

CONTENTS

TITLE SHEET	i
APPROVAL SHEET	ii
DECLARATION	iii
TRIBUTE PAGE	iv
MOTTO PAGE	v
PREFACE	vi
CONTENTS	ix
LIST OF TABLES	xi
LIST OF PICTURES	xii
LIST OF SYMBOL	xvi
ABSTRACT	.xviii
INTISARI	xix
I INTRODUCTION	1
1.1. Background	1
1.2. Problems Formulation	7
1.3. Research Purposes and Impacts	9
1.4. Literature Review	10
1.4.1. Algebraic properties	10
1.4.2. Applications in cryptography	13
1.4.3. Application in coding theory	14
1.5. Research Methods	18
1.6. Overview of the Chapters	24
II BASIC THEORY	27
2.1. Ring of Eisenstein Integers	27
2.1.1. Divisibility	29
2.1.2. Euclidean and hexagonal distances	33
2.1.3. Prime and primitive Eisenstein integers	35
2.1.4. On the quotient ring of Eisenstein integers	39
2.1.5. Unit group in the quotient ring of Eisenstein integers	42
2.1.6. Even and odd Eisenstein integers	44
2.2. Lattice and Lattice Codes	45
2.2.1. Primitive lattice	60
2.2.2. Division algorithm	62

2.3. Lattice Constellations in Additive White Gaussian Noise Channel . . .	66
2.4. RSA Cryptography	68
III FURTHER ALGEBRAIC PROPERTIES OF EISENSTEIN INTEGERS	69
3.1. Algebraic Properties of Even, Odd and Primitive Eisenstein Integers	69
3.2. Distribution of Eisenstein Primes	78
3.3. Primality Test for Eisenstein Integers	80
3.4. Equivalence of Classes in Eisenstein Integers	81
3.5. The Group of Units in Quotient Ring of Eisenstein Integers	84
3.5.1. Euler's totient function	84
3.5.2. A cyclic group	86
3.6. Hexagonal Distance Properties	89
IV APPLICATIONS OF EISENSTEIN INTEGERS ON SIGNAL CON- STELLATIONS AND RSA CRYPTOSYSTEM	95
4.1. Signal Constellations over Quotient Ring of Eisenstein Integers . . .	96
4.1.1. Quotient rings as Eisenstein constellations and code alpha- bet sets	97
4.1.2. Fields and field extensions of Eisenstein integers	101
4.1.3. Eisenstein constellations	102
4.1.4. Set partitioning	103
4.1.5. Comparison	122
4.1.6. Potential Applications	129
4.2. RSA-like scheme over Eisenstein integers	130
4.2.1. The algorithms	131
4.2.2. Successful decryption guarantee	133
4.2.3. Message and key spaces	137
4.2.4. Comparison of parameter of RSA algorithms	139
4.2.5. Security	139
4.2.6. Overheads of the RSA-Like Scheme over Eisenstein Integers	141
V CONCLUSIONS AND OPEN PROBLEMS	143
5.1. Conclusions	143
5.2. Further Research	145
REFERENCES	146