

สารบัญ

	หน้า
บทคัดย่อภาษาไทย.....	ก
บทคัดย่ออังกฤษ.....	ข
กิตติกรรมประกาศ.....	ค
สารบัญ.....	ง
สารบัญตาราง.....	ฉ
สารบัญรูป.....	ญ
บทที่ 1 บทนำ	
1.1 ที่มาและความสำคัญของโครงการ.....	1
1.2 วัตถุประสงค์โครงการ.....	1
1.3 ขอบข่ายการทำงาน.....	2
1.4 ขั้นตอนดำเนินงาน.....	2
1.5 แผนการดำเนินงาน.....	2
1.6 ผลที่คาดว่าจะได้รับ.....	3
1.7 งบประมาณ.....	3
บทที่ 2 หลักการและทฤษฎีที่เกี่ยวข้อง	
2.1 การเข้ารหัสข้อมูลลับ(Cryptography).....	4
2.2 ประเภทของการเข้ารหัสลับข้อมูล.....	4
2.3 ลักษณะของการเข้ารหัสลับที่ดี.....	6
2.4 ประโยชน์ของการเข้ารหัส.....	7
2.5 อัลกอริทึมที่ใช้ในการเข้ารหัส.....	7
2.6 ตารางสรุปคุณสมบัติของแต่ละอัลกอริทึม.....	21
บทที่ 3 ขั้นตอนการดำเนินงาน	
3.1 การศึกษาทฤษฎีและหลักการของอัลกอริทึมในการเข้ารหัส.....	22
3.2 การศึกษาและพัฒนาโปรแกรม.....	23
3.3 การทดสอบประสิทธิภาพในการเข้ารหัสแต่ละอัลกอริทึม.....	26

สารบัญ (ต่อ)

	หน้า
บทที่ 4 ผลการทดลองและการวิเคราะห์ผล	
4.1 ผลการทดสอบโปรแกรม.....	32
4.2 ตารางสรุปผลการทดลอง.....	60
4.3 สรุปเวลาที่ใช้ในการเข้ารหัสของแต่ละประเภทไฟล์.....	63
บทที่ 5 สรุปผล	
5.1 การสรุป และอภิปรายผล.....	65
5.2 ปัญหาที่พบ.....	66
5.3 ข้อเสนอแนะ.....	66
บรรณานุกรม.....	67
ประวัติผู้เขียนโครงการ.....	68

สารบัญตาราง

ตารางที่	หน้า
2.1	เปรียบเทียบคุณสมบัติของอัลกอริทึมในการเข้ารหัส21
4.1	ตารางผลการเข้ารหัสข้อมูล Plan Text ด้วยอัลกอริทึมแบบ AES (คีย์ 128 บิต)33
4.2	ตารางผลการเข้ารหัสข้อมูล Semi Binary File ด้วยอัลกอริทึมแบบ AES (คีย์ 128 บิต)33
4.3	ตารางผลการเข้ารหัสข้อมูล Pure Binary File ด้วยอัลกอริทึมแบบ AES (คีย์ 128 บิต)34
4.4	ตารางผลการเข้ารหัสข้อมูล Plan Text ด้วยอัลกอริทึมแบบ AES (คีย์ 192 บิต)34
4.5	ตารางผลการเข้ารหัสข้อมูล Semi Binary File ด้วยอัลกอริทึมแบบ AES (คีย์ 192 บิต)35
4.6	ตารางผลการเข้ารหัสข้อมูล Pure Binary File ด้วยอัลกอริทึมแบบ AES (คีย์ 192 บิต)35
4.7	ตารางผลการเข้ารหัสข้อมูล Plan Text ด้วยอัลกอริทึมแบบ AES (คีย์ 256 บิต)36
4.8	ตารางผลการเข้ารหัสข้อมูล Semi Binary File ด้วยอัลกอริทึมแบบ AES (คีย์ 256 บิต)36
4.9	ตารางผลการเข้ารหัสข้อมูล Pure Binary File ด้วยอัลกอริทึมแบบ AES (คีย์ 256 บิต)37
4.10	ตารางผลการเข้ารหัสข้อมูล Plan Text ด้วยอัลกอริทึมแบบ Serpent (คีย์ 128 บิต)37
4.11	ตารางผลการเข้ารหัสข้อมูล Semi Binary File ด้วยอัลกอริทึมแบบ Serpent (คีย์ 128 บิต)38
4.12	ตารางผลการเข้ารหัสข้อมูล Pure Binary File ด้วยอัลกอริทึมแบบ Serpent (คีย์ 128 บิต)38
4.13	ตารางผลการเข้ารหัสข้อมูล Plan Text ด้วยอัลกอริทึมแบบ Serpent (คีย์ 192 บิต)39

สารบัญตาราง (ต่อ)

ตารางที่	หน้า
4.14 ตารางผลการเข้ารหัสข้อมูล Semi Binary File ด้วยอัลกอริทึมแบบ Serpent (คีย์ 192 บิต)	39
4.15 ตารางผลการเข้ารหัสข้อมูล Pure Binary File ด้วยอัลกอริทึมแบบ Serpent (คีย์ 192 บิต)	40
4.16 ตารางผลการเข้ารหัสข้อมูล Plan Text ด้วยอัลกอริทึมแบบ Serpent (คีย์ 256 บิต)	40
4.17 ตารางผลการเข้ารหัสข้อมูล Semi Binary File ด้วยอัลกอริทึมแบบ Serpent (คีย์ 256 บิต)	41
4.18 ตารางผลการเข้ารหัสข้อมูล Pure Binary File ด้วยอัลกอริทึมแบบ Serpent (คีย์ 256 บิต)	41
4.19 ตารางผลการเข้ารหัสข้อมูล Plan Text ด้วยอัลกอริทึมแบบ RC2 (คีย์ 8 บิต)	42
4.20 ตารางผลการเข้ารหัสข้อมูล Semi Binary File ด้วยอัลกอริทึมแบบ RC2 (คีย์ 8 บิต)	42
4.21 ตารางผลการเข้ารหัสข้อมูล Pure Binary File ด้วยอัลกอริทึมแบบ RC2 (คีย์ 8 บิต)	43
4.22 ตารางผลการเข้ารหัสข้อมูล Plan Text ด้วยอัลกอริทึมแบบ RC2 (คีย์ 64 บิต)	43
4.23 ตารางผลการเข้ารหัสข้อมูล Semi Binary File ด้วยอัลกอริทึมแบบ RC2 (คีย์ 64 บิต)	44
4.24 ตารางผลการเข้ารหัสข้อมูล Pure Binary File ด้วยอัลกอริทึมแบบ RC2 (คีย์ 64 บิต)	44
4.25 ตารางผลการเข้ารหัสข้อมูล Plan Text ด้วยอัลกอริทึมแบบ RC2 (คีย์ 128 บิต)	45
4.26 ตารางผลการเข้ารหัสข้อมูล Semi Binary File ด้วยอัลกอริทึมแบบ RC2 (คีย์ 128 บิต)	45
4.27 ตารางผลการเข้ารหัสข้อมูล Pure Binary File ด้วยอัลกอริทึมแบบ RC2 (คีย์ 128 บิต)	46

สารบัญตาราง (ต่อ)

ตารางที่	หน้า
4.28 ตารางผลการเข้ารหัสข้อมูล Plan Text ด้วยอัลกอริทึมแบบ CAST6 (คีย์ 128 บิต)	46
4.29 ตารางผลการเข้ารหัสข้อมูล Semi Binary File ด้วยอัลกอริทึมแบบ CAST6 (คีย์ 128 บิต)	47
4.30 ตารางผลการเข้ารหัสข้อมูล Pure Binary File ด้วยอัลกอริทึมแบบ CAST6 (คีย์ 128 บิต)	47
4.31 ตารางผลการเข้ารหัสข้อมูล Plan Text ด้วยอัลกอริทึมแบบ CAST6 (คีย์ 192 บิต)	48
4.32 ตารางผลการเข้ารหัสข้อมูล Semi Binary File ด้วยอัลกอริทึมแบบ CAST6 (คีย์ 192 บิต)	48
4.33 ตารางผลการเข้ารหัสข้อมูล Pure Binary File ด้วยอัลกอริทึมแบบ CAST6 (คีย์ 192 บิต)	49
4.34 ตารางผลการเข้ารหัสข้อมูล Plan Text ด้วยอัลกอริทึมแบบ CAST6 (คีย์ 256 บิต)	49
4.35 ตารางผลการเข้ารหัสข้อมูล Semi Binary File ด้วยอัลกอริทึมแบบ CAST6 (คีย์ 256 บิต)	50
4.36 ตารางผลการเข้ารหัสข้อมูล Pure Binary File ด้วยอัลกอริทึมแบบ CAST6 (คีย์ 256 บิต)	50
4.37 ตารางผลการเข้ารหัสข้อมูล Plan Text ด้วยอัลกอริทึมแบบ Blowfish (คีย์ 48 บิต)	51
4.38 ตารางผลการเข้ารหัสข้อมูล Semi Binary File ด้วยอัลกอริทึมแบบ Blowfish (คีย์ 48 บิต)	51
4.39 ตารางผลการเข้ารหัสข้อมูล Pure Binary File ด้วยอัลกอริทึมแบบ Blowfish (คีย์ 48 บิต)	52
4.40 ตารางผลการเข้ารหัสข้อมูล Plan Text ด้วยอัลกอริทึมแบบ Blowfish (คีย์ 128 บิต)	52
4.41 ตารางผลการเข้ารหัสข้อมูล Semi Binary File ด้วยอัลกอริทึมแบบ Blowfish (คีย์ 128 บิต)	53

สารบัญตาราง (ต่อ)

ตารางที่	หน้า
4.42 ตารางผลการเข้ารหัสข้อมูล Pure Binary File ด้วยอัลกอริทึมแบบ Blowfish (คีย์ 128 บิต)	53
4.43 ตารางผลการเข้ารหัสข้อมูล Plan Text ด้วยอัลกอริทึมแบบ Blowfish (คีย์ 448 บิต)	54
4.44 ตารางผลการเข้ารหัสข้อมูล Semi Binary File ด้วยอัลกอริทึมแบบ Blowfish (คีย์ 448 บิต)	54
4.45 ตารางผลการเข้ารหัสข้อมูล Pure Binary File ด้วยอัลกอริทึมแบบ Blowfish (คีย์ 448 บิต)	55
4.46 ตารางผลการเข้ารหัสข้อมูล Plan Text ด้วยอัลกอริทึมแบบ Twofish (คีย์ 128 บิต)	55
4.47 ตารางผลการเข้ารหัสข้อมูล Semi Binary File ด้วยอัลกอริทึมแบบ Twofish (คีย์ 128 บิต)	56
4.48 ตารางผลการเข้ารหัสข้อมูล Pure Binary File ด้วยอัลกอริทึมแบบ Twofish (คีย์ 128 บิต)	56
4.49 ตารางผลการเข้ารหัสข้อมูล Plan Text ด้วยอัลกอริทึมแบบ Twofish (คีย์ 192 บิต)	57
4.50 ตารางผลการเข้ารหัสข้อมูล Semi Binary File ด้วยอัลกอริทึมแบบ Twofish (คีย์ 192 บิต)	57
4.51 ตารางผลการเข้ารหัสข้อมูล Pure Binary File ด้วยอัลกอริทึมแบบ Twofish (คีย์ 192 บิต).....	58
4.52 ตารางผลการเข้ารหัสข้อมูล Plan Text ด้วยอัลกอริทึมแบบ Twofish (คีย์ 256 บิต).....	58
4.53 ตารางผลการเข้ารหัสข้อมูล Semi Binary File ด้วยอัลกอริทึมแบบ Twofish (คีย์ 256 บิต).....	59
4.54 ตารางผลการเข้ารหัสข้อมูล Pure Binary File ด้วยอัลกอริทึมแบบ Twofish (คีย์ 256 บิต).....	59
5.1 เปรียบเทียบประสิทธิภาพของแต่ละอัลกอริทึม.....	66

สารบัญรูป

รูปที่	หน้า
2.1 วิธีการเข้าและถอดรหัสที่ใช้ในการรับส่งข้อความแบบ Secret Key	5
2.2 วิธีการเข้ารหัสและถอดรหัสที่ใช้ในการรับส่งข้อความแบบ Public Key	6
2.3 การเข้ารหัสด้วยอัลกอริทึมแบบ Serpent	8
2.4 การทำงานของฟังก์ชัน Feistel Network.....	11
2.5 กระบวนการการเข้ารหัสแบบ Twofish	13
2.6 ฟังก์ชัน h.....	17
2.7 การคำนวณใน 1 รอบของฟังก์ชัน F (128 bit key)	19
2.8 แผนผังการเข้ารหัสแบบ Twofish.....	20
3.1 Flow chart โปรแกรม Cryptie.....	23
3.2 User Case Diagram	24
3.3 Class Diagram	24
3.4 Collaboration Diagram.....	25
3.5 ขั้นตอนการ Encrypt/Decrypt ของ Library Bouncycastle.....	25
3.6 ขั้นตอนการสร้าง key ของ Library Bouncycastle.....	26
3.7 หน้าต่างโปรแกรม Cryptie.....	27
3.8 หน้าต่างเพื่อให้หาตำแหน่งของข้อมูลที่ต้องการ.....	27
3.9 การใส่ Password การเลือก Solution ต่างๆ ในการเข้ารหัส.....	28
3.10 ข้อความเมื่อการเข้ารหัสเสร็จแล้ว.....	28
3.11 ตำแหน่งของข้อมูลหลังการเข้ารหัสแล้ว.....	29
3.12 การใส่ Password การเลือก Solution ต่างๆ ในการถอดรหัส.....	29
3.13 ข้อความแสดงว่าในตำแหน่งนั้นมีไฟล์ชื่อนี้อยู่แล้ว ต้องการเปลี่ยนชื่อหรือไม่.....	30
4.1 คุณสมบัติของเครื่องคอมพิวเตอร์ที่ใช้ทดสอบ.....	31
4.2 เปรียบเทียบเวลาในการเข้ารหัสและถอดรหัสด้วยอัลกอริทึมแบบ AES.....	60
4.3 เปรียบเทียบเวลาในการเข้ารหัสและถอดรหัสด้วยอัลกอริทึมแบบ Serpent.....	60
4.4 เปรียบเทียบเวลาในการเข้ารหัสและถอดรหัสด้วยอัลกอริทึมแบบ RC2.....	61
4.5 เปรียบเทียบเวลาในการเข้ารหัสและถอดรหัสด้วยอัลกอริทึมแบบ CAST6.....	61
4.6 เปรียบเทียบเวลาในการเข้ารหัสและถอดรหัสด้วยอัลกอริทึมแบบ Blowfish.....	62
4.7 เปรียบเทียบเวลาในการเข้ารหัสและถอดรหัสด้วยอัลกอริทึมแบบ Twofish.....	62

สารบัญรูป (ต่อ)

รูปที่	หน้า
4.8	
เปรียบเทียบเวลาในการเข้ารหัสไฟล์ประเภท Plan Text ของแต่ละอัลกอริทึม.....	63
4.9	
เปรียบเทียบเวลาในการเข้ารหัสไฟล์ประเภท Semi Binary File ของแต่ละอัลกอริทึม.....	63
4.10	
เปรียบเทียบเวลาในการเข้ารหัสไฟล์ประเภท Pure Binary File ของแต่ละอัลกอริทึม.....	64

