

การพัฒนาอเทENTIเคเตอร์และเอนคริปเตอร์เพื่อรักษาความปลอดภัยของข้อมูล



นาย นริศ รังษีนพมาศ

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

ภาควิชาวิศวกรรมไฟฟ้า

บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย

พ.ศ.2538

ISBN 974-631-401-7

ลิขสิทธิ์ของบัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย

I16814343

Development of an Authenticator and Encryptor for Data Security

Mr. Naris Rangsinoppamas

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Engineering

Department of Electrical Engineering

Graduate School

Chulalongkorn University

1995

ISBN 974-631-401-7



หัวข้อวิทยานิพนธ์    การพัฒนาอเทนทีเคเตอร์และเอนคริปเตอร์เพื่อรักษาความปลอดภัยของข้อมูล  
โดย                            นาย นริศ รังษีนพมาศ  
ภาควิชา                        วิศวกรรมไฟฟ้า  
อาจารย์ที่ปรึกษา        รองศาสตราจารย์ ดร.ประสิทธิ์ ประพัฒน์มงคลการ

---

บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้บัณฑิตวิทยาลัยนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรบัณฑิต

.....คณบดีบัณฑิตวิทยาลัย  
( รองศาสตราจารย์ ดร. สันติ กุงสุวรรณ )

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ  
( รองศาสตราจารย์ ดร.สมชาย จิตะพันธ์กุล )

.....อาจารย์ที่ปรึกษา  
( รองศาสตราจารย์ ดร.ประสิทธิ์ ประพัฒน์มงคลการ )

.....กรรมการ  
( ดร.วาทิต เบญจพลกุล )

.....กรรมการ  
( นาวาโท มิ่ง อิมวิทยา )

พิมพ์ต้นฉบับบทคัดย่อวิทยานิพนธ์ภายในกรอบสี่เหลี่ยมนี้เพียงแผ่นเดียว



นริศ รังษีนพมาศ : การพัฒนาอเทวนิโคเดเตอร์และเอนคริปเตอร์เพื่อรักษาความปลอดภัยของข้อมูล  
(DEVELOPMENT OF AN AUTHENTICATOR AND ENCRYPTOR FOR DATA SECURITY) อ.ที่ปรึกษา :  
รศ.ดร.ประสิทธิ์ ประพัฒน์มงคลการ, 142 หน้า. ISBN 974-631-401-7

ในวิทยานิพนธ์ฉบับนี้นับเป็นความก้าวหน้าอีกขั้นหนึ่งในการพัฒนาระบบการรักษาความปลอดภัยของข้อมูล ด้วยการเข้ารหัสลับตามมาตรฐาน DES (Data Encryption Standard) ที่มีโหมดในการเข้ารหัสทั้ง 4 โหมด คือ ECB (Electronic Codebook), CBC (Cipher Block Chaining), CFB (Cipher Feedback) และ OFB (Output Feedback) ในการ์ดเดียวกัน ซึ่งแต่ละโหมดจะมีคุณสมบัติที่เหมาะสมสำหรับชนิดข้อมูลที่แตกต่างกัน และยังได้นำเสนอวิธีรับรองข้อความที่ต้องมีการลงทะเบียนไฟล์ (File Registration) ก่อน เพื่อป้องกันข้อมูลถูกแก้ไขในขณะที่ถูกเก็บอยู่ในที่ที่ไม่มีการควบคุมการเข้าถึง โดยวิธีนี้จะสร้างรหัสรับรองข้อความ (Authentication Code) จากไซเฟอร์เท็กซ์แทนการสร้างจากเพลนเท็กซ์ ทำให้มีความปลอดภัยมากขึ้น อย่างไรก็ตามวิธีการที่นำเสนอนี้จะใช้เวลาในการรับรองข้อความสูงขึ้น การ์ดดังกล่าวจะใช้ร่วมกับเครื่องไมโครคอมพิวเตอร์ โดยผู้วิจัยได้พัฒนาโปรแกรมควบคุมการทำงานและโปรแกรมอรรถประโยชน์สำหรับแสดงเวลาที่ใช้ในการเข้ารหัสโหมดต่าง ๆ และสามารถดูข้อมูลเปรียบเทียบก่อนและหลังจากเข้ารหัส นอกจากนี้ยังสามารถพิมพ์ข้อมูลซึ่งประกอบด้วยอักขระพิเศษออกจากเครื่องพิมพ์เพื่ออำนวยความสะดวกแก่ผู้ใช้งาน

ภาควิชา .....  
สาขาวิชา .....  
ปีการศึกษา .....

ลายมือชื่อนิสิต .....  
ลายมือชื่ออาจารย์ที่ปรึกษา .....  
ลายมือชื่ออาจารย์ที่ปรึกษาร่วม .....

## C315524 : MAJOR ELECTRICAL ENGINEERING  
KEY WORD: AUTHENTICATION / ENCRYPTION / DATA SECURITY  
NARIS RANGSINOPPAMAS : DEVELOPMENT OF AN  
AUTHENTICATOR AND ENCRYPTOR FOR DATA SECURITY.  
THESIS ADVISOR :  
ASSO.PROF.PRASIT PRAPINMONGKOLKARN,PH.D.  
142 pp. ISBN 974-631-401-7

This thesis presents another significant development of the data security system that uses a Data Encryption Standard (DES) algorithm. There are 4 DES modes of operations that are appropriate for different application of work. The operation modes are Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), and Output Feedback (OFB) and all of them are incorporated in a single computer interface card. In addition, it presents an authentication technique which the file has to register (File Registration) prior to authenticate and the authentication code (AC) is generated from a ciphertext instead of plaintext. This technique, in term of security, improves the system performance but however it takes more time. All operations are controlled by a software written in a menu driven style with many utilities to support the user to do the work in an easy way.

ภาควิชา..... วิศวกรรมไฟฟ้า .....

สาขาวิชา..... วิศวกรรม.....

ปีการศึกษา..... 2537 .....

ลายมือชื่อนิสิต..... น.น. รังสินอภามาส .....

ลายมือชื่ออาจารย์ที่ปรึกษา.....  .....

ลายมือชื่ออาจารย์ที่ปรึกษาร่วม.....



## กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลงได้เนื่องมาจากการให้ความช่วยเหลือความรู้คำแนะนำและปรึกษาอย่างใกล้ชิดของรองศาสตราจารย์ ดร.ประสิทธิ์ ประพัฒน์มงคล ซึ่งนอกจากจะเป็นอาจารย์ที่ปรึกษาในด้านวิชาการแล้วท่านยังเป็นผู้ที่เป็นแบบอย่างที่ดีของข้าพเจ้าในด้านการงานที่ทุ่มเทเต็มกำลังความสามารถเพื่อให้เกิดประโยชน์ต่อหน่วยงานและสังคมซึ่งข้าพเจ้าถือว่าเป็นพระคุณอันยิ่งใหญ่ จึงขอกราบขอบพระคุณมา ณ. โอกาสนี้

ข้าพเจ้าขอกราบขอบพระคุณรองศาสตราจารย์ ดร.สมชาย จิตะพันธ์กุล, ดร.วาทิต เบญจพลกุล และ นท.มิ่ง อิมวิทยา ที่ได้คำแนะนำในการทำวิทยานิพนธ์ฉบับนี้สมบูรณ์

นอกจากนี้ข้าพเจ้าขอกราบขอบพระคุณครูและอาจารย์ที่ได้ถ่ายทอดวิชาความรู้อันเป็นเบื้องต้นขอขอบคุณ นต.ชาติชาย ดิษฐกุล และผู้เกี่ยวข้องทุกท่านที่ได้ให้ความช่วยเหลือในด้านต่าง ๆ

สุดท้ายนี้ ข้าพเจ้าขอกราบขอบพระคุณ คุณพ่อ คุณแม่ที่ท่านคอยห่วงใย สั่งสอน ดูแลเอาใจใส่จนข้าพเจ้าเติบโตมาจนสำเร็จการศึกษาในครั้งนี้ ไว้ ณ . ที่นี้ด้วย

นริศ รังษีนพมาศ

สารบัญ



	หน้า
บทคัดย่อภาษาไทย.....	ง
บทคัดย่อภาษาอังกฤษ.....	จ
กิตติกรรมประกาศ.....	ฉ
สารบัญตาราง.....	ช
สารบัญภาพ.....	ฅ
บทที่	
1. บทนำ.....	1
2. มาตรฐานการเข้ารหัสข้อมูล.....	4
3. บล็อกไซเฟอร์และสตรีมไซเฟอร์.....	20
4. ออเทENTIเคชัน.....	43
5. แนวทางในการออกแบบและรายละเอียดการทำงาน.....	50
6. การทดสอบการทำงาน.....	77
7. สรุปการวิจัยและข้อเสนอแนะ.....	100
เอกสารอ้างอิง.....	103
ภาคผนวก.....	104
ประวัติผู้เขียน.....	142

## สารบัญตาราง

ตารางที่		หน้า
2.1	การเลื่อนของข้อมูลที่ใช้ในการคำนวณหาค่าคีย์ของการเข้าและถอดรหัส.....	8
2.2	ตำแหน่งบิตของข้อมูลที่ใช้ในการคำนวณคีย์ที่ถูกเก็บไว้ในรีจิสเตอร์ C.....	10
2.3	ตำแหน่งบิตของข้อมูลที่ใช้ในการคำนวณคีย์ที่ถูกเก็บไว้ในรีจิสเตอร์ D.....	10
2.4	24 บิตแรกของคีย์ K(i) ในแต่ละรอบ.....	11
2.5	24 บิตหลังของคีย์ K(i) ในแต่ละรอบ.....	12
2.6	รายละเอียดใน S-BOX.....	15
5.1	การใช้งานแอดเดรสสำหรับพอร์ท I/O บนการ์ดต่าง ๆ.....	58
5.2	ตำแหน่งแอดเดรสในแต่ละกลุ่ม.....	59
5.3	รีจิสเตอร์ภายใน DEU.....	61
6.1	ผลการทดสอบเวลาที่ใช้ในการเข้ารหัสโหมด ECB.....	77
6.2	ผลการทดสอบเวลาที่ใช้ในการเข้ารหัสโหมด CBC.....	78
6.3	ผลการทดสอบเวลาที่ใช้ในการเข้ารหัสโหมด CFB.....	78
6.4	ผลการทดสอบเวลาที่ใช้ในการเข้ารหัสโหมด OFB.....	79
6.5	ผลการทดสอบการทำงานต่อเนื่อง.....	82
6.6	ผลการทดสอบความเชื่อถือได้ของเครื่องเข้ารหัส.....	83
6.7	แสดงขนาดของไฟล์ก่อนและหลังการเข้ารหัส.....	84



สารบัญภาพ

รูปที่		หน้า
1.1	การเข้ารหัสลับข้อมูล.....	1
2.1	การไหลของข้อมูลในมาตรฐานการเข้ารหัสข้อมูล.....	4
2.2	อัลกอริทึมของมาตรฐานการเข้ารหัสข้อมูล.....	5
2.3	การแปลงของบล็อกข้อมูลขาเข้า L(0) และ R(0).....	6
2.4	การแปลงเพื่อให้ได้ L(0).....	6
2.5	การคำนวณหาคีย์ K สำหรับการเข้ารหัสในแต่ละรอบ.....	7
2.6	รายละเอียดของฟังก์ชัน f.....	14
3.1	คอนเวนชันแนลอัลกอริทึมของบล็อกไซเฟอร์.....	22
3.2	การแปลงของบล็อกข้อมูลขาเข้า L(0) และ R(0).....	23
3.3	การแปลงเพื่อให้ได้ L(0).....	24
3.4	ตัวอย่างอัลกอริทึมในการเข้ารหัสด้วยบล็อกไซเฟอร์ 2 รอบ.....	25
3.5	การถอดรหัสโดยใช้ฟังก์ชันเดียวกับการเข้ารหัส.....	26
3.6	แนวคิดของสตรีมไซเฟอร์.....	27
3.7	การใช้วิธีการสร้างบิตสตรีมและการบวกแบบโมดูโล-2 ในสตรีมไซเฟอร์.....	28
3.8	สตรีมไซเฟอร์.....	29
3.9	การเข้ารหัสบล็อกแรกของเพลนเท็กซ์โดยใช้สตรีมไซเฟอร์.....	30
3.10	ตัวอย่างของเพลนเท็กซ์ที่มีความมึนรูปแบบของข้อมูลมาก.....	31
3.11	ไซเฟอร์เท็กซ์ที่ได้จากการเข้ารหัสเพลนเท็กซ์โดยใช้ DES ที่ไม่มีการเซอเน็ง.....	32
3.12	ตัวอย่างของการเซอเน็งในบล็อกไซเฟอร์โดยวิธีเพลนเท็กซ์-ไซเฟอร์เท็กซ์ฟีดแบ็ค.....	32
3.13	ไซเฟอร์บล็อกเซอเน็ง (CBC).....	33
3.14	รายละเอียดของไซเฟอร์บล็อกเซอเน็ง.....	34
3.15	ไซเฟอร์เท็กซ์ที่ได้จากการเข้ารหัสโดยใช้ไซเฟอร์บล็อกเซอเน็ง.....	35
3.16	การเข้ารหัสข้อมูลที่ไม่ครบเต็มบล็อก.....	36
3.17	สตรีมไซเฟอร์ที่มีคุณสมบัติของการกระจายความผิดพลาด.....	37
3.18	ไซเฟอร์เท็กซ์ออโตคีย์ไซเฟอร์.....	40

## สารบัญภาพ (ต่อ)

หน้า

รูปที่

3.19	ไซเฟอร์พีดแบ็ค.....	41
3.20	แสดงข้อมูลทางด้านผู้ส่งและผู้รับของไซเฟอร์พีดแบ็คที่มีคุณสมบัติเชลฟ์ ซินโครไนซ์.....	42
4.1	วิธีตรวจสอบข้อความโดยใช้รหัสรับรองข้อความ.....	43
4.2	การเข้ารหัสโดยใช้คีย์ที่ต่างกัน.....	44
4.3	แสดงการรับรองการเป็นผู้สร้างข้อความ.....	45
4.4	แสดงวิธีการรับรองความถูกต้องของเนื้อหาข้อความ.....	46
4.5	แสดงวิธีการรับรองความถูกต้องเนื้อหาของข้อความที่รหัสรับรองข้อความถูกสร้าง ภายใต้คีย์ที่รู้เฉพาะผู้รับและผู้ส่ง.....	47
4.6	วิธีการสำหรับการทำการรับรองข้อความ.....	48
5.1	การเข้ารหัสในโหมดไซเฟอร์บล็อกเซนนิ่ง.....	51
5.2	การเข้ารหัสในโหมดไซเฟอร์พีดแบ็ค.....	52
5.3	การเข้ารหัสในโหมดเอาท์พุทพีดแบ็ค.....	53
5.4	บล็อกไดอะแกรมออเทนทิเคเตอร์และเอนคริปเตอร์.....	55
5.5	อุปกรณ์ถอดรหัสแอดเดรส.....	57
5.6	อุปกรณ์สร้างสัญญาณควบคุมการเข้ารหัส.....	59
5.7	การต่อวงจรแบบ Polling Interface.....	60
5.8	วงจรมบรูณ์ของเอนคริปเตอร์และออเทนทิเคเตอร์.....	63
5.9	เมนูหลัก.....	64
5.10	เมนู Encryption.....	65
5.11	เมนู Encryp/ECB.....	66
5.12	การสร้าง AC ใน File Registration.....	68
5.13	เมนูใน View.....	72
5.14	โปรแกรม File Contents.....	73
5.15	โปรแกรม Processing Time.....	74

## . สารบัญภาพ (ต่อ)

รูปที่		หน้า
5.16	เมนูใน Print.....	75
5.17	รูปแบบการพิมพ์โปรแกรม Print.....	75
5.18	ตัวอย่างการพิมพ์ผิดพลาด.....	76
6.1	ความเร็วในการเข้ารหัสของโหมด ECB ,CBC และ CFB.....	79
6.2	ความเร็วในการเข้ารหัสของโหมด OFBที่ป้อนกลับด้วยพีดีบีเคคาร์เรคเตอร์ค่าต่างๆ	80
6.3	เวลาที่ใช้ในการเข้ารหัสไฟล์ขนาดเท่ากันโดยใช้จำนวนพีดีบีเคคาร์เรคเตอร์ ที่ไม่เท่ากันของโหมด OFB.....	80
6.4	ตัวอย่างของเพลนเท็กซ์ที่มีความมีรูปแบบ.....	86
6.5	ไซเฟอร์เท็กซ์ที่ได้จากการเข้ารหัสเพลนเท็กซ์ในรูป 6.1 ด้วยโหมด ECB.....	86
6.6	ไซเฟอร์เท็กซ์ที่ได้จากการเข้ารหัสเพลนเท็กซ์ในรูป 6.1 ด้วยโหมด CBC.....	87
6.7	ไซเฟอร์เท็กซ์ที่ได้จากการเข้ารหัสเพลนเท็กซ์ในรูป 6.1 ด้วยโหมด CFB.....	87
6.8	ไซเฟอร์เท็กซ์ที่ได้จากการเข้ารหัสเพลนเท็กซ์ในรูป 6.1 ด้วยโหมด OFB.....	88
6.9	ไฟล์ทดสอบ DES.DOC ที่ใช้ทดสอบการเข้ารหัส.....	88
6.10	ผลของการถอดรหัสด้วยโหมด CBC โดยใช้เวคเตอร์เริ่มต้น '1234567X'.....	89
6.11	ผลของการถอดรหัสด้วยโหมด CFB โดยใช้เวคเตอร์เริ่มต้น '1234567X'.....	89
6.12	ผลของการถอดรหัสด้วยโหมด OFB โดยใช้เวคเตอร์เริ่มต้น '1234567X'.....	90
6.13	ผลของการถอดรหัสด้วยโหมด ECB ที่ไซเฟอร์ไฟล์ถูกแก้ไขโดยการเปลี่ยนแปลงค่า....	91
6.14	ผลของการถอดรหัสด้วยโหมด CBC ที่ไซเฟอร์ไฟล์ถูกแก้ไขโดยการเปลี่ยนแปลงค่า....	91
6.15	ผลของการถอดรหัสด้วยโหมด CFB ที่ไซเฟอร์ไฟล์ถูกแก้ไขโดยการเปลี่ยนแปลงค่า....	92
6.16	ผลของการถอดรหัสด้วยโหมด OFB ที่ไซเฟอร์ไฟล์ถูกแก้ไขโดยการเปลี่ยนแปลงค่า....	92
6.17	ผลของการถอดรหัสด้วยโหมด ECB ที่ไซเฟอร์ไฟล์ถูกแก้ไขโดยการตัดออกบางส่วน....	93
6.18	ผลของการถอดรหัสด้วยโหมด ECB ที่ไซเฟอร์ไฟล์ถูกแก้ไขโดยการตัดออกบางส่วน....	94
6.19	ผลของการถอดรหัสด้วยโหมด ECB ที่ไซเฟอร์ไฟล์ถูกแก้ไขโดยการตัดออกบางส่วน....	94
6.20	ผลของการถอดรหัสด้วยโหมด ECB ที่ไซเฟอร์ไฟล์ถูกแก้ไขโดยการตัดออกบางส่วน....	95
6.21	การเกิดเซลฟ์ซินโครไนซ์ในโหมด CFB.....	95

สารบัญภาพ (ต่อ)

รูปที่		หน้า
6.21	การตรวจพบไฟล์ที่ลงทะเบียนแล้วถูกแก้ไข.....	97
6.22	แสดงการตรวจพบการแก้ไขในไฟล์ที่ผ่านการรับรองข้อความ.....	98