by US Govt, the same is selected for study and its development for use by Pakistan Navy. The main idea behind writing this chapter here, is to provide the culture of Selection/Implementation of an Advance Encryption System (AES) at National/Organizational level.

Design of the cipher is discussed in Chapter 3. Rijndael is a block cipher which uses non-feistel structure. It can be implemented on 128, 192 & 256 bits key lengths. Key features of its design are: resistance against well known attacks, speed and code compactness on a wide range of platforms and design simplicity. The Cipher uses a non-feistel structure with 10, 12 or 14 rounds depending on the value of the key. Each round consists of Byte substitution, Shift row, Mix Column and Add round key functions.

Chapter 4 deals with strength of Rijndael Encryption System against the known attacks, Chapter 5 covers some implementation aspects of the cipher. Interestingly the four functions of the design can be combined together into new lookup tables resulting in a very fast and compact implementation.

Abstract

ACKNOWLEDGEMENTS

Pakistan Navy has its own Intranet, which is being extensively utilized for information sharing and transmission of electronic mail among various units. Due to non-availability of adequate security measures, information of higher security classification cannot be transmitted through this Intranet. Hence, there is a need to implement some encryption system, for secure transmission of classified information.

My present project deals with selection, study and development of an appropriate Encryption System, for Pakistan Navy. First chapter provides general introduction of Naval Intranet and an overview of Encryption Systems. Chapter 2 enlists the selection procedure adopted by National Institute of Standards and Technology (NIST) for selection of Advance Encryption Standard (AES) to be used by US Govt. Rijndael Encryption System presented by Joan Daemen and Vincent Rijmen has been selected as AES for use by US Govt, the same is selected for study and its development for use by Pakistan Navy. The main idea behind writing this chapter here, is to promote the culture of Selection/Implementation of an Advance Encryption System (AES) at National/Organizational level.

Design of the cipher is discussed in Chapter 3. Rijndael is a block cipher which uses non-feistel structure. It can be implemented on 128,192 & 256 bits key lengths. Key features of its design are: resistance against well known attacks, speed and code compactness on a wide range of platforms and design simplicity. The Cipher uses a non feistel structure with 10,12 or 14 rounds depending on the value of the key. Each round consists of Byte substitution, Shift row, Mix Column and Add round key functions.

Chapter 4 deals with strength of Rijndael Encryption System against the known attacks. Chapter 5 covers some implementation aspects of the cipher. Interestingly the four functions of the design can be combined together into new lookup tables resulting in a very fast and compact implementation.

ACKNOWLEDGEMENTS

The desire to obtain a Master's degree in Computer Science arisen soon after I did Post Graduate Diploma in Computer Science in 1995. But it is God, who well decides about what one has to do at which time. By the grace of Almighty Allah my this desire is coming true at a crucial stage of my career in Pakistan Navy.

There is a handsome contribution of prayers, inspirations, encouragement, guidance and support from some personalities around me, for completing this task. I thank to Rear Admiral Asaf Humayun (then Naval Secretary at Naval Headquarters) for granting me permission to continue my studies in the evening, in spite of the fact that the usual office timings at my office often extended beyond 6 PM. Capt Khalid Saeed's (then Deputy Naval Secretary at Naval Headquarters) personal efforts in sparing me from office after 4 PM are worth mentioning here. I also thank to Cdr Ishrat Mahmood Shakir and Cdr Muhammad Shafique for their continuous inspiration and encouragement.

It may be mentioned that this task would not have been completed without the personal interest, encouragement and guidance provided by Mr. Fazal-e-Wahab, the Programme Leader Computer Sciences and Dr. M A Khan, the supervisor of this project.

Thank to my parents and whole family whose prayers showed their presence as they did throughout my academic career. Many thanks to my wife Mehreen for her patience and courage as she had to spent long lonely hours but she always admired and encouraged me. Finally I would like to extend a lot of love to my two daughters Reshail and Zenab.

TABLE OF CONTENTS

<u>CONTENT</u>	<u>PAGE #</u>
Abstract	i
Acknowledgements	ii
Table of contents	iii
List of figures	iv
CHAPTER 1	
INTRODUCTION	1
1.1 Dawn of Intranet in Pakistan Navy	1
1.2 Need of an Encryption System in Pakistan Navy	1
1.3 Development of Encryption System for Pakistan Navy	2
1.4 Over View of Encryption Systems	2
1.5 Benefits of Cryptography	2
1.6 Symmetric Key Algorithms	3
1.7 Public Key Algorithms	3
1.8 Choice of Algorithm for Encryption/Decryption	4
CHPATER 2	
SELECTION OF ADVANCE ENCRYPTION STANDARD	5
2.1 Overview of the Development Process for the AES	5
2.2 Background	6
2.3 Overview of the Finalists	6
2.3.1 MARS	7
2.3.2 RC6	7
2.3.3 Rijndael	8
2.3.4 Serpent	8
2.3.4 Twofish	8
2.4 Evaluation Criteria	9
2.5 Results from Round 2	10
2.6 The Selection Process	11
2.7 Approach to Selection	12
2.8 Quantitative vs. Qualitative Review	12
2.9 Number of AES Algorithms	13
2.10 Backup Algorithm	14
2.11 Modifying the Algorithms	15
2.12 Summary Assessments of the Finalists	16
2.13 General Security	17
2.14 Software Implementations	17
2.15 Restricted-Space Environments	18

2.16	Hardware Implementations	18
2.17	Attacks on Implementations	18
2.18	Encryption vs. Decryption	19
2.19	Key Agility	19
2.20	Other Versatility and Flexibility	20
2.21	Potential for Instruction-level Parallelism	20
2.22	Final Selection	20

CHAPTER 3

DESIGN OF RIJNDAEL		22
3.1	Introduction	22
3.2	Glossary of Terms and Acronyms	22
3.3	Algorithm Parameters, Symbols, Terms, and Functions	23
3.4	Notation and Conventions	25
3.4.1	Inputs and Outputs	25
3.4.2	Bytes	25
3.4.3	Arrays of Bytes	26
3.5.	Mathematical Preliminaries	27
3.5.1	The Field $GF(2^8)$	27
3.5.2	Addition	27
3.5.3	Multiplication	28
3.5.3.1	Multiplication by x	29
3.5.4	Polynomials with coefficients in $GF(2^8)$	30
3.5.4.1	Multiplication by x	31
3.6	Design Rationale	32
3.7	Specification	33
3.7.1	The State, the Cipher Key and the Number of Rounds	33
3.7.2	The Round Transformation	35
3.7.2.1	The ByteSub Transformation	39
3.7.2.2	The ShiftRow Transformation	40
3.7.2.3	The MixColumn Transformation	41
3.7.2.4	The Round Key Addition	42
3.7.3	Key Schedule	43
3.7.3.1	Key Expansion	43
3.7.3.2	Round Key Selection	45
3.7.4	The Cipher	46
3.7.5	The Inverse Cipher	48
3.7.5.1	InvShiftRows() Transformation	48
3.7.5.2	InvSubBytes() Transformation	49
3.7.5.3	InvMixColumns() Transformation	49

3.7.5.4	Inverse of the AddRoundKey()	50
3.7.5.5	Inverse of A Two-Round Rijndael Variant	50
3.7.5.6	Algebraic Properties	51
3.7.5.7	The Equivalent Inverse Cipher Structure	52
CHAPTER 4		
STRENGTH AGAINST ATTACKS		55
4.1	Symmetry Properties and Weak Keys of The DES Type	55
4.2	Truncated differentials	55
4.3	The Square Attack	56
4.4	Related-Key Attacks	56
4.5	Timing and Power Attacks	57
4.6	Implicit Key Schedule Weaknesses	57
4.6.1	A Power Analysis Variant	57
4.7	Defenses Against Implementation-Dependent Attacks	58
CHAPTER 5		
SOFTWARE IMPLEMENTATION		60
5.1	Implementation Aspects	60
5.2	8-bit Processor	60
5.3	32-bit Processor	61
5.3.1	The Round Transformation	61
5.3.2	Parallelism	63
5.3.3	Hardware Suitability	64
CHAPTER 6		
DISCUSSION		65
6.1	Wide-Trail Strategy	65
6.2	Non-Feistel Structure	65
6.3	Low Memory Requirement	65
6.4	Implementation	66
6.5	Future Enhancement	66
6.6	Recommendations	66
REFERENCES		68
APPENDIX A		73

LIST OF FIGURES

Figure No	Description	Page #
Figure 3.1	Round Functions of Rijndael	37
Figure 3.2	Another Representation of Round Functions of Rijndael	38
Figure 3.3	Illustration of ByteSub()	39
Figure 3.4	S-box, showing substitution values for the byte xy	40
Figure 3.5	Representation of ShiftRows()	41
Figure 3.6	Representation of MixColumn operation	42
Figure 3.7	AddRoundKey() function	43
Figure 3.8	Flow Chart of the Cipher	46
Figure 3.9	InvShiftRow() Transformation	48

1.2 Need of an Encryption System in Pakistan Navy

Official mail in defense forces has following five categories from security point of view:

- i. Un-classified
- ii. Restricted
- iii. Confidential
- iv. Secret
- v. Top Secret

Presently, the mail upto Restricted classification is allowed to be transmitted through Pakistan Navy Intranet, due to security concerns, as there is no any encryption system ever used by Pakistan Navy on its Intranet. Hence there is a dire need of using modern encryption technology so that Pakistan Navy can be able to transmit mail at least upto Secret classification, through its own Intranet, in order to be more secure and speedy.