

การปรับเปลี่ยนวิธีการเข้ารหัสลับข้อมูลแบบอัลกอริทึมเดส



นางสาว สมศรี จตุรนิพนธ์ชัย

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

ภาควิชาวิศวกรรมคอมพิวเตอร์

บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย

พ.ศ. 2533

ISBN 974-578-120-7

ลิขสิทธิ์ของบัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย

016968

i 1031023 X

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

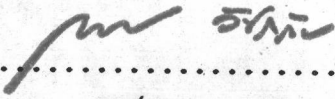
ISBN 974-578-120-7

หัวข้อวิทยานิพนธ์  
โดย  
ภาควิชา  
อาจารย์ที่ปรึกษา

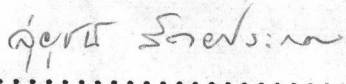
การปรับเปลี่ยนวิธีการเข้ารหัสลับข้อมูลแบบอัลกอริทึมเดส  
นางสาว สมศรี จตุรนิพนธ์ชัย  
วิศวกรรมคอมพิวเตอร์  
รองศาสตราจารย์ ดร. ศุภชัย ตั้งวงศ์ศานต์  
ผู้ช่วยศาสตราจารย์ ดร. วีระ ธีรวิทักษ์

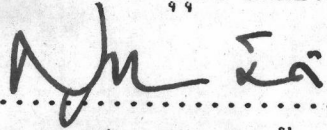


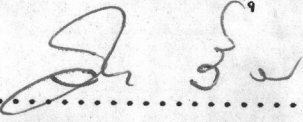
บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้บัณฑิตวิทยาลัยฉบับนี้เป็นส่วนหนึ่งของ  
การศึกษาตามหลักสูตรปริญญาวิทยาศาสตรบัณฑิต

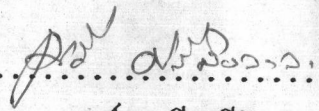
  
..... คณบดีบัณฑิตวิทยาลัย  
( ศาสตราจารย์ ดร. ถาวร วัชรภักย์ )

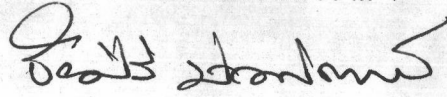
คณะกรรมการสอบวิทยานิพนธ์

  
..... ประธานกรรมการ  
( ผู้ช่วยศาสตราจารย์ สุชนัน สัตยประกอบ )

  
..... อาจารย์ที่ปรึกษา  
( รองศาสตราจารย์ ดร. ศุภชัย ตั้งวงศ์ศานต์ )

  
..... อาจารย์ที่ปรึกษาร่วม  
( ผู้ช่วยศาสตราจารย์ ดร. วีระ ธีรวิทักษ์ )

  
..... กรรมการ  
( ผู้ช่วยศาสตราจารย์ เมธี ศรีสังวาล )

  
..... กรรมการ  
( อาจารย์ ชัยศิริ บัณฑิตานนท์ )





พิมพ์ต้นฉบับบทคัดย่อวิทยานิพนธ์ภายในกรอบสี่เหลี่ยมนี้เพียงแผ่นเดียว

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

จุดประสงค์ของการวิจัยนี้เพื่อศึกษาหาอัลกอริทึมสำหรับการเข้ารหัสลับที่มีความซับซ้อนและประสิทธิภาพสูงกว่าวิธีการเดิม จากการศึกษาพบว่า ในปัจจุบันอัลกอริทึม เดส (Data Encryption Standard Algorithm : DES) เป็นอัลกอริทึมที่มีประสิทธิภาพ มีขั้นตอนการทำงานที่ซับซ้อน สามารถจะนำมาปรับเปลี่ยนขั้นตอนการทำงาน โดยการเปลี่ยนวิธีการแบ่งกลุ่มแบบเดิมที่เป็นแบบคงที่ (fixed box size) เป็นการแบ่งกลุ่มที่แปรเปลี่ยนได้ (variable box size) และมีการปรับเปลี่ยนค่าในตาราง S-boxes ให้เหมาะสมกับการแบ่งกลุ่ม เพื่อให้ได้อัลกอริทึมใหม่ที่มีประสิทธิภาพยิ่งขึ้น จากการเปรียบเทียบพบว่าอัลกอริทึมที่ได้ปรับเปลี่ยนแล้วมีความซับซ้อนกว่าอัลกอริทึม เดส เดิม จะเรียกอัลกอริทึมนี้ว่า อัลกอริทึม ไอเดส (Improved DES หรือ IDES) และอัลกอริทึม เดส ที่ปรับเปลี่ยนแล้วนี้จะไม่เป็นมาตรฐานอีกต่อไป

สำหรับความซับซ้อนของอัลกอริทึม ไอเดส จะวัดจากปริมาณงานที่ต้องค้นหาค่าคีย์สำหรับการเข้ารหัสลับ และคำนวณได้ว่าจะเป็น  $(N + 1) 2^{32}$  เท่าของอัลกอริทึม เดส โดยที่ N คือ จำนวนวิธีการแบ่งกลุ่มที่เป็นไปได้ทั้งหมด และเฉพาะปริมาณงานเฉลี่ยที่ต้องทำเพื่อค้นหาค่าคีย์ของอัลกอริทึม เดส จะประมาณ  $2^{55}$  ครั้ง นอกจากนี้ในการทดสอบเพื่อดูประสิทธิภาพในการเข้ารหัสลับข้อมูลของอัลกอริทึม ไอเดส กับข้อมูลขนาดต่าง ๆ พบว่าอัลกอริทึม ไอเดส มีประสิทธิภาพกว่าอัลกอริทึม เดส ผลของการวิจัยนี้ คือ ได้อัลกอริทึม สำหรับการเข้ารหัสลับ ที่มีความซับซ้อนยิ่งขึ้น สามารถป้องกันข้อมูลที่มีความสำคัญให้ปลอดภัยได้

ภาควิชา ..... วิศวกรรมคอมพิวเตอร์ .....  
สาขาวิชา ..... วิทยาศาสตร์คอมพิวเตอร์ .....  
ปีการศึกษา ..... 2533 .....

ลายมือชื่อนิสิต ..... สมศรี จตุรพิชพรชัย .....  
ลายมือชื่ออาจารย์ที่ปรึกษา ..... ..





พิมพ์ต้นฉบับบทคัดย่อวิทยานิพนธ์ภายในกรอบสี่เหลี่ยมนี้เพียงแผ่นเดียว

SOMSRI CHATURAPITPORNCHEI : 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 extremely 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 ..... *สมศรี จงกฤษ*  
ลายมือชื่ออาจารย์ที่ปรึกษา ..... *สมศรี จงกฤษ*



### กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้ สำเร็จลุล่วงไปได้ด้วยความช่วยเหลือให้คำแนะนำอย่างดียิ่งของ  
รองศาสตราจารย์ ดร. ศุภชัย ตั้งวงศ์ศานต์ และ ผู้ช่วยศาสตราจารย์ ดร. วีระ ธีรวิทักษ์  
อาจารย์ที่ปรึกษาวิทยานิพนธ์ ซึ่งท่านทั้งสองได้กรุณาให้ข้อคิดเห็นต่าง ๆ ที่เป็นประโยชน์ต่อการ  
ทำวิจัยอย่างมาก

ขอขอบคุณ อาจารย์สุดสงวน งามสุริยโรจน์ ผู้ให้คำปรึกษาที่เป็นประโยชน์ต่อการทำ  
วิจัยนี้ และขอขอบคุณเพื่อน ๆ ทุกคนที่ให้ความช่วยเหลือ ให้คำปรึกษาทั้งทางด้านวิชาการและ  
กำลังใจ จนกระทั่งงานวิจัยนี้สำเร็จด้วยดี

สมศรี จตุรนิพนทรัพย์





สารบัญ

หน้า

บทคัดย่อภาษาไทย .....	ง
บทคัดย่อภาษาอังกฤษ .....	จ
กิตติกรรมประกาศ .....	ฉ
สารบัญตาราง .....	ญ
สารบัญภาพ .....	ฎ

บทที่

1. บทนำ .....	1
1.1 ความเป็นมาของปัญหา .....	1
1.2 การเข้ารหัสลับ (Cryptography) .....	2
1.3 การปรับเปลี่ยนอัลกอริทึมสำหรับการเข้ารหัสลับ .....	3
1.4 วัตถุประสงค์ของการวิจัย .....	3
1.5 ขอบเขตการวิจัย .....	4
1.6 ขั้นตอนและวิธีการดำเนินการวิจัย .....	4
1.7 ประโยชน์ที่คาดว่าจะได้รับ .....	4
2. แนวความคิดพื้นฐานเกี่ยวกับการเข้ารหัสข้อมูล .....	5
2.1 ประวัติความเป็นมาของการเข้ารหัสข้อมูล .....	5
2.2 ระบบการเข้ารหัสลับ (Cryptography System หรือ Cipher System) .....	6
2.2.1 ระบบการเข้ารหัสลับแบบสลับนิยม .....	8
2.2.2 ระบบการเข้ารหัสแบบคีย์สาธารณะ .....	8
2.2.3 ข้อสังเกตเกี่ยวกับระบบการเข้ารหัสแบบสลับนิยมและคีย์สาธารณะ .....	9
2.3 อัลกอริทึมเดส (Data Encryption Standard : DES) .....	10
2.3.1 ประวัติความเป็นมาของอัลกอริทึมเดส .....	10
2.3.2 หลักการในการเข้ารหัสของอัลกอริทึมเดส .....	11
2.3.3 ขั้นตอนในการทำงานของอัลกอริทึมเดส .....	12
2.3.4 การวิเคราะห์โครงสร้างของอัลกอริทึมเดส .....	16



3.	แนวความคิดในการปรับเปลี่ยนอัลกอริทึมเดส .....	19
3.1	แนวความคิดในการปรับเปลี่ยนอัลกอริทึมเดส .....	19
3.1.1	การเปลี่ยนวิธีการแบ่งกลุ่มข้อมูล .....	21
3.1.2	การเปลี่ยนตาราง S-boxes .....	24
3.2	การวิเคราะห์เชิงประสิทธิภาพของอัลกอริทึมไอเดส .....	26
3.2.1	การวัดความซับซ้อนของอัลกอริทึมไอเดส .....	26
3.2.2	การเพิ่มความซับซ้อนของอัลกอริทึมไอเดสเนื่องจาก ต้องค้นหาค่าจากตาราง S-boxes ที่เปลี่ยนไป .....	28
3.3	แนวความคิดอื่นในการเปลี่ยนอัลกอริทึมเดส .....	29
4.	ผลการทดสอบการทำงานของอัลกอริทึมไอเดส .....	30
4.1	ความสัมพันธ์ของข้อมูลขาเข้าและข้อมูลขาออก .....	32
4.1.1	การเปลี่ยนแปลงของข้อมูลเข้ารหัสเมื่อ ข้อมูลเนื้อแท้เปลี่ยนไป 1 บิต .....	33
4.1.2	การเปลี่ยนแปลงของข้อมูลเข้ารหัสเมื่อคีย์ สำหรับเข้ารหัสลับเปลี่ยนไป 1 บิต .....	36
4.2	การวิเคราะห์ความสัมพันธ์ของข้อมูลเข้ารหัสที่ขึ้นต่อข้อมูลเนื้อแท้ ...	40
4.3	ความสัมพันธ์ของข้อมูลขาเข้าและข้อมูลออกต้องไม่เป็น ความสัมพันธ์แบบเชิงเส้น .....	48
4.4	การวัดเวลาที่ใช้ในการประมวลผล .....	49
4.5	การวัดขนาดของหน่วยความจำที่อัลกอริทึมไอเดสใช้ .....	60
4.6	การทดสอบการเปลี่ยนวิธีการคำนวณค่าสับคีย์ .....	63
4.7	การหลีกเลี่ยงการใช้คีย์ (Weak Key) และ (Semi-Weak Key) .....	66
5.	สรุปผลการวิจัยและข้อเสนอแนะ .....	68
5.1	สรุปผลการวิจัย .....	68
5.2	ข้อควรพิจารณาในการใช้อัลกอริทึมไอเดสเพื่อเข้ารหัสลับข้อมูล .....	70
5.3	ข้อเสนอแนะ .....	72

บรรณานุกรม .....	73
ภาคผนวก ผลการทดสอบการเปลี่ยนแปลงของข้อมูลเข้ารหัสเมื่อข้อมูลเนื้อแท้หรือคีย์ สำหรับเข้ารหัสลับเปลี่ยนไป 1 บิต .....	75
ประวัติผู้เขียน .....	98



## สารบัญตาราง

ตารางที่	หน้า
4.1 แสดงการเปลี่ยนแปลงของข้อมูลเข้ารหัสเมื่อข้อมูลเนื้อแท้มีความแตกต่าง 1 บิต .....	34
4.2 แสดงระยะแอมมิงของข้อมูลเข้ารหัสเมื่อข้อมูลเนื้อแท้เปลี่ยนไป 1 บิต โดยใช้อัลกอริทึมเดส และ อัลกอริทึม ไอเดส .....	35
4.3 แสดงการเปลี่ยนแปลงของข้อมูลเข้ารหัสเมื่อคีย์สำหรับเข้ารหัสลับมีความแตกต่าง 1 บิต .....	38
4.4 แสดงระยะแอมมิงของข้อมูลเข้ารหัสเมื่อคีย์สำหรับเข้ารหัสลับเปลี่ยนไป 1 บิต โดยใช้อัลกอริทึมเดส และ อัลกอริทึม ไอเดส .....	39
4.5 แสดงความสัมพันธ์ระหว่างข้อมูลออกและข้อมูลเข้า ตามจำนวนรอบของการทำงาน โดยใช้อัลกอริทึมเดส .....	41
4.6 แสดงความสัมพันธ์ระหว่างข้อมูลออกและข้อมูลเข้า ตามจำนวนรอบของการทำงาน โดยใช้อัลกอริทึม ไอเดส แบบกรณีที่ 1.....	42
4.7 แสดงความสัมพันธ์ระหว่างข้อมูลออกและข้อมูลเข้า ตามจำนวนรอบของการทำงาน โดยใช้อัลกอริทึม ไอเดส แบบกรณีที่ 2.....	43
4.8 แสดงความสัมพันธ์ระหว่างข้อมูลออกและข้อมูลเข้า ตามจำนวนรอบของการทำงาน โดยใช้อัลกอริทึม ไอเดส แบบกรณีที่ 3.....	43
4.9 แสดงความสัมพันธ์ระหว่างข้อมูลออกและข้อมูลเข้า ตามจำนวนรอบของการทำงาน โดยใช้อัลกอริทึม ไอเดส แบบกรณีที่ 4.....	44
4.10 แสดงความสัมพันธ์ระหว่างข้อมูลออกและข้อมูลเข้า ตามจำนวนรอบของการทำงาน โดยใช้อัลกอริทึม ไอเดส แบบกรณีที่ 5.....	44
4.11 แสดงความสัมพันธ์ระหว่างข้อมูลออกและข้อมูลเข้า ตามจำนวนรอบของการทำงาน โดยใช้อัลกอริทึม ไอเดส แบบกรณีที่ 6.....	45
4.12 แสดงความสัมพันธ์ระหว่างข้อมูลออกและข้อมูลเข้า ตามจำนวนรอบของการทำงาน โดยใช้อัลกอริทึม ไอเดส แบบกรณีที่ 7.....	45



4.13	แสดงความสัมพันธ์ระหว่างข้อมูลออกและข้อมูลเข้า ตามจำนวนรอบ ของการทำงาน โดยใช้อัลกอริทึม ไอเดส แบบกรณีที่ 8.....	46
4.14	แสดงความสัมพันธ์ระหว่างข้อมูลออกและข้อมูลเข้า ตามจำนวนรอบ ของการทำงาน โดยใช้อัลกอริทึม ไอเดส แบบกรณีที่ 9.....	46
4.15	แสดงความสัมพันธ์ระหว่างข้อมูลออกและข้อมูลเข้า ตามจำนวนรอบของการทำงาน โดยเปรียบเทียบระหว่างการใช้อัลกอริทึม ไอเดส กับอัลกอริทึมเดส .....	47
4.16	แสดงเวลาการเข้ารหัสลับของอัลกอริทึม ไอเดสและอัลกอริทึมเดสและแสดง อัตราส่วนของเวลาที่อัลกอริทึม ไอเดส ใช้เมื่อเทียบกับอัลกอริทึมเดส .....	50
4.17	แสดงเวลาการถอดรหัสลับของอัลกอริทึม ไอเดสและอัลกอริทึมเดสและแสดง อัตราส่วนของเวลาที่อัลกอริทึม ไอเดส ใช้เมื่อเทียบกับอัลกอริทึมเดส .....	51
4.18	แสดงขนาดหน่วยความจำที่อัลกอริทึมเดส และอัลกอริทึม ไอเดส ในกรณีต่าง ๆ ใช้	61
4.19	แสดงผลลัพธ์ของข้อมูลที่ถูกเลื่อนตำแหน่งบิต โดยการหมุนเวียนไปทางซ้ายและขวา	64
4.20	ตำแหน่งบิตสำหรับการเลื่อนบิต .....	65



## สารบัญภาพ

รูปที่	หน้า
2.1 แสดงการดำเนินการเข้ารหัสลับและการดำเนินการถอดรหัสลับ .....	7
2.2 แสดงขั้นตอนการทำงานของอัลกอริทึมเดส .....	13
2.3 แสดงการทำงานของฟังก์ชัน $f$ .....	14
2.4 แสดงการคำนวณค่าสับคีย์ (Subkey) .....	15
4.1 การเปรียบเทียบเวลาที่ใช้ในการเข้ารหัสลับข้อมูลที่มีขนาดต่าง ๆ กัน โดยใช้อัลกอริทึมเดสและอัลกอริทึมไอเดส แบบกรณีที่ 1-4 .....	52
4.2 การเปรียบเทียบเวลาที่ใช้ในการเข้ารหัสลับข้อมูลที่มีขนาดต่าง ๆ กัน โดยใช้อัลกอริทึมเดสและอัลกอริทึมไอเดส แบบกรณีที่ 5-9 .....	53
4.3 การเปรียบเทียบเวลาที่ใช้ในการถอดรหัสลับข้อมูลที่มีขนาดต่าง ๆ กัน โดยใช้อัลกอริทึมเดสและอัลกอริทึมไอเดส แบบกรณีที่ 1-4 .....	54
4.4 การเปรียบเทียบเวลาที่ใช้ในการถอดรหัสลับข้อมูลที่มีขนาดต่าง ๆ กัน โดยใช้อัลกอริทึมเดสและอัลกอริทึมไอเดส แบบกรณีที่ 5-9 .....	55
4.5 การเปรียบเทียบอัตราส่วนของเวลาที่ใช้ในการเข้ารหัสลับข้อมูลขนาด ต่าง ๆ กันโดยใช้อัลกอริทึมไอเดส กรณีที่ 1-4 เทียบกับเดส .....	56
4.6 การเปรียบเทียบอัตราส่วนของเวลาที่ใช้ในการเข้ารหัสลับข้อมูลขนาด ต่าง ๆ กันโดยใช้อัลกอริทึมไอเดส กรณีที่ 5-9 เทียบกับเดส .....	57
4.7 การเปรียบเทียบอัตราส่วนของเวลาที่ใช้ในการถอดรหัสลับข้อมูลขนาด ต่าง ๆ กันโดยใช้อัลกอริทึมไอเดส กรณีที่ 1-4 เทียบกับเดส .....	58
4.8 การเปรียบเทียบอัตราส่วนของเวลาที่ใช้ในการถอดรหัสลับข้อมูลขนาด ต่าง ๆ กันโดยใช้อัลกอริทึมไอเดส กรณีที่ 5-9 เทียบกับเดส .....	59