การปรับเปลี่ยนวิธีการเข้ารหัสลับข้อมูลแบบอัลกอริทึมเดส

นางสาว สมศรี จตุรพิธพรชัย

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
ภาควิชาวิศวกรรมคอมพิวเตอร์
บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย
พ.ศ. 2533

ISBN 974-578-120-7

AN IMPROVEMENT SCHEME OF DES ALGORITHM IN DATA ENCRYPTION

Miss Somsri Chaturapitpornchai

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science
Department of Computer Engineering
Graduate School
Chulalongkorn University
1990

ISBN 974-578-120-7

หัวข้อวิทยานิพนธ์	การปรับเปลี่ยนวิธีการเข้ารหัสลับข้อมูลแบบอัลกอริทึมเดส
โดย	นางสาว สมศรี จตุรพิธพรชัย
ภาควิชา	วิศวกรรมคอมพิวเตอร์
อาจารย์ที่ปรึกษา	รองศาสตราจารย์ ดร. ศุภชัย ตั้งวงศ์ศานต์
	ผู้ช่วยศาสตราจารย์ ดร. วีระ ริ้วพิทักษ์

บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีบัณฑิตวิทยาลัย

(ศาสตราจารย์ ดร. ถาวร วัชราภัย)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ

(ผู้ช่วยศาสตราจารย์ สุยุชน์ สัตยประกอบ)

..... อาจารย์ที่ปรึกษา

(รองศาสตราจารย์ ดร. ศุภชัย ตั้งวงศ์ศานต์)

..... อาจารย์ที่ปรึกษาร่วม

(ผู้ช่วยศาสตราจารย์ ดร. วีระ ริ้วพิทักษ์)

..... กรรมการ

(ผู้ช่วยศาสตราจารย์ เมธี ศรีสังวาล)

..... กรรมการ

(อาจารย์ ชัยศิริ บัณฑิตานนท์)

พิมพ์ต้นฉบับบทคัดย่อวิทยานิพนธ์ภายในกรอบสีเขียวนี้เพียงแผ่นเดียว

สมศรี จตุรพิธพรชัย : การปรับเปลี่ยนวิธีการเข้ารหัสลับข้อมูลแบบอัลกอริทึมเดส (AN IMPROVEMENT SCHEME OF DES ALGORITHM IN DATA ENCRYPTION) อ.ที่ปรึกษา: รศ.ดร.ศุภชัย ตั้งวงศ์ศานต์ อ.ที่ปรึกษาร่วม: ผศ.วีระ ริ้วพิทักษ์, 98 หน้า. ISBN 974-578-120-7

จุดประสงค์ของการวิจัยนี้ เพื่อศึกษาหาอัลกอริทึมสำหรับการเข้ารหัสลับที่มีความซับซ้อนและประสิทธิภาพสูงกว่าวิธีการเดิม จากการศึกษาพบว่า ในปัจจุบันอัลกอริทึมเดส (Data Encryption Standard Algorithm : DES) เป็นอัลกอริทึมที่มีประสิทธิภาพ มีขั้นตอนการทำงานที่ซับซ้อน สามารถจะนำมาปรับเปลี่ยนขั้นตอนการทำงาน โดยการเปลี่ยนวิธีการแบ่งกลุ่มแบบเดิมที่เป็นแบบคงที่ (fixed box size) เป็นการแบ่งกลุ่มที่แปรเปลี่ยนได้ (variable box size) และมีการปรับเปลี่ยนค่าในตาราง S-boxes ให้เหมาะสมกับการแบ่งกลุ่ม เพื่อให้ได้อัลกอริทึมใหม่ที่มีประสิทธิภาพยิ่งขึ้น จากการเปรียบเทียบพบว่าอัลกอริทึมที่ได้ปรับเปลี่ยนแล้วมีความซับซ้อนกว่าอัลกอริทึมเดสเดิม จะเรียกอัลกอริทึมนี้ว่า อัลกอริทึมไอเดส (Improved DES หรือ IDES) และอัลกอริทึมเดสที่ปรับเปลี่ยนแล้วนี้จะไม่เป็นมาตรฐานอีกต่อไป

สำหรับความซับซ้อนของอัลกอริทึมไอเดส จะวัดจากปริมาณงานที่ต้องค้นหาค่าคีย์สำหรับการเข้ารหัสลับ และคำนวณได้ว่าจะเป็น $(N + 1)2^{32}$ เท่าของอัลกอริทึมเดส โดยที่ N คือ จำนวนวิธีการแบ่งกลุ่มที่เป็นไปได้ทั้งหมด และเฉพาะปริมาณงานเฉลี่ยที่ต้องทำเพื่อค้นหาค่าคีย์ของอัลกอริทึมเดสจะประมาณ 2^{55} ครั้ง นอกจากนี้ในการทดสอบเพื่อดูประสิทธิภาพในการเข้ารหัสลับข้อมูลของอัลกอริทึมไอเดสกับข้อมูลขนาดต่าง ๆ พบว่าอัลกอริทึมไอเดสมีประสิทธิภาพกว่าอัลกอริทึมเดส ผลของการวิจัยนี้ คือได้อัลกอริทึมสำหรับการเข้ารหัสลับ ที่มีความซับซ้อนยิ่งขึ้น สามารถป้องกันข้อมูลที่มีความสำคัญให้ปลอดภัยได้

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต สมศรี จตุรพิธพรชัย

สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์

ปีการศึกษา 2533 ลายมือชื่ออาจารย์ที่ปรึกษา

SOMSRI CHATURAPITPORNCHAI : AN IMPROVEMENT SCHEME OF DES ALGORITHM IN DATA ENCRYPTION. THESIS ADVISOR : ASSO.PROF. SUPACHAI TANGWONGSAN, Ph.D., ASST.PROF. VEERA REWPITAK, Ph.D. 98 PP. ISBN 974-578-120-7

This research is to study and search for a 'better' encryption algorithm which improves the performance and contains real complicated characteristics of data encryption. Through investigation DES (Data Encryption Standard) has been found to be an effective algorithm with extreamly complex process-stage. From the study, the process-stage of DES algorithm can be further improved such as : by modifying from the fixed box size division to variable box size division, and changing the contents of S-boxes table to match the changing division method in order to produce a more effective algorithm. Compared to the original DES version, this modified version appears to have more complicated processes. Hence, this new version has been named as an improved DES or IDES. Through some modification, IDES would no longer be considered as standard.

The complexity of IDES, measured by quantities of work to search for the cryptographic key accounts for $(N + 1)2^{32}$ times of DES algorithm, where N is the possible way to divide box size, and for DES, the average of work is 2^{55}. From the experiment, examples of various file sizes are presented to demonstrate the IDES performance, and compare it with DES, IDES has proved to be more effective than DES. Therefore, a more complex encryption algorithm which ensures better secrecial data security is the result of this research.

ภาควิชา วิศวกรรมคอมพิวเตอร์

สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์

ปีการศึกษา 2533

ลายมือชื่อนิสิต .....

ลายมือชื่ออาจารย์ที่ปรึกษา .....

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้ สำเร็จลุล่วงไปได้ด้วยความช่วยเหลือให้คำแนะนำอย่างดียิ่งของ รองศาสตราจารย์ ดร. ศุภชัย ตั้งวงศ์ศานต์ และ ผู้ช่วยศาสตราจารย์ ดร. วีระ ริ้วพิทักษ์ อาจารย์ที่ปรึกษาวิทยานิพนธ์ ซึ่งท่านทั้งสองได้กรุณาให้ข้อคิดเห็นต่าง ๆ ที่เป็นประโยชน์ต่อการทำวิจัยอย่างมาก

ขอขอบคุณ อาจารย์สุดสงวน งามสุริยโรจน์ ผู้ให้คำปรึกษาที่เป็นประโยชน์ต่อการทำวิจัยนี้ และขอขอบคุณเพื่อน ๆ ทุกคนที่ให้ความช่วยเหลือ ให้คำปรึกษาทั้งทางด้านวิชาการและกำลังใจ จนกระทั่งงานวิจัยนี้สำเร็จด้วยดี

สมศรี จตุรพิธพรชัย

สารบัญ

หน้า

หน้า

สารบัญตาราง

หน้า

สารบัญภาพ

รูปที่ หน้า