สารบัญ

	หน้า
บทคัดย่อภาษาไทย	ก
บทคัดย่อภาษาอังกฤษ	ข
กิตติกรรมประกาศ	ค
สารบัญตาราง	ง
สารบัญภาพ	ฉ
บทที่ 1 บทนำ	1
1. ความเป็นมาและความสำคัญของปัญหา	1
2. จุดประสงค์ของงานวิจัย	2
3. ขอบเขตของงานวิจัย	2
4. ประโยชน์ที่คาดว่าจะได้รับจากงานวิจัย	2
บทที่ 2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง	4
1. วิทยาการรหัสลับ	4
2. อัลกอริทึมที่ใช้ในการดำเนินงาน	5
3. ยูนิโค้ด	45
4. งานวิจัยที่เกี่ยวข้อง	48
บทที่ 3 วิธีการดำเนินการวิจัย	53
บทที่ 4 ผลการทดลอง	65
บทที่ 5 สรุปผลการศึกษา	70
1. สรุปผลการทดลอง	70
2. ข้อเสนอแนะ	70
เอกสารอ้างอิง	72
ภาคผนวก	73
ประวัติผู้เขียน	119

มหาวิทยาลัยขอนแก่น

สารบัญตาราง

		หน้า
ตารางที่ 1	Initial Permutation (IP)	7
ตารางที่ 2	Permuted Choice 1 (PC-1)	8
ตารางที่ 3	Left Shift	8
ตารางที่ 4	Permuted Choice 2 (PC-2)	9
ตารางที่ 5	Expansion (E)	11
ตารางที่ 6	ตัวอย่างการ XOR ของ f(R,K) ขนาด 48 บิต	15
ตารางที่ 7	ตัวอย่างการลดขนาดบิตโดยใช้ S-Box ทั้ง 8	17
ตารางที่ 8	Primitive function P	18
ตารางที่ 9	ตัวอย่างการ XOR ของ f(R,K) ขนาด 32 บิต	19
ตารางที่ 10	Inverse of the initial permutation	20
ตารางที่ 11	Key Schedule	40
ตารางที่ 12	เปรียบเทียบเวลาการทำงาน (หน่วย วินาที) ของอัลกอริทึมกุญแจรหัสลับในโหมดของ ECB บนเครื่องแบบ Pentium-II 266 MHz.	51
ตารางที่ 13	เปรียบเทียบเวลาการทำงาน (หน่วย วินาที) ของอัลกอริทึมกุญแจรหัสลับในโหมดของ ECB บนเครื่องแบบ Pentium-4 2.4 GHz.	52
ตารางที่ 14	อธิบายแถวในการอ่านค่าในตารางที่ 15 สำหรับการแสดงผลภาษาไทย	55
ตารางที่ 15	แสดงค่า Unicode สำหรับการแสดงผลภาษาไทย	55
ตารางที่ 16	อธิบายแถวในการอ่านค่าในตารางที่ 17 สำหรับการแสดงผลภาษาอังกฤษ	56
ตารางที่ 17	แสดงค่า Unicode สำหรับการแสดงผลภาษาอังกฤษ	56
ตารางที่ 18	แสดงค่าเวลาที่ใช้ในการเข้าและถอดรหัสชุดข้อความภาษาไทยที่ขนาด 4 kb โดย DES Algorithm และคำนวณค่าเวลาเฉลี่ย	66
ตารางที่ 19	แสดงค่าเวลาที่ใช้ในการเข้าและถอดรหัสชุดข้อความภาษาไทยที่ขนาด 10 kb โดย DES Algorithm และคำนวณค่าเวลาเฉลี่ย	67
ตารางที่ 20	แสดงค่าเวลาที่ใช้ในการเข้าและถอดรหัสชุดข้อความภาษาไทยที่ขนาด 14 kb โดย DES Algorithm และคำนวณค่าเวลาเฉลี่ย	67

สารบัญตาราง (ต่อ)

		หน้า
ตารางที่ 21	แสดงค่าเวลาที่ใช้ในการเข้าและถอดรหัสชุดข้อความภาษาไทยที่ขนาด 4 kb โดย AES Algorithm และคำนวณค่าเวลาเฉลี่ย	67
ตารางที่ 22	แสดงค่าเวลาที่ใช้ในการเข้าและถอดรหัสชุดข้อความภาษาไทยที่ขนาด 10 kb โดย AES Algorithm และคำนวณค่าเวลาเฉลี่ย	68
ตารางที่ 23	แสดงค่าเวลาที่ใช้ในการเข้าและถอดรหัสชุดข้อความภาษาไทยที่ขนาด 14 kb โดย AES Algorithm และคำนวณค่าเวลาเฉลี่ย	68
ตารางที่ 24	แสดงค่าเวลาเฉลี่ยที่ใช้ในการเข้าและถอดรหัสข้อความภาษาไทยที่มีขนาดที่แตกต่างกันสำหรับ อัลกอริทึม DES และ AES	69

มหาวิทยาลัยขอนแก่น

สารบัญภาพ

		หน้า
ภาพที่ 1	แสดงการทำงานของอัลกอริทึม DES โดย การนำเข้าข้อมูลขนาด 64 บิต และ กุญแจขนาด 54 บิต	6
ภาพที่ 2	Left Shift	9
ภาพที่ 3	สรุปขั้นตอนการสร้างกุญแจย่อยจำนวน 16 ดอก	10
ภาพที่ 4	การคำนวณรอบที่ของการทำงานของ DES algorithm	10
ภาพที่ 5	การลดขนาดบิตโดยผ่าน S-BOX ถูกลดความยาวลงเหลือ 32 บิต	12
ภาพที่ 6	แปลงข้อมูล 6 บิตเหลือ 4 บิต	12
ภาพที่ 7	ตัวอย่าง การอ้างอิงตัวเลขจากตาราง s box ในการลดขนาดบิต	13
ภาพที่ 8	แปลงข้อมูล 6 บิตเหลือ 4 บิต โดยผ่าน ตาราง s1	13
ภาพที่ 9	ค่าอ้างอิงตาราง S box ทั้ง 8 ตาราง ของการลดขนาดบิต	14
ภาพที่ 10	สรุปขั้นตอนการคำนวณอัลกอริทึมแบบ DES	20
ภาพที่ 11	โครงสร้างการเข้ารหัสและถอดรหัสของอัลกอริทึมเออีเอสอย่างง่าย	22
ภาพที่ 12	Hexadecimal representation of bit patterns	23
ภาพที่ 13	State array input and output	24
ภาพที่ 14	แสดงตัวอย่างอาร์เรย์ของสี่คำ	25
ภาพที่ 15	Key-Block-Round Combinations	28
ภาพที่ 16	SubBytes ( ) ที่ประยุกต์ใช้ S-box ในแต่ละ ไบท์ ของ State	28
ภาพที่ 17	S-box สำหรับการแทนที่ค่า byte xy (ในรูปแบบเลขฐานสิบหก)	29
ภาพที่ 18	ShiftRow ( ) การเลื่อน 3 แถว	30
ภาพที่ 19	MixColumns ( ) ทำงานแบบ คอลัมน์ต่อคอลัมภ์	31
ภาพที่ 20	AddRoundKey ( ) XORs แต่ละคอลัมน์ของ State กับคำ จากตารางกุญแจ	31
ภาพที่ 21	Pseudo code สำหรับ Key Expansion	32
ภาพที่ 22	สรุปการคำนวณ AES อัลกอริทึม ขนาด 128 บิต ซึ่ง มีค่าในรูปเลขฐานสิบหก	38
ภาพที่ 23	สรุปค่าการคำนวณในการสร้างกุญแจ AES 128 บิต	44
ภาพที่ 24	ตัวอย่างการเข้ารหัสตัวอักษร ASCII และ Unicode	46

สารบัญภาพ (ต่อ)

		หน้า
ภาพที่ 25	ตัวอย่างรูปแบบการเข้ารหัสที่ออกแบบให้ประหยัดที่เก็บข้อมูลมากขึ้น	47
ภาพที่ 26	การแทนตัวอักษรภาษาไทยด้วยตัวเลข	48
ภาพที่ 27	ขั้นตอนการวิธีการวิจัยและพัฒนาโปรแกรมประยุกต์	53
ภาพที่ 28	แสดงการทำงานเบื้องต้นของอัลกอริทึม DES	60
ภาพที่ 29	แสดงการทำงานเบื้องต้นของอัลกอริทึม AES	61
ภาพที่ 30	แสดงการเข้าและถอดรหัสด้วยเทคนิค mapping	63
ภาพที่ 31	แสดงหน้าจอส่วนประกอบของซอฟต์แวร์ที่สร้าง	64
ภาพที่ 32	ตัวอย่างการเข้าและถอดรหัสข้อความภาษาไทยขนาด 14 kb ด้วยอัลกอริทึม AES	65
ภาพที่ 33	กราฟแสดงความสัมพันธ์ขนาดของข้อความที่นำเข้าเทียบกับเวลาที่ใช้ในการประมวลของแต่ละอัลกอริทึม	69

มหาวิทยาลัยขอนแก่น