

Universiti Teknologi MARA

ENCRYPTED EMAIL USING 3D-AES BLOCK CIPHER
ALGORITHM

UiTM Shah Alam

Khairah Binti Mohd Wi

Bachelor of Computer Science (Hons)
Faculty of Computer and Mathematical Science

JANUARY 2015

ACKNOWLEDGEMENT

Alhamdulillah, praise and thank to Allah because of His Almighty and His utmost blessings, I was able to have the courage and strength to complete this project.

I would like to thank and gives utmost appreciation to my supervisor, Dr. Suriyani Ariffin for all her valuable guidance and her willingness to help me during the stages of this project development. Her advice's and guidance has been invaluable in the completion of this thesis and I really appreciate it.

Last but not least, my greatest gratitude and appreciation to my family, friends, and colleagues who have supported and encouraged me in doing my project. All their help in this project are priceless and are kindly appreciated.

Khairah Binti Mohd Wi

Table of Contents

SUPERVISOR'S APPROVAL.....	i
DECLARATION.....	ii
ACKNOWLEDGEMENT.....	iii
Table of Contents.....	iv
Table of Figure.....	vii
List of Tables.....*	viii
ABSTRACT.....	ix
CHAPTER 1: INTRODUCTION.....	1
1.1 Introduction.....	1
1.2 Background.....	1
1.3 Problem Statement.....	1
1.4 Objective.....	2
1.5 Scope of Project.....	3
1.6 Project Aim.....	4
CHAPTER 2: LITERATURE REVIEW.....	5
2.0 Introduction.....	5
2.1 Email Encryption.....	5
2.2 Encryption.....	6
2.3 Cryptography.....	6
2.1.1 Symmetric key.....	7
2.1.2 Block Cipher Algorithm.....	8
2.1.3 Asymmetric key.....	9
2.4 Encryption of Block Cipher Algorithm.....	10
2.2.1 DES.....	11

2.2.2	AES	12
2.2.3	Shark Algorithm	12
2.2.4	Blowfish	13
	(Source: SchneierB, 1994)	14
2.2.5	3D-AES	15
2.5	Development of Email	15
2.5.1	Technique	15
2.5.2	Encryption Tools	17
2.5.2.1	Email	17
2.5.2.2	PGP	17
2.5.2.3	HushMail	18
2.5.2.2	FILE ENCRYPTION	18
CHAPTER 3: PROJECT METHODOLOGY		20
3.0	Introduction	20
3.1	Project formulation Framework	20
	Table	21
3.2	Preliminary Study	21
3.3	Analysis of Literatures	21
3.1.1	Design of Prototype Application	22
3.4	User Interface Flow Diagrams (UI Storyboards)	23
3.3.1	Homepage (Login, Sign up)	24
3.3.2	Compose Email	25
3.3.3	List Email Message (Inbox, Sent)	26
3.3.4	Inbox Message Content	26
3.3	Implementation of Prototype Application	27
3.4	Testing and Evaluation	27
3.5	System Architecture	28
3.6	Project Planning	29

ABSTRACT

Encrypted email is addition mail that comes up with prototype application called, 3D-AES block cipher. There are three objective designed: To identify an encrypted email application development of 3D AES block cipher algorithm and hash process, to develop encrypted email using 3D AES process on email and lastly to measure the validity of the encrypted & decrypted email message by comparing the hash value generate before encrypt and after decrypt. The purpose of this project is to develop encrypted email application equip with confidentiality and integrity message using 3D-AES block cipher for confidential and integrity. The main finding of this project will produces a security of message content. This new application will produces a higher security services: authentication, confidential and integrity. Lastly, this project had accomplish all their objective which important in process of developing the mail prototype application using 3D-AES block cipher as confidential process as integrity purpose.