การพัฒนาออเทนทิเคเตอร์และเอนคริปเตอร์เพื่อรักษาความปลอดภัยของข้อมูล

นาย นริศ รังษีนพมาศ

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
ภาควิชาวิศวกรรมไฟฟ้า
บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย
พ.ศ.2538

ISBN 974-631-401-7

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 การพัฒนาออเทนทิเคเตอร์และเอนคริปเตอร์เพื่อรักษาความปลอดภัยของข้อมูล

โดย นาย นริศ รังษีนพมาศ

ภาควิชา วิศวกรรมไฟฟ้า

อาจารย์ที่ปรึกษา รองศาสตราจารย์ ดร.ประสิทธิ์ ประพิณมงคลการ

บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

.....คณบดีบัณฑิตวิทยาลัย

(รองศาสตราจารย์ ดร. สันติ ถุงสุวรรณ)

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ

(รองศาสตราจารย์ ดร.สมชาย จิตะพันธ์กุล)

.....อาจารย์ที่ปรึกษา

(รองศาสตราจารย์ ดร.ประสิทธิ์ ประพิณมงคลการ)

.....กรรมการ

(ดร.วาทิต เบญจพลกุล)

.....กรรมการ

(นาวาโท มิ่ง อิ่มวิทยา)

พิมพ์ต้นฉบับบทคัดย่อวิทยานิพนธ์ภายในกรอบสีเขียวนี้เพียงแผ่นเดียว

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

ในวิทยานิพนธ์ฉบับนี้นับเป็นความก้าวหน้าอีกขั้นหนึ่งในการพัฒนาระบบการรักษาความปลอดภัยของข้อมูลด้วยการเข้ารหัสลับตามมาตรฐาน DES (Data Encryption Standard) ที่มีโหมดในการเข้ารหัสทั้ง 4 โหมด คือ ECB (Electronic Codebook), CBC (Cipher Block Chaining), CFB (Cipher Feedback) และ OFB (Output Feedback) ในคาร์ดเดียวกัน ซึ่งแต่ละโหมดจะมีคุณสมบัติที่ดีเหมาะสำหรับชนิดข้อมูลที่แตกต่างกัน และยังได้นำเสนอวิธีรับรองข้อความที่ต้องมีการลงทะเบียนไฟล์ (File Registration) ก่อน เพื่อป้องกันข้อมูลถูกแก้ไขในขณะที่ถูกเก็บอยู่ในที่ที่ไม่มีการควบคุมการเข้าถึง โดยวิธีนี้จะสร้างรหัสรับรองข้อความ (Authentication Code) จากไซเฟ่อร์เท็กซ์แทนการสร้างจากเพลนเท็กซ์ ทำให้มีความปลอดภัยมากขึ้น อย่างไรก็ตามวิธีการที่นำเสนอนี้จะใช้เวลาในการรับรองข้อความสูงขึ้น คาร์ดดังกล่าวจะใช้ร่วมกับเครื่องไมโครคอมพิวเตอร์ โดยผู้วิจัยได้พัฒนาโปรแกรมควบคุมการทำงานและโปรแกรมอรรถประโยชน์สำหรับแสดงเวลาที่ใช้ในการเข้ารหัสโหมดต่าง ๆ และสามารถดูข้อมูลเปรียบเทียบก่อนและหลังจากเข้ารหัส นอกจากนี้ยังสามารถพิมพ์ข้อมูลซึ่งประกอบด้วยอักขระพิเศษออกทางเครื่องพิมพ์เพื่ออำนวยความสะดวกแก่ผู้ใช้งาน

ภาควิชา วิศวกรรมไฟฟ้า ลายมือชื่อนิสิต .....

สาขาวิชา วิศวกรรม ลายมือชื่ออาจารย์ที่ปรึกษา .....

ปีการศึกษา 2531 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 ลายมือชื่อนิสิต นริส รังสิโนปพรมาส

สาขาวิชา วิศวกรรมไฟฟ้า ลายมือชื่ออาจารย์ที่ปรึกษา ประสิทธิ์ ประพินมงคลกาญจน์

ปีการศึกษา 2537 ลายมือชื่ออาจารย์ที่ปรึกษาร่วม

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลงได้เนื่องมาจากการให้ความช่วยเหลือความรู้คำแนะนำและปรึกษาอย่างใกล้ชิดของรองศาสตราจารย์ ดร.ประสิทธิ์ ประพิณมงคลการ ซึ่งนอกจากจะเป็นอาจารย์ที่ปรึกษาในด้านวิชาการแล้วท่านยังเป็นผู้ที่เป็นแบบอย่างที่ดีของข้าพเจ้าในด้านการทำงานที่ทุ่มเทเต็มกำลังความสามารถเพื่อให้เกิดประโยชน์ต่อหน่วยงานและสังคมซึ่งข้าพเจ้าถือว่าเป็นพระคุณอันยิ่งใหญ่ จึงขอกราบขอบพระคุณมา ณ. โอกาสนี้

ข้าพเจ้าขอกราบขอบพระคุณรองศาสตราจารย์ ดร.สมชาย จิตะพันธ์กุล, ดร.วาทิต เบญจพลกุล และ นท.มิ่ง อิ่มวิทยา ที่ได้คำแนะนำในการทำให้วิทยานิพนธ์ฉบับนี้สมบูรณ์

นอกจากนี้ข้าพเจ้าขอกราบขอบพระคุณครูและอาจารย์ที่ได้ถ่ายทอดวิชาความรู้อันเป็นเบื้องต้น ขอขอบคุณ นต.ชาติชาย ดิษฐกุล และผู้เกี่ยวข้องทุกท่านที่ได้ให้ความช่วยเหลือในด้านต่าง ๆ

สุดท้ายนี้ ข้าพเจ้าขอกราบขอบพระคุณ คุณพ่อ คุณแม่ที่ท่านคอยห่วงใย สั่งสอน ดูแลเอาใจใส่จนข้าพเจ้าเติบโตมาจนสำเร็จการศึกษาในครั้งนี้ ไว้ ณ . ที่นี้ด้วย

นริศ รังษีนพมาศ

สารบัญ

หน้า

สารบัญตาราง

หน้า

ตารางที่

สารบัญภาพ

หน้า

รูปที่

สารบัญภาพ (ต่อ)

หน้า

รูปที่

สารบัญภาพ (ต่อ)

หน้า

รูปที่

สารบัญภาพ (ต่อ)

หน้า

รูปที่