สารบัญ

หน้า

สารบัญ…….....(6)
รายการตาราง ……(8)
รายการภาพประกอบ…….……(9)
สัญลักษณ์คำย่อและตัวย่อ…….....(10)
บทที่
1. บทนำ…….....1
ความสำคัญและที่มาของการวิจัย…….……1
การตรวจเอกสาร…….2
วัตถุประสงค์ของโครงการวิจัย…….....5
ขั้นตอนของการวิจัย…….…5
ประโยชน์ที่คาดว่าจะได้รับจากการวิจัย…….....5
สรุปท้ายบท……6
2. หลักการพื้นฐานกุญแจเล็กทรอนิกส์…….……. ……7
พอร์ต USB …….…….....8
การเข้ารหัสข้อมูล…….…….....12
การเข้ารหัสลับแบบ RSA…….…..13
การลดทอนสมการรูปแบบ RSA……..... 14
สรุปท้ายบท…….…….....26
3. การออกแบบกุญแจอิเล็กทรอนิกส์…….... 28
ข้อพิจารณาในการออกแบบ…….. .28
ขั้นตอนการออกแบบ…….……29
การประยุกต์ใช้งาน……37
สรุปท้ายบท…….……39
4. ผลการทดสอบกุญแจอิเล็กทรอนิกส์…….....40
วิธีการทดสอบ…….……. 40
ผลการทดสอบ…….....41

สารบัญ (ต่อ)

หน้า

การป้องกันการเจาะระบบ……. 43

ประสิทธิภาพการลดทอนของ Montgomery Reduction Algorithm…….…… 43

ความเร็วในการประมวลผลการเข้ารหัสแบบ RSA…… 47

สรุปท้ายบท……..... 50

5. สรุปปัญหาและข้อเสนอแนะ…….……... 51

ปัญหาและข้อเสนอแนะ…… 51

แนวโน้มในการพัฒนาต่อไปในอนาคต…… 52

บรรณานุกรม…….……53

ภาคผนวก……..……..... 54

ก. การประยุกต์ใช้งานกุญแจอิเล็กทรอนิกส์เบื้องต้น.....55

ข. รายละเอียดของวงจร และการออกแบบวงจร…… 61

ค. ประสิทธิภาพของการลดทอนแบบ Montgomery ……..……66

ง. การตีพิมพ์เผยแพร่ผลงาน……..72

ประวัติผู้เขียน…….…….....79

รายการตาราง

ตาราง **หน้า**

2-1 ตัวอย่างการคำนวณของวิธีการทวินิยม..... 15

2-2 การเตรียมค่า M^w ก่อนการคำนวณและแบ่ง e ออกเป็นกลุ่ม ๆ ละ 2 บิต..... 17

2-3 ตัวอย่างการคำนวณวิธีการจตุนิยม.....17

2-4 การเตรียมค่า M^w ก่อนคำนวณและแบ่ง e ออกเป็นกลุ่มละ 3 บิต..... 18

2-5 ตัวอย่างการคำนวณวิธีการอัฐนิยม..... 18

2-6 การเตรียมค่า M^w ก่อนคำนวณ หลังจากปรับปรุง..... 19

2-7 การเปรียบเทียบวิธีการทวินิยมกับวิธีการ m-ary 20

2-8 การเตรียมการคำนวณของ CLNW 22

2-9 ตัวอย่างการคำนวณแบบ CLNW..... 22

4-1 ขนาดของโค้ดโปรแกรมและไฟล์กระทำ..... 48

รายการภาพประกอบ

ภาพประกอบ **หน้า**

1-1 ลักษณะฮาร์ดแวร์ล็อกผ่านทางพอร์ตขนาน……..2

1-2 FDI โมดูล FT245BM ……..…….....3

1-3 ลักษณะของฮาร์ดล็อก……..... 4

2-1 ลักษณะการติดต่อระหว่างซอฟต์แวร์กับฮาร์แวร์…….…….. 9

2-2 โครงสร้างการส่งข้อมูลของ USB ……... 11

2-3 ระบบการเข้าและถอดรหัส แบบกุญแจอสมมาตร……..13

3-1 โครงสร้างภายในกุญแจอิเล็กทรอนิกส์……29

3-2 ลักษณะการประกอบอุปกรณ์เพื่อรับส่งข้อมูลผ่านพอร์ต USB …….……30

3-3 การประกอบอุปกรณ์เพื่อสื่อสารระหว่าง PC 2 เครื่อง …….……... 31

3-4 โพรโทคอลในการสื่อสาร…….……31

3-5 ผังงานการสื่อสารระหว่าง PC 2 เครื่อง..... 33

3-6 การเข้ารหัสลับแบบ RSA โดยใช้วิธีการลดทอน Montgomery …….……..... 35

3-7 ลักษณะการจัดวงจรเพื่อสื่อสารระหว่าง PC กับไมโครคอนโทรลเลอร์……... 36

3-8 ผังงานการทำงานของกุญแจอิเล็กทรอนิกส์…….…….…….…..... 38

3-9 วงจรของกุญแจอิเล็กทรอนิกส์……..…….. 39

4-1 ผู้ใช้ล็อกอิน…… 41

4-2 กรณีผู้ใช้ไม่เสียบกุญแจก่อนใช้งาน……41

4-3 กรณีผู้ใช้กรอกบัญชีผู้ใช้ หรือรหัสผ่านผิด……...……..42

4-4 กรณีผู้ใช้เสียบกุญแจผิดดอก……..... 42

4-5 กรณีผู้ใช้แสดงสิทธิการใช้ได้อย่างถูกต้อง.....42

4-6 ประสิทธิภาพการลดทอน……..……..44

4-7 เปรียบเทียบตัวเลขที่เกิดจากการเข้ารหัสแบบ RSA โดยใช้ทฤษฎีการลดทอนแบบ Montgomery และการไม่ใช้ทฤษฎีลดทอน……..……44

4-8 ประสิทธิภาพการลดทอนจากการทดลอง…… 46

4-9 ประสิทธิภาพการลดทอนจากการปรับเส้นโค้ง…… 47

4-10 ความเร็วในการประมวลผลบน CPU …… 47

รายการภาพประกอบ (ต่อ)

ภาพประกอบ **หน้า**

4-11 การวัดความเร็วในการประมวลผลบนไมโครคอลโทรลเลอร์..... 49

ก-1 การแทรกโค้ดโปรแกรมเพื่อประยุกต์ใช้งาน กุญแจอิเล็กทรอนิกส์..... 56

ก-2 Package wizard 57

ก-3 Package Type..... 57

ก-4 Package Folder 57

ก-5 Create Folder..... 57

ก-6 Include Files 58

ก-7 Cab Options 58

ก-8 Installation Title 58

ก-9 Start Menu Items..... 59

ก-10 Install Locations 59

ก-11 Shared Files..... 59

ก-12 Finished 60

ก-13 Packaging Report 60

ข-1 บอร์ด U Board 62

ข-2 บอร์ด JX-876 62

ข-3 วงจร U Board..... 63

ข-4 วงจร JX-876 Board..... 64

ข-5 ลายวงจรกุญแจอิเล็กทรอนิกส์..... 64

ข-6 การวางอุปกรณ์ของกุญแจอิเล็กทรอนิกส์..... 65

สัญลักษณ์คำย่อและตัวอักษร

ACK = Acknowledge

A*B = A คูณ B

$A \cdot B$ = A คูณ B

$\phi(n)$ = Euler Totient Function

GCD = หารร่วมมาก (Greatest Common Divisor)

Mod = Modular

MonPro() = Montgomery product algorithm

ModExp() = Modular Exponentiation

PC = Personal Computer

r^{-1} เป็นค่าผกผันของ r modulo n