

TABLE OF CONTENTS

HALAMAN PENGESAHAN.....	ii
PREFACE	iii
TABLE OF CONTENTS	v
LIST OF FIGURES	ix
LIST OF TABLES	xii
LIST OF EQUATIONS	xiii
LIST OF GRAPHS	xiv
INTISARI.....	15
ABSTRACT.....	16
CHAPTER I INTRODUCTION	17
1.1. Background	17
1.2. Preliminary Research	18
1.3. Problem Statement	19
1.4. Scope of Problems.....	20
1.5. Research Purpose	20
1.6. Research Benefits	20
1.7. Research Methodology	21
1.8. Thesis Structure	22
CHAPTER II LITERATURE REVIEW.....	23
2.1. Cryptography on Microcontroller.....	23
2.2. AES and CBC Mode of Operation	24
CHAPTER III THEORETICAL BASIS.....	28
3.1. Cryptography	28

3.2.	Advanced Encryption Standard (AES).....	30
3.3.	CBC (Cipher Block Chaining) Modes of Operation	34
3.4.	Microcontroller.....	35
CHAPTER IV RESEARCH METHODOLOGY		37
4.1.	Research Procedures.....	37
4.2.	Tools and Materials	38
4.3.	System Design.....	39
4.3.1.	Hardware Architectural Design.....	39
4.3.2.	Hardware Model Design	40
4.3.3.	Cryptographic Algorithm Implementation.....	41
4.3.4.	Data Buffering and Memory Management	43
4.3.5.	Encryption and Decryption Flow	45
4.4.	System Testing Step	46
4.4.1.	Hardware Testing.....	46
4.4.2.	Algorithm Testing	47
4.4.3.	Performance Testing	48
4.4.4.	Attack Testing	53
CHAPTER V IMPLEMENTATION.....		54
5.1.	Hardware Implementation.....	54
5.2.	AES Algorithm Implementation	55
5.2.1.	Encryption Process.....	56
5.2.2.	Decryption Process.....	59
5.2.3.	Padding.....	63
5.3.	CBC Mode Implementation	66

5.4.	Data Handling and Memory Management	66
5.4.1.	Data Buffering.....	66
5.4.2.	File Storage and Management.....	67
5.5.	System Workflow	68
5.5.1.	File Encryption Workflow	69
5.5.2.	File Decryption Workflow	70
5.5.3.	Compiler Optimization Implementation	72
5.6.	Overall System Implementation	73
5.7.	Security Testing Implementation	74
CHAPTER VI RESULTS AND DISCUSSION.....		75
6.1.	Hardware Testing	75
6.1.1.	SPI Communication Test	75
6.1.2.	Read/Write Test	75
6.2.	Algorithm Testing	76
6.2.1.	Encryption Test	76
6.2.2.	Decryption Test	81
6.2.3.	IV Usage Test.....	86
6.3.	Performance Testing.....	87
6.3.1.	File Size Test.....	87
6.3.2.	Processing Speed Test.....	89
6.3.3.	Compiler Optimization Test.....	98
6.4.	Attacking Test	99
CHAPTER VII CONCLUSION		101
7.1.	Conclusion.....	101



UNIVERSITAS
GADJAH MADA

Implementation of AES-128 Algorithm on a Microcontroller for File Encryption and Decryption
Keitaro Wildan Ramadhan, Oskar Natan, S.ST., M.Tr.T.; Prof. Dr. Jazi Eko Istiyanto, M.Sc.
Universitas Gadjah Mada, 2024 | Diunduh dari <http://etd.repository.ugm.ac.id/>

7.2. Suggestions.....	102
REFERENCES.....	103