TABLE OF CONTENTS

ABSTRACT I
ACKNOWLEDGEMENT II
TABLE OF CONTENTS III
LIST OF FIGURES VI
LIST OF TABLES VIII
NOTATIONS IX
CHAPTER 1 1
INTRODUCTION 1
1.1 BREAKING PUBLIC KEY CRYPTOSYSTEM 1
1.2 PROJECT MOTIVATION 2
1.3 PROJECT OBJECTIVES 2
1.4 PROJECT SCOPE 3
1.5 EXPECTED OUTCOME 4
1.6 PROJECT SCHEDULING 5
CHAPTER 2 6
LITERATURE REVIEW 6
2.1 RSA ENCRYPTION ALGORITHM 6
2.1.1 Choice of *p* and *q* 8
2.1.2 Choice of *e* and *d* 8
2.1.3 Advantages 8
2.1.4 Disadvantages 9
2.2 FUNDAMENTAL THEOREM OF ARITHMETIC 10
2.3 FACTORING ALGORITHM 11
2.3.1 Trial Division 12
2.3.2 Pollard - ρ algorithm 13
2.3.3 Quadratic Sieve Algorithm 14
2.3.3.1 Fermat's difference-of-square Technique 14
2.3.3.2 Enhancement of difference-of-square Technique 15
2.3.3.3 Smooth Number and Complexity 17
2.3.3.4 The Quadratic Sieve 18
2.3.3.5 Solving Congruence 19
2.3.3.6 Building Factor Base 20
2.3.3.7 Sieving 21
2.3.3.8 Choosing Appropriate Congruence 22
2.3.3.9 Variants of Quadratic Sieve 24
2.4 DISTRIBUTED AND PARALLEL COMPUTING 24
2.4.1 Benefits of Distributed Computing 25
2.4.2 Challenges 26
2.4.3 Tuple Space 27
2.4.4 JavaSpaces 30
2.4.4.1 JavaSpaces Operations 31
2.4.4.2 Associative Lookup 31
2.4.4.3 Atomic Transaction 32
2.4.5 Space-based Communication and Parallel Computing 32
2.4.6 JINI (Java Intelligent Network Infrastructure) 33
2.4.6.1 *JINI* Service Architecture 34

2.5 DIFFERENCES BETWEEN LINDA AND JAVASPACES 36

2.6 CURRENT RESEARCH 37

2.7 CHAPTER SUMMARY 38

CHAPTER 3 40
REQUIREMENT ANALYSIS AND SYSTEM SPECIFICATION 40
3.1 SYSTEM PRE-REQUISITION 40

3.2 NON-FUNCTIONAL REQUIREMENTS 42

3.3 USE CASS DRIVEN ANALYSIS 42

3.3.3 Use Case Diagram 42
3.3.2 Use Case: Start Factoring Process 44
3.3.3 Use case: Resume Previous Incomplete Process 46
3.3.4 Use Case: Access Task Pool and Access Result Pool 47
3.3.5 Use Case: Remote Access Control 49
3.4 CHAPTER SUMMARY 49

CHAPTER 4 50
SYSTEM DESIGN 50
4.1 CRITERIA FOR PARALLEL IMPLEMENTATION 50

4.2 SPACE-BASED PARALLEL APPLICATION PATTERNS 51

4.3 CHOSEN FACTORIZATION ALGORITHM 53

4.4 QS-SPACE ARCHITECTURE 54

4.4.1 System Operational Analysis 57

4.4.2 Data Type 58

4.4.3 Classes Identification and Design 59

4.5 USER INTERFACE DESIGN 65

4.5.1 GUI for Master Module 65

4.5.2 GUI for Slave Module 74

4.6 DATABASE DESIGN 74

4.7 CHAPTER SUMMARY 76

CHAPTER 5 78
SYSTEM IMPLEMENTATION AND DEPLOYMENT 78
5.1 DEVELOPMENT ENVIRONMENT 78

5.2 PLATFORM INDEPENDENT PROGRAMMING LANGUAGE 79

5.3 COOPERATING JINI INTO QS-SPACE DESIGN 80

5.3.1 JINI enabled system 80

5.3.2 JavaSpaces 80

5.4 CLASS DIAGRAM REFINEMENT 82

5.5 QS-SPACE IMPLEMENTATION 87

5.5.1 Accessing JavaSpaces 87

5.5.2 Quadratic Sieve (QS) Algorithm Implementation 95

5.5.3 Integrating Sieving Stage into QSTask 96

5.5.3.1 Sieving Algorithm 98
5.5.3.2 Consideration 104
5.5.4 Master Module 105

5.5.4.1 Tasks Generating and Results Collecting 105
5.5.4.2 Ticket Dispenser and Sieve Queue 108

5.5.4.3 Slaves Coordination 110
5.5.4.4 SieveQueue Entries Collector....116
5.5.4.5 Execution/Running Time Analysis....117
5.5.4.6 Remote Access Service 120
5.5.4.7 Mathematic Utilities....123
5.5.5 Slave Module....126
5.5.5.1 *CommandListener* class....126
5.5.5.2 Task Retrieval and Execution....128
5.6 QS-SPACE DEPLOYMENT....129
5.6.1 JINI's Services Deployment....129
5.6.2 Master and Slave Module Deployment 131
5.6.3 HTTP Servers....132
5.6.4 Hardware and Software 133
5.7 CHAPTER SUMMARY....136
CHAPTER 6....137
COMPUTATIONAL RESULT....137
6.1 PERFORMANCE EVALUATION....137
6.1.1 Parallel Benchmark 139
6.1.2 Execution Time Proportion 142
6.1.3 Effect of Factor Base Size towards Running Time....150
6.2 PERFORMANCE ANALYSIS 152
6.3 OPTIMIZATION....155
6.4 CHAPTER SUMMARY....155
CHAPTER 7....156
CONCLUSION AND FUTURE WORK 156
7.1 CONCLUSION....156
7.2 SUGGESTION FOR FUTURE WORKS....157
REFERENCES....159
APPENDIX A 161
APPENDIX B....168
APPENDIX C....171

LIST OF FIGURES

FIGURE 1.1 PROJECT SCHEDULE 5

FIGURE 1.1 PROJECT SCHEDULE 5

FIGURE 2.1 POLLARD- ρ 14

FIGURE 2.2 LINDA OPERATION ENVIRONMENTS 29

FIGURE 2.3 AN OVERVIEW OF *JAVASPACES* OPERATIONS: *WRITE, TAKE AND READ* 31

FIGURE 2.4 INTERACTION BETWEEN *JINI*'S CLIENT AND SERVICE 36

FIGURE 2.5 *JINI*'S *DISCOVERY, JOIN* AND *LOOKUP* 36

FIGURE 3.1 USE CASE DIAGRAM FOR QS-SPACE APPLICATION 43

FIGURE 3.2 SEQUENCE DIAGRAM **START FACTORING PROCESS** USE CASE 45

FIGURE 3.3 ACTIVITY DIAGRAM FOR **START FACTORING PROCESS::SINGLE OPERATION** AND **START FACTORING PROCESS::CONSECUTIVE OPERATION** 46

FIGURE 3.4 ACTIVITY DIAGRAM FOR **RESUME PREVIOUS INCOMPLETE PROCESS** USE CASE 47

FIGURE 3.5 ACCESS TASK POOL USE CASES 48

FIGURE 3.6 ACCESS RESULT POOL USE CASES 48

FIGURE 3.7 REMOTE ACCESS CONTROL USE CASES 49

FIGURE 4.1 REPLICATED-WORKER PATTERN 52

FIGURE 4.2 COMMAND PATTERN 53

FIGURE 4.3 2-TIER ARCHITECTURE OF QS-SPACE 54

FIGURE 4.4 PEER-TO-PEER DESIGN 55

FIGURE 4.5 MASTER/SLAVE APPROACH WITH DYNAMIC CODES DISTRIBUTION 56

FIGURE 4.6 QS-SPACE MAIN COMPONENTS REPRESENTED IN CLASS DIAGRAM 56

FIGURE 4.7 SEQUENCE DIAGRAM FOR OVERALL SYSTEM PROCESS 59

FIGURE 4.8 CLASS DIAGRAM OF QS-SPACE 61

FIGURE 4.9 MASTER MODULE GUI CLASS DIAGRAM 66

FIGURE 4.10 GUI FOR QSMASTER CONTROL PANEL 68

FIGURE 4.11 DATABASE CONNECTIVITY SETUP (CLASS: DBCONNDIALOG) 69

FIGURE 4.12 INPUT BOX TO GENERATE A NEW COMPOSITE NUMBER 69

FIGURE 4.13 QS-SPACE SYSTEM CONFIGURATIONS (CLASS: SYSCONFDIALOG) 69

FIGURE 4.14 CONFIRMATION BOX FOR CONSECUTIVE BATCH 70

FIGURE 4.15 INPUT FORM FOR CONSECUTIVE BATCH COMPOSITE NUMBERS (CLASS:CONBATCHDIALOG) 70

FIGURE 4.16 MESSAGE BOX FOR ACCESSIBLE SLAVE NODES IN NETWORK 71

FIGURE 4.17 SYSTEM PERFORMANCE GRAFT (CLASS:GRAFTDISPLAYER) 71

FIGURE 4.18 PARALLELISM CHART FOR SIEVING PROCESS (CLASS:PARALLELISMCHART) 72

FIGURE 4.19 REMOTE ACCESS THROUGH JAVA APPLET 73

FIGURE 4.20 SLAVE ACTIVITIES CONSOLE 74

FIGURE 5.1 POSSIBLE ARRANGEMENT OF JINI-ENABLED COMPONENTS 80

FIGURE 5.2 ALL ENTRIES ARE SERIALIZED BY LOCAL PROXY OBJECT AND TRANSMITTED AND STORED IN THE REMOTE SPACE IN SERIALIZED FORM 81

FIGURE 5.3 REFINED VERSION OF QS-SPACE CLASS DIAGRAM 83

FIGURE 5.4 UML SEQUENCE DIAGRAM FOR DISCOVERY AND LOOKUP PROCESSES. 93

FIGURE 5.5 ACTIVITY DIAGRAM OF QS ALGORITHM PROCESS 97

FIGURE 5.6 SIEVING PATTERN FOR EACH TASK ENTRY 99

FIGURE 5.7 ACTIVITY DIAGRAM FOR NODESCOORDINATOR 111

FIGURE 5.8 ACTIVITY DIAGRAM FOR *NODESCOORDINATOR::DISCOVERNODES()* 113

FIGURE 5.9 ACTIVITY DIAGRAM FOR *NODESCOORDINATOR::RECRUITENODES()* 114

FIGURE 5.10 ACTIVITY DIAGRAM FOR *NODESCOORDINATOR::PATROL()* 115

FIGURE 5.11 POSSIBLE ARRANGEMENT OF SIEVE TIME 118

FIGURE 5.12 REMOTE ACCESS VIA RMI 122

FIGURE 5.13 ACTIVITY DIAGRAM FOR COMMANDLISTNER 127

FIGURE 5.14 PACKAGES AND THEIR RELATIONSHIP 129

FIGURE 5.15 INTERACTION IN QS-SPACE 130

FIGURE 5.16 DEPLOYMENT DIAGRAM FOR QS-SPACE 135

FIGURE 6.1 TOTAL EXECUTION TIME 140

FIGURE 6.2 TOTAL SPEEDUP RELATIVE TO SERIAL IMPLEMENTATION 141

FIGURE 6.3 RUN TIME COMPOSITION FOR PARALLEL IMPLEMENTATION [SLAVE NODES=0] 143

FIGURE 6.4 RUN TIME COMPOSITION FOR PARALLEL IMPLEMENTATION [SLAVE NODES=1] 144

FIGURE 6.5 RUN TIME COMPOSITION FOR PARALLEL IMPLEMENTATION [SLAVE NODES=2] 145

FIGURE 6.6 RUN TIME COMPOSITION FOR PARALLEL IMPLEMENTATION [SLAVE NODES=3] 146
FIGURE 6.7 RUN TIME COMPOSITION FOR PARALLEL IMPLEMENTATION [SLAVE NODES=4] 147
FIGURE 6.8 RUN TIME COMPOSITION FOR PARALLEL IMPLEMENTATION [SLAVE NODES=5] 148
FIGURE 6.9 RUN TIME COMPOSITION FOR PARALLEL IMPLEMENTATION [SLAVE NODES=6] 149
FIGURE 6.10 RELATIONSHIP BETWEEN FACTOR BASE AND QS EXECUTION TIME 150
FIGURE 6.11 TOTAL EXECUTION TIME WITH DIFFERENT FACTOR BASE SIZE (DIGIT LENGTH=45) 151
FIGURE 6.12 TOTAL EXECUTION TIME WITH DIFFERENT FACTOR BASE SIZE (DIGIT LENGTH=50) 151
FIGURE 6.13 TOTAL EXECUTION TIME WITH DIFFERENT FACTOR BASE SIZE (DIGIT LENGTH=55) 152

List of Tables

TABLE 2.1 PRIME FACTORS FOR POSITIVE INTEGER 10
TABLE 2.2 *C* VALUE 22
TABLE 2.3 FACTORING RECORD SINCE 1970 [MON1995] 24
TABLE 4.1 **BATCH** TABLE 75
TABLE 4.2 **SIEVETIME** TABLE 76
TABLE 4.3 **B_SMOOTH_RETURNED** TABLE 76
TABLE 4.4 **SLAVEINFO** TABLE 76
TABLE 6.1 NUMBER TO BE FACTORIZED IN EACH TEST RUNS 138
TABLE 6.2 PARAMETER VALUES ASSIGNED TO EACH TEST NUMBER 139
TABLE 6.3 TOTAL EXECUTION TIME FOR EACH FACTORING EXERCISE WITH INCREASING NUMBER OF SLAVE NODES 139
TABLE 6.4 SPEEDUP RELATIVE TO SERIAL IMPLEMENTATION 141
TABLE 6.5 EXECUTION TIME FOR SERIAL IMPLEMENTATION 143
TABLE 6.6 EXECUTION TIME FOR NUMBER OF SLAVE NODES =1 144
TABLE 6.7 EXECUTION TIME FOR NUMBER OF SLAVE NODES =2 145
TABLE 6.8 EXECUTION TIME FOR NUMBER OF SLAVE NODES =3 146
TABLE 6.9 EXECUTION TIME FOR NUMBER OF SLAVE NODES =4 147
TABLE 6.10 EXECUTION TIME FOR NUMBER OF SLAVE NODES =5 148
TABLE 6.11 EXECUTION TIME FOR NUMBER OF SLAVE NODES =6 149
TABLE 6.12 COMMUNICATION/COMPUTATION RATIO IN 6 SLAVE NODES 153
TABLE 6.13 ENTRY SIZE 154
TABLE 6.14 SPEEDUP OPTIMIZATION ON SIEVE TIME [NODES=6] 155

Notations

Symbol	Meaning
$a \equiv b \pmod{n}$	a is congruent to b modulus n
$a \mid b$	a divides b
$a \nmid b$	a does not divide b
$\varphi(n)$	Euler's totient function
G.C.D(a ,b)	greatest common divisor of a and b
$[a, b]$	the interval $a \leq \mathrm{x} \leq b$
$\prod$	product symbol where $\prod_{i=1}^{n} a_1 \cdot a_2 \cdot ..... \cdot a_n$
p	a prime number
$\left[\frac{a}{p}\right]$	Legendre symbol, defined if p is an odd prime
N	Modulus of RSA algorithm