โครงการสิ่งประดิษฐ์

รายงาน

ซอฟต์แวร์รักษาความปลอดภัยของข้อมูล
โดยใช้มาตรฐานการเข้ารหัสลับข้อมูลแบบ DES

โดย

ผู้ช่วยศาสตราจารย์ ดร.วาทิต เบญจพลกุล

มิถุนายน 2541

กิตติกรรมประกาศ

ผู้วิจัยขอขอบคุณจุฬาลงกรณ์มหาวิทยาลัยที่ให้ทุนโครงการสิ่งประดิษฐ์ประเภทซอฟต์แวร์ กองทุนรัชดาภิเษกสมโภช ปีการเงิน 2540 จนโครงการสิ่งประดิษฐ์นี้สำเร็จลุล่วงด้วยดี

ขอขอบคุณ คุณเสกสรรค์ ชีวพูนผล ซึ่งเป็นผู้ช่วยวิจัย ที่ช่วยในการวิจัยจนโครงการสิ่งประดิษฐ์นี้สำเร็จลุล่วงได้ และขอขอบคุณ คุณศิริวรรณ ณรงค์ตะณุพล ที่ได้ช่วยในการจัดรูปเล่มและจัดพิมพ์รายงานฉบับสมบูรณ์จนสำเร็จ

ชื่อโครงการ	ซอฟต์แวร์รักษาความปลอดภัยของข้อมูลโดยใช้มาตรฐานการเข้ารหัสลับแบบ DES
ชื่อผู้ดำเนินงาน	ผู้ช่วยศาสตราจารย์ ดร.วาทิต เบญจพลกุล
เดือนและปีที่ทำการวิจัยเสร็จ	มิถุนายน 2541

บทคัดย่อ

โครงการ "ซอฟต์แวร์รักษาความปลอดภัยของข้อมูลโดยใช้มาตรฐานการเข้ารหัสลับข้อมูลแบบ DES" นี้ทำการสร้างซอฟต์แวร์สำหรับทำการเข้ารหัสลับและถอดรหัสลับข้อมูลประเภท textfile โดยอาศัย algorithm ของการเข้ารหัสลับแบบ DES หรือ Data Encryption Standard โปรแกรมเขียนขึ้นด้วยภาษา C และเป็นโปรแกรมที่ใช้งานในระบบปฏิบัติการ DOS โปรแกรมที่เสร็จสมบูรณ์มีชื่อว่า DES software release 1.0 ซึ่งสามารถติดต่อรับคำสั่งจากผู้ใช้ นำแฟ้มข้อมูลที่ผู้ใช้ต้องการมาทำการเข้ารหัสลับหรือถอดรหัสลับด้วย key ที่ผู้ใช้เป็นผู้กำหนดขึ้นเองได้ ผู้ใช้สามารถเลือกระดับความปลอดภัยของข้อมูลในการเข้ารหัสลับ โดยใช้ key mode ในการเข้ารหัสลับต่างๆ กัน ซึ่งหมายถึงจำนวน key ที่จะใช้เข้ารหัสลับข้อมูลที่ผู้ใช้ต้องการ นอกจากนี้ยังสามารถแสดงข้อมูลเดิม ข้อมูลที่เข้ารหัสลับแล้ว และข้อมูลที่ถอดรหัสลับแล้วเปรียบเทียบกันได้เพื่อความสะดวกของผู้ใช้ในการตรวจสอบ ข้อมูลที่ผ่านการเข้ารหัสจะมีความปลอดภัยอยู่เสมอตราบเท่าที่ key ที่ใช้ในการเข้ารหัสลับยังถูกเก็บไว้เป็นความลับ ซึ่งเป็นคุณสมบัติของ algorithm การเข้ารหัสแบบ DES

Project Title : Software for Data Security by using Data Encryption Standard

Name of the Investigator : Asst.Prof. Dr. Watit Benjapolakul

Year : 1998

Abstract

The purpose of this project is to create software that can encrypt or decrypt textfiles with DES or Data Encryption Standard algorithm. Complete software has been given name as DES software release 1.0 . DES software has the abilities of encrypting or decrypting textfiles that user need to protect with the keys he chose. Software can not only encrypting or decrypting data , but also displaying the original data , encrypted data and decrypted data in contrast to give the user easiness to see if the keys is not suitable in encryption or what is the message in the decrypted data. The encrypted data will be safe as long as the keys is in secret that is the property of the DES algorithm.

สารบัญ

รายการตารางประกอบ

รายการภาพประกอบ

หน้า

หน้า

หน้า

บทที่ 1
บทนำ

1.1 ความเบื้องต้น

ในปัจจุบันเทคโนโลยีทางการสื่อสารข้อมูล ได้เจริญก้าวหน้าไปอย่างรวดเร็ว ข้อมูลข่าวสารต่างๆในปัจจุบัน ถือได้ว่ามีความสำคัญเป็นอย่างยิ่ง ในการใช้งานบางประเภท ต้องการความปลอดภัยของข้อมูล ไม่ให้ถูกขโมยหรือลอกเลียนแบบไปได้ ทำให้เกิดมีการคิดวิธีเข้ารหัสลับข้อมูลขึ้น ซึ่งในปัจจุบัน การเข้ารหัสลับได้ถูกพัฒนาไปมาก เกิดเป็นวิธีการเข้ารหัสลับที่สลับซับซ้อนหลายรูปแบบ และวิธีในการเข้ารหัสลับบางประเภทมักจะถูกเก็บไว้เป็นความลับเพื่อความมั่นคงของระบบการเข้ารหัสลับ ดังนั้นการใช้งานจึงจำกัดอยู่ในวงแคบกับข้อมูลบางประเภทเท่านั้น ยังมีวิธีการเข้ารหัสลับบางแบบที่มีการเผยแพร่ให้ใช้งานได้ทั่วไป หนึ่งในวิธีเหล่านั้นได้แก่การเข้ารหัสลับแบบ Data Encryption Standard ซึ่งให้ความปลอดภัยของข้อมูลได้แม้ว่าขั้นตอนการเข้ารหัสลับจะถูกเปิดเผยออกไปก็ตาม

algorithm ของการเข้ารหัสลับแบบ Data Encryption Standard นี้ มีลักษณะที่ซับซ้อนยุ่งยากและมีขั้นตอนมากมาย เนื่องจากไม่ได้ใช้การคำนวณทางคณิตศาสตร์เหมือนกับการเข้ารหัสลับบางแบบ แต่ใช้การสลับที่และการแทนที่ข้อมูลและใช้ข้อมูลในหน่วยที่เป็นบิตทำให้ปริมาณข้อมูลมีมาก ด้วยเหตุนี้การที่จะทำการถอดรหัสลับข้อมูลโดยปราศจาก key ที่ใช้ในการเข้ารหัสที่ถูกต้องจึงสามารถทำได้ยากด้วยเช่นกัน ข้อมูลจึงมีความปลอดภัยสูง

อย่างไรก็ตามเนื่องจากขั้นตอนในการเข้ารหัสลับนั้นมีลักษณะที่วนซ้ำเป็นรอบๆ ทำให้เหมาะกับการเขียนเป็นโปรแกรมอย่างยิ่ง อีกทั้งโปรแกรมยังสามารถเผยแพร่ออกไปได้ง่ายและรวดเร็ว รวมทั้งการใช้งานก็สามารถทำได้ง่าย ใช้เพียงอุปกรณ์คอมพิวเตอร์ก็เป็นการเพียงพอ ดังนั้นถ้าสามารถสร้างเป็น software ขึ้นมาได้ก็จะเป็นประโยชน์อย่างยิ่ง เพราะจะทำให้สามารถทำการเข้ารหัสลับและถอดรหัสลับข้อมูลที่ต้องการได้ เป็นการเพิ่มความปลอดภัยให้กับข้อมูลได้ นอกจากนี้ยังสามารถพัฒนาให้เป็นส่วนประกอบหนึ่งของระบบที่มีการส่งข้อมูลผ่านโครงข่ายได้ เช่นการส่ง E-mail ในระบบโครงข่าย Internet เป็นต้น การส่งข้อมูลต่างก็จะมีความปลอดภัยสูงขึ้นโดยไม่ต้องใช้อุปกรณ์หรือ วิธีการที่ยุ่งยากเลย

1.2 วัตถุประสงค์ของโครงการ

วัตถุประสงค์หลักของโครงการนี้คือสร้าง software ที่ทำงานบนระบบปฏิบัติการ DOS บนเครื่องคอมพิวเตอร์ทั่วไป ให้สามารถทำหน้าที่และมีคุณสมบัติดังนี้

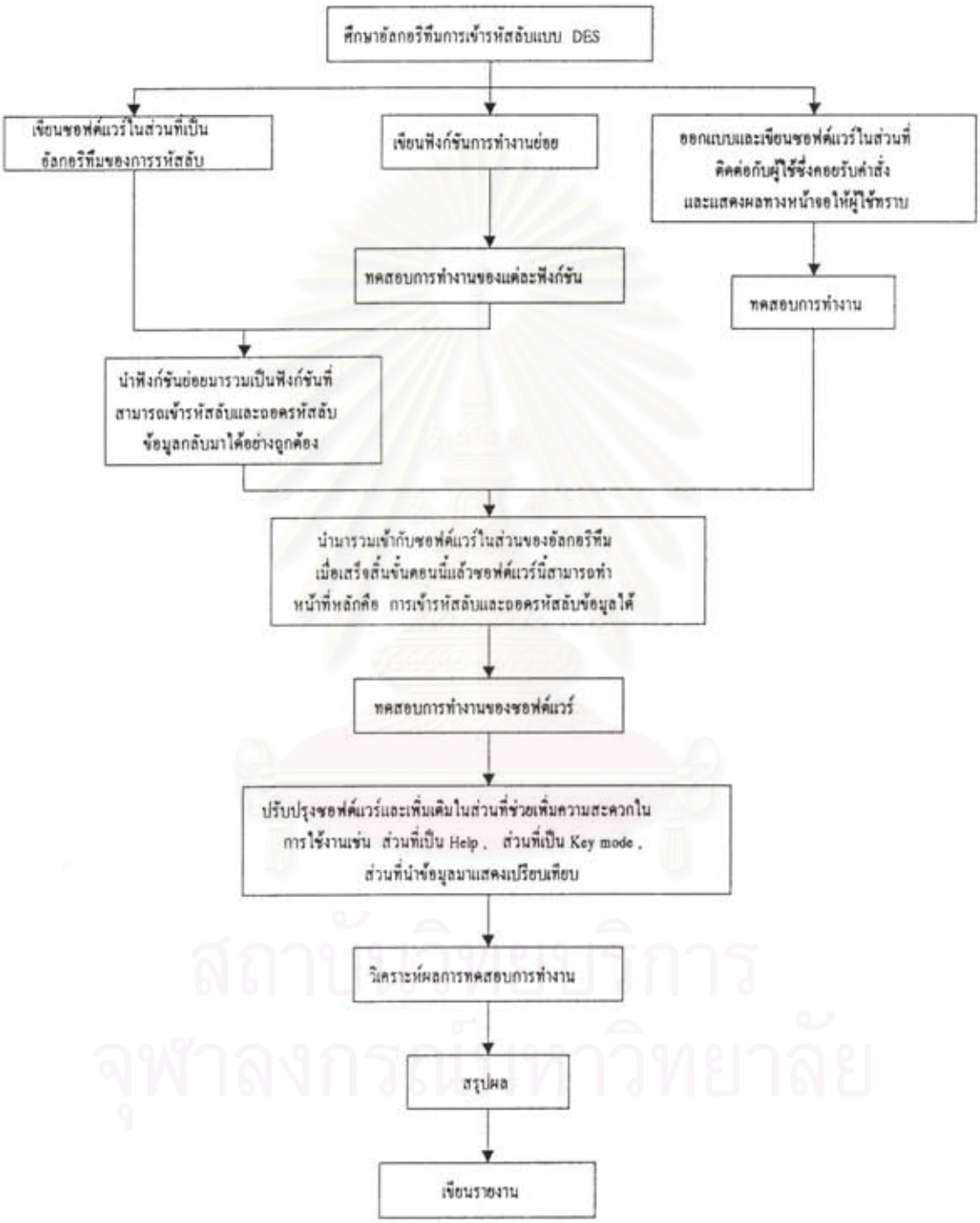
1. สามารถทำการเข้ารหัสลับและถอดรหัสลับข้อมูลที่เป็น textfile ได้ โดยอาศัย algorithm การเข้ารหัสลับแบบ Data Encryption Standard

2. ข้อมูลที่ทำการเข้ารหัสลับแล้ว จะต้องมีความปลอดภัยถึงแม้ว่าขั้นตอนการเข้ารหัสลับจะถูกเปิดเผยออกไป ซึ่งเป็นคุณสมบัติข้อหนึ่งของการเข้ารหัสลับแบบ Data Encryption Standard

3. เป็นโปรแกรมที่สามารถใช้ได้ง่าย มีการติดต่อรับคำสั่งจากผู้ใช้ในลักษณะที่เป็นเมนูให้เลือก และแสดงผลการทำงานให้ผู้ใช้ทราบทางหน้าจอ

1.3 วิธีดำเนินการโดยย่อ

สามารถสรุปวิธีดำเนินการโครงการได้ดังรูปที่ 1.1



รูปที่ 1.1 วิธีดำเนินการโครงการซอฟต์แวร์รักษาความปลอดภัยของข้อมูลโดยใช้มาตรฐานการเข้ารหัสลับข้อมูลแบบ DES

บทที่ 2
หลักการเข้ารหัสลับข้อมูลแบบ DES

สำหรับ DES หรือ Data Encryption Standard เป็นรูปแบบหนึ่งของการเข้ารหัสลับข้อมูล ที่เป็นที่ยอมรับเป็นมาตรฐานโดยทั่วไป ตัวของ algorithm หรือขั้นตอนในการเข้ารหัสลับสามารถเปิดเผยได้ โดยไม่มีผลต่อความปลอดภัยของข้อมูล ทำให้เป็นที่นิยมใช้ในระบบ hardware และ software เป็นจำนวนมาก

2.1 การเข้ารหัสลับใน DES

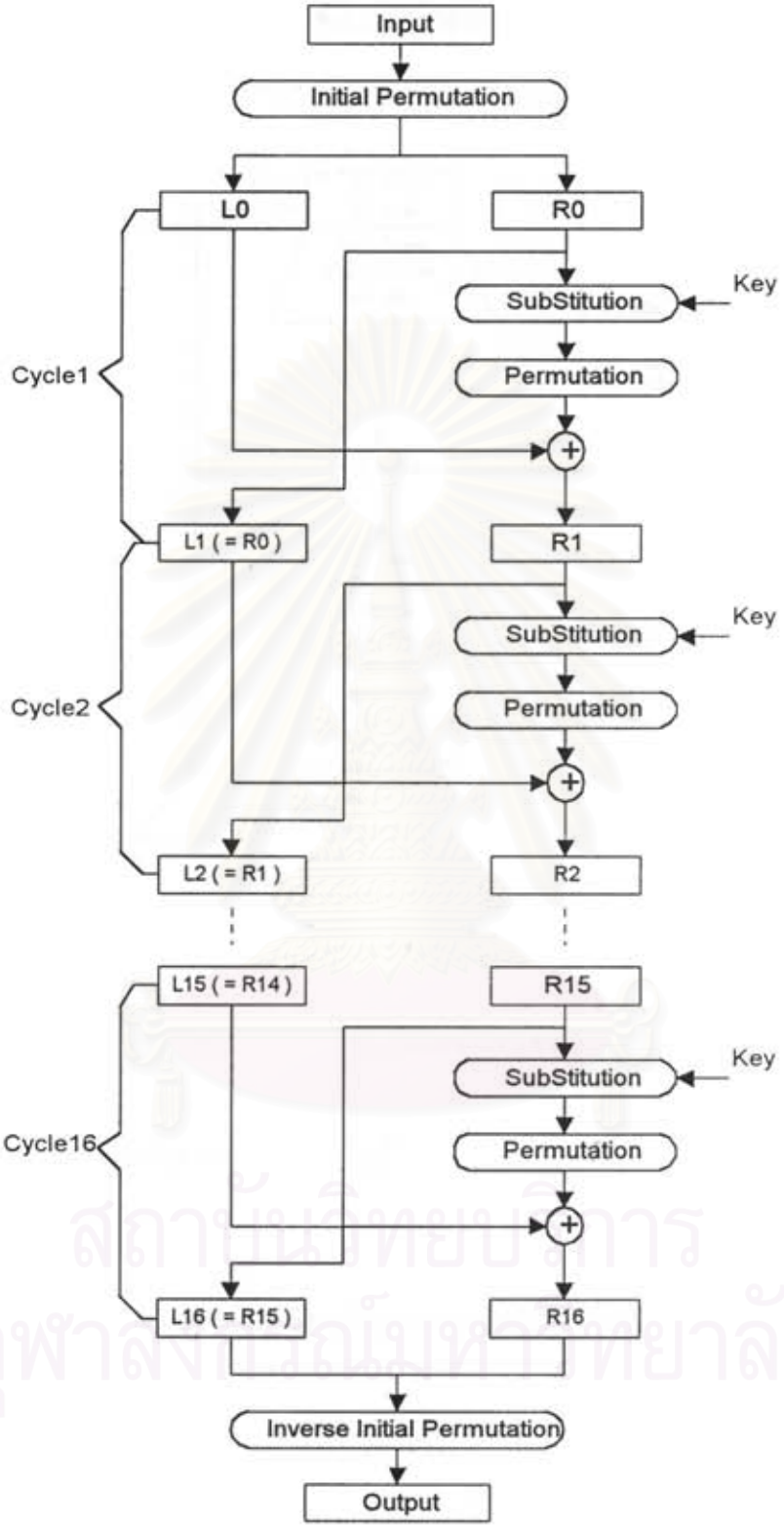
algorithm ของ DES นี้มีหลักการจากทฤษฎีเรื่องความปลอดภัยของข้อมูลของ Shannon ที่ตีพิมพ์ในปี ค.ศ.1949 แชนนอนได้ให้เทคนิคสองอย่างในการปกป้องข้อมูล คือ confusion และ diffusion

confusion จะเปลี่ยนชิ้นของข้อมูลทำให้ข้อมูลขาออกจากการเข้ารหัสลับมีลักษณะที่ต่างออกไปจากข้อมูลก่อนการเข้ารหัสลับ ส่วน diffusion จะพยายามกระจายผลของข้อมูลส่วนหนึ่งไปยังส่วนอื่นๆ

ใน DES นั้น หลักทั้งสองของแชนนอนได้ถูกนำมาใช้ โดยใน algorithm จะเป็นการรวมเอาบล็อกพื้นฐาน 2 บล็อกเข้ามาใช้ทำการเข้ารหัสลับอย่างรัดกุม บล็อกทั้ง 2 ก็คือ Substitution หรือการแทนที่ และ Permutation (Transposition) หรือการสลับที่ และจากการใช้บล็อกทั้ง 2 นี้ทำเป็น algorithm ในลักษณะที่ซ้ำๆ เป็นรอบๆ ทั้งหมด 16 รอบ ทำให้ DES มีจุดเด่นอยู่ที่ความซับซ้อนจนทำให้ไม่สามารถสืบหาขั้นตอนการเข้ารหัสลับจากข้อมูลเพียงบิตเดียวได้

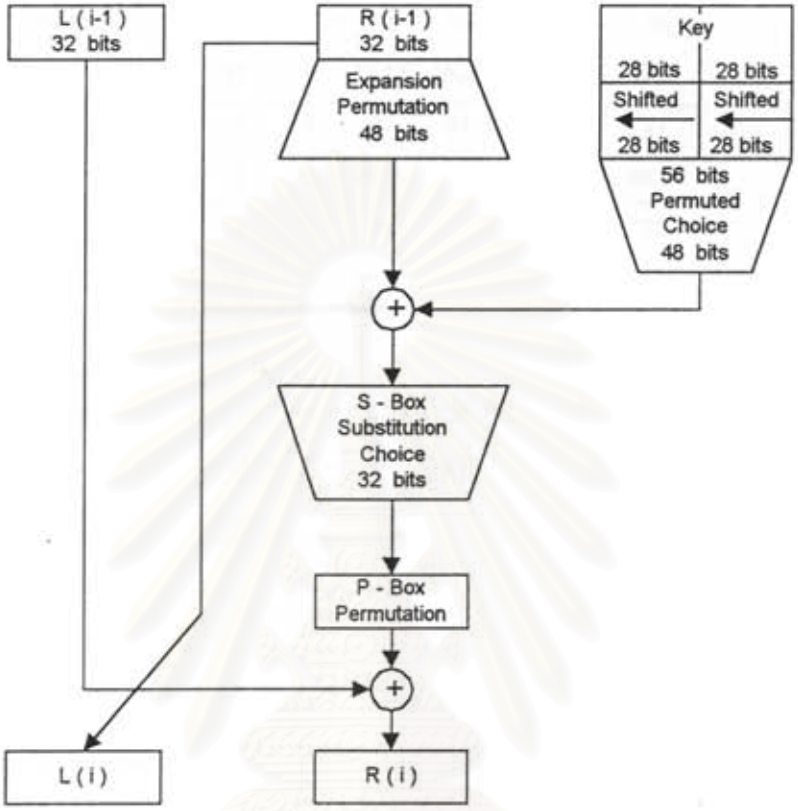
ข้อมูลที่จะเข้ารหัสลับจะถูกนำมา เข้ารหัสเป็นบล็อก ๆ ละ 64 บิต นำมาผ่านกระบวนการเข้ารหัสทั้ง 16 รอบร่วมกับ key ที่กำหนดขึ้นเองอีก 16 ชุดเช่นกัน โดยที่ key แต่ละชุดจะยาว 64 บิต และสามารถเปลี่ยนได้ตามที่ต้องการถ้าหากไม่แน่ใจในความปลอดภัยของ key การแทนที่ข้อมูลบางบิตด้วยบิตอื่นนั้น จะทำให้ข้อมูลมีลักษณะที่ต่างไปจากข้อมูลเดิม ส่วนการสลับที่อย่างมีแบบแผนจะทำให้เกิดการแพร่กระจายของข้อมูลจากบิตหนึ่งไปยังบิตอื่น ลักษณะของ algorithm การเข้ารหัสจะเป็นดังรูปที่ 2.1

การเข้ารหัสลับจะเริ่มต้นโดย DES จะดึงข้อมูลมา 64 บิต นำมาสลับที่แต่ละบิตโดยไม่เกี่ยวข้องกันโดยบล็อกที่เรียกว่า "initial permutation" หลังจากนั้นบล็อกของข้อมูลจะถูกแบ่งครึ่งออกเป็นสองส่วน และจะทำการเข้ารหัสลับข้อมูลทั้งสองส่วนโดยไม่เกี่ยวข้องกัน โดยจะรวมครึ่งหนึ่งเข้ากับ key ที่ผ่านกระบวนการ แล้วจะทำการสลับที่ข้อมูลทั้งสองส่วน ซึ่งจะกระทำเช่นนี้ทั้งหมด 16 ครั้ง key ที่ใช้ในการเข้ารหัสก็จะถูกผ่านกระบวนการเช่นกัน โดย key ที่จะนำมาผ่านกระบวนการจะมีแค่ 56 บิตเท่านั้น เนื่องจากจะมีการทิ้งบิตที่ 8,16,24,....64 ของ key ไป ทำให้เหลือ key เพียง 56 บิตจากเดิมที่มี 64 บิต หลังจากที่ครบ 16 รอบข้อมูลก็จะผ่านขั้นตอนสุดท้ายคือบล็อก "inverse initial permutation" ซึ่งเป็นกระบวนการย้อนกลับกับ initial permutation



รูปที่ 2.1 แสดง algorithm ของการเข้ารหัสลับ

ในแต่ละรอบของการเข้ารหัสลับ อาจแบ่งเป็นบล็อกที่มีการกระทำกับข้อมูลต่างๆกัน ทั้งหมด 4 อย่างซึ่งสามารถเขียนได้ดังในรูปที่ 2.2



รูปที่ 2.2 แสดงรายละเอียดขั้นตอนในแต่ละรอบของการเข้ารหัสลับ

แต่ละบล็อกจะทำหน้าที่ต่างๆ กันดังต่อไปนี้

Expansion Permutation

กระบวนการนี้จะนำข้อมูลชุดหนึ่ง ซึ่งจะมีขนาด 32 บิตมาทำการขยายให้มีขนาดเป็น 48 บิต โดยที่จะมีการสลับที่ข้อมูลและทำซ้ำข้อมูลบางบิตดังในตารางที่ 2.1

ตารางที่ 2.1 การทำ Expansion Permutation

Bit	1	2	3	4	5	6	7	8
Moves to	2,48	3	4	5,7	6,8	9	10	11,13
Bit	9	10	11	12	13	14	15	16
Moves to	12,14	15	16	17,19	18,20	21	22	23,25
Bit	17	18	19	20	21	22	23	24
Moves to	24,26	27	28	29,31	30,32	33	34	35,37
Bit	25	26	27	28	29	30	31	32
Moves to	36,38	39	40	41,43	42,44	45	46	47,1

ซึ่งจะเห็นว่าบล็อกของข้อมูล 4 บิต จะถูกดึงไปยังบิตใหม่ของข้อมูล ยกตัวอย่างเช่น ข้อมูลในบิตที่ 1 จะถูกดึงไปเป็นบิตใหม่ซ้ำกันถึง 2 บิต บิตที่ 4 ก็เช่นเดียวกัน ในขณะที่บิตที่ 2 และ 3 จะถูกดึงไปเป็นบิตใหม่เพียงบิตเดียว

Key Transformation

จากรูปที่ 3 จะพบว่า key ที่นำมาใช้จะใช้เพียง 56 บิต จากทั้งหมด 64 บิต โดยการทิ้งบิตที่ 8,16,24,...,64 ไป หลังจากนั้นในแต่ละรอบ key จะถูกแบ่งครึ่งเป็นสองส่วน ส่วนละ 28 บิต และแต่ละส่วนจะถูกเลื่อนไปทางซ้ายเป็นวงกลมตามจำนวนบิตที่กำหนดไว้ ซึ่งจะขึ้นอยู่กับแต่ละรอบของการเข้ารหัสดังในตารางที่ 2.2

ตารางที่ 2.2 จำนวนบิตที่จะเลื่อน key ไปในแต่ละรอบ

Cycle Number	Bit Shifted
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

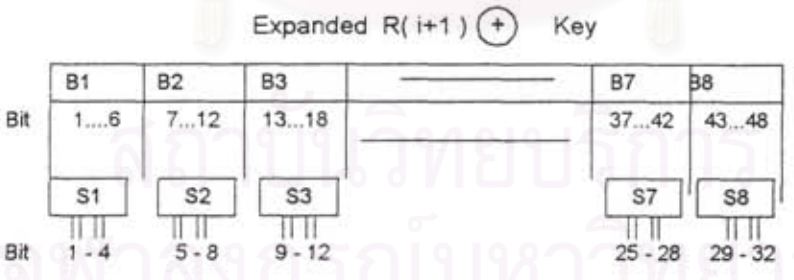
หลังจากที่ถูกเลื่อนไปแล้ว key ก็จะถูกนำมาผ่านการทำ Choice Permutation ดังในตารางที่ 2.3 ซึ่งจะทำให้ key มีขนาดเหลือเป็น 48 บิตเท่านั้น key ที่ได้นี้จะถูกนำมารวมกับข้อมูลขนาด 48 บิตที่ผ่านการทำ Expansion Permutation โดยรวมกันด้วย exclusive-or ผลลัพธ์ที่ได้จะผ่านไปยัง S-Boxes ต่อไป

ตารางที่ 2.3 ตารางในการทำ Choice Permutation

Key bit	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Selected for position	5	24	7	16	6	10	20	18	-	12	3	15	23	1
Key bit	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Selected for position	9	19	2	-	14	22	11	-	13	4	-	17	21	8
Key bit	29	30	31	32	33	34	35	36	37	38	39	40	41	42
Selected for position	47	31	27	48	35	41	-	46	28	-	39	32	25	44
Key bit	43	44	45	46	47	48	49	50	51	52	53	54	55	56
Selected for position	-	37	34	43	29	36	38	45	33	26	42	-	30	40

S-Boxes

ผลลัพธ์จากการรวมกันระหว่างข้อมูลและ key ขนาด 48 บิต จะถูกนำมาผ่าน S_Boxes ซึ่งจะทำการอัดข้อมูลขนาด 48 บิตให้เหลือเป็น 32 บิต ดังในรูปที่ 2.3 โดยอาศัยตารางที่ 2.4



รูปที่ 2.3 ลักษณะของการอัดข้อมูลใน S-Boxes

ข้อมูลขาเข้า 48 บิต จะถูกแบ่งเป็นบล็อกๆ ละ 6 บิต ซึ่งอาจแทนด้วย B1 B2 B3 .... B8 ดังในรูปที่ 2.3

S-Boxes จะทำการแทนที่โดยใช้ตารางที่ 2.4 ขนาด 4 แถว 16 หลัก ยกตัวอย่างเช่น ข้อมูลบล็อก Bi ขนาด 6 บิตคือ b1 b2 b3 b4 b5 b6 บิต b1 และ b6 จะถูกนำมารวมกันเป็นเลขฐาน 2 สองหลัก b1 b6 และมีค่าในฐาน 10 ช่วง 0-3 เรียกค่านี้ว่า r ส่วนบิต b2 b3 b4 b5 จะถูกนำมารวม เป็นเลขฐาน 2 ซึ่งมีค่าในฐาน 10 ในช่วง 0-15 เรียกค่าเหล่านี้ว่า c ข้อมูลทั้ง 6 บิต จะถูกแทนค่า โดยใช้ค่าจากเลขฐาน 10 ที่อยู่ในแถวที่ r และหลักที่ c ในตารางที่ 4 เช่นถ้าข้อมูลในบล็อกที่ 7 (B7) เป็น 010011 ดังนั้นจะได้ว่า r=01=1 และ c=1001=9 ซึ่งในตารางที่ 4 บล็อกข้อมูลที่ 7 หรือ S7 ในตาราง แถวที่1 หลักที่9 มีค่าเป็น 3 ค่าที่จะได้จาก S-Boxes = 3=0011 จากที่เดิมเป็น 010011

ตารางที่ 2.4 ตารางในการทำ S-Boxes

Row \ Column	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	4	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	15	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	10	6	10	0	9	10	4	5	3
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

P-Boxes

หลังจากผ่าน S-Boxes แล้ว ข้อมูลที่มีขนาด 32 บิต จะถูกนำมาทำการสลับที่ดังในตารางที่ 2.5 ซึ่งจะแสดงตำแหน่งของการสลับที่แต่ละบิต เช่นบิตที่ 1 จะถูกย้ายไปเป็นบิตที่ 16 ส่วนบิตที่ 10 จะถูกย้ายไปเป็นบิตที่ 15 เป็นต้น และหลังจากนี้ข้อมูลก็จะถูกนำมารวมกับข้อมูลทางซีกซ้ายโดย exclusive-or

ตารางที่ 2.5 ตารางในการทำ P-Boxes

Bit	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Goes to position	16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
Bit	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Goes to position	2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

2.2 การถอดรหัสลับข้อมูล

ถึงแม้ว่าลักษณะของการแทนที่และสลับที่ในการเข้ารหัสลับ จะดูเหมือนว่าได้กระทำอย่างสุ่มเพราะไม่มีรูปแบบการเปลี่ยนแปลงของข้อมูลที่แน่นอน แต่เนื่องจากมีการจัดวางขั้นตอนเหล่า นี้อย่างดี ทำให้เกิดผลลัพธ์ที่น่าประหลาดใจ นั่นคือเราสามารถใช้ algorithm เดียวกับที่ใช้ในการเข้ารหัสลับ มาทำการถอดรหัสลับได้ สิ่งนี้เป็นจริงซึ่งอาจพิสูจน์ได้โดย

ในแต่ละรอบของการเข้ารหัสลับรอบที่ i สามารถเขียนได้จากรอบที่ i-1 ดังนี้

$$L_j = R_{j-1} \qquad (1)$$

$$R_j = L_{j-1} + f(R_{j-1}, k_j) \qquad (2)$$

โดยที่ R_j และ L_j คือข้อมูลซีกขวาและซีกซ้ายในรอบที่ j ตามลำดับ เครื่องหมาย + คือการทำ exclusive-or และฟังก์ชัน f เป็นการกระทำที่มีการคำนวณ การขยาย การเลื่อน การแทนที่และการสลับที่เช่นเดียวกับในแต่ละรอบของการเข้ารหัสลับ ซึ่งจากทั้งสองสมการแสดงให้เห็นว่าผลลัพธ์ในแต่ละรอบของการเข้ารหัสลับ จะขึ้นอยู่กับผลลัพธ์ในรอบก่อนหน้านี้เท่านั้น

โดยการเขียนสมการเหล่านี้อีกครั้ง จะพบว่า

$$R_{j-1} = L_j \qquad (3)$$

$$L_{j-1} = R_j + f(R_{j-1}, k_j) \qquad (4)$$

แทนค่า (3) ใน (4)

$$L_{j-1} = R_j + f(L_j, k_j) \qquad (5)$$

สมการที่ (3) และ (5) แสดงให้เห็นว่าค่าของข้อมูลในรอบก่อนหน้านี้สามารถหาออกมาได้โดยใช้กระบวนการ (ฟังก์ชัน f) เดียวกัน สมบัติข้อนี้ทำให้ DES เป็นกระบวนการย้อนกลับได้ เราจึงสามารถถอดรหัสลับกลับคืนมาได้โดยอาศัยกระบวนการเดียวกัน

ข้อแตกต่างเพียงเล็กน้อยของ algorithm ในการถอดรหัสลับก็คือ กระบวนการต่างๆ ในฟังก์ชัน f จะถูกใช้กับข้อมูลในซีกซ้าย (ในขณะที่ในการเข้ารหัสจะใช้กับซีกขวา) และ key ที่นำมาใช้ในการเข้ารหัสจะนำมาใช้ในลำดับที่ย้อนกลับกับ key ในการเข้ารหัสลับ ยกตัวอย่างเช่น key แรกในการเข้ารหัสจะเป็น key สุดท้ายในการเข้ารหัสลับ ดังนั้น DES จึงเหมาะที่จะทำเป็น hardware หรือ software เป็นอย่างยิ่ง

บทที่ 3

DES Software release 1.0

ในโครงการนี้ได้นำเอา algorithm การเข้ารหัสลับแบบ DES มาทำการสร้างเป็นโปรแกรมขึ้น มีชื่อว่า DES software release 1.0 ซึ่งมีรายละเอียดของโปรแกรมที่ได้สร้างขึ้น ดังต่อไปนี้

3.1 การเขียนโปรแกรมใน DES software

โปรแกรม DES software นี้ ประกอบไปด้วย file ทั้งหมด 2 files ได้แก่ DES.EXE ซึ่งเป็นตัวโปรแกรมหลักและ DES.HLP ซึ่งเป็น help ของโปรแกรม

ตัวโปรแกรม DES.EXE จะเขียนขึ้นด้วยภาษา C ให้สามารถทำงานบนเครื่องคอมพิวเตอร์ทั่วไปที่ใช้ระบบปฏิบัติการ DOS โปรแกรมอาจแบ่งออกเป็นส่วนใหญ่ๆ ซึ่งทำหน้าที่ต่างกันได้สองส่วนคือ

1. ส่วนของ algorithm ในการเข้ารหัสลับ
2. ส่วนที่ทำการ interface กับผู้ใช้

ในส่วนโปรแกรมทั้งสองส่วนจะประกอบไปด้วยฟังก์ชันย่อยๆ ซึ่งทำหน้าที่ต่างๆ กันโดยมีรายละเอียดดังนี้

1. ส่วนของ algorithm ในการเข้ารหัสลับ

ในส่วนโปรแกรมส่วนนี้หน้าที่หลักในการนำข้อมูลที่ผู้ใช้ต้องการ มาทำการเข้ารหัสลับโดยใช้ algorithm ของ DES ดังที่กล่าวไว้ในรายละเอียดเกี่ยวกับการเข้ารหัสลับแบบ DES โปรแกรมส่วนนี้จะต้องดึงข้อมูลที่เป็น textfile ที่ส่วน interface ได้เปิดไว้ให้ (โดยรับชื่อแฟ้มข้อมูลมาจากผู้ใช้อีกที) มาทำการเข้ารหัส โดยใช้ key ที่ผู้ใช้ป้อนเข้ามาผ่านทางส่วน interface และนำข้อมูลที่เข้ารหัสลับแล้วไปเก็บในแฟ้มข้อมูลที่กำหนด (ซึ่งส่วน interface รับชื่อมาจากผู้ใช้เช่นกัน) และถ้ามีการผิดพลาดในการเข้ารหัสลับก็จะแสดงผลให้ผู้ใช้ทราบโดยอาศัยโปรแกรมในส่วน interface นอกจากนี้โปรแกรมในส่วนนี้จะใช้ในการถอดรหัสข้อลับมูลด้วยเช่นกัน

ฟังก์ชันย่อยต่างๆ ในโปรแกรมส่วนนี้อาจแบ่งได้เป็น

- *ฟังก์ชันย่อยที่ทำการอ่านและเก็บข้อมูล*

ได้แก่ฟังก์ชัน loaddata() , savedata() ซึ่งทำหน้าที่ในการอ่านข้อมูลและจัดเก็บข้อมูลในแฟ้มข้อมูลที่ฟังก์ชันย่อยในโปรแกรมส่วน interface ได้ทำการเปิดไว้ โดยจะอ่านข้อมูลมาใช้เข้ารหัสลับหรือถอดรหัสลับ และเก็บข้อมูลครั้งละ 64 บิตหรือ 8 ไบต์ และถ้ามีการผิดพลาดในการอ่านหรือเขียนข้อมูลก็จะให้ค่ากลับไปยังโปรแกรมหลักเป็น -1

- *ฟังก์ชันย่อยที่ทำการเตรียมข้อมูล*

เนื่องจาก algorithm ของ DES จะดำเนินการกับข้อมูลเป็นบิต แต่ในภาษา C การอ่านหรือเขียนข้อมูลจะทำเป็นไบต์ และตัวแปรต่างๆ ก็จะมีหน่วยเป็นไบต์ จึงจำเป็นที่จะต้องเขียนฟังก์ชันย่อยเหล่านี้ขึ้นเพื่อใช้ในการเตรียมข้อมูลให้สามารถนำมาใช้ได้ทีละบิต ฟังก์ชันย่อยเหล่านี้ได้แก่

crebit(i) ฟังก์ชันนี้จะให้ค่าของข้อมูลบิตที่ i ในตัวแปร input ซึ่งเก็บข้อมูลที่จะนำมาเข้ารหัสไว้ แต่เก็บเป็นไบต์

make_bit() ฟังก์ชันนี้จะอาศัยฟังก์ชัน crebit() มาทำการแปลงข้อมูลทั้ง 8 ไบต์ในตัวแปร input ให้เป็นข้อมูล 64 บิตซึ่งสามารถนำมาใช้เป็นบิตได้

left_right() จะทำการแบ่งครึ่งข้อมูลที่เป็นบิต ให้เป็นสองส่วนคือซีกซ้ายและซีกขวาขนาด 32 บิต

set_bit(i) และ clear_bit(i) จะทำหน้าที่กลับกับ crebit() คือจะทำการ set หรือ clear ข้อมูลในตัวแปร input บิตที่ i ให้กลายเป็น 1 และ 0 ตามลำดับ

combine() จะทำการรวมข้อมูลซีกซ้ายและขวาเข้าเป็นข้อมูลขนาด 64 บิตดังเดิม

make_char() จะทำหน้าที่กลับกับ make_bit() โดยจะอาศัยฟังก์ชัน set_bit() และclear_bit() มาทำการรวมข้อมูลที่แยกกันเป็น 64 บิต ให้กลับเป็นข้อมูล 8 ไบต์ดังเดิม

- *ฟังก์ชันย่อยที่ทำการเตรียม key*

ในการใช้ key ใน algorithm ก็จะใช้เป็นบิตเช่นกัน จึงต้องมีการสร้างฟังก์ชันย่อยที่ทำการเตรียม key เหมือนกับในการเตรียมข้อมูล ฟังก์ชันเหล่านี้ได้แก่

crekey(i,j) จะให้ค่าของบิตที่ i ของ key ชุดที่ j จากทั้งหมด 16 ชุด

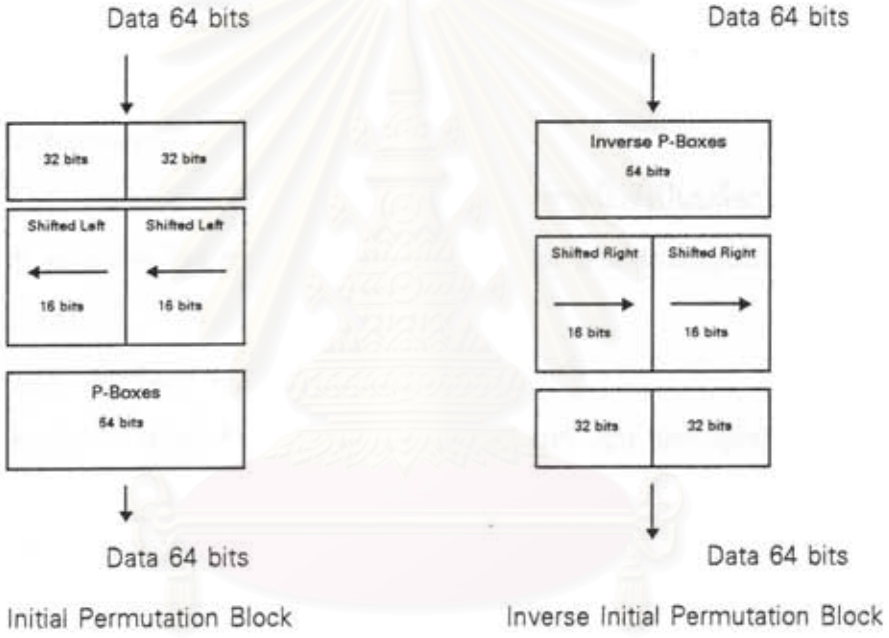
make_key(j) จะนำฟังก์ชัน crekey(i,j) มาทำการเตรียม key ชุดที่ j ที่เป็นไบต์ให้สามารถนำไปใช้เป็นบิตได้

le_ri_key(j) จะทำการแบ่งครึ่ง key ชุดที่ j ที่เป็นบิตให้เป็นซีกซ้ายและซีกขวา

comb_key(j) จะทำการรวม key ชุดที่ j ซีกซ้ายและซีกขวาให้กลับเป็น key ขนาด 64 บิต

- *ฟังก์ชันย่อยที่เป็น algorithm*

ฟังก์ชันย่อยในส่วนนี้ จะทำหน้าที่เป็นบล็อกต่างๆ ใน algorithm การเข้ารหัส นอกจากนี้ยังมีส่วนของบล็อก initial permutation และ inverse initial permutation ที่ได้ทำการสร้างและกำหนดวิธีการเข้ารหัสขึ้นเอง ซึ่งบล็อกทั้งสองจะทำหน้าที่ดังในรูปที่ 3.1



รูปที่ 3.1 แสดงบล็อก initial permutation และ inverse initial permutation

ส่วนของบล็อกที่เป็น Inverse P-Boxes จะทำหน้าที่กลับกับ P-Boxes นั่นคือจะทำให้ข้อมูลที่ถูกสลับโดย P-Boxes มีลักษณะเหมือนเดิม และจะมีตารางในการทำ Inverse P-Boxes ดังในตารางที่ 3.1

ตารางที่ 3.1 ตารางในการทำ Inverse P-Boxes

Bit	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Goes to position	9	17	23	31	13	28	2	18	24	16	30	6	26	20	10	1
Bit	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Goes to position	8	14	25	3	4	29	11	19	32	12	22	7	5	27	15	21

ฟังก์ชันย่อยในส่วนนี้จะประกอบไปด้วย

shiftright(n,size,pt) และ shiftleft(n,size,pt) จะทำการเลื่อนข้อมูลที่ถูกชี้โดย pointer pt ขนาด size บิต ไปทางขวาและซ้ายเป็นวงกลมเป็นจำนวน n บิต

ch_per(j) ฟังก์ชันนี้จะทำหน้าที่เป็นบล็อก Choice Permutation ใน algorithm โดยจะนำ key ชุดที่ j มาผ่านกระบวนการ

p_box(pt,ppt) และ inv_p_box(pt,ppt) ฟังก์ชันทั้งสองจะทำหน้าที่เป็นบล็อก P-Boxes และ Inverse P-Boxes ใน algorithm โดยจะนำข้อมูลที่ชี้โดย pointer pt มาผ่านกระบวนการและเก็บไว้โดยใช้ pointer ppt เป็นตัวชี้

int_per() และ invs_per() จะทำหน้าที่เป็นบล็อก Initial Permutation และ Inverse Initial Permutation ใน algorithm โดยอาศัยฟังก์ชันย่อยอื่นๆ ที่กล่าวมา เช่น shiftright() , shiftleft() , p_box() , inv_p_box() เป็นต้น

ex_per(pt,expt) ทำหน้าที่เป็นบล็อก Expansion Permutation ใน algorithm โดยจะนำข้อมูลที่ชี้ด้วย pointer pt มาผ่านกระบวนการและเก็บไว้โดยชี้โดย pointer expt

s_box(pt,spt) ทำหน้าที่เป็นบล็อก S-Boxes ใน algorithm โดยจะนำข้อมูลที่ชี้ด้วย pointer pt มาผ่านกระบวนการและเก็บไว้โดยชี้โดย pointer spt

ex_or(i,j) ฟังก์ชันนี้จะนำข้อมูลในตัวแปร I และ j มาทำการ exclusive-or กัน และจะให้ค่าเป็นผลลัพธ์กลับไป

encryp() เป็นฟังก์ชันที่รวมเอาฟังก์ชันย่อยอื่นๆ มาเป็น algorithm ในการเข้ารหัส

decryp() เป็นฟังก์ชันที่รวมเอาฟังก์ชันย่อยอื่นๆ มาเป็น algorithm ในการถอดรหัส

2. *ส่วนที่ทำการ interface กับผู้ใช้*

โปรแกรมส่วนนี้ทำหน้าที่ในการติดต่อกับผู้ใช้ โดยสร้างหน้าจอเป็นเมนูขึ้นมา รอรับคำสั่งจากผู้ใช้ แล้วทำการเรียกโปรแกรมย่อยในส่วนที่เกี่ยวข้องมาทำหน้าที่นั้น และแสดงผลการทำงานให้ผู้ใช้ได้ทราบทางหน้าจอ โปรแกรมในส่วนนี้จะประกอบไปด้วยฟังก์ชันย่อยที่ทำหน้าที่ต่างๆกันดังต่อไปนี้

- ฟังก์ชันย่อยที่ทำการเปิดแฟ้มข้อมูลและจัดการเกี่ยวกับชื่อแฟ้มข้อมูล

ได้แก่ฟังก์ชันต่างๆดังนี้

opfile() , opsfile() , opdesfile() และ opsavefile() ทั้ง 4 ฟังก์ชันย่อยนี้ทำหน้าที่ในการเปิดแฟ้มข้อมูลเพื่อนำมาใช้งานต่างๆ กัน โดย opfile() จะเปิดแฟ้มข้อมูลที่เก็บข้อมูลที่จะนำมาเข้ารหัสลับ opsfile() จะเปิดแฟ้มข้อมูลสำหรับเก็บข้อมูลที่เข้ารหัสลับแล้ว opdesfile() จะเปิดแฟ้มข้อมูลที่จะนำมาถอดรหัสลับ และ opsavefile() จะเปิดแฟ้มข้อมูลเพื่อเก็บข้อมูลที่ถอดรหัสลับแล้ว (แฟ้มข้อมูลที่จะนำมาเข้ารหัสลับนั้นจะต้องเป็น text file และเมื่อทำการเข้ารหัสลับแล้ว DES software จะทำการเก็บไว้ในแฟ้มข้อมูลใหม่โดยมีนามสกุลเป็น .DES) โปรแกรมเหล่านี้จะรับชื่อของแฟ้มข้อมูลจากผู้ใช้ทางแป้นพิมพ์ ซึ่งผู้ใช้จะพิมพ์ชื่อหรือจะเลือกจากรายชื่อแฟ้มข้อมูลที่ปรากฏบนหน้าจอก็ได้

opdis1file() , opdis2file() และ opdis3file() จะทำการเปิดแฟ้มข้อมูลมาใช้ในการแสดงข้อมูลทางหน้าจอใน mode Display ของ DES software โดยจะทำการรับชื่อของแฟ้มข้อมูลจากผู้ใช้ในลักษณะเดียวกับ 4 ฟังก์ชันย่อยข้างต้น

blankchk(pt) จะทำการตรวจสอบชื่อของแฟ้มข้อมูลที่ชี้โดย pointer pt ว่าเป็นตัวว่างทั้งหมดหรือไม่

txtchk(pt) จะทำการตรวจสอบชื่อของแฟ้มข้อมูลที่ชี้โดย pointer pt ว่าเป็นชื่อของ textfile หรือไม่

deschk(pt) จะทำการตรวจสอบชื่อของแฟ้มข้อมูลที่ชี้โดย pointer pt ว่าเป็นชื่อของแฟ้มข้อมูลที่ถูกเข้ารหัสลับโดย DES software หรือไม่ (มีนามสกุลเป็น . DES)

makesname(pt) จะทำการเติมชื่อแฟ้มข้อมูลที่ชี้โดย pointer pt ให้มีนามสกุลเป็น . DES

upname(pt) จะทำการเปลี่ยนชื่อแฟ้มข้อมูลที่ชี้โดย pointer pt ให้เป็นตัวอักษรตัวใหญ่ทั้งหมด

clearname() จะทำการลบชื่อแฟ้มข้อมูลในตัวแปรสำหรับเก็บชื่อแฟ้มข้อมูล (ใช้ในการ clear ค่าตัวแปร)

- ฟังก์ชันที่ทำการแสดงผลการทำงานหรือการออกจากโปรแกรม

ได้แก่ฟังก์ชันย่อยดังต่อไปนี้

error1() , error2() , error3() , error4() , error5() , error6() , error7() และ error8() จะทำหน้าที่ในแสดงข้อผิดพลาดที่เกิดขึ้นต่างๆกันบนหน้าจอ

quit_show(h) ทำหน้าที่แสดงข้อความบอกผู้ใช้ก่อนที่จะออกจากโปรแกรมในแต่ละเมนู และรอรับค่าคำตอบจากผู้ใช้เป็น Yes หรือ No ว่าต้องการออกจากโปรแกรมหรือไม่ ค่าในตัวแปร h จะบอกให้ฟังก์ชันนี้ทราบว่าเป็นการออกจากส่วนใดของโปรแกรม ทำให้สามารถแสดงข้อความได้ถูกต้อง

quit_des() ทำหน้าที่เหมือนกับฟังก์ชัน quit_show() แต่เป็นการจบการทำงานและออกจากโปรแกรม DES software เลย

seemore() แสดงข้อความและรอรับการตัดสินใจของผู้ใช้ใน Display mode ว่าต้องการจะดูข้อมูลในแฟ้มข้อมูลอื่นอีกหรือไม่

- ฟังก์ชันที่ทำการรับค่า key จากผู้ใช้

ได้แก่ฟังก์ชันดังต่อไปนี้

inputkey(n) ฟังก์ชันนี้จะทำการสร้างหน้าจอเพื่อรับค่า key จากผู้ใช้เป็นจำนวน n ชุด ค่า n นี้จะเป็น key mode ของข้อมูล (รายละเอียดเกี่ยวกับ key mode จะกล่าวถึงในวิธีการใช้งาน DES software ในรายงานฉบับสมบูรณ์)

prekey(n) จะทำการเตรียม key ซึ่งมีอยู่ n ชุดซึ่งรับค่ามาจากผู้ใช้มาเตรียมเป็น key ให้ครบ 16 ชุด เพื่อใช้ในการเข้ารหัส

fillkey(pt) จะทำการตรวจสอบ key ที่ชี้โดย pointer pt ว่าครบ 8 ตัวอักษรหรือไม่ (8 ไบต์) ถ้ายังไม่ครบจะทำการเติมด้วยตัวว่าง (blank) จนครบ

- ฟังก์ชันย่อยที่ทำการแสดงข้อมูลบนหน้าจอ

เป็นฟังก์ชันที่ใช้ใน Display mode ของโปรแกรม ทำหน้าที่ต่างๆ กันดังนี้

showtext() ฟังก์ชันนี้จะทำการนำข้อมูลที่ผู้ใช้ต้องการจะแสดงใน Display mode มาแสดงบนหน้าจอ

control() ฟังก์ชันนี้จะใช้ในการควบคุมหน้าจอแสดงข้อมูลใน Display mode เช่นจะรับค่าปุ่ม PgUp และ PgDw จากทางแป้นพิมพ์และทำการเลื่อนข้อมูลขึ้นหรือลงไปหนึ่งหน้าเป็นต้น

- *ฟังก์ชันในเมนูหลัก*

main() ฟังก์ชันนี้จะเป็นฟังก์ชันหลัก ซึ่งจะทำการสร้างหน้าจอหลัก สร้างระบบ help ในโปรแกรม คอยรับคำสั่งจากผู้ใช้ และทำการเรียกใช้ฟังก์ชันย่อยอื่นๆ ให้ทำหน้าที่นั้นๆ ฟังก์ชันย่อยหลักที่มีการเรียกใช้จากฟังก์ชันนี้มีดังต่อไปนี้

encryption(n) เป็นฟังก์ชันที่ถูกเรียกจากฟังก์ชันหลักเพื่อทำหน้าที่ในการเข้ารหัสลับข้อมูล ซึ่งฟังก์ชันนี้ก็จะทำการเรียกใช้ฟังก์ชันย่อยอื่นๆ อีกที เช่น ฟังก์ชัน encryp() เป็นต้น ค่า n จะบอกให้ทราบถึง key mode ที่ผู้ใช้เลือกในการเข้ารหัสลับ

decryption(n) ถูกเรียกใช้เช่นเดียวกับ encryption(n) เพื่อทำการถอดรหัสลับข้อมูล ฟังก์ชันนี้จะเรียกใช้ฟังก์ชันย่อยอื่นๆ อีกที เช่น ฟังก์ชัน encryp() เป็นต้น ค่า n จะบอกให้ทราบถึง key mode ที่ผู้ใช้เลือกในการเข้ารหัส

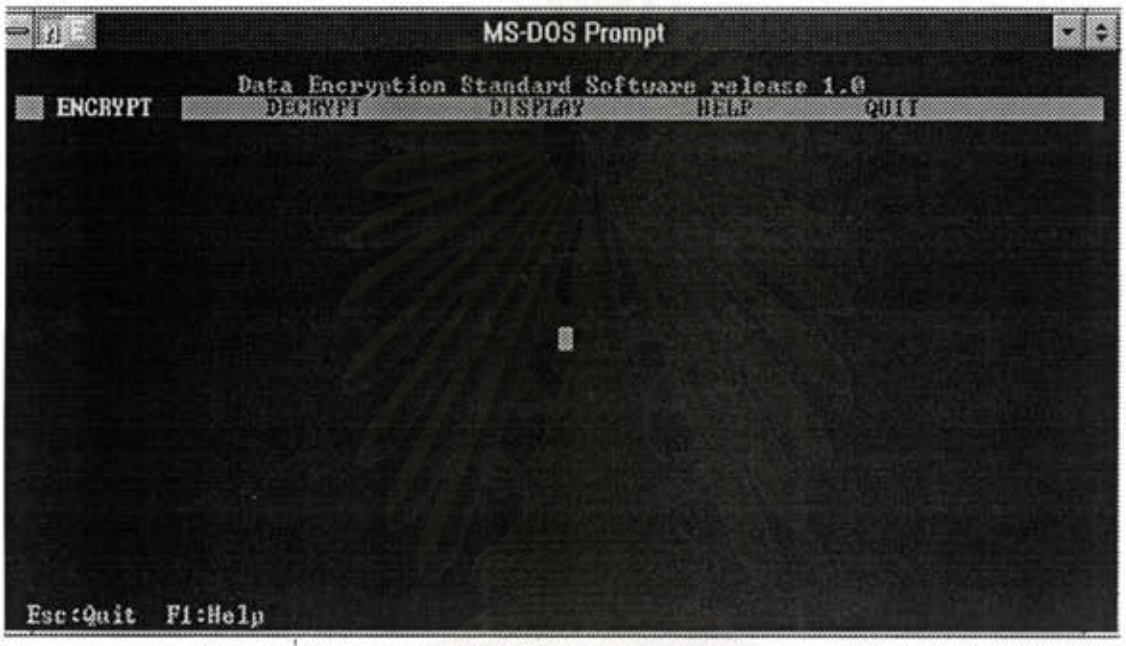
display_1() และ display_2() เป็นฟังก์ชันที่ฟังก์ชันหลักเรียกใช้เพื่อทำการแสดงข้อมูลใน Display mode ซึ่งก็จะมีการเรียกใช้ฟังก์ชันย่อยอื่นๆ เช่นฟังก์ชัน showtext() , control() อีกทีหนึ่ง ข้อมูลที่แสดงในฟังก์ชัน display_1() จะเป็นข้อมูลที่ยังไม่เข้ารหัสลับกับข้อมูลที่เข้ารหัสลับแล้ว ส่วน display_2() จะแสดงข้อมูลที่เข้ารหัสลับแล้วกับข้อมูลที่ถอดรหัสลับแล้ว

helpfunct() เป็นฟังก์ชันที่ถูกเรียกใช้เมื่อผู้ใช้เลือกเมนู Help ในเมนูหลัก จะแสดงข้อความบอกให้ผู้ใช้ทราบวิธีการใช้ Help ใน DES software

quit() เป็นฟังก์ชันที่มีการเรียกเมื่อผู้ใช้ต้องการออกจาก DES software โดยเลือกเมนู Quit ในเมนูหลัก จะมีผลเหมือนกับการกดปุ่ม Esc ในหน้าจอหลัก

3.2 วิธีการใช้ DES software

การใช้งาน DES software นั้น จะเริ่มต้นโดยการเรียกใช้โปรแกรม DES.EXE ที่ command line ใน DOS หลังจากนั้นผู้ใช้ก็จะเข้าสู่ menu หลักหรือ main menu ของ DES software ซึ่งมีลักษณะดังในรูปที่ 3.2



รูปที่ 3.2 แสดง main menu หลัก ของ DES software *

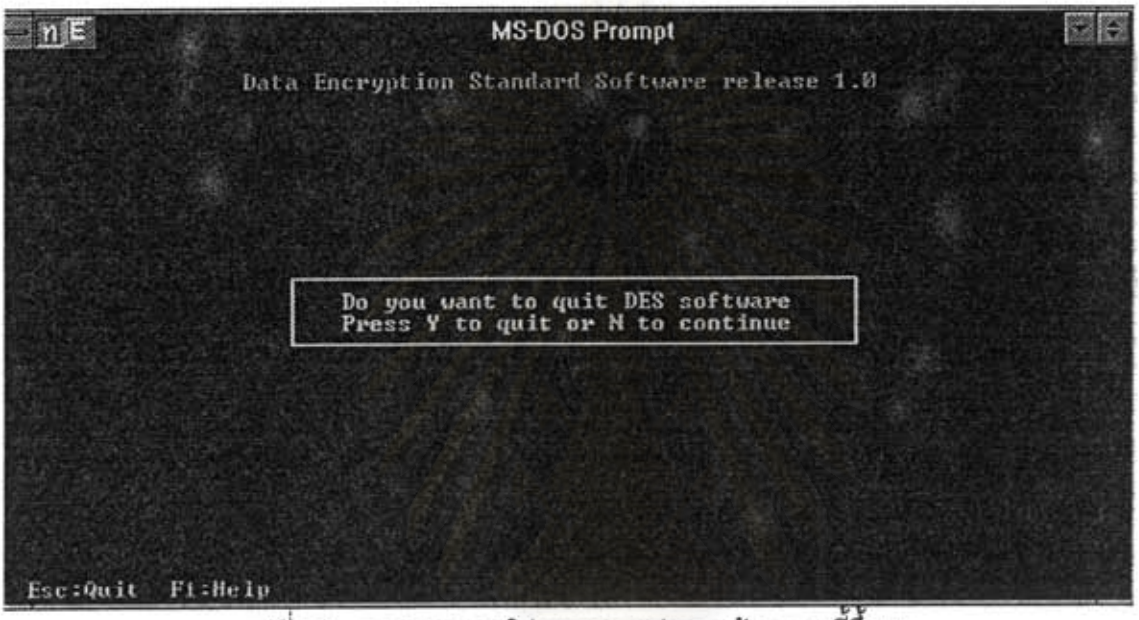
จากรูปที่ 3.2 DES software จะมี menu หลักให้เลือกใช้ดังนี้

1. Encryption mode หรือ การเข้ารหัสลับ
2. Decryption mode หรือ การถอดรหัสลับ
3. Display mode หรือ การแสดงข้อมูล
4. Help หรือ คำอธิบาย
5. Quit หรือ คำสั่งออกจากโปรแกรม

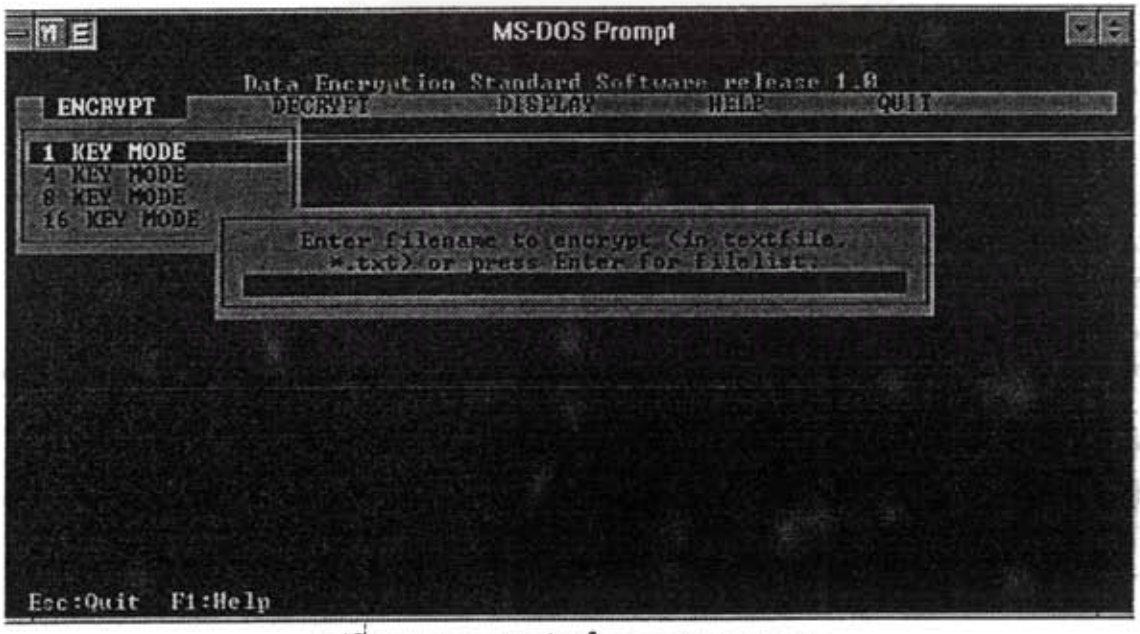
การเลือกใช้งานใน mode ใดๆ สามารถทำได้โดยการใช้ปุ่ม cursor เลื่อนแถบสว่างหรือ selection bar ไปยัง menu ที่ต้องการ แล้วกด Enter หรืออาจจะใช้ quick key ของแต่ละ menu ซึ่ง จะแสดงด้วยตัวอักษรสว่างในแต่ละ menu นอกจากนี้ยังสามารถเลือกโดยใช้ mouse click บน menu ที่ผู้ใช้ต้องการถ้ามี mouse อยู่ด้วย

*หมายเหตุ รูปทุกรูปในวิธีการใช้ DES software นี้สร้างโดยใช้โปรแกรมใน Windows จึงมีขอบของหน้าต่างใน Windows อยู่ด้วย

ที่ main menu นี้ ถ้าผู้ใช้ต้องการออกจากโปรแกรม DES software ก็สามารถทำได้โดยการกดปุ่ม Esc (Escape) หรือเลือก menu Quit หลังจากนั้นจะปรากฏข้อความดังในรูปที่ 3.3 ถ้าผู้ใช้ต้องการจบการใช้งาน DES software ก็ทำได้โดยการกด Y ซึ่งจะทำให้ออกจากโปรแกรมไปสู่command line ใน DOS แต่ถ้าผู้ใช้ต้องการใช้งาน DES software ต่อไปก็ทำได้โดยการกด N ซึ่งจะทำให้กลับเข้าสู่เมนูหลักอีกครั้ง



รูปที่ 3.3 การออกจากโปรแกรมจะปรากฏข้อความนี้ขึ้นมา



รูปที่ 3.4 แสดงเมนูย่อยใน Encryption mode

3.2.1 การใช้ DES software เข้ารหัสลับ (Encryption mode)

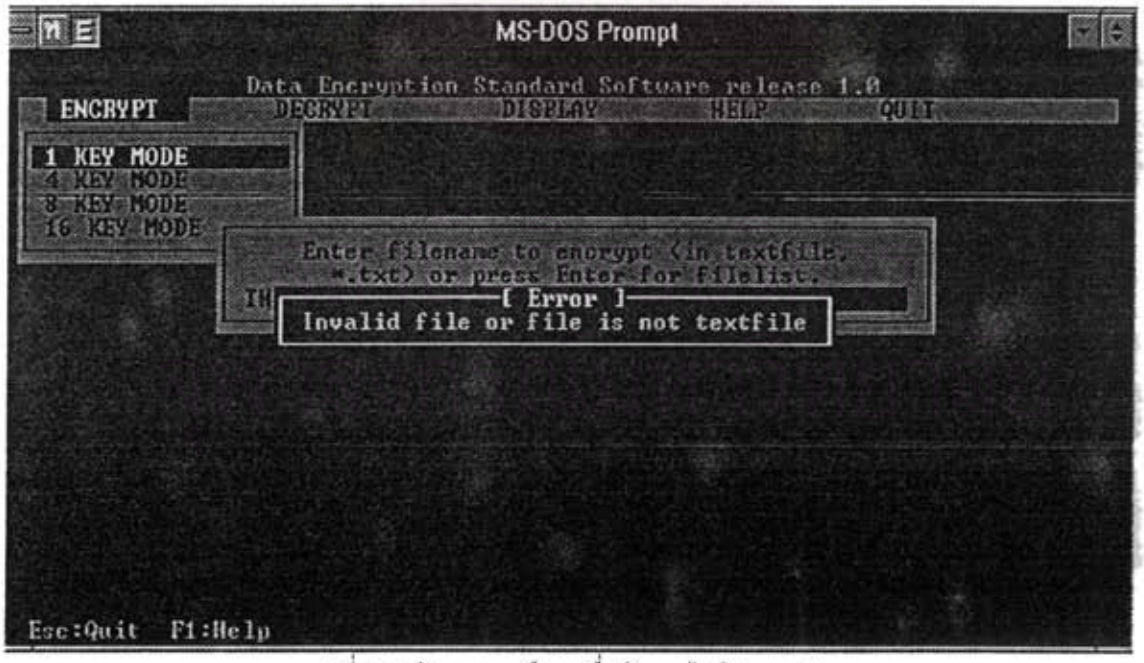
เมื่อผู้ใช้ต้องการใช้ DES software ในการเข้ารหัสลับข้อมูล ก็ทำได้โดยการเลือกไปที่เมนูEncryption หลังจากนั้นจะปรากฏเมนูย่อยให้เลือกอีก และเมื่อเลือกเมนูย่อยแล้วก็จะเข้าสู่หน้าจอดังในรูปที่ 3.4

เมนูย่อยนี้จะแสดงถึง key mode ต่างๆกัน ซึ่งช่วยให้สามารถเข้ารหัสลับข้อมูลได้สะดวกขึ้น key mode หมายถึงจำนวน key ที่จะใช้ในการเข้ารหัสลับข้อมูล ยกตัวอย่างเช่น ถ้าผู้ใช้ต้องการเข้ารหัสลับข้อมูลโดยไม่ต้องการความปลอดภัยสูงมากนักก็อาจจะใช้ key เพียง 4 ชุดในการเข้ารหัสลับ ซึ่งสามารถทำได้โดยการเลือกไปที่เมนู 4 key mode การเข้ารหัสโดยใช้ key หลายๆ ชุดที่ต่างกัน จะมีความปลอดภัยของข้อมูลสูงกว่า การใช้ key เพียงไม่กี่ชุดหรือหลายชุดแต่ซ้ำกัน

ใน DES software จะมี mode ของ key ให้เลือกอยู่ 4 mode คือ

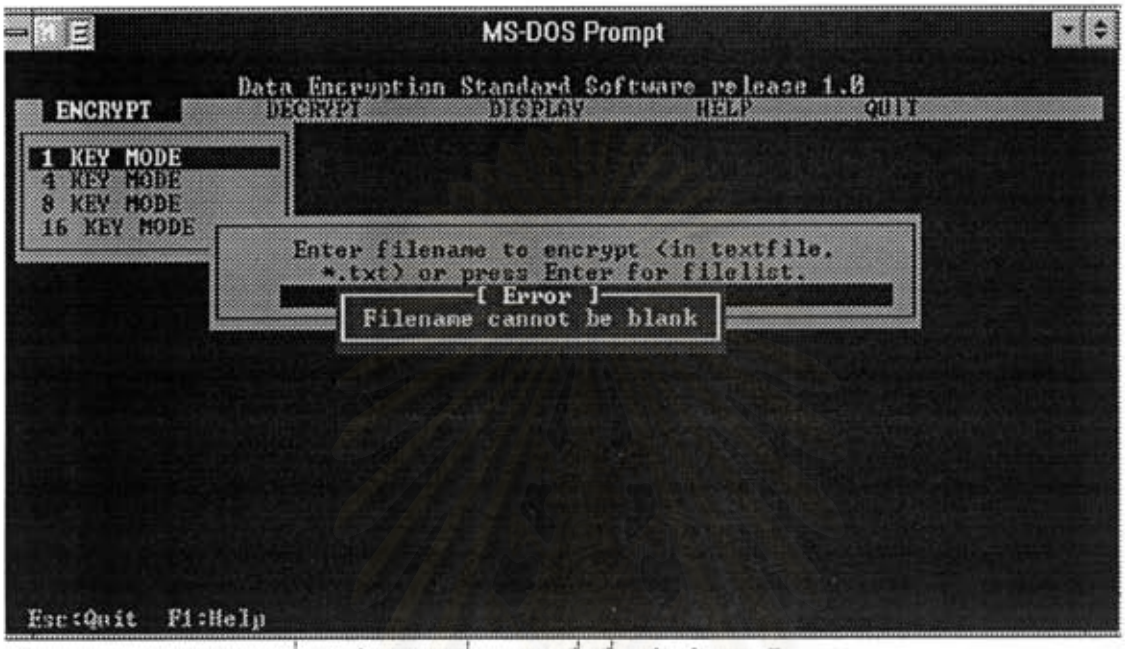
- 1 key mode
- 4 key mode
- 8 key mode
- 16 key mode

หลังจากที่ผู้ใช้เลือก key mode แล้ว จะปรากฏหน้าจอให้ใส่ชื่อของแฟ้มข้อมูล ซึ่งแฟ้มข้อมูลจะต้องเป็นข้อมูลประเภท textfile เท่านั้น ถ้าไม่ใช่ก็จะปรากฏข้อความเตือนดังในรูปที่ 3.5

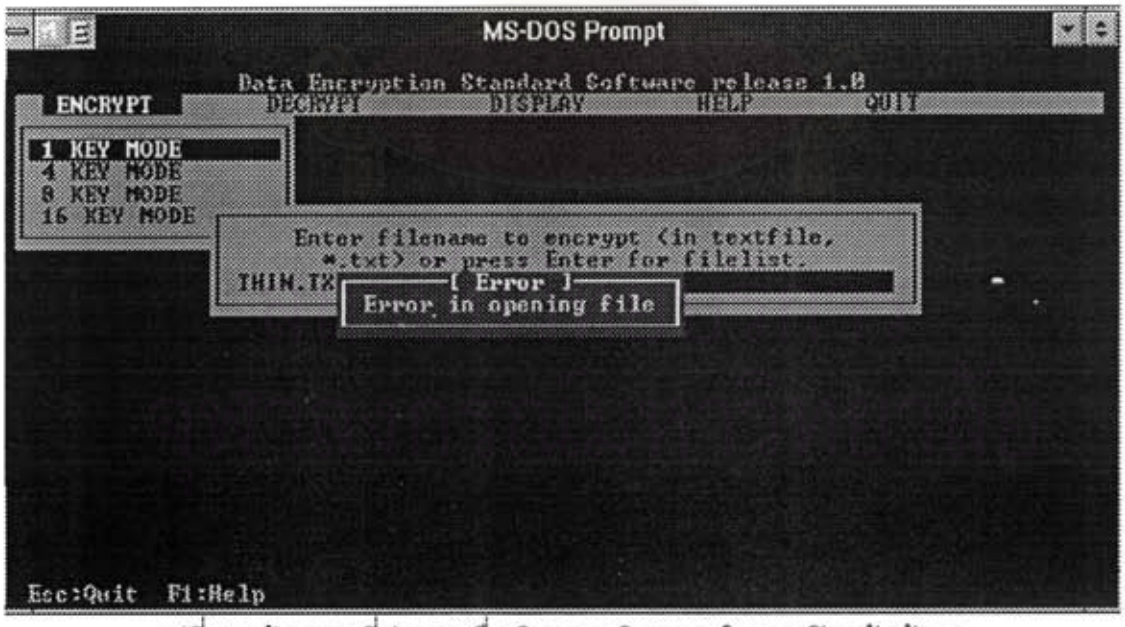


รูปที่ 3.5 ข้อความเตือนเมื่อข้อมูลไม่ใช่ textfile

ถ้าชื่อของแฟ้มข้อมูลเป็นตัวว่างทั้งหมดก็จะปรากฏข้อความในรูปที่ 3.6 และถ้าในการเปิดแฟ้มข้อมูลอันนั้นมีความผิดพลาดเกิดขึ้นเช่น แฟ้มข้อมูลมีการชำรุดเสียหาย ก็จะปรากฏข้อความดังในรูปที่ 3.7

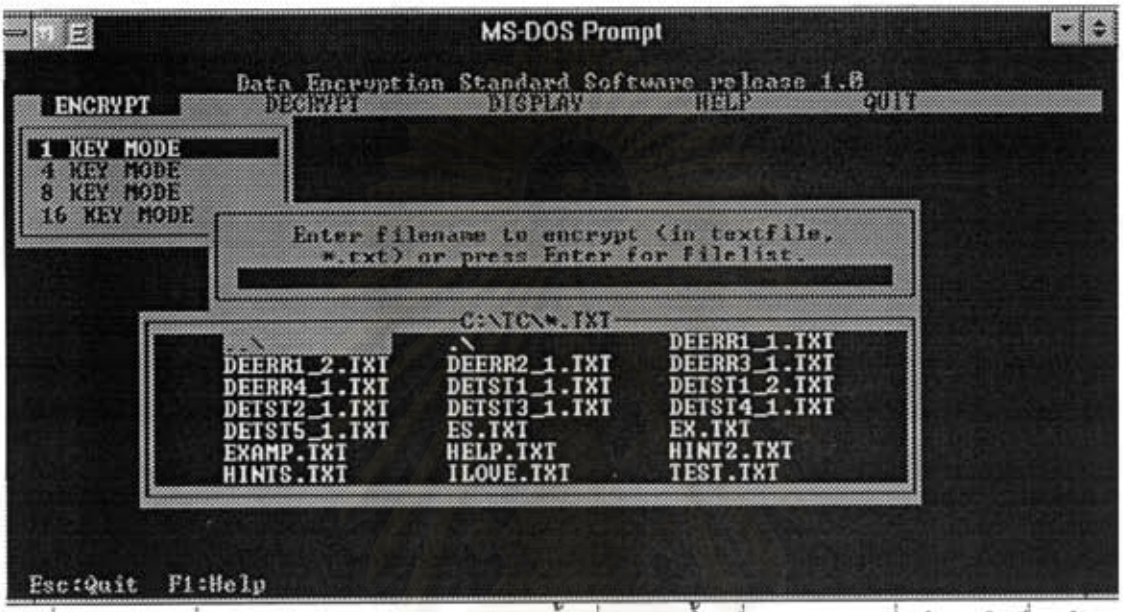


รูปที่ 3.6 ข้อความที่ปรากฏเมื่อชื่อแฟ้มข้อมูลเป็นตัวว่าง



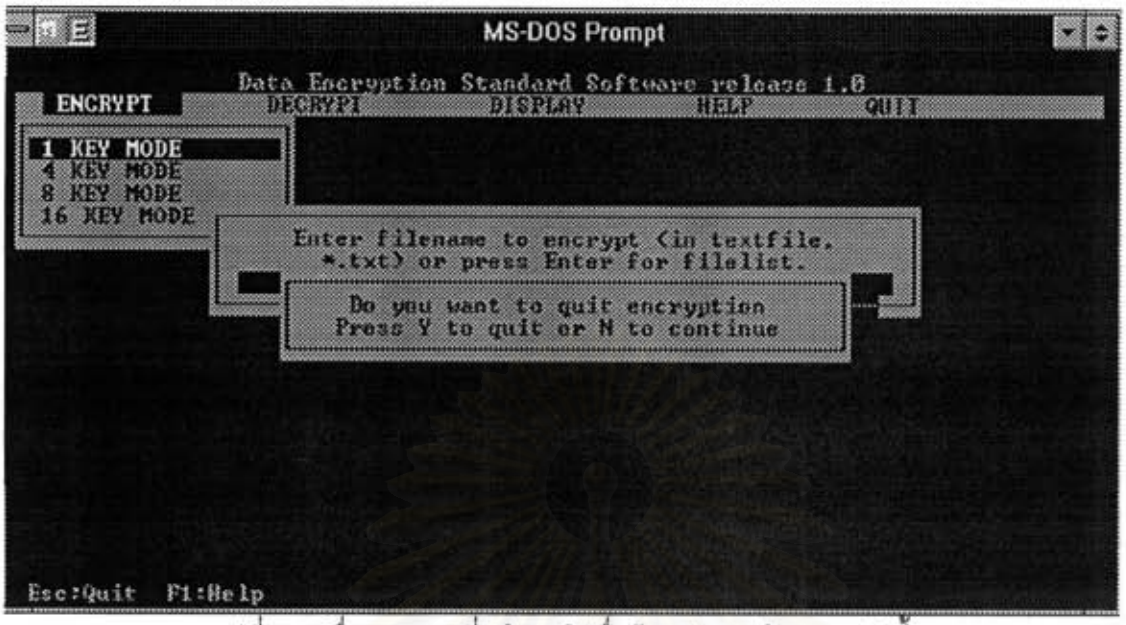
รูปที่ 3.7 ข้อความที่ปรากฏเมื่อเกิดความผิดพลาดในการเปิดแฟ้มข้อมูล

ถ้าหากผู้ใช้ต้องการทราบว่ามีแฟ้มข้อมูลอะไรบ้างที่เป็น textfile ใน directory นั้น ก็จะสามารถทำได้โดยการกด Enter ที่หน้าจอใส่ชื่อแฟ้มข้อมูล จะปรากฏรายชื่อของแฟ้มข้อมูลออกมาดังในรูปที่ 3.8 ผู้ใช้สามารถเลือกแฟ้มข้อมูลมาจากรายชื่อเหล่านี้ แล้วกด Enter ซึ่งจะเหมือนกับการป้อนชื่อแฟ้มข้อมูลนั้นที่หน้าจอ



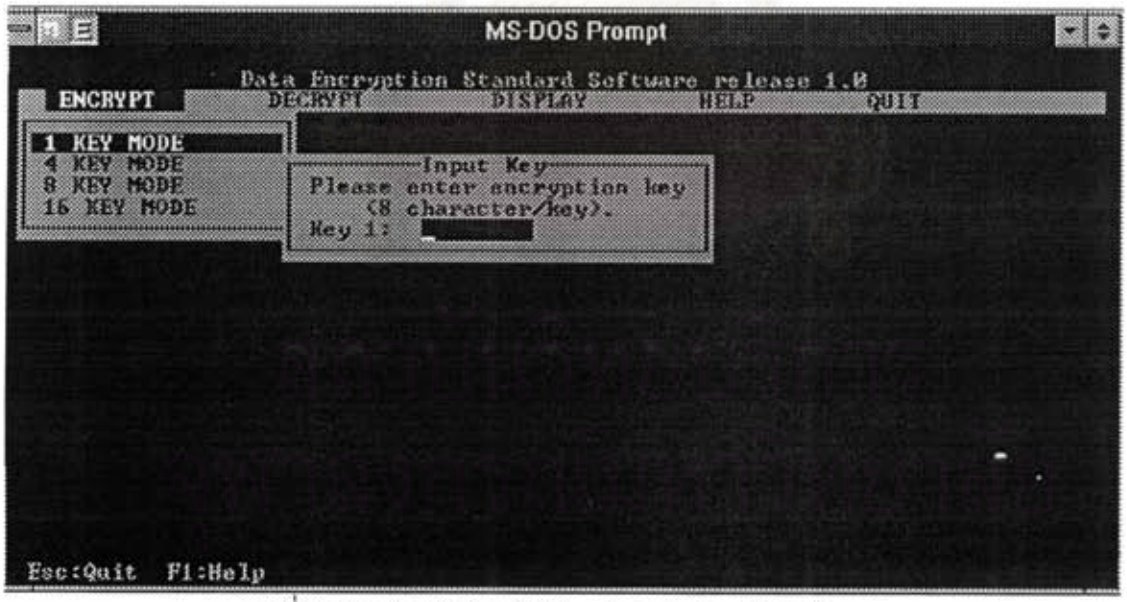
รูปที่ 3.8 รายชื่อของแฟ้มข้อมูลใน directory นั้นที่ปรากฏขึ้นเมื่อกด Enter ที่หน้าจอใส่ชื่อแฟ้มข้อมูล

ถ้าในขณะที่อยู่ในหน้าจอใส่ชื่อแฟ้มข้อมูลนี้ ผู้ใช้ต้องการออกจากการเข้ารหัสลับไปสู่เมนูหลัก ก็สามารถทำได้โดยการกดปุ่ม Esc ซึ่งจะปรากฏข้อความดังในรูปที่ 3.9 เมื่อผู้ใช้กด Y ก็จะกลับไปสู่เมนูหลัก แต่ถ้ากด N ก็จะกลับเข้าสู่หน้าจอใส่ชื่ออีกครั้ง



รูปที่ 3.9 เมื่อกด Esc ที่หน้าจอใส่ชื่อก็จะปรากฏข้อความดังนี้

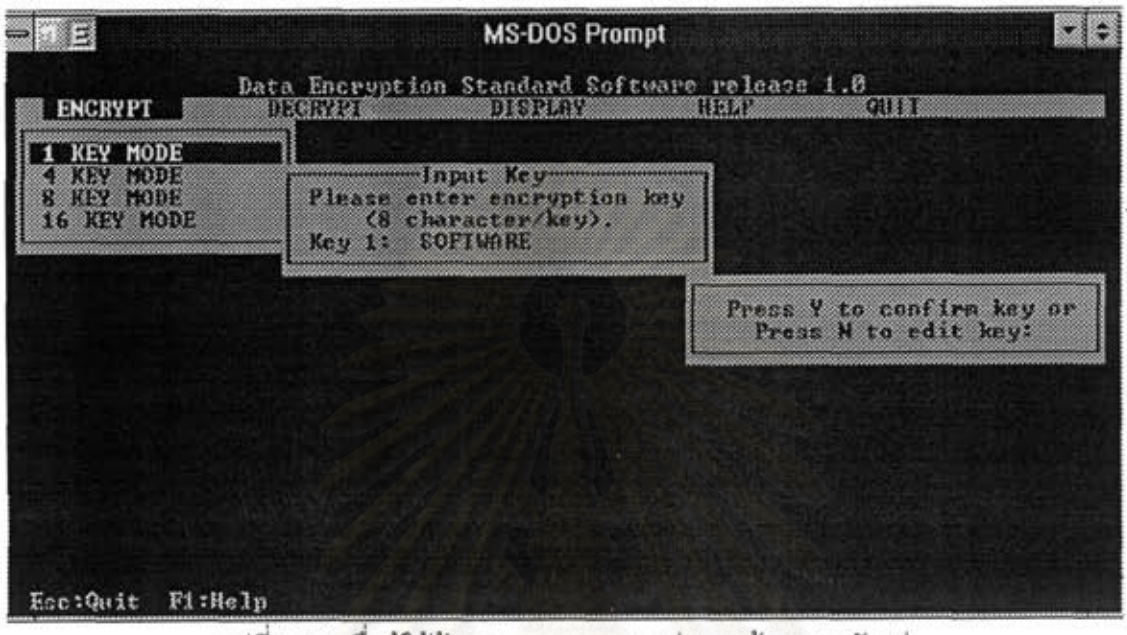
หลังจากที่ผู้ใช้ทำการใส่ชื่อแฟ้มข้อมูลแล้ว ก็จะเข้าสู่การใส่ key ที่จะใช้ในการเข้ารหัสลับข้อมูลดังในรูปที่ 3.10



รูปที่ 3.10 แสดงหน้าจอใส่ key ในการเข้ารหัสลับข้อมูล

ในการใส่ key นั้น key แต่ละชุดจะประกอบด้วยตัวอักษรทั้งหมด 8 ตัวซึ่งจะเป็นตัวใดในแป้นพิมพ์หรือเป็นสัญลักษณ์ต่างๆ ในแป้นพิมพ์ก็ได้ เมื่อผู้ใช้ใส่ key จนครบ(ตาม mode ของ key) จะปรากฏข้อความให้ผู้ใช้ยืนยัน key ที่ป้อนเข้ามาดังในรูปที่ 3.11 ซึ่งถ้าผู้ใช้ยืนยันการใช้

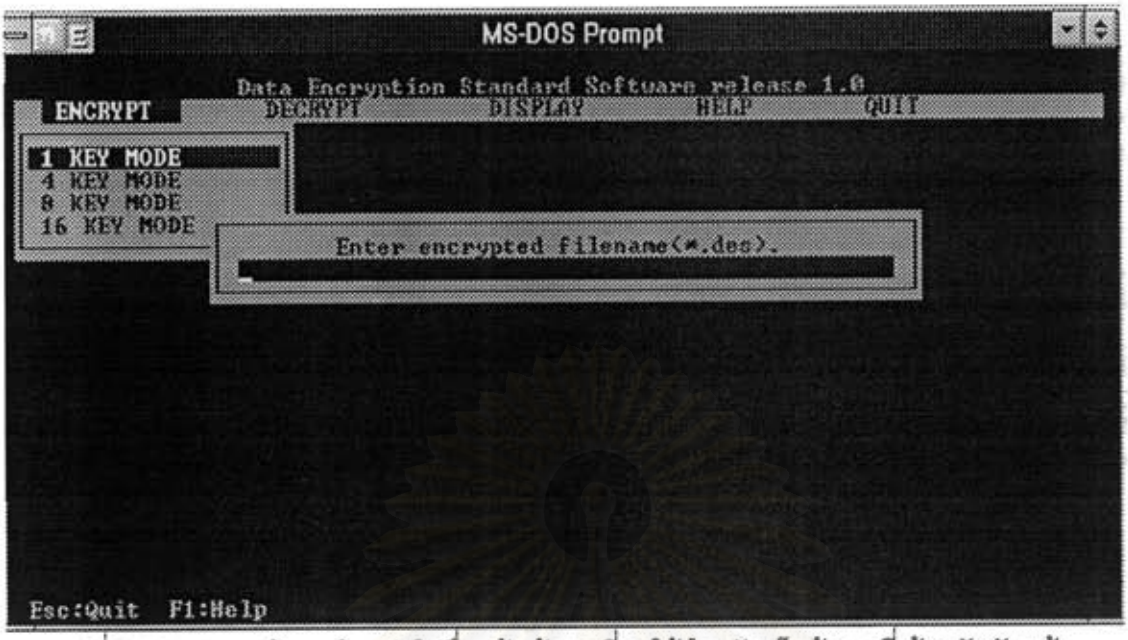
key นั้น โดยการกด Y key นั้นก็จะถูกนำไปใช้ในการเข้ารหัส แต่ถ้าผู้ใช้กด N key นั้นก็จะไม่ถูกใช้สำหรับเข้ารหัสลับและจะกลับเข้าสู่การป้อน key อีกครั้ง



รูปที่ 3.11 เมื่อผู้ใช้ป้อน key จนครบจะปรากฏข้อความดังรูป

ถ้าในระหว่างการป้อน key ผู้ใช้ต้องการออกจากการเข้ารหัสลับไปสู่เมนูหลัก ก็สามารถทำได้เช่นเดียวกับที่หน้าจอใส่ชื่อแฟ้มข้อมูล โดยการกดปุ่ม Esc ซึ่งจะปรากฏข้อความดังในรูปที่ 3.9 เมื่อผู้ใช้กด Y ก็จะกลับไปสู่เมนูหลัก แต่ถ้ากด N ก็จะกลับเข้าสู่การป้อน key อีกครั้ง

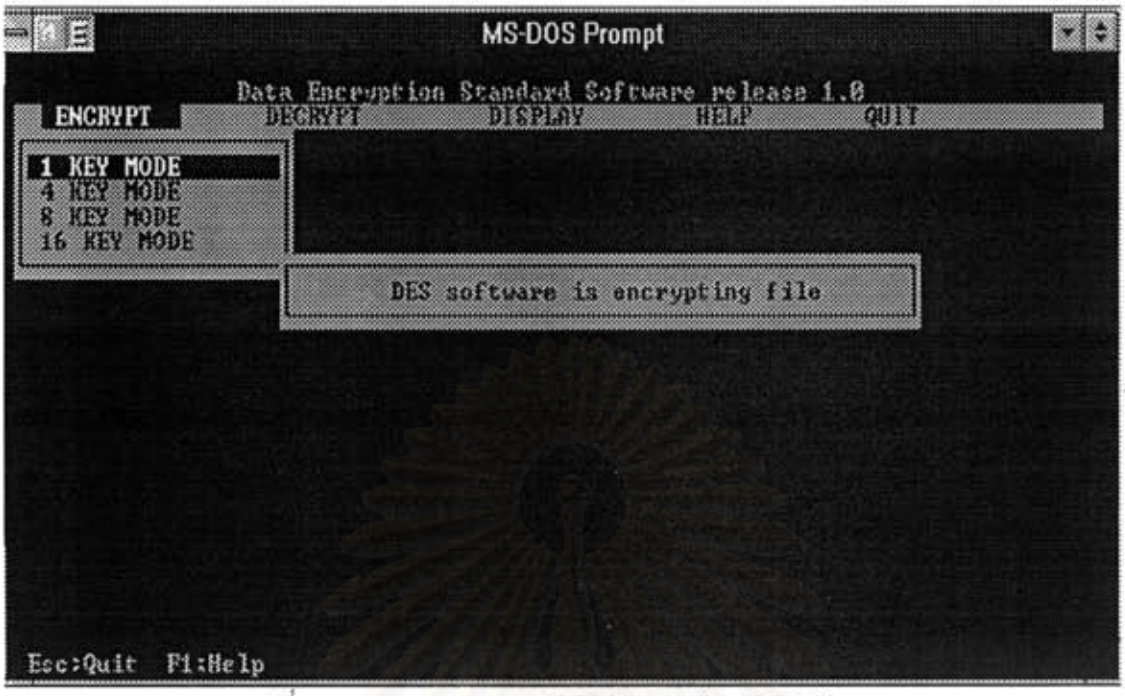
หลังจากผู้ใช้ป้อน key เสร็จแล้ว DES software ก็จะให้ผู้ใช้ใส่ชื่อแฟ้มของข้อมูลที่จะใช้เก็บข้อมูลที่เข้ารหัสลับแล้วดังในรูปที่ 3.12 ซึ่งจะเป็นชื่ออะไรก็ได้ที่ไม่ใช่ตัวว่างทั้งหมด (ถ้าใช่ก็จะมีข้อความเตือนดังในรูปที่ 3.6) และใช้หลักเดียวกับการตั้งชื่อแฟ้มข้อมูลใน DOS ซึ่งถ้าไม่ถูกตามหลักเกณฑ์ก็จะมีข้อความเตือนดังในรูปที่ 3.7 เนื่องจากไม่สามารถทำการเปิดแฟ้มข้อมูลได้ ชื่อแฟ้มข้อมูลที่ใช้เก็บข้อมูลที่เข้ารหัสแล้วนี้ DES software จะให้นามสกุลเป็น .DES โดยอัตโนมัติ



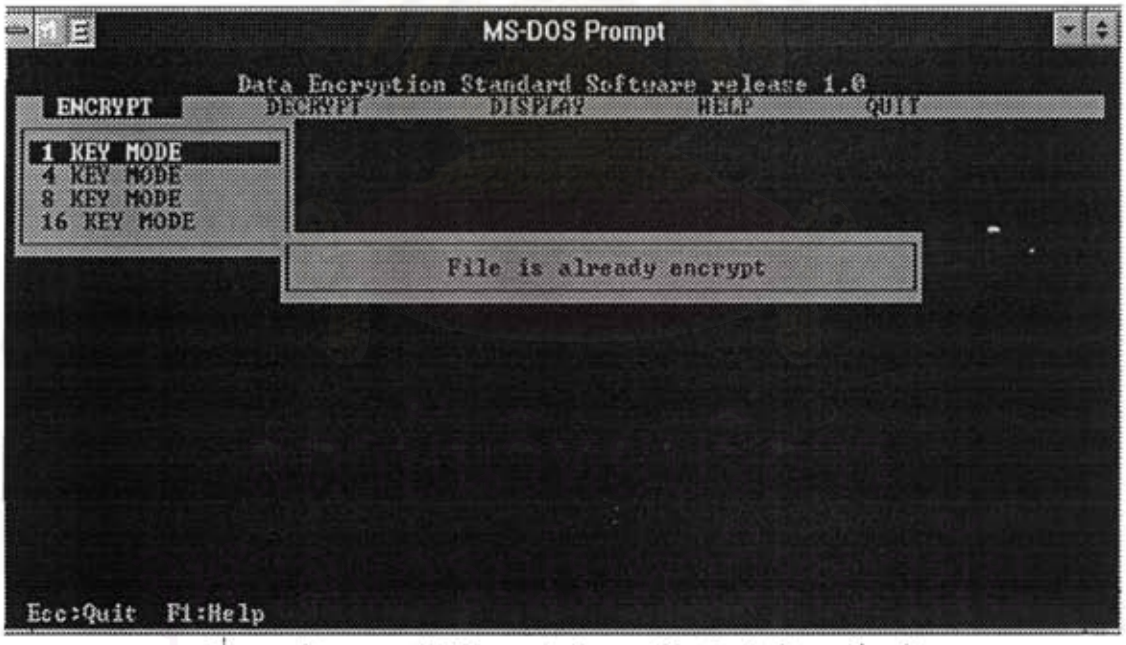
รูปที่ 3.12 แสดงหน้าจอสำหรับใส่ชื่อแฟ้มข้อมูลที่จะใช้สำหรับเก็บข้อมูลที่เข้ารหัสลับแล้ว

ถ้าผู้ใช้ต้องการออกจากการเข้ารหัสลับข้อมูล ก็สามารถทำได้เช่นเดียวกับในหน้าจอก่อนหน้านี้ และจะปรากฏข้อความดังในรูปที่ 3.9 เช่นกัน การกด N จะทำให้กลับเข้าสู่การใส่ชื่อแฟ้มข้อมูลอีกครั้ง

หลังจากนี้ DES software จะนำข้อมูลที่ผู้ใช้ต้องการมาทำการเข้ารหัสลับด้วย key ที่ผู้ใช้ได้กำหนดไว้ และเก็บข้อมูลไว้ในแฟ้มข้อมูลที่ผู้ใช้เลือกไว้ ซึ่งขณะที่ทำการเข้ารหัสลับข้อมูลก็จะปรากฏข้อความดังในรูปที่ 3.13 และเมื่อทำการเข้ารหัสลับเสร็จแล้ว ก็จะปรากฏข้อความแจ้งให้ผู้ใช้ทราบดังในรูปที่ 3.14 ซึ่งหลังจากนี้ผู้ใช้ก็จะกลับเข้าสู่เมนูหลัก



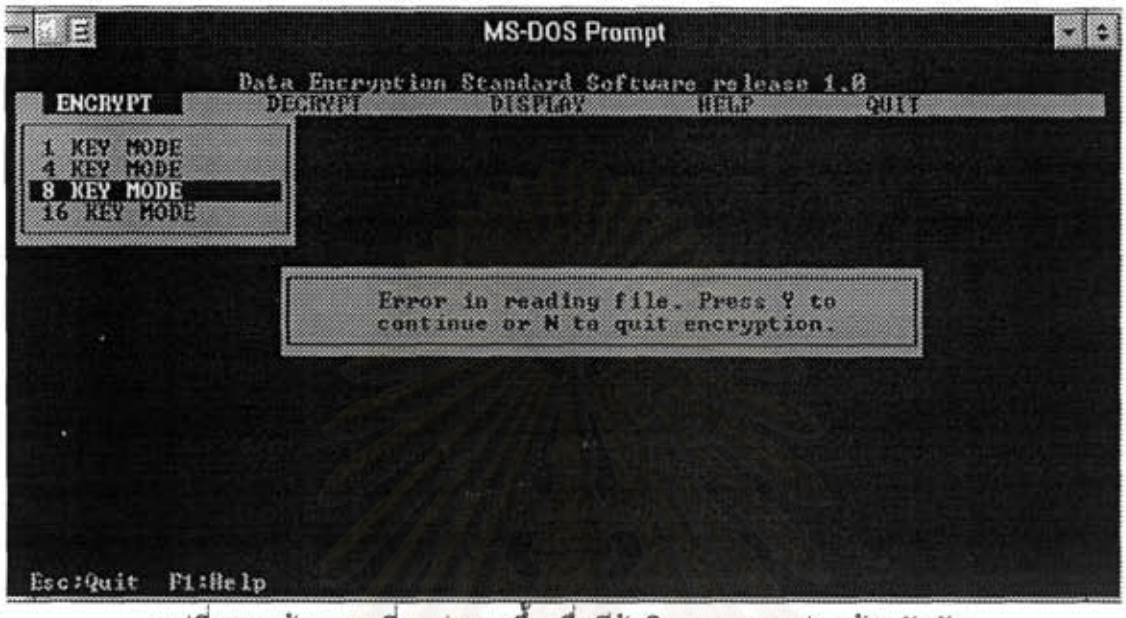
รูปที่ 3.13 DES software กำลังทำการเข้ารหัสลับข้อมูล



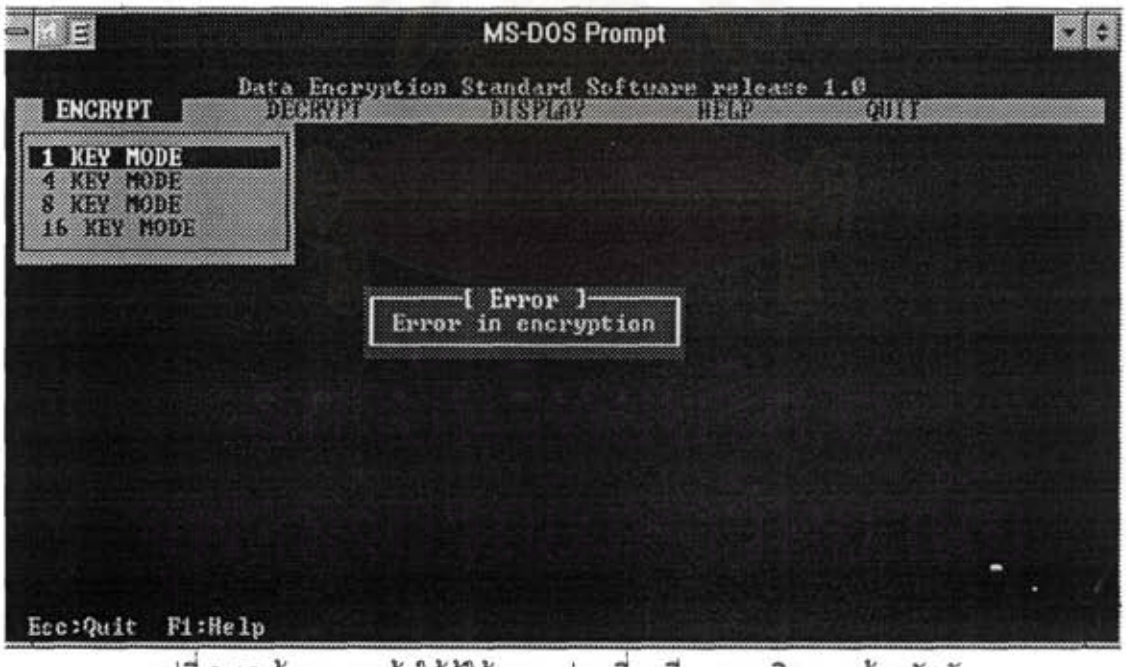
รูปที่ 3.14 ข้อความแจ้งให้ทราบว่าทำการเข้ารหัสลับข้อมูลเรียบร้อย

ในขณะทำการเข้ารหัสลับถ้ามีข้อผิดพลาดเกิดขึ้นเช่น ไม่สามารถอ่านข้อมูลจากแฟ้มข้อมูลได้ หรือไม่สามารถเขียนข้อมูลได้ จะปรากฏข้อความดังในรูปที่ 3.15 (ไม่สามารถอ่านข้อมูลได้) โดยจะมีการถามผู้ใช้ว่าต้องการจะยกเลิกการเข้ารหัสลับหรือไม่ ซึ่งถ้าผู้ใช้กด Y ก็จะเป็นการ

ยกเลิกการใช้โปรแกรมและจะปรากฏข้อความให้ผู้ใช้ทราบดังในรูปที่ 3.16 แต่ถ้าต้องการที่จะเข้ารหัสลับต่อ ก็ทำได้โดยการกด N โปรแกรมก็จะทำการเข้ารหัสลับต่อไป



รูปที่ 3.15 ข้อความที่จะปรากฏขึ้นเมื่อมีข้อผิดพลาดระหว่างเข้ารหัสลับ



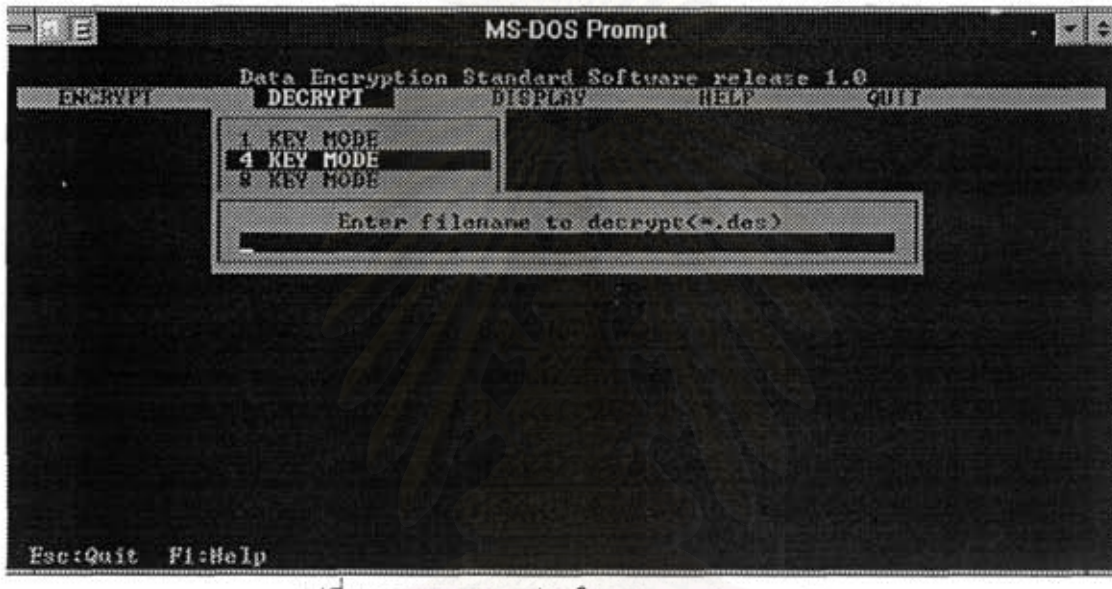
รูปที่ 3.16 ข้อความแจ้งให้ผู้ใช้ทราบก่อนที่จะมีการยกเลิกการเข้ารหัสลับ

แฟ้มข้อมูลของข้อมูลที่ทำการเข้ารหัสลับแล้ว ในบางครั้งอาจจะมีขนาดเพิ่มขึ้น และจะมีขนาดที่หารด้วยเลข 8 ลงตัว เนื่องมาจากในการเข้ารหัสลับ DES software จะทำการเข้ารหัสลับ

ข้อมูลครั้งละ 64 บิต หรือ 8 ไบต์ ข้อมูลที่ไม่ครบ 8 ไบต์ก็จะถูกเติมด้วยตัวว่างให้ครบแปด แล้วจึงทำการเข้ารหัสลับ จึงมีโอกาสที่แฟ้มข้อมูลจะมีขนาดเพิ่มขึ้นได้

3.2.2 การใช้ DES software ถอดรหัสลับ (Decryption mode)

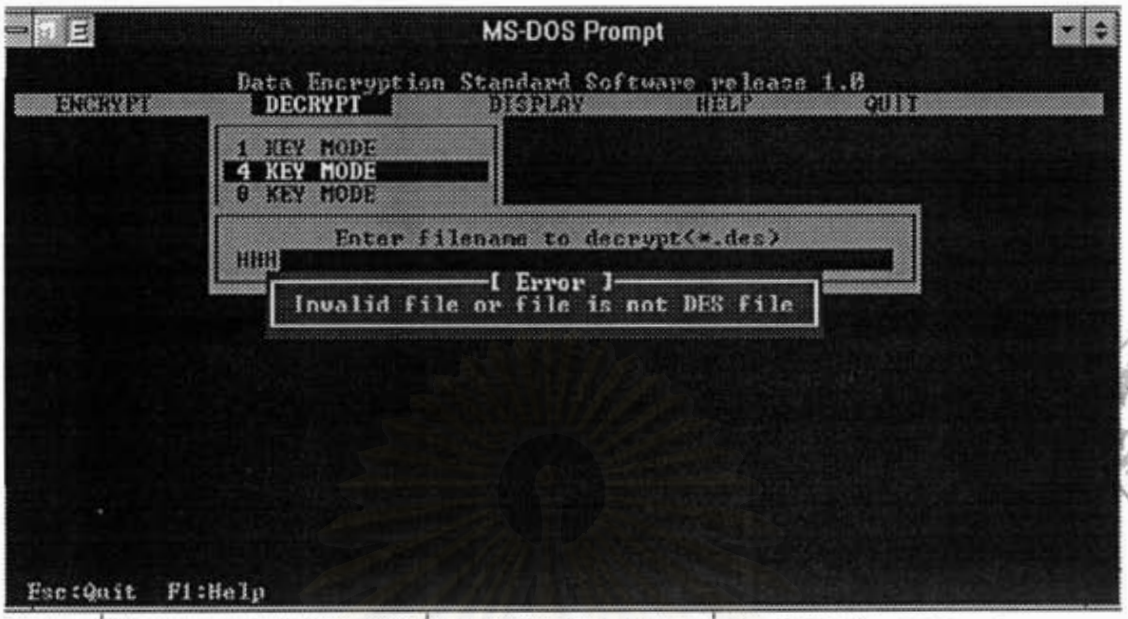
การใช้ DES software ในการถอดรหัสลับนั้นสามารถทำได้โดยการเลือกไปยังเมนู Decryption ในเมนูหลัก ซึ่งจะปรากฏเมนูย่อยขึ้นมาให้เลือกดังในรูปที่ 3.17



รูปที่ 3.17 แสดงเมนูย่อยใน Decryption mode

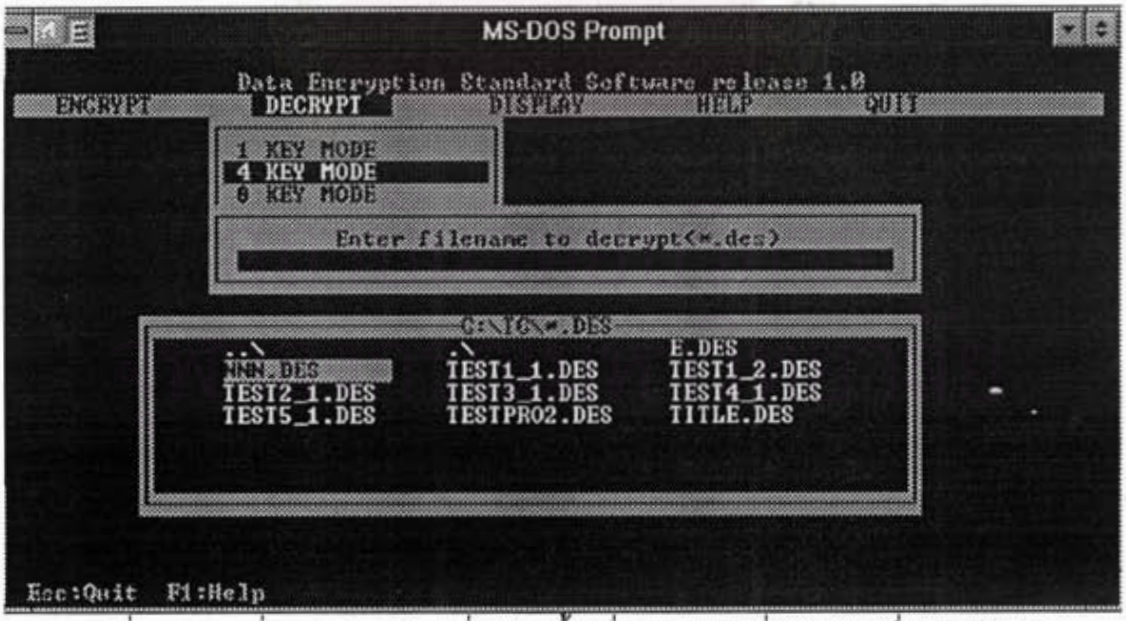
เมนูย่อยนี้จะเหมือนกับเมนูย่อยใน Encryption mode นั่นคือจะเป็นเมนูย่อยเกี่ยวกับ key mode หรือจำนวนของ key ที่จะใช้ในการถอดรหัสลับ ซึ่งจะต้องเลือกให้ตรงกับที่ใช้ในการเข้ารหัสลับข้อมูลนั้นๆ ถ้าไม่ตรงกันจะทำให้ไม่สามารถถอดรหัสลับข้อมูลได้ถูกต้อง ข้อมูลที่ได้ก็จะไม่เหมือนข้อมูลเดิม

หลังจากที่เลือก key mode แล้วก็จะเข้าสู่หน้าจอของการใส่ชื่อแฟ้มข้อมูลที่ผู้ใช้ต้องการถอดรหัสลับ ซึ่งจะต้องเป็นแฟ้มข้อมูลที่ผ่านการเข้ารหัสลับด้วย DES software เท่านั้น นั่นคือต้องมีนามสกุลของชื่อเป็น .DES ถ้าไม่ใช่จะมีข้อความเตือนดังในรูปที่ 3.18 หรือถ้าชื่อของแฟ้มข้อมูลเป็นตัวว่างทั้งหมดก็จะปรากฏข้อความดังในรูปที่ 3.6 และถ้าในการเปิดแฟ้มข้อมูลมีความผิดพลาดเกิดขึ้นก็จะมีข้อความเตือน ดังในรูปที่ 3.7



รูปที่ 3.18 แสดงข้อความเตือนเมื่อแฟ้มข้อมูลไม่ใช่ข้อมูลที่เข้ารหัสลับด้วย DES software

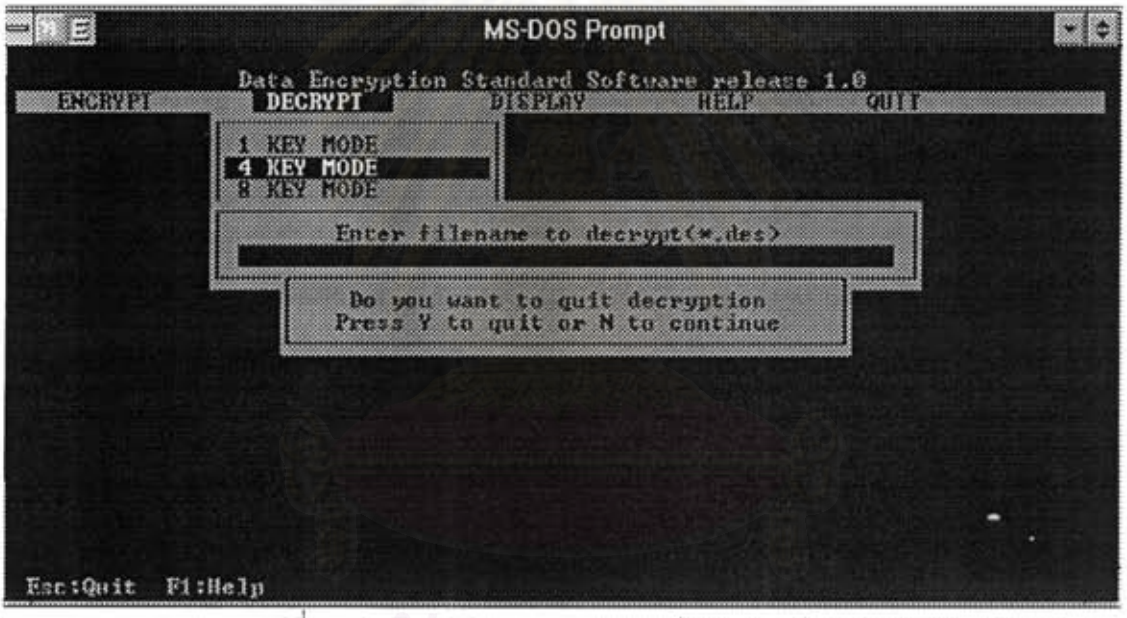
ถ้าผู้ใช้ต้องการทราบว่ามีแฟ้มข้อมูลอะไรบ้างที่เข้ารหัสลับด้วย DES software ใน directory นั้น ก็สามารถทำได้โดยการกด Enter จะปรากฏรายชื่อของแฟ้มข้อมูลออกมาดังในรูปที่ 3.19 ผู้ใช้สามารถเลือกแฟ้มข้อมูลมาจากรายชื่อเหล่านี้ แล้วกด Enter ซึ่งจะเหมือนกับการป้อนชื่อแฟ้มข้อมูลนั้นที่หน้าจอ



รูปที่ 3.19 รายชื่อของแฟ้มข้อมูลที่ปรากฏขึ้นเมื่อกด Enter ที่หน้าจอใส่ชื่อแฟ้มข้อมูล

ในระหว่างการใส่ชื่อแฟ้มข้อมูล ถ้าผู้ใช้ต้องการออกจากการถอดรหัสลับก็สามารถทำได้โดยการกดปุ่ม Esc ซึ่งจะปรากฏข้อความดังในรูปที่ 3.20 ผู้ใช้สามารถออกไปสู่เมนูหลักได้โดยการกดY แต่ถ้าต้องการถอดรหัสลับต่อจะสามารถทำได้โดยการกด N

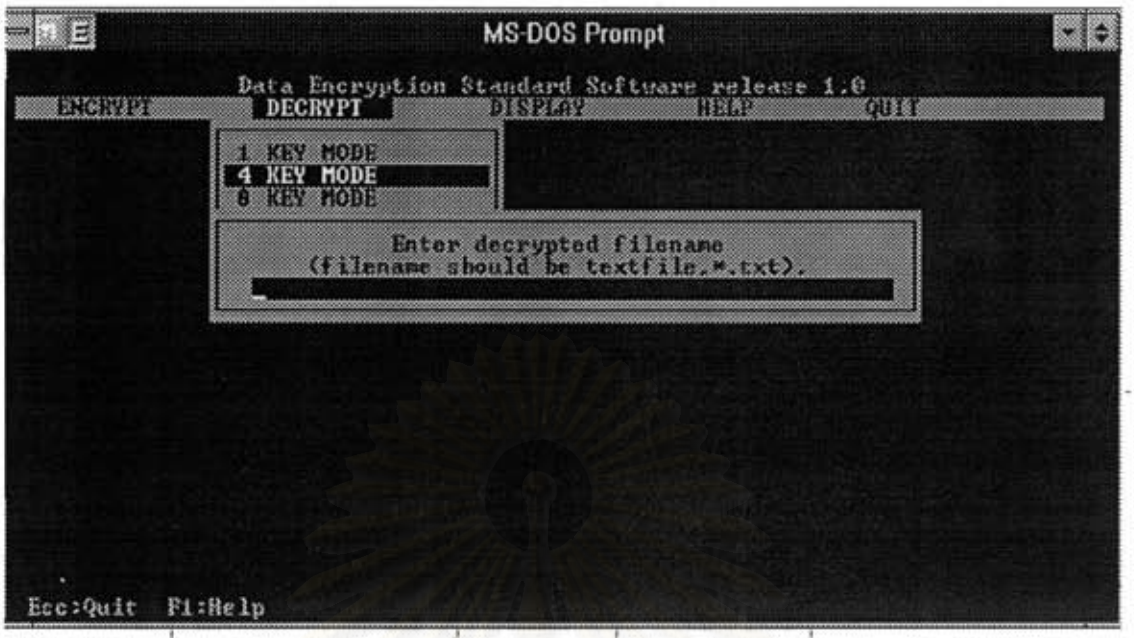
หลังจากที่ทำการใส่ชื่อแฟ้มข้อมูลที่ต้องการถอดรหัสลับแล้ว ก็จะเข้าสู่หน้าจอสำหรับใส่ key ที่ใช้ในการถอดรหัสลับ ซึ่ง key นี้จะต้องเป็น key ชุดเดียวกับที่ใช้ทำการเข้ารหัสลับ ซึ่งจะสามารถถอดรหัสลับได้ข้อมูลออกมาอย่างถูกต้อง ขั้นตอนในการป้อน key จะเหมือนกับขั้นตอนในการป้อน key ในการเข้ารหัสลับทุกประการ ส่วนการออกจากการถอดรหัสลับที่หน้าจอนี้ ก็สามารถทำได้โดยการกด Esc แล้วกดปุ่ม Y เมื่อมีข้อความดังในรูปที่ 3.20 การ กด N จะทำให้กลับเข้าสู่การป้อน key อีกครั้งหนึ่ง



รูปที่ 3.20 การกดปุ่ม Esc จะปรากฏข้อความดังในรูป

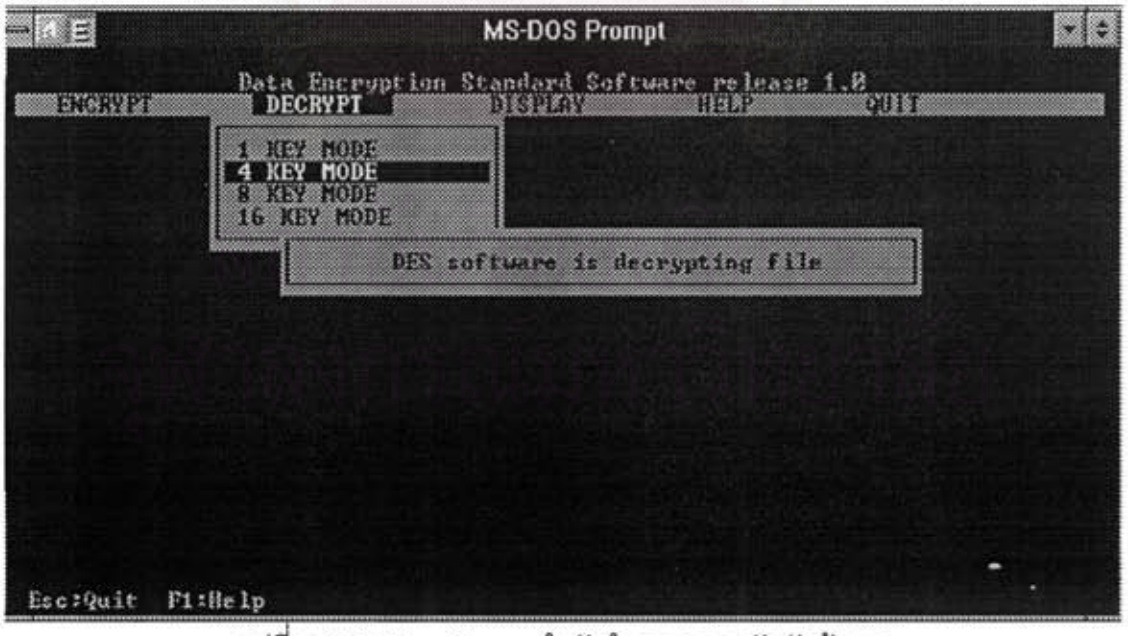
เมื่อป้อน key เสร็จแล้ว DES software จะให้ผู้ใช้ทำการใส่ชื่อแฟ้มข้อมูลที่จะใช้เก็บข้อมูลที่ทำการถอดรหัสลับแล้วดังในรูปที่ 3.21 ชื่อแฟ้มข้อมูลนี้จะต้องไม่เป็นตัวว่างทั้งหมด (ถ้าใช่ก็จะมีข้อความเตือนดังในรูปที่ 3.6) และต้องเป็นไปตามหลักเกณฑ์การตั้งชื่อใน DOS ซึ่งถ้าไม่เป็นไปตามหลักเกณฑ์ก็จะทำให้ไม่สามารถเปิดแฟ้มข้อมูลนั้นได้ และจะปรากฏข้อความเตือนดังในรูปที่ 3.7

ที่หน้าจอนี้การออกจากโปรแกรมสามารถทำได้เหมือนกับในหน้าจอที่ผ่านมา การกด N จะทำให้กลับเข้าสู่การใส่ชื่ออีกครั้งหนึ่ง

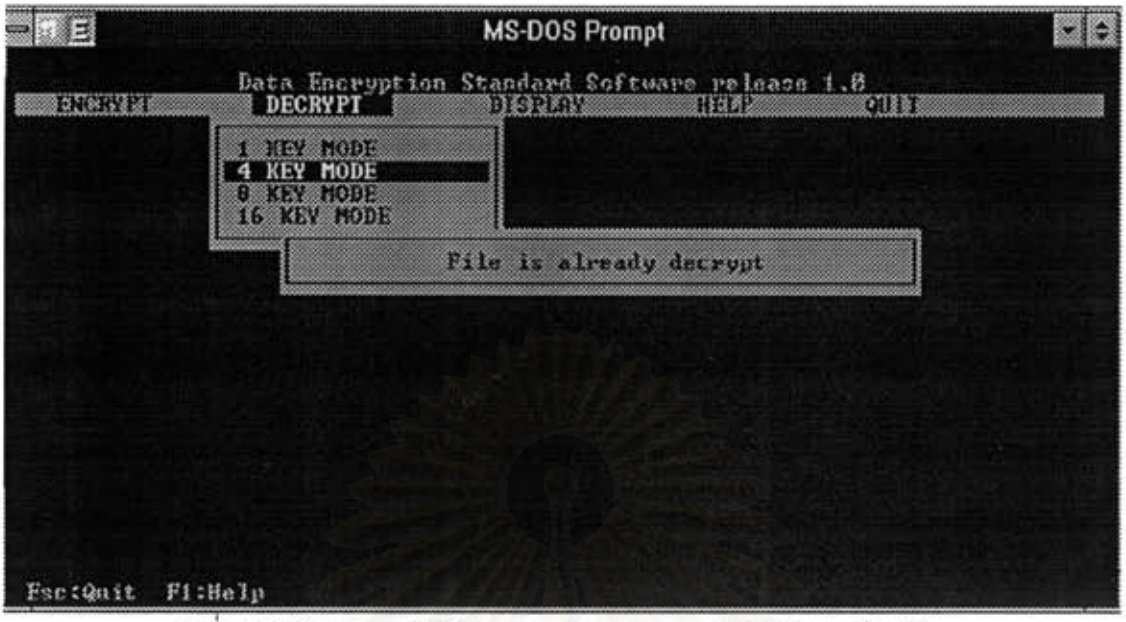


รูปที่ 3.21 หน้าจอสำหรับใส่ชื่อแฟ้มข้อมูลที่จะใช้เก็บข้อมูลที่ถอดรหัสลับแล้ว

หลังจากนี้ DES software จะทำการถอดรหัสลับข้อมูลที่ผู้ใช้ต้องการ ด้วย key ที่ผู้ใช้ป้อนไว้ และเก็บข้อมูลที่ถอดรหัสลับแล้วไว้ในแฟ้มข้อมูลที่ผู้ใช้เลือกไว้ ในขณะที่ DES software ทำการถอดรหัสลับจะปรากฏข้อความที่หน้าจอดังในรูปที่ 3.22 เมื่อทำการถอดรหัสลับเสร็จแล้วจะปรากฏข้อความแจ้งให้ผู้ใช้ทราบดังในรูปที่ 3.23

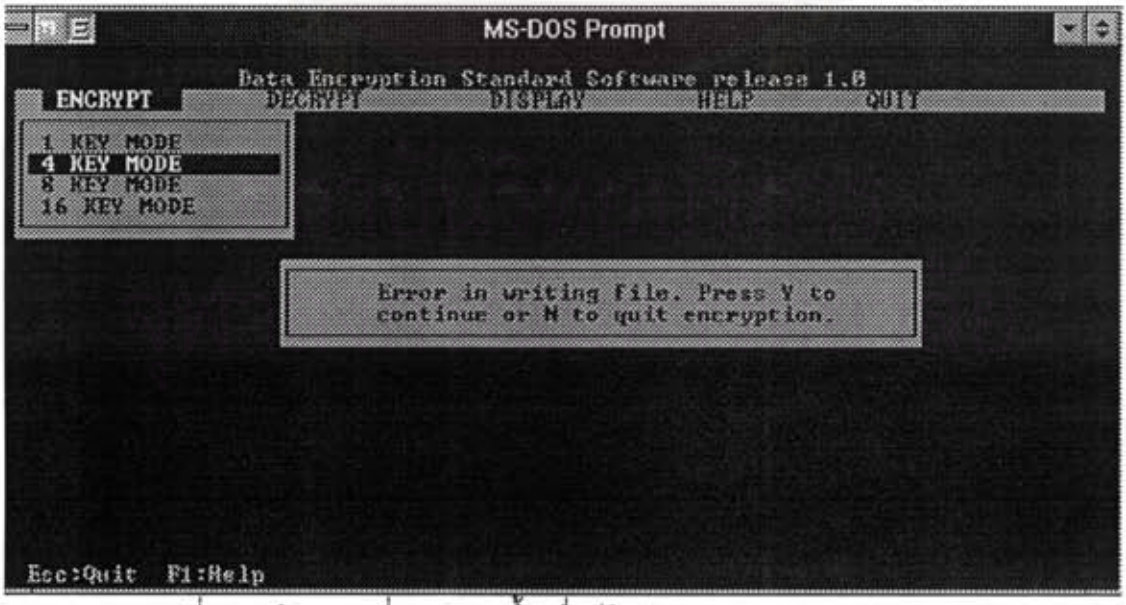


รูปที่ 3.22 DES software กำลังทำการถอดรหัสลับข้อมูล

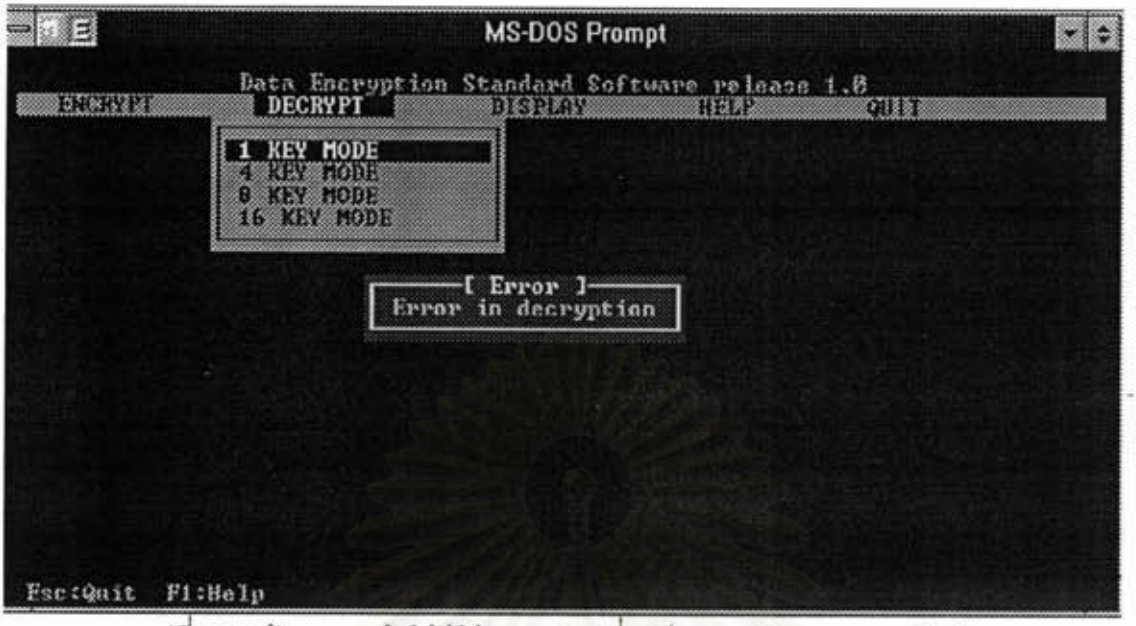


รูปที่ 3.23 ข้อความแจ้งให้ทราบว่าทำการถอดรหัสลับข้อมูลเรียบร้อย

ในระหว่างที่ทำการถอดรหัสลับข้อมูลอยู่นั้น ถ้ามีข้อผิดพลาดเกิดขึ้นเช่น ไม่สามารถอ่านข้อมูลจากแฟ้มข้อมูลได้ หรือไม่สามารถเขียนข้อมูลได้ จะปรากฏข้อความดังในรูปที่ 3.24 (ไม่สามารถเขียนข้อมูลได้) โดยจะมีการถามผู้ใช้ว่าต้องการจะยกเลิกการถอดรหัสลับหรือไม่ ซึ่งถ้าผู้ใช้กด Y ก็จะเป็นการยกเลิกการใช้โปรแกรมและจะ ปรากฏข้อความให้ผู้ใช้ทราบดังในรูปที่ 3.25 แต่ถ้าต้องการที่จะถอดรหัสลับต่อ ก็ทำได้โดยการกด N โปรแกรมก็จะทำการถอดรหัสลับต่อไป



รูปที่ 3.24 ข้อความที่จะปรากฏขึ้นเมื่อมีข้อผิดพลาดระหว่างถอดรหัสลับ



รูปที่ 3.25 ข้อความแจ้งให้ผู้ใช้ทราบก่อนที่จะมีการยกเลิกการถอดรหัสลับ

หลังจากนี้ก็จะกลับเข้าสู่เมนูหลักอีกครั้ง เป็นการสิ้นสุด Decryption mode

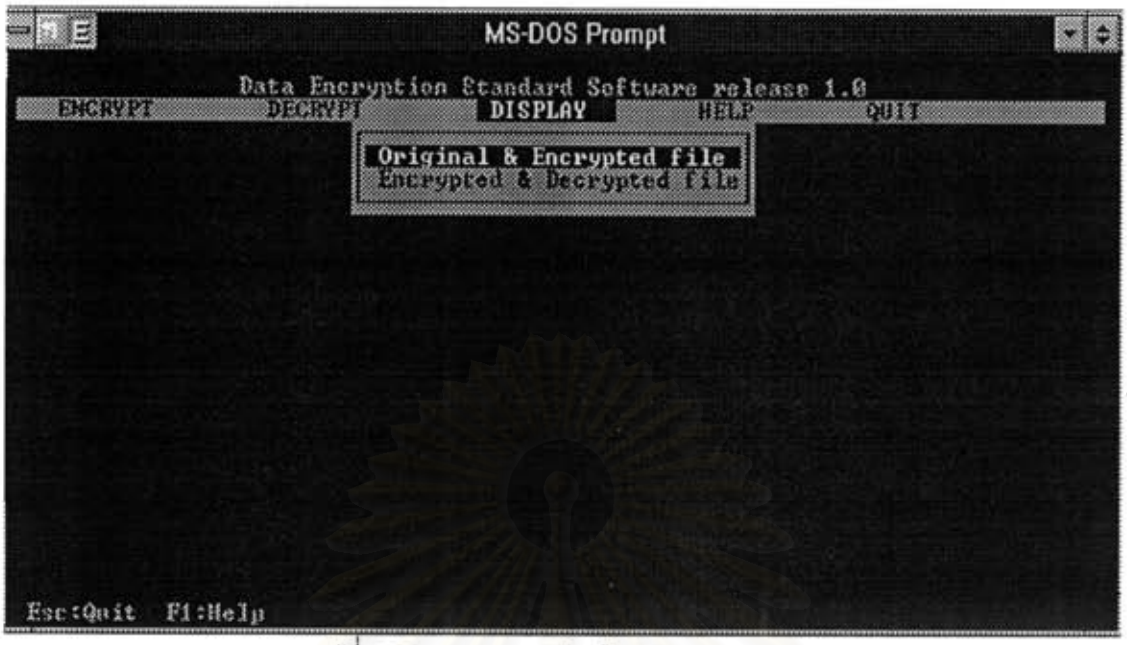
3.2.3 การแสดงข้อมูลเปรียบเทียบบนหน้าจอ (Display mode)

ใน DES software นั้น ผู้ใช้สามารถแสดงข้อมูลที่ยังไม่ได้เข้ารหัสลับ กับที่ผ่านการเข้ารหัสลับแล้วเปรียบเทียบกัน เพื่อให้ผู้ใช้สามารถดูผลของการเข้ารหัสลับด้วย key ที่ผู้ใช้กำหนดว่ามีความปลอดภัยตรงตามที่ต้องการหรือไม่ ทำให้ผู้ใช้สามารถเลือก key ให้ใช้ได้ผลตามต้องการได้ นอกจากนี้ยังสามารถแสดงข้อมูลที่ยังไม่ได้ถอดรหัสลับ เปรียบเทียบกับที่ทำการถอดรหัสลับแล้วว่า สามารถถอดรหัสลับมาได้เป็นอย่างไร

ผู้ใช้สามารถเลือกใช้ mode นี้ได้โดยเลือกที่เมนู Display ซึ่งจะปรากฏเมนูย่อยให้ผู้ใช้เลือก 2 อย่าง คือ

1. Original & Encrypted file
2. Encrypted & Decrypted file

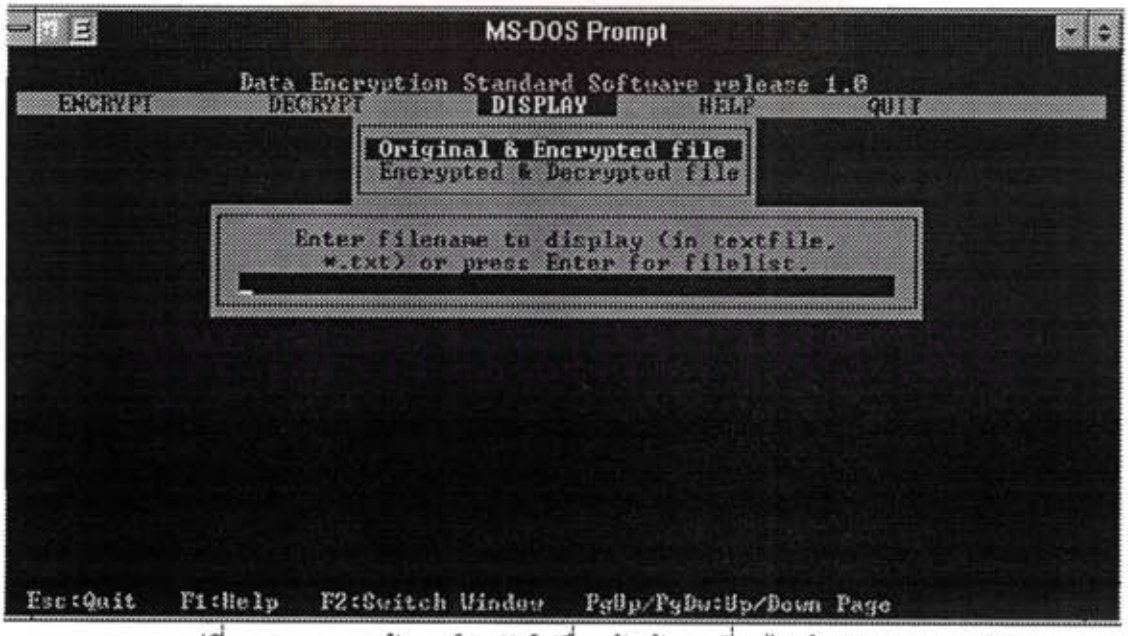
ดังในรูปที่ 3.26



รูปที่ 3.26 แสดงเมนูย่อยใน Display mode

3.2.3.1 Original & Encrypted file

เมนูย่อยนี้ใช้สำหรับแสดงข้อมูลที่ยังไม่ได้เข้ารหัสลับ เปรียบเทียบกับข้อมูลที่เข้ารหัสลับแล้ว เมื่อผู้ใช้เลือกเมนูนี้ก็จะเข้าสู่หน้าจอสำหรับใส่ชื่อแฟ้มข้อมูลที่ต้องการจะแสดง โดยเริ่มจากแฟ้มข้อมูลที่ยังไม่ได้เข้ารหัสลับก่อนดังในรูปที่ 3.27



รูปที่ 3.27 แสดงหน้าจอสำหรับใส่ชื่อแฟ้มข้อมูลที่ยังไม่เข้ารหัสลับ

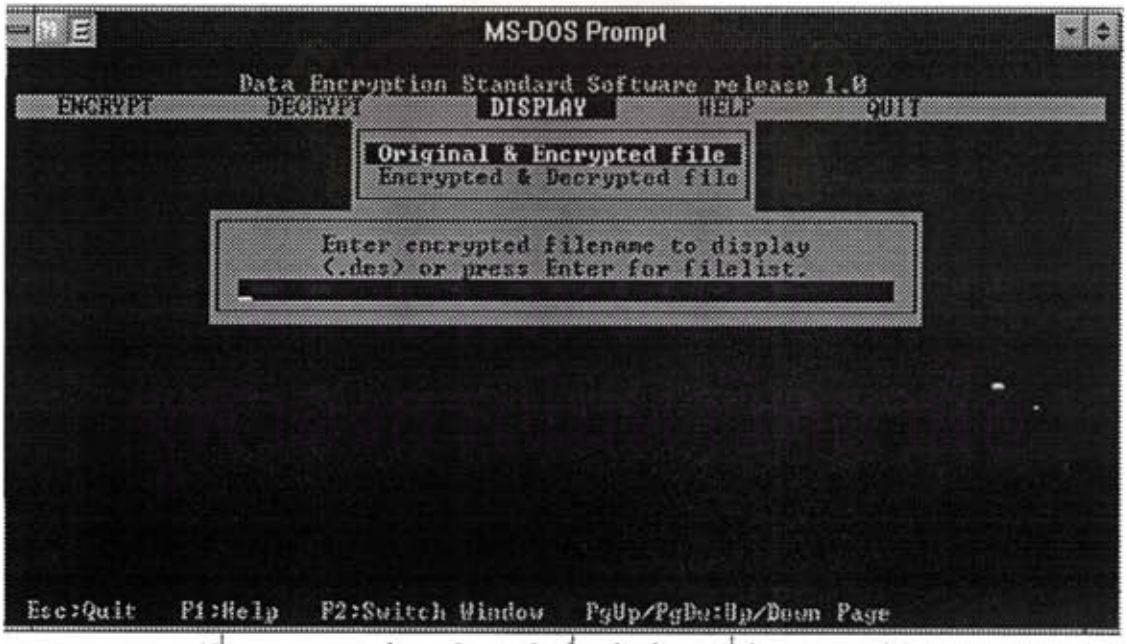
แฟ้มข้อมูลที่ยังไม่ได้เข้ารหัสลับจะต้องเป็น textfile และชื่อจะต้องไม่เป็นตัวว่าง ซึ่งถ้าไม่ใช่ textfile หรือเป็นตัวว่าง จะมีข้อความเตือนปรากฏบนหน้าจอดังในรูปที่ 3.5 และ 3.6 ตามลำดับ และถ้ามีข้อผิดพลาดเช่น ชื่อแฟ้มข้อมูลไม่ตรงตามเกณฑ์การตั้งชื่อของ DOS ทำให้ไม่สามารถทำการเปิดแฟ้มข้อมูลได้จะมีข้อความเตือนดังในรูปที่ 3.7 นอกจากนี้ผู้ใช้ยังสามารถเลือกชื่อแฟ้มข้อมูลจากรายชื่อได้ โดยการกดปุ่ม Enter ที่หน้าจอใส่ชื่อแฟ้มข้อมูลซึ่งจะปรากฏรายชื่อดังในรูปที่ 3.28

รูปที่ 3.28 รายชื่อแฟ้มข้อมูลที่ผู้ใช้สามารถเลือกได้จากหน้าจอนี้

การออกจาก Display mode ที่หน้าจอนี้สามารถทำได้โดยการกดปุ่ม Esc ซึ่งจะปรากฏข้อความดังในรูปที่ 3.29 ถ้าผู้ใช้ต้องการออกจาก mode นี้กลับไปสู่เมนูหลัก ก็สามารถทำได้โดยการกดปุ่ม Y แต่ถ้าไม่ต้องการออกจาก mode นี้ ก็ให้กดปุ่ม N ก็จะกลับเข้าสู่การใส่ชื่ออีกครั้งหนึ่ง

รูปที่ 3.29 เมื่อกดปุ่ม Esc ก็จะปรากฏข้อความนี้ขึ้น

หลังจากที่ใส่ชื่อแฟ้มข้อมูลที่ยังไม่เข้ารหัสลับแล้ว ก็จะเข้าสู่หน้าจอสำหรับใส่ชื่อแฟ้มข้อมูลที่เข้ารหัสลับแล้วดังในรูปที่ 3.30



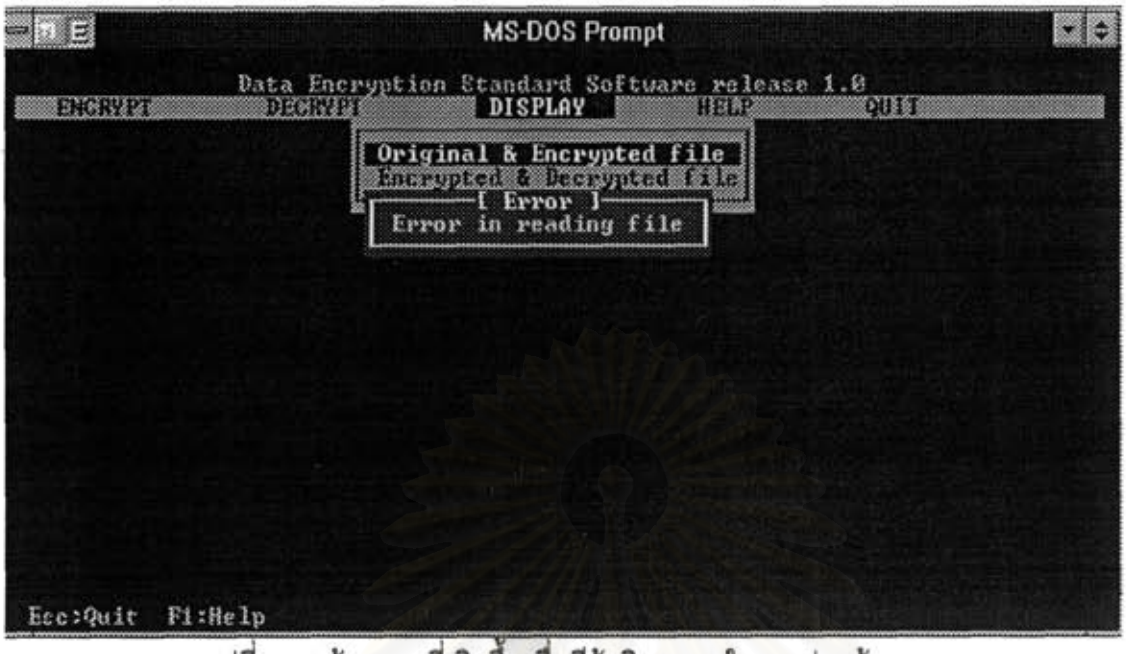
รูปที่ 3.30 แสดงหน้าจอสำหรับใส่ชื่อแฟ้มข้อมูลที่เข้ารหัสลับแล้ว

แฟ้มข้อมูลนี้จะต้องเป็นข้อมูลที่เข้ารหัสลับด้วย DES software เท่านั้น นั่นคือต้องมีนามสกุลเป็น .DES และจะต้องไม่เป็นตัวว่าง ซึ่งถ้าไม่ได้เข้ารหัสลับด้วย DES software หรือชื่อเป็นตัวว่างทั้งหมด จะมีข้อความเตือนปรากฏบนหน้าจอดังในรูปที่ 3.5 และ 3.6 ตามลำดับ และถ้ามีข้อผิดพลาดเช่น ชื่อแฟ้มข้อมูลไม่ตรงตามเกณฑ์การตั้งชื่อของ DOS ทำให้ไม่สามารถทำการเปิดแฟ้มข้อมูลได้จะมีข้อความเตือนดังในรูปที่ 3.7 นอกจากนี้ผู้ใช้ยังสามารถเลือกชื่อแฟ้มข้อมูลจากรายชื่อได้ โดยการกดปุ่ม Enter ที่หน้าจอใส่ชื่อแฟ้มข้อมูลซึ่งจะปรากฏรายชื่อดังในรูปที่ 3.31

รูปที่ 3.31รายชื่อของแฟ้มข้อมูลที่ปรากฏขึ้นเมื่อกด Enter ที่หน้าจอใส่ชื่อแฟ้มข้อมูล

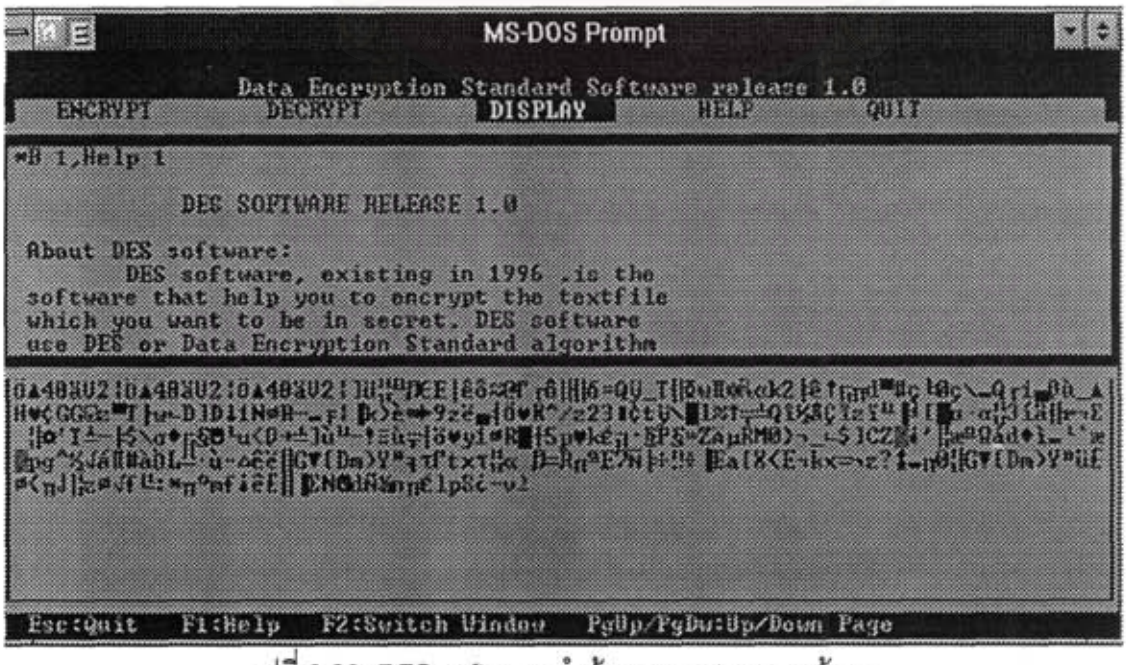
ในการออกจาก Display mode ที่หน้าจอนี้สามารถทำได้เช่นเดียวกับที่หน้าจอก่อนหน้านี้ โดยการกดปุ่ม Esc แล้วกด Y การกด N จะทำให้กลับเข้าสู่การใส่ชื่อคืน

หลังจากนี้ DES software จะจัดการนำแฟ้มข้อมูลที่ผู้ใช้ต้องการมาแสดง ซึ่งถ้ามีข้อผิดพลาดเกิดขึ้นในการอ่านข้อมูล ก็จะปรากฏข้อความเตือนดังในรูปที่ 3.32



รูปที่ 3.32 ข้อความที่เกิดขึ้นเมื่อมีข้อผิดพลาดในการอ่านข้อมูล

เมื่อข้อมูลถูกนำมาแสดงจะปรากฏเป็นหน้าจอดังในรูปที่ 3.33 ซึ่งในหน้าต่างบนจะเป็นข้อมูลที่ยังไม่ได้เข้ารหัสลับ และในหน้าต่างล่างจะเข้ารหัสลับแล้ว การดูข้อมูลในหน้าถัดไปหรือก่อนหน้านี้สามารถทำได้โดยใช้ปุ่ม PgUp และ PgDw และผู้ใช้สามารถย้ายจากหน้าต่างหนึ่งไปยังอีกหน้าต่างหนึ่งได้โดยการกดปุ่ม F2

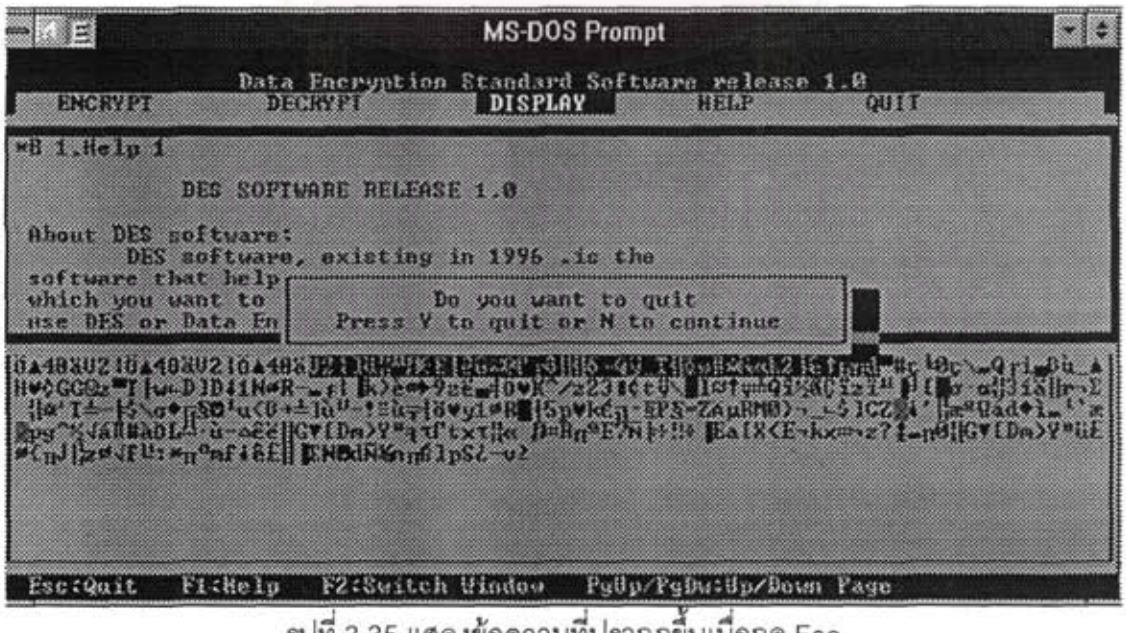


รูปที่ 3.33 DES software นำข้อมูลมาแสดงบนหน้าจอ

ข้อจำกัดของการแสดงข้อมูลใน DES software คือ จะไม่สามารถแก้ไขข้อมูลได้เหมือนในโปรแกรม edit text อื่นๆ นอกจากนี้ถ้าข้อมูลที่นำมาแสดงมีขนาดใหญ่เกินไป (ใหญ่กว่า 7,000ไบต์) ก็จะไม่สามารถทำการแสดงได้ โดยจะปรากฏข้อความขึ้นดังในรูปที่ 3.34

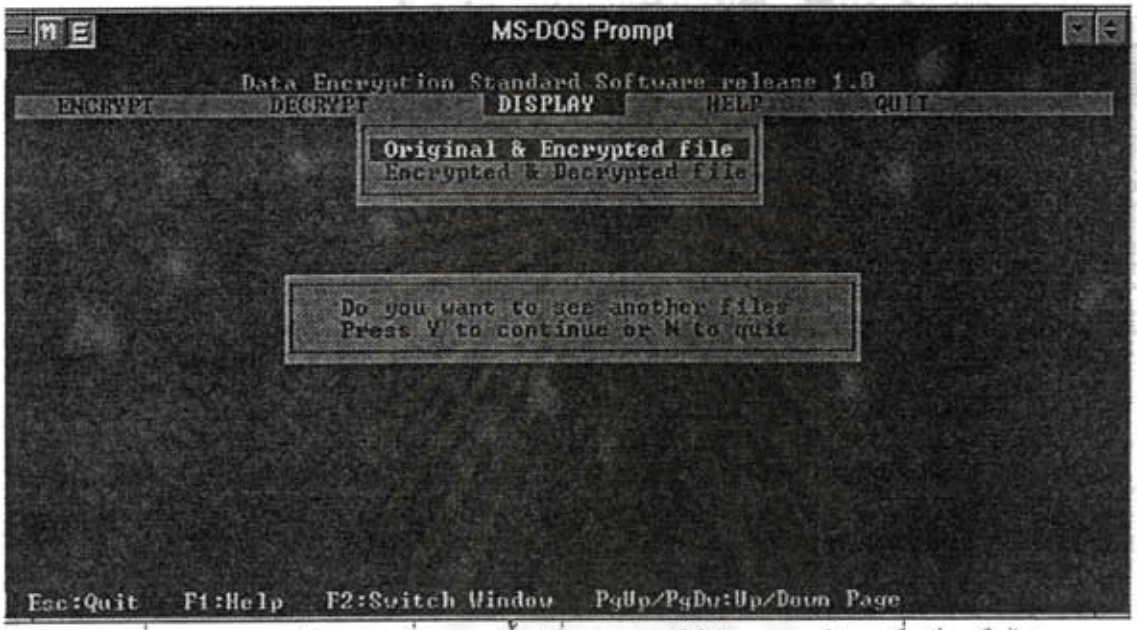
รูปที่ 3.34 แสดงข้อความที่ปรากฏเมื่อไม่สามารถแสดงข้อมูลที่มีขนาดใหญ่เกินไป

เมื่อผู้ใช้ต้องการออกจากการแสดงข้อมูลก็จะสามารถทำได้โดยการกดปุ่ม Esc จะปรากฏข้อความดังในรูปที่ 3.35



รูปที่ 3.35 แสดงข้อความที่ปรากฏขึ้นเมื่อกด Esc

ถ้าผู้ใช้กด N ก็จะกลับเข้าสู่การแสดงข้อมูลคืน แต่ถ้ากด Y จะเป็นการออกจากการแสดงข้อมูลโดยข้อมูลจะหายไป และจะปรากฏข้อความถามว่าต้องการดูข้อมูลอื่นเพิ่มเติมอีกหรือเปล่า ดังในรูปที่ 3.36 ซึ่งถ้าผู้ใช้กด Y ก็จะกลับไปเริ่มต้นการใส่ชื่อข้อมูลที่ต้องการแสดงใหม่อีกครั้ง แต่ถ้าผู้ใช้กด N ก็จะออกจาก Display mode ไปยังเมนูหลัก

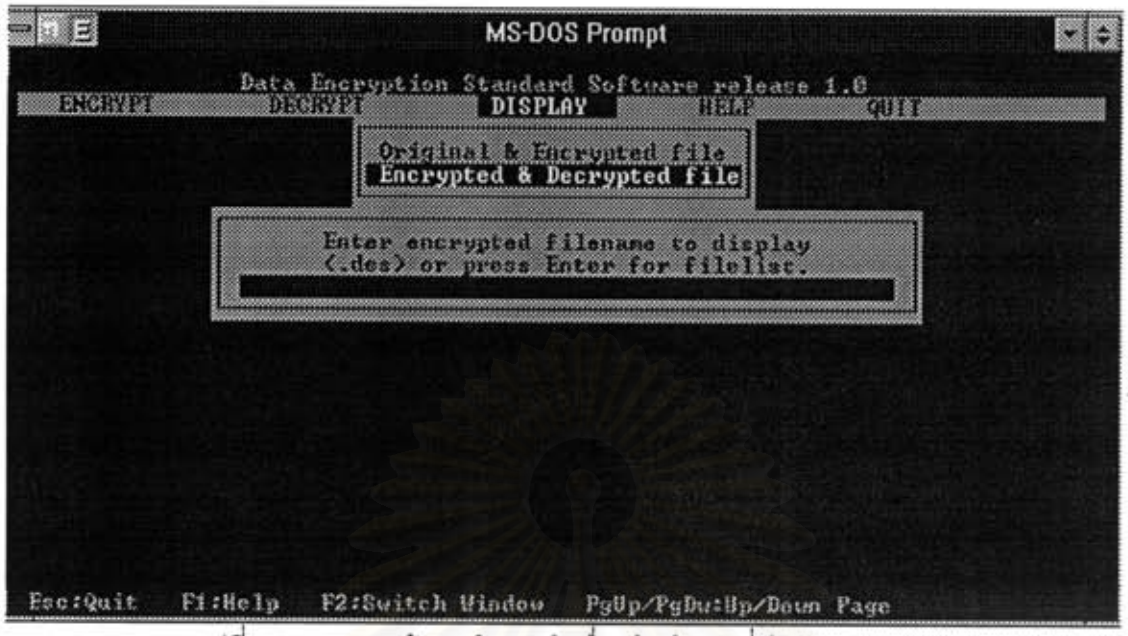


รูปที่ 3.36 แสดงข้อความที่ปรากฏขึ้นเพื่อถามว่าผู้ใช้ต้องการดูข้อมูลอื่นอีกหรือไม่

3.2.3.2 Encrypted & Decrypted file

เมนูย่อยนี้ใช้สำหรับแสดงข้อมูลที่ผ่านการเข้ารหัสลับด้วย DES software เปรียบเทียบกับข้อมูลที่ถอดรหัสลับแล้ว เมื่อผู้ใช้เลือกเมนูนี้ก็จะเข้าสู่หน้าจอสำหรับใส่ชื่อแฟ้มข้อมูลที่ต้องการจะแสดง โดยเริ่มจากแฟ้มข้อมูลที่เข้ารหัสลับแล้วก่อนดังในรูปที่ 3.37

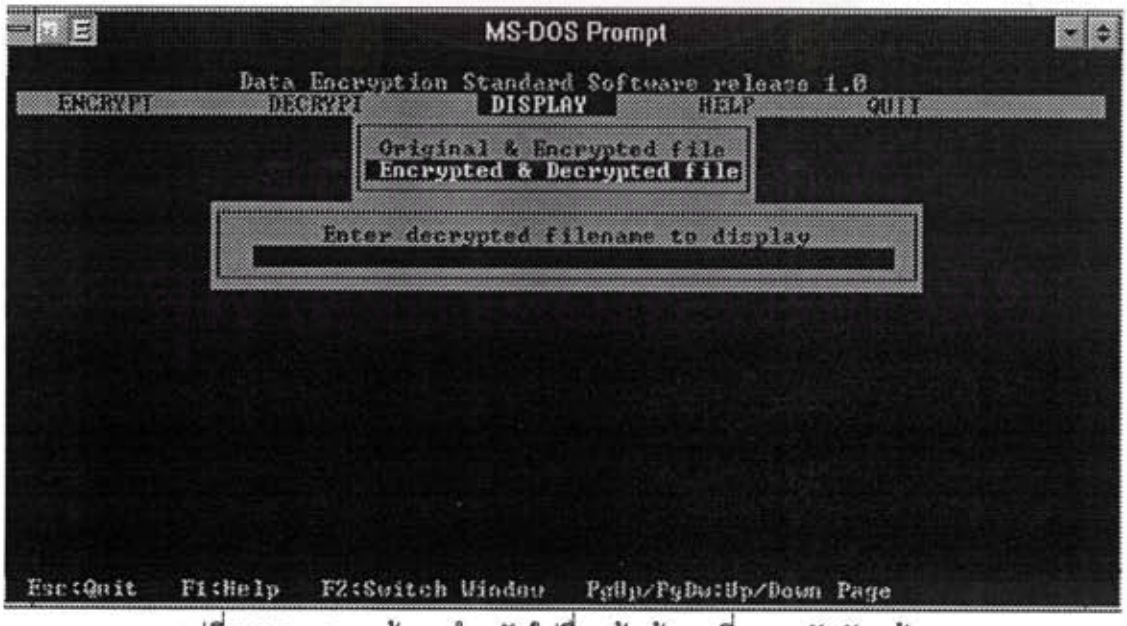
การใส่ชื่อแฟ้มข้อมูลที่เข้ารหัสลับแล้วนี้ จะเหมือนกับในเมนูย่อย Original & Encrypted file กล่าวคือ ชื่อแฟ้มข้อมูลจะต้องไม่เป็นตัวว่างและมีนามสกุลเป็น .DES ซึ่งถ้าไม่ใช่ ตามที่กล่าวมา จะมีข้อความเตือนปรากฏบนหน้าจอดังในรูปที่ 3.6 และ 3.18 ตามลำดับ และถ้ามีข้อผิดพลาดเช่น ชื่อแฟ้มข้อมูลไม่ตรงตามเกณฑ์การตั้งชื่อของ DOS ทำให้ไม่สามารถทำการเปิดแฟ้มข้อมูลได้จะมีข้อความเตือนดังในรูปที่ 3.7 ผู้ใช้ยังสามารถเลือกชื่อแฟ้มข้อมูลจากรายชื่อได้ เช่นเดียวกัน โดยการกดปุ่ม Enter ที่หน้าจอใส่ชื่อแฟ้มข้อมูลซึ่งจะปรากฏรายชื่อดังในรูปที่ 3.28



รูปที่ 3.27 แสดงหน้าจอสำหรับใส่ชื่อแฟ้มข้อมูลที่เข้ารหัสลับแล้ว

การออกจาก Display mode ที่หน้าจอนี้สามารถทำได้เช่นเดียวกับที่ผ่านมา คือโดยการกดปุ่ม Esc ซึ่งจะปรากฏข้อความดังในรูปที่ 3.29 การกดปุ่ม Y จะเป็นการออกจาก mode นี้กลับไปสู่เมนูหลัก ส่วนการกดปุ่ม N จะเป็นการกลับเข้าสู่การใส่ชื่ออีกครั้งหนึ่ง

หลังจากที่ใส่ชื่อแฟ้มข้อมูลที่เข้ารหัสลับเรียบร้อยแล้ว ก็จะเข้าสู่หน้าจอสำหรับใส่ชื่อแฟ้มข้อมูลที่ถอดรหัสลับแล้วดังในรูปที่ 3.38



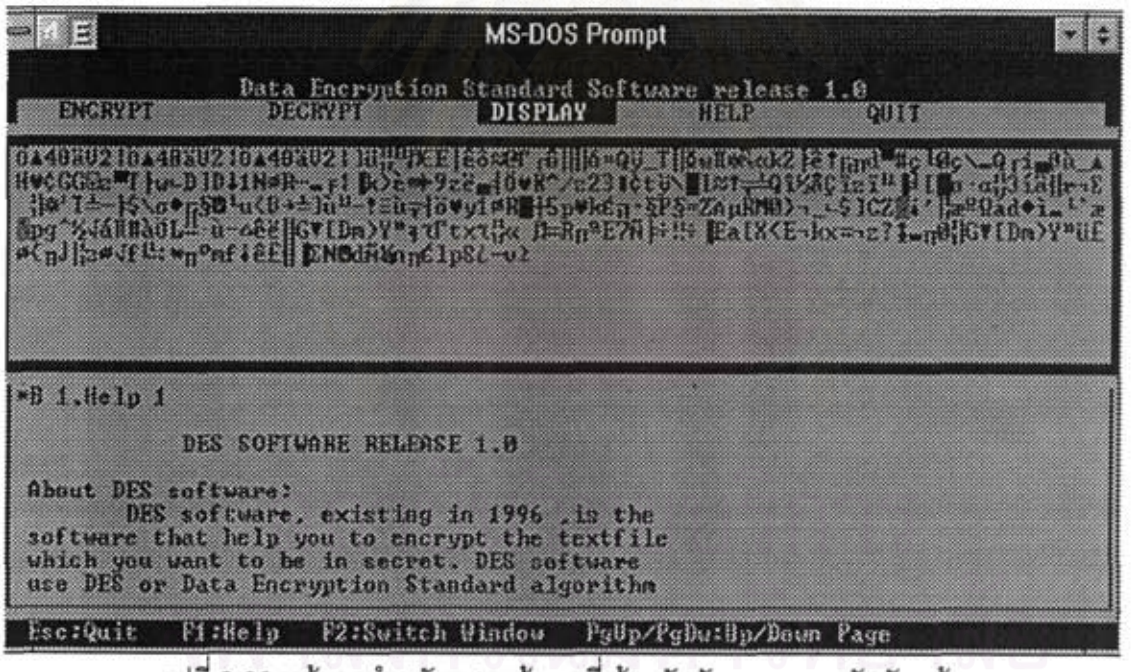
รูปที่ 3.38 แสดงหน้าจอสำหรับใส่ชื่อแฟ้มข้อมูลที่ถอดรหัสลับแล้ว

การใส่ชื่อแฟ้มข้อมูลนี้จะต้องไม่เป็นตัวว่าง (ถ้าชื่อเป็นตัวว่างทั้งหมด จะมีข้อความเตือนปรากฏบนหน้าจอดังในรูปที่ 3.6) ถ้ามีข้อผิดพลาดเช่น ชื่อแฟ้มข้อมูลไม่ตรงตามเกณฑ์การตั้งชื่อของ DOS ทำให้ไม่สามารถทำการเปิดแฟ้มข้อมูลได้จะมีข้อความเตือนดังในรูปที่ 3.7 แต่ในหน้าจอนี้ จะไม่มีหน้าจอสำหรับเลือกชื่อแฟ้มข้อมูลจากรายชื่อเหมือนกับในหน้าจอที่ผ่านมา

ในการออกจาก Display mode ที่หน้าจอนี้ สามารถทำได้เช่นเดียวกับที่หน้าจอก่อนหน้านี้ โดยการกดปุ่ม Esc แล้วกด Y การกด N จะทำให้กลับเข้าสู่การใส่ชื่อคืน

หลังจากที่ป้อนชื่อเสร็จแล้ว DES software จะจัดการนำแฟ้มข้อมูลที่ผู้ใช้ต้องการมาแสดง ซึ่งถ้ามีข้อผิดพลาดเกิดขึ้นในการอ่านข้อมูล ก็จะปรากฏข้อความเตือนดังในรูปที่ 3.32

เมื่อข้อมูลถูกนำมาแสดงจะปรากฏเป็นหน้าจอดังในรูปที่ 3.39 ซึ่งในหน้าต่างบนจะแสดงข้อมูลที่เข้ารหัสลับแล้ว และในหน้าต่างล่างจะแสดงข้อมูลที่ถอดรหัสลับแล้ว การดูข้อมูลในหน้าถัดไปหรือก่อนหน้านี้สามารถทำได้โดยใช้ปุ่ม PgUp และ PgDw และผู้ใช้สามารถย้ายจากหน้าต่างหนึ่งไปยังอีกหน้าต่างหนึ่งได้โดยการกดปุ่ม F2



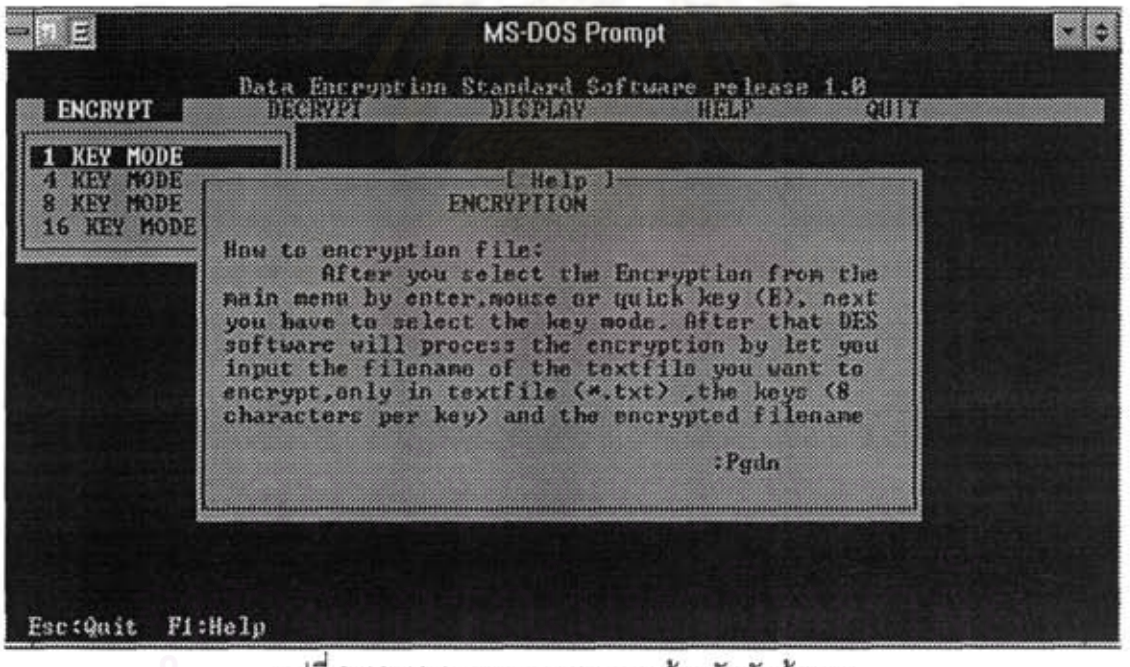
รูปที่ 3.39 หน้าจอสำหรับแสดงข้อมูลที่เข้ารหัสลับและถอดรหัสลับแล้ว

ข้อจำกัดของการแสดงข้อมูลในเมนูย่อยนี้ก็คงมีเหมือนกับในเมนูย่อยที่แล้ว ดังนั้นถ้าข้อมูลที่นำมาแสดงมีขนาดใหญ่เกินไป ก็จะไม่สามารถทำการแสดงได้ และจะปรากฏข้อความขึ้นดังในรูปที่ 3.34 เช่นเดียวกัน

เมื่อผู้ใช้ต้องการออกจากการแสดงข้อมูลก็จะสามารถทำได้เช่นเดียวกัน โดยการกดปุ่ม Esc จะปรากฏข้อความดังในรูปที่ 3.35 และถ้าผู้ใช้กด N ก็จะกลับเข้าสู่การแสดงข้อมูลคืน แต่ถ้ากด Y จะเป็นการออกจากการแสดงข้อมูล โดยข้อมูลจะหายไป และจะปรากฏข้อความถามว่าต้องการดูข้อมูลอื่นเพิ่มเติมอีกหรือเปล่า ดังในรูปที่ 3.36 ซึ่งถ้าผู้ใช้กด Y ก็จะกลับไปเริ่มต้นการใส่ชื่อข้อมูลที่ต้องการแสดงใหม่อีกครั้ง แต่ถ้าผู้ใช้กด N ก็จะออกจาก Display mode ไปยังเมนูหลัก เป็นการจบการใช้งานใน Display mode

3.2.4 Help

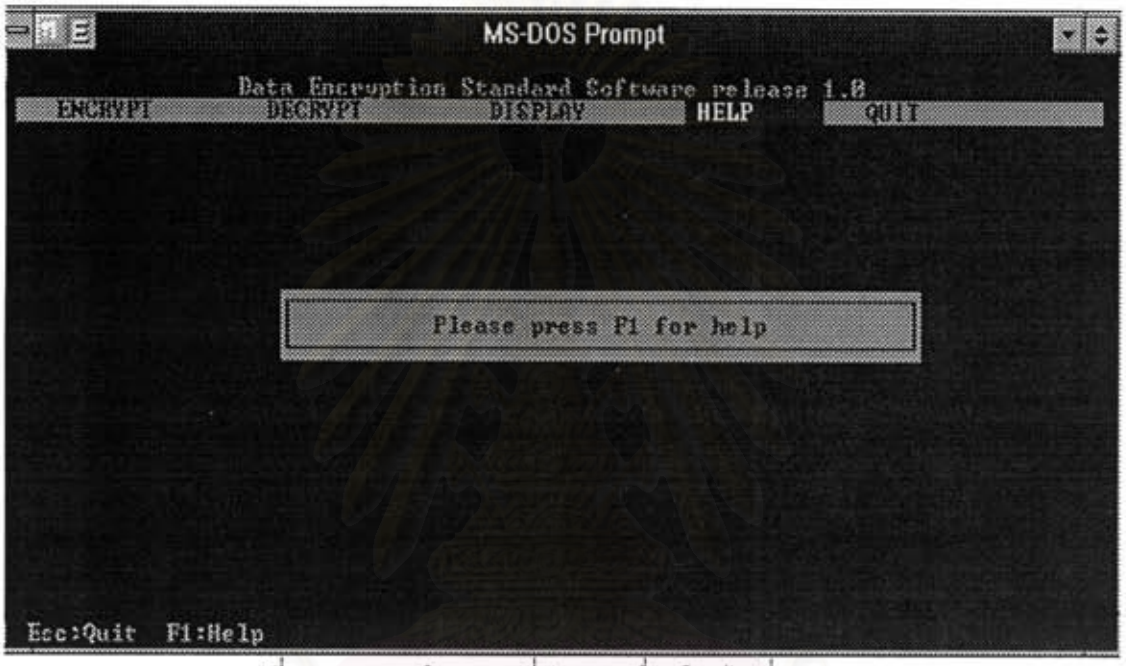
ใน DES software นี้จะมีระบบ Help ซึ่งช่วยให้สามารถศึกษาและใช้งานได้ง่ายขึ้น เมื่อผู้ใช้ที่อยู่ในหน้าจอใดหรือ mode ใดก็ตามใน DES software ทำการกดปุ่ม F1 จะปรากฏข้อความที่เป็น help ที่เกี่ยวข้องกับ mode นั้นอยู่ ยกตัวอย่างเช่น เมื่อผู้ใช้ใน mode การเข้ารหัสลับข้อมูลกดปุ่ม F1 ก็จะปรากฏข้อความที่เป็น help เกี่ยวกับการเข้ารหัสลับขึ้นบนหน้าจอดังในรูปที่ 3.40



รูปที่ 3.40 Help ของ mode การเข้ารหัสลับข้อมูล

สำหรับ help รวมของ DES software จะสามารถเรียกมาดูได้โดยการเลือกไปที่เมนู Help ในเมนูหลักจะปรากฏข้อความขึ้นดังในรูปที่ 3.41

ที่หน้าจอนี้เมื่อกดปุ่ม F1 ก็จะปรากฏ help รวม ขึ้นมาที่หน้าจอ การดูข้อความใน help ในหน้าก่อนหรือหลังจากหน้าปัจจุบัน ทำได้โดยใช้ปุ่ม PgUp และ PgDw และใน help จะมีแถบสว่างให้เลือกเพื่อเข้าไปดู help อื่นที่เกี่ยวข้อง การเลือกก็ทำได้โดยการกด Enter เมื่อแถบสว่างอยู่ที่ตัวเลือกอันนั้น ส่วนการออกจาก Help ก็สามารถทำได้โดยกดปุ่ม Esc ซึ่งจะทำให้กลับมาสู่หน้าจอหลัก



รูปที่ 3.41 แสดงข้อความที่ปรากฏเมื่อเลือกไปที่เมนู Help

3.2.5 Quit

เมนูนี้ใช้ในการออกจากโปรแกรมกลับเข้าสู่ DOS command line ซึ่งมีผลเหมือนกับการกดปุ่ม Esc จะปรากฏข้อความดังในรูปที่ 3.3 เช่นกัน การกด Y จะทำให้ออกจาก DES software ไปสู่ DOS command line ส่วนการกด N จะกลับเข้าสู่เมนูหลักในโปรแกรม

บทที่ 4
การทดสอบการเข้ารหัสลับและถอดรหัสลับของโปรแกรม

ในการทดสอบการทำงานของ DES software นั้น ได้ทำการทดสอบการเข้ารหัสลับและถอดรหัสลับข้อมูล เพื่อดูผลการทำงานของโปรแกรมว่า สามารถเข้ารหัสลับและถอดรหัสลับได้ถูกต้องหรือไม่ และระบบการดึง key ไปใช้ในการเข้าและถอดรหัสลับในแต่ละ key mode ทำงานได้ถูกต้องหรือไม่ โดยการทดสอบนั้นได้กระทำและได้ผลดังนี้

4.1 การทดสอบการเข้ารหัสลับและถอดรหัสลับใน 1 key mode

ในการทดสอบนี้ ได้นำข้อมูลที่เตรียมไว้มาทำการเข้ารหัสลับและถอดรหัสลับด้วย key 2 ชุดใน 1 key mode โดย key ใช้ทั้ง2ชุดจะต่างกันดังนี้

1. key ชุดที่1 " software "
2. key ชุดที่2 " 1-*^%#l@ "

นำ key มาเข้ารหัสลับโดยใช้ข้อมูลเดียวกัน ซึ่งข้อมูลที่ใช้ในการทดสอบเป็นข้อความดังนี้

This is a test to DES software release 1.0.

DES software is used to encrypt or decrypt file with the key that you choose. After encryption, the data in textfile will be in the confuse form that's very difficult to read,such as, character that cannot read ,no line break or paragraph.

Example:

abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

1234567890+-*/()[]{}<>;:,.?/\'"=_*&^%$#@!~`

ABCDEFG

HIJKLMNOPQ

RSTUVWXYZ

1.ENCRYPTION Q W E R T Y U I O P 7 8 9

รูปที่ 4.1 ข้อมูลที่ใช้ในการทดสอบ

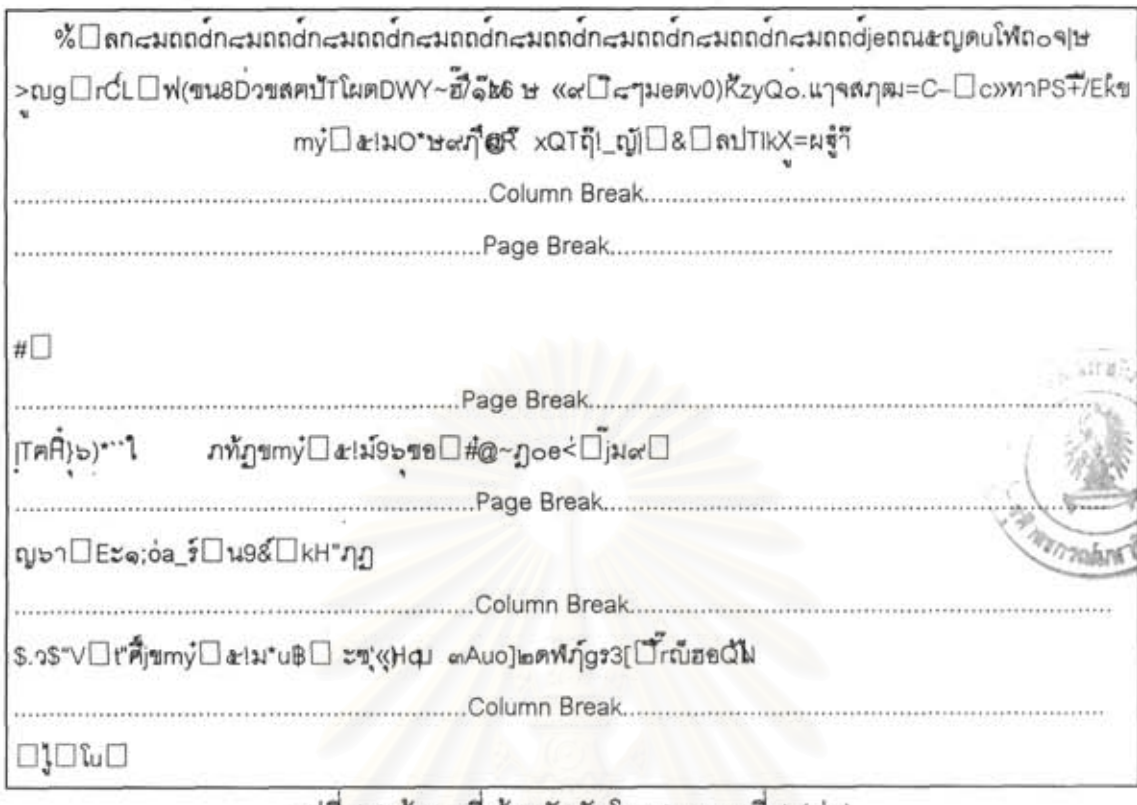
```
2.DECRYPTION            A S D F G H J K L ;   4 5 6
3.DISPLAY                 Z X C V B N M , .   1 2 3
**********************************************************
*  DDDDD   EEEEEE   SSSS           RRRRR      11      00000  *
*  D      D E         S              R       R   11      0      0 *
*  D      D EEEEEE    SSSS           RRRRR      11     0      0 *
*  D      D E                S         R       R   11      0      0 *
*  DDDDD   EEEEEE    SSSS    OOOOO  R        R   11   0   00000  *
**********************************************************
```

รูปที่ 4.1 ข้อมูลที่ใช้ในการทดสอบ (ต่อ)

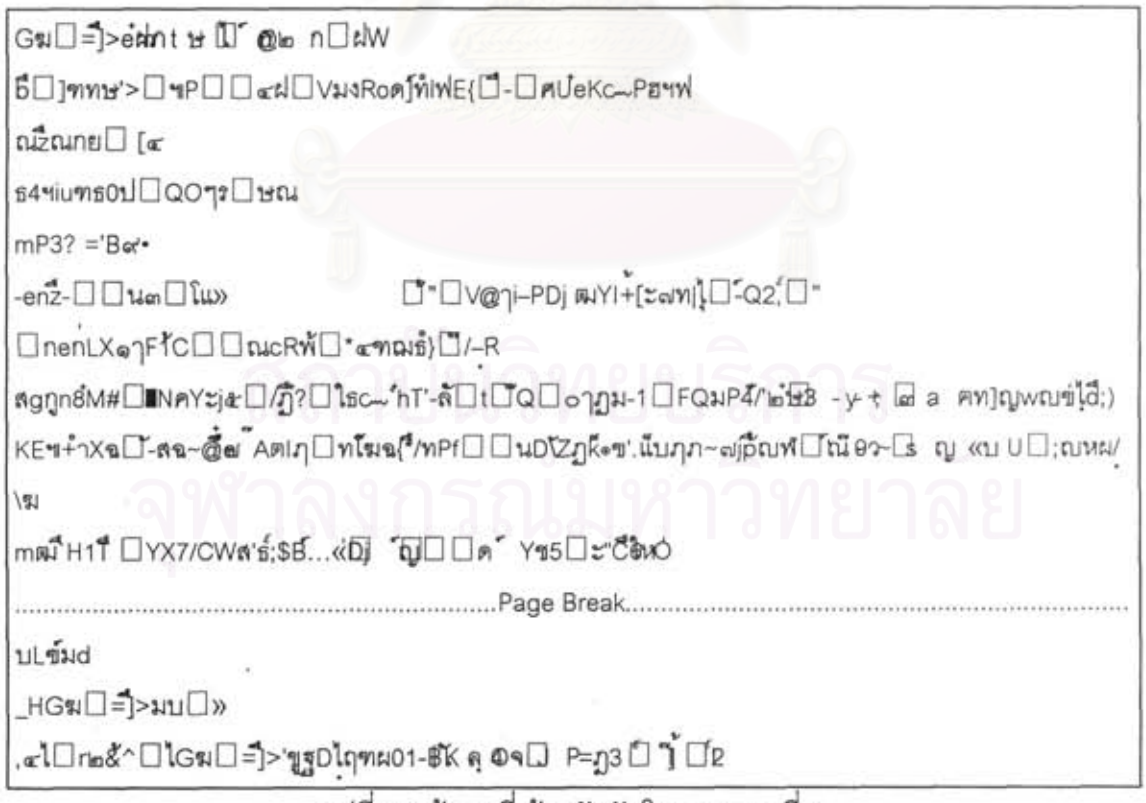
เมื่อทำการเข้ารหัสลับข้อมูลจะได้เป็นข้อมูลซึ่งเมื่อนำแสดงในโปรแกรม Microsoft Word ใน Windows โดยแสดงข้อมูลแบบ textfile จะได้ดังรูปที่ 4.2 และ 4.3 ซึ่งเป็นการเข้ารหัสลับโดย key ชุดที่ 1 และ ชุดที่ 2 ตามลำดับ

```
ะmy่~ะ!ม(~r'...-อาdคๅ|•>\ •ฐ๑Hห|ฒจ:&ล~ฑQ|โ.fต
ฬีกคณะ์  ฟ๊0ซ&ห็wฅwx้า|~บค~~|DX๊~79ญปฐ□ไ1uqฑ)ก้Cฏc\EHซ~~j~๙^$/โใซX~ื#ม่o~~๗/ฅยน9ั_ซS ฒ•ฏ
%ฒ๊_''rpไถ่C#M1ฉะ~ด:<N2#m@m่ช่i(F!S4~P๊~Kฏธบ'ฤ'ไ
.....................................................Page Break.....................................................
ธ็ฒzฏsẽ~'TงGf<~V~
ไr(+%ร□ ๓4ทตqกม~7ไ|เอถพเ~ธxซOp■กFฒ้:...]|อ[UN■ตซ~"ฮ์Tqซ
.....................................................Column Break.....................................................
Z|ยอ>*4ซๅฝู่Fฬ<ฯๆฒL~@~ฯบ~>ห(w%ฺB-ะ~Po*
.....................................................Page Break.....................................................
M~Uํา?ส~ศ~;2o๊ฏ?...Zฬฒcฌ|K2el±B~ภ|๓  ธ็~ๆธ0qA l~คๅ์|~นี้TมMs|ะญีถ9'ฒญ@'ง
pVะ2ฐ;ไBYต?S แ~๔Mี~Fฏ|ย'2ุหDญชmy่~ะ!ม[
'ษ์Tห้กหก8*า□ถCl๕ี|~ย>ซmy่~ะ!มซmy่~ะ!มต4~ีธิ๙ฬ|~6q'$u|6'
ไE;ฝฏ~a...!sซmy่~ะ!มiCWC~ซ.~ษ•U(—U::ฅนิ์ฑBฮี่ปฏbฏฮ์
~P%ั!wห'@ฏ็ตเฎ(qณาบ้ซmy่~ะ!มNFฤ
x‹‹
        p(x̃b7ntๅฒีD~ึง&...`๘~ึ้vีซ~+ึ'โGงลcอM<~jซmy่~ะ!ม0/ฬีr~~~~ซ~ฮ;ม'q)T'ค~ํ%/~ค•x~7*ะ
```

รูปที่ 4.2 ข้อมูลที่เข้ารหัสลับโดย key ชุดที่ 1



รูปที่ 4.2 ข้อมูลที่เข้ารหัสลับโดย key ชุดที่ 1 (ต่อ)



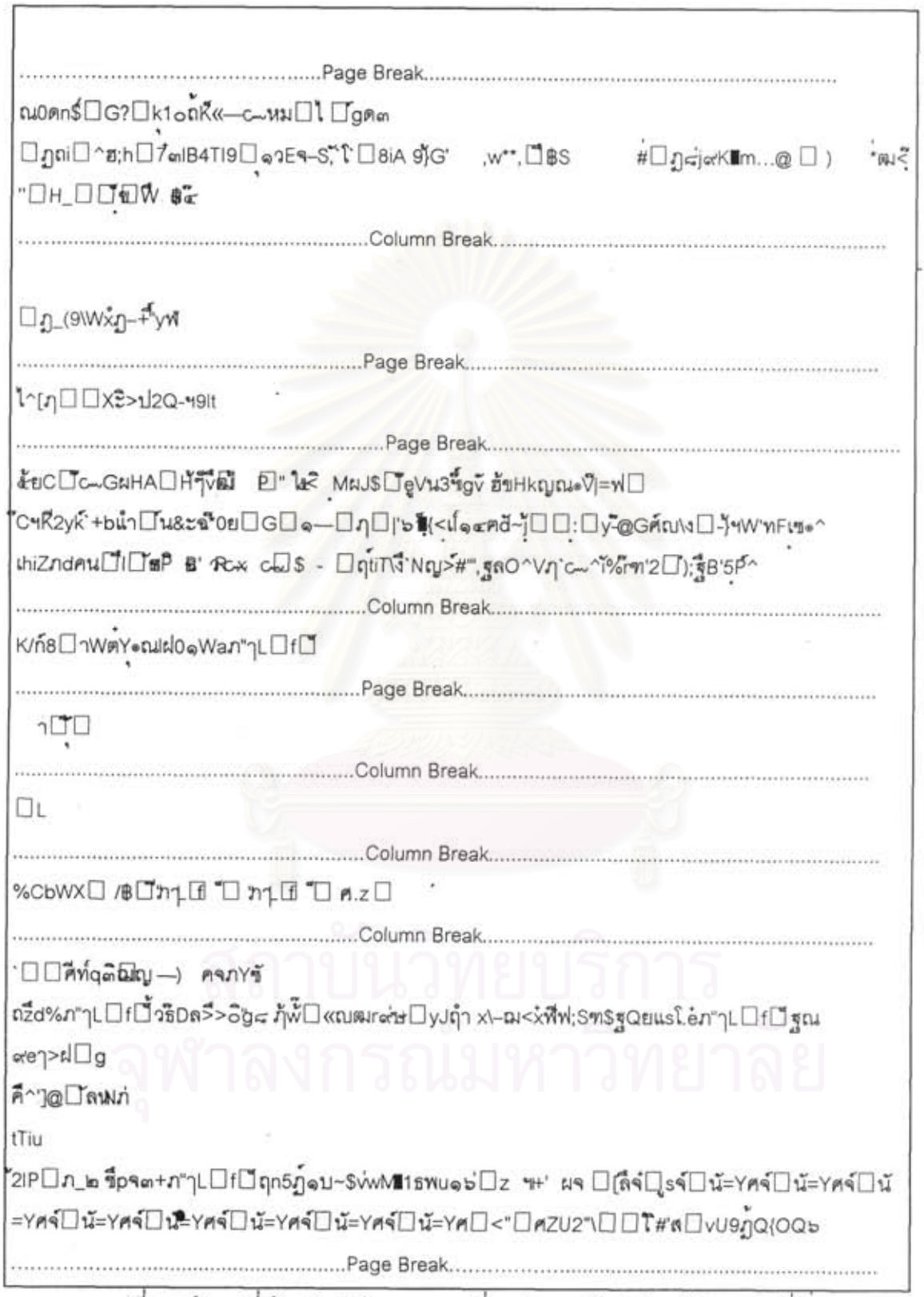
รูปที่ 4.3 ข้อมูลที่เข้ารหัสลับโดย key ชุดที่ 2

รูปที่ 4.3 ข้อมูลที่เข้ารหัสลับโดย key ชุดที่ 2 (ต่อ)

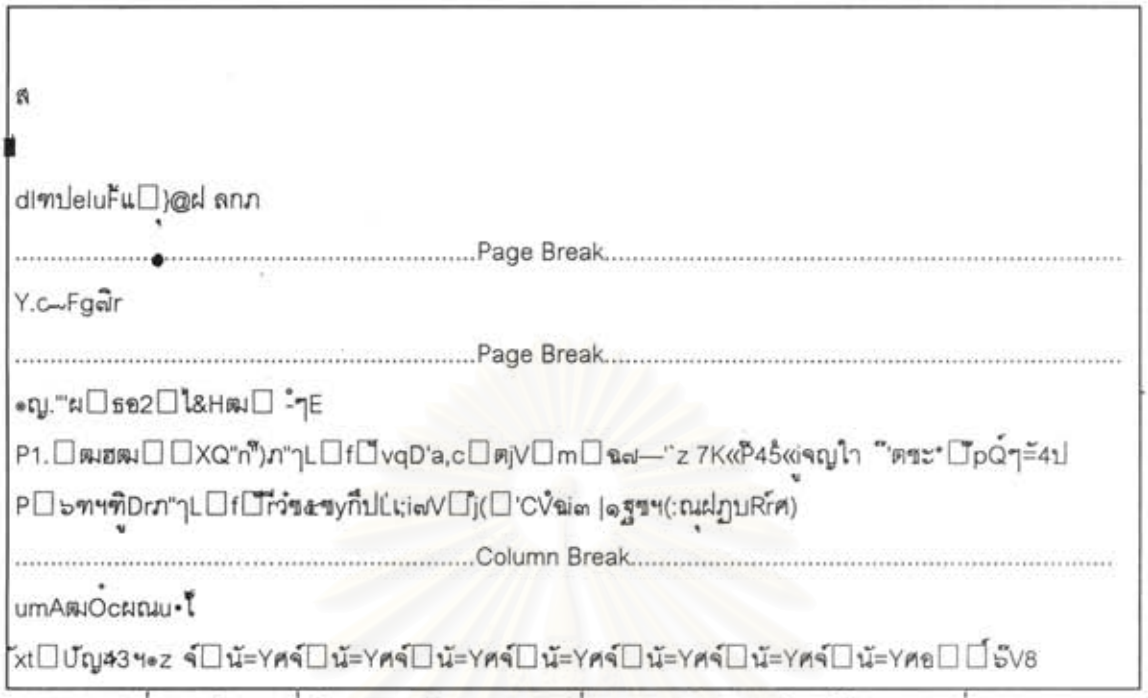
จากข้อมูลในรูปจะเห็นได้ว่าข้อมูลที่ได้มีลักษณะที่ไม่เหมือนข้อมูลเดิมและไม่สามารถตีความออกมาได้ นอกจากนี้ข้อมูลที่เข้ารหัสลับด้วย key ที่ต่างกันก็ไม่เหมือนกัน จากผลอันนี้แสดงให้เห็นว่า DES software สามารถเข้ารหัสลับข้อมูลได้ และการเข้ารหัสลับด้วย key ที่ต่างกัน ก็จะให้ผลที่ต่างกันด้วย ซึ่งได้ผลตามที่ต้องการ

หลังจากนี้ได้นำข้อมูลมาถอดรหัสลับ โดยใช้ key เดิมและ key สลับกัน ซึ่งเมื่อใช้ key เดิมถอดรหัสลับจะได้ข้อมูลเหมือนกัน ดังในรูปที่ 4.4 แต่เมื่อใช้ key สลับกันคือ ใช้ key ชุดที่ 2 ถอดรหัสลับข้อมูลที่เข้ารหัสลับด้วย key ชุดที่ 1 และใช้ key ชุดที่ 1 ถอดรหัสลับข้อมูลที่เข้ารหัสลับด้วย key ชุดที่ 2 จะได้ผลดังในรูปที่ 4.5 และ 4.6 ตามลำดับ

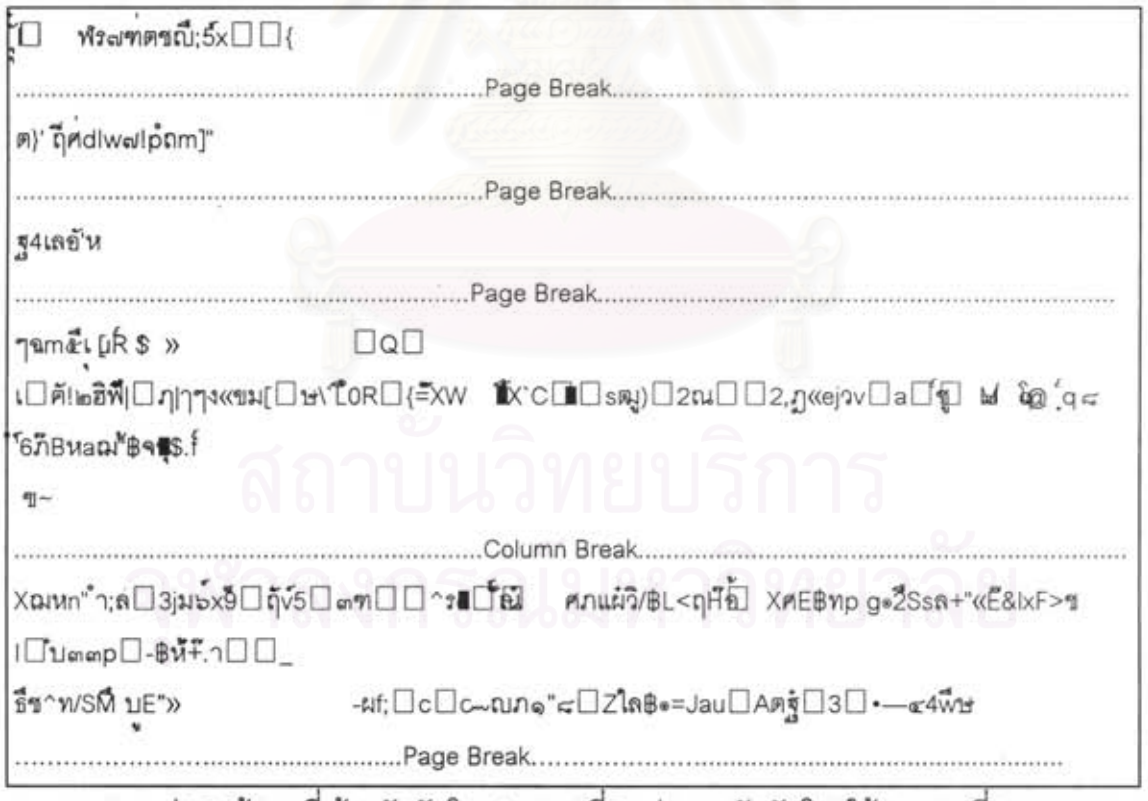
รูปที่ 4.4 ข้อมูลที่ถอดรหัสลับออกมาโดยใช้ key เดิม



รูปที่ 4.5 ข้อมูลที่เข้ารหัสลับโดย key ชุดที่1 แต่ถอดรหัสลับโดยใช้ key ชุดที่2



รูปที่ 4.5 ข้อมูลที่เข้ารหัสลับโดย key ชุดที่1 แต่ถอดรหัสลับโดยใช้ key ชุดที่2 (ต่อ)



.รูป4.6 ข้อมูลที่เข้ารหัสลับโดย key ชุดที่2 แต่ถอดรหัสลับโดยใช้ key ชุดที่1

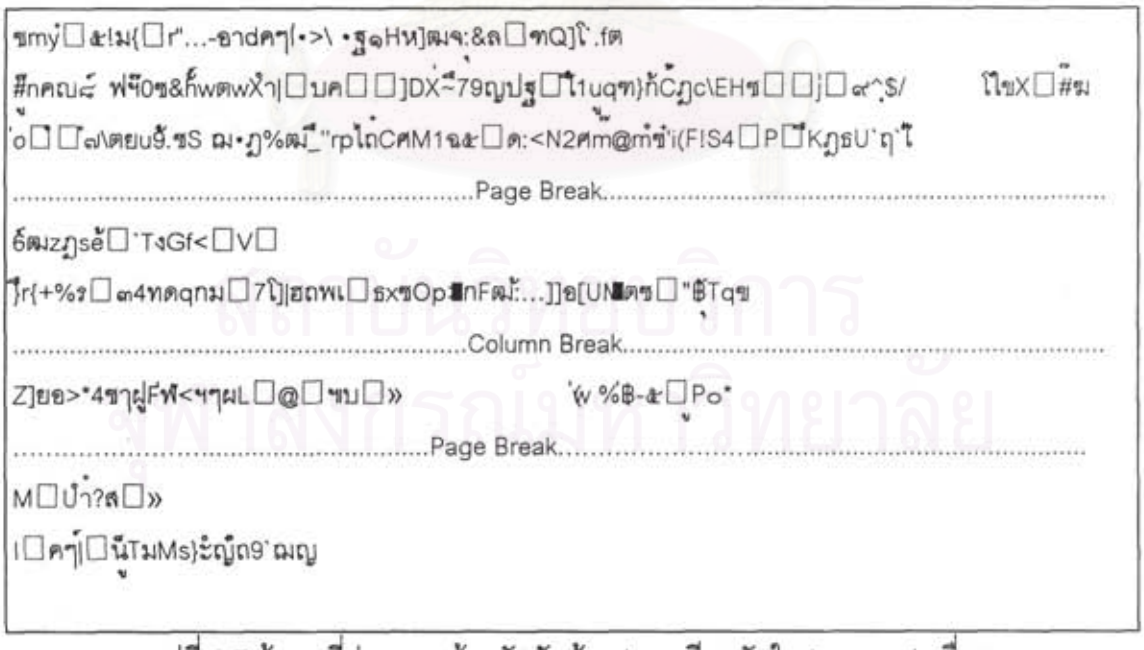
รูปที่ 4.6 ข้อมูลที่เข้ารหัสลับโดย key ชุดที่2 แต่ถอดรหัสลับโดยใช้ key ชุดที่1 (ต่อ)

จากผลในรูปที่ 4.4 ,4.5 และ 4.6 แสดงให้เห็นว่า DES software สามารถถอดรหัสลับข้อมูลได้ถูกต้อง ได้เป็นข้อมูลเดิมกลับคืนมา ในขณะที่การใช้ key ผิดจะทำให้ไม่สามารถถอดรหัสลับกลับคืนมาได้ แสดงว่าข้อมูลมีความปลอดภัยถ้า key ยังถูกรักษาไว้เป็นความลับได้

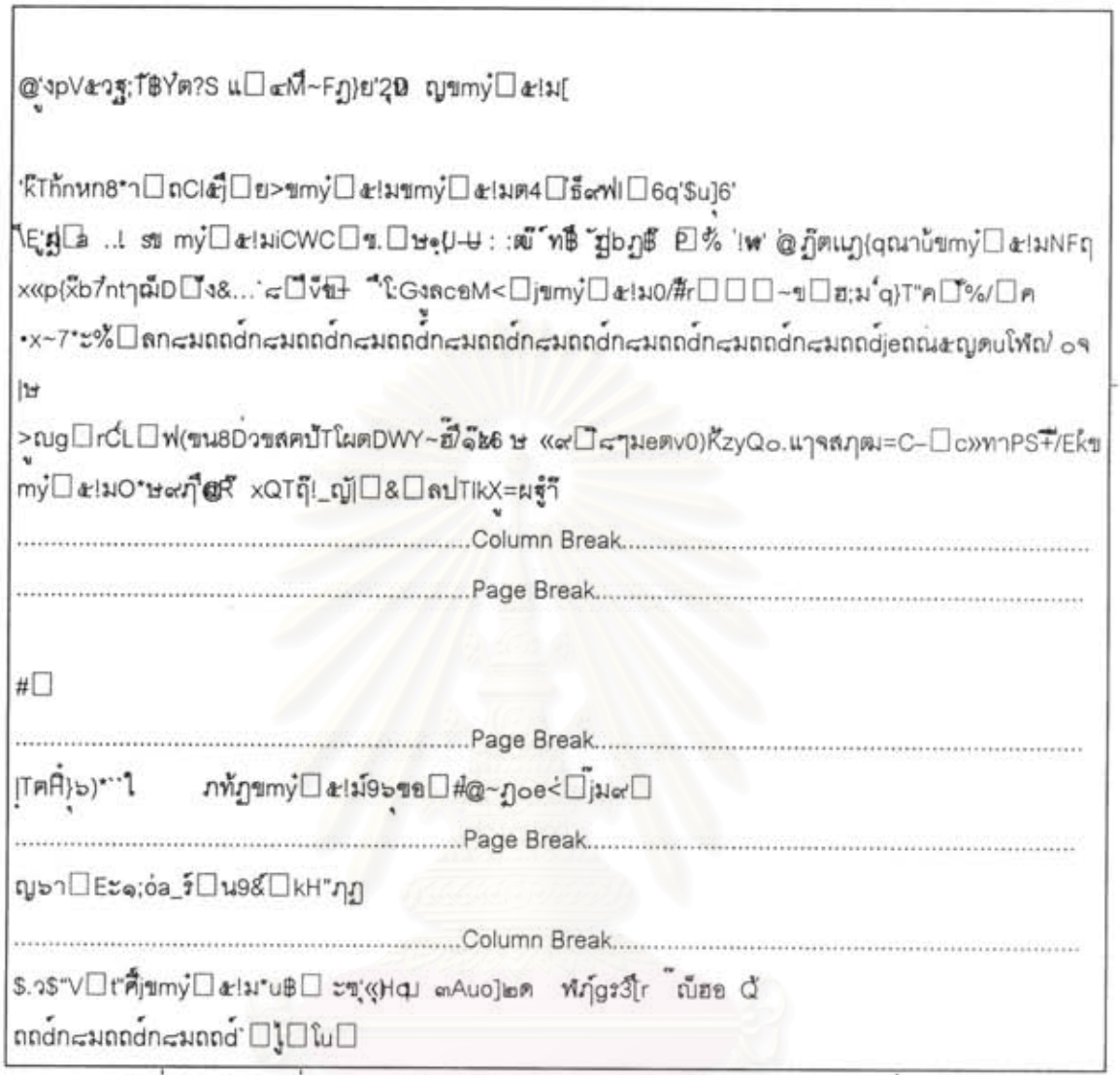
ในการเข้ารหัสลับนั้น เดิมแฟ้มข้อมูลที่ใช้ในการทดสอบมีขนาด 1,182 ไบต์ หลังผ่านการเข้ารหัสลับแล้วจะมีขนาดใหญ่ขึ้นเป็น 1,184 ไบต์ ทั้งนี้เนื่องมาจาก ในขั้นตอนของการเข้ารหัสลับจะทำการดึงข้อมูลมาเข้ารหัสลับครั้งละ 8 ไบต์ (64 บิต) ถ้าข้อมูลไม่ครบ 8 ไบต์ DES software จะทำการเติมข้อมูลด้วยตัวว่างจนครบ 8 ไบต์ ดังนั้นขนาดของแฟ้มข้อมูลจึงอาจเพิ่มขึ้นได้และจะเพิ่มเป็นขนาดที่หารด้วย 8 ลงตัว ส่วนในการถอดรหัสลับใช้ algorithm เดียวกันจึงมีโอกาสเกิดได้เหมือนกัน แต่เนื่องจากมักทำการถอดรหัสลับข้อมูลที่มีการเติมจนครบหรือครบอยู่แล้วจึงไม่เห็นผล ยกตัวอย่างเช่น ข้อมูลที่ถอดรหัสลับออกมาแล้วในรูปที่ 4.4 ,4.5 และ 4.6 จะมีขนาดเป็น 1,184 ไบต์ เท่ากับข้อมูลที่ผ่านการเข้ารหัสลับแล้ว และนำมาถอดรหัสลับ

4.2 การทดสอบการเข้ารหัสลับและถอดรหัสลับใน key mode อื่นๆ

ในการทดสอบช่วงนี้จะทำการทดสอบโดยทำการเข้ารหัสลับข้อมูลเดิมในรูปที่ 4.1 ใน key mode อื่นๆ และใช้ key เหมือนกันหมดคือ "software" ซึ่งถ้าขั้นตอนต่างๆถูกต้องควรจะได้ข้อมูลที่เข้ารหัสลับแล้วตรงกัน ซึ่งจากผลการทดสอบนั้นสามารถเข้ารหัสลับได้เป็นข้อมูลดังในรูปที่ 4.7 ซึ่งเหมือนกับในรูปที่ 4.2



รูปที่ 4.7 ข้อมูลที่ผ่านการเข้ารหัสลับด้วย key เดียวกันใน key mode อื่นๆ



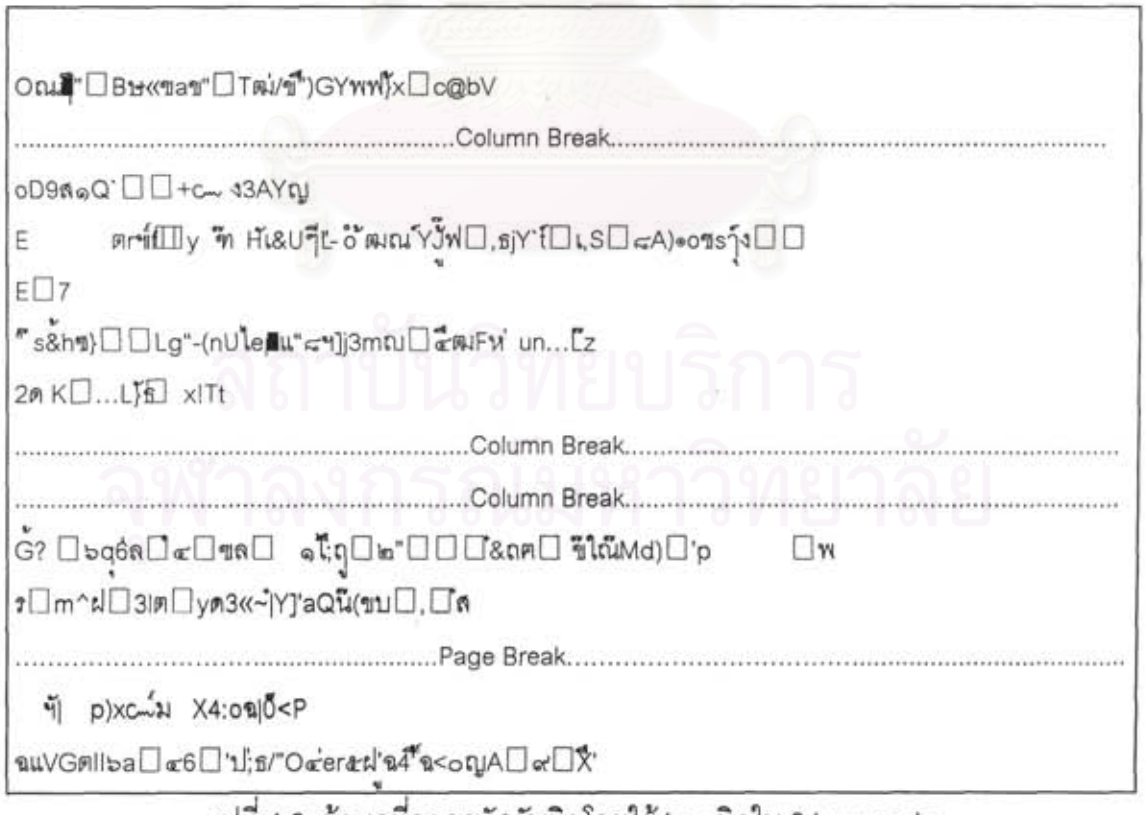
รูปที่ 4.7 ข้อมูลที่ผ่านการเข้ารหัสลับด้วย key เดียวกันใน key mode อื่นๆ (ต่อ)

และเมื่อนำข้อมูลมาถอดรหัสลับด้วย key เดียวกัน จะได้ข้อมูลเดิมออกมาเหมือนกับในรูปที่ 4.4 ซึ่งแสดงว่าใน key mode อื่นๆ ก็สามารถทำการเข้ารหัสลับและถอดรหัสลับได้เช่นเดียวกัน และกระบวนการในการสร้าง key ขึ้นมาให้ครบ 16 ชุดในแต่ละ key mode นั้นสามารถทำงานได้อย่างถูกต้องจึงสามารถเข้ารหัสลับได้เหมือนกัน

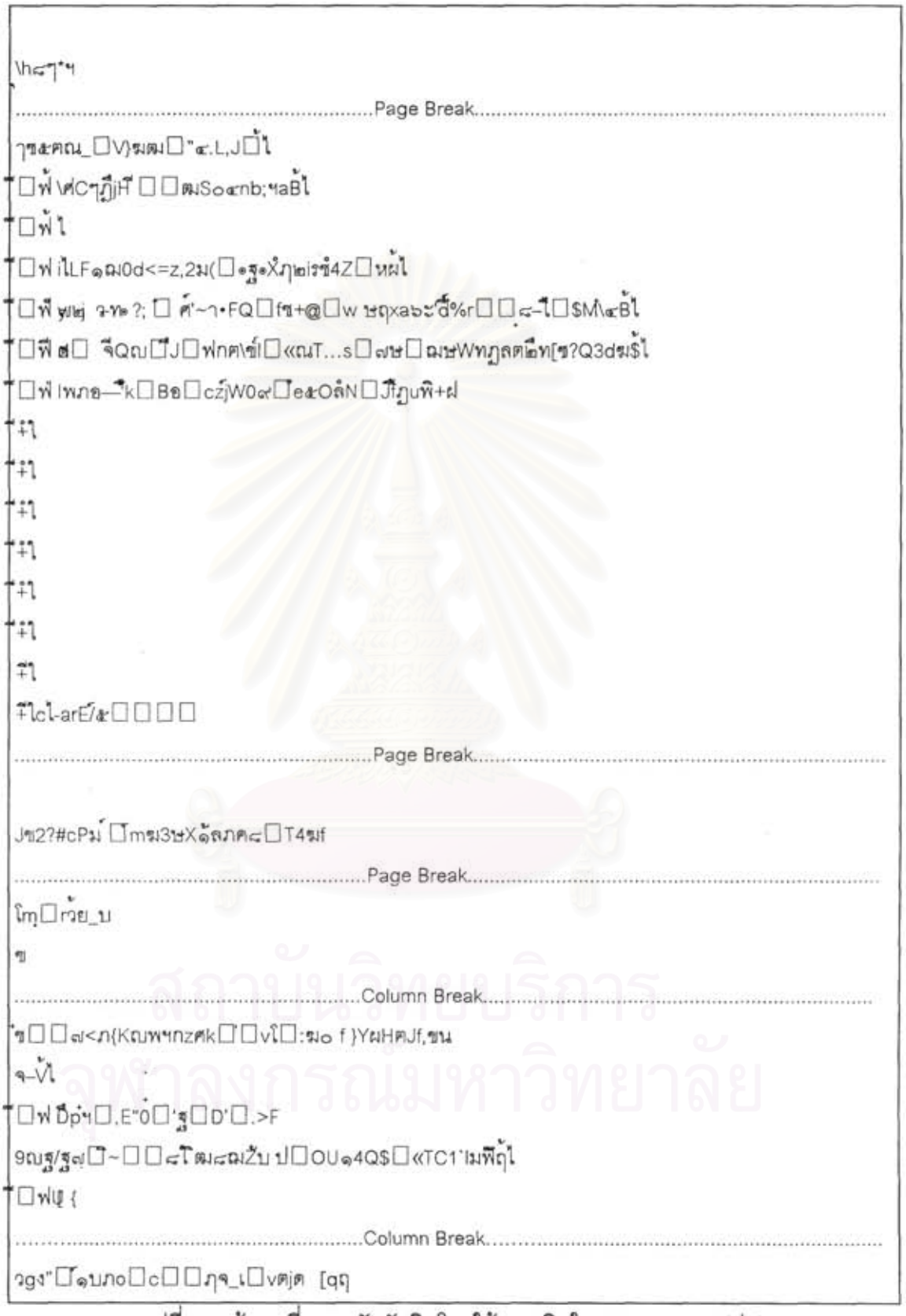
แต่เมื่อนำข้อมูลมาถอดรหัสลับโดยใช้ key ที่ไม่เหมือนเดิม โดยใช้ key ตัวสุดท้ายผิดไป 1 ตัวอักษรคือใช้เป็น "sfotware" จะทำให้ถอดรหัสลับออกมาเป็นข้อมูลที่ผิดพลาดไม่เหมือนเดิม และไม่สามารถตีความได้ ดังในรูป ข้อมูลที่ถอดรหัสออกมาได้จาก 4 key mode , 8 key mode และ 16 key mode เป็นดังในรูปที่ 4.8 ,4.9 และ 4.10 ตามลำดับ

รูปที่ 4.8 ข้อมูลที่ถอดรหัสลับผิดโดยใช้ key ผิดใน 4 key mode

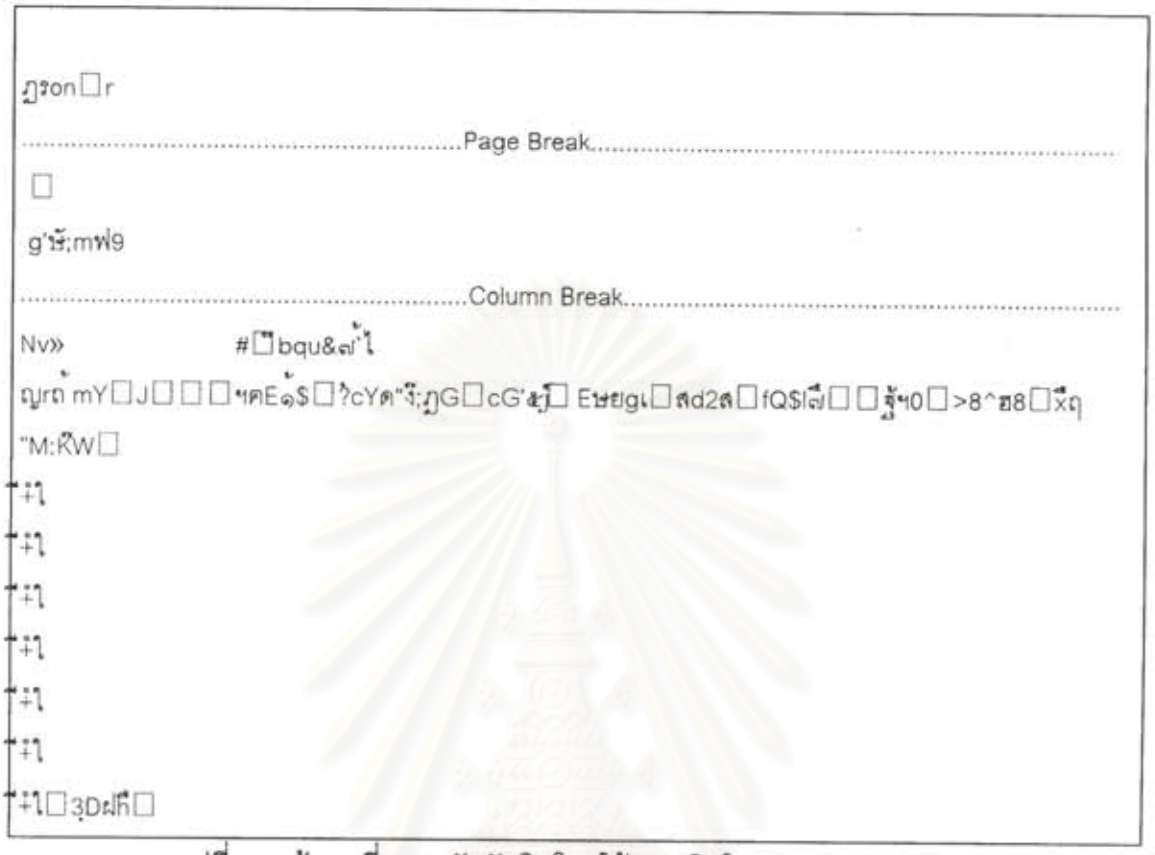
รูปที่ 4.8 ข้อมูลที่ถอดรหัสลับผิดโดยใช้ key ผิดใน 4 key mode (ต่อ)



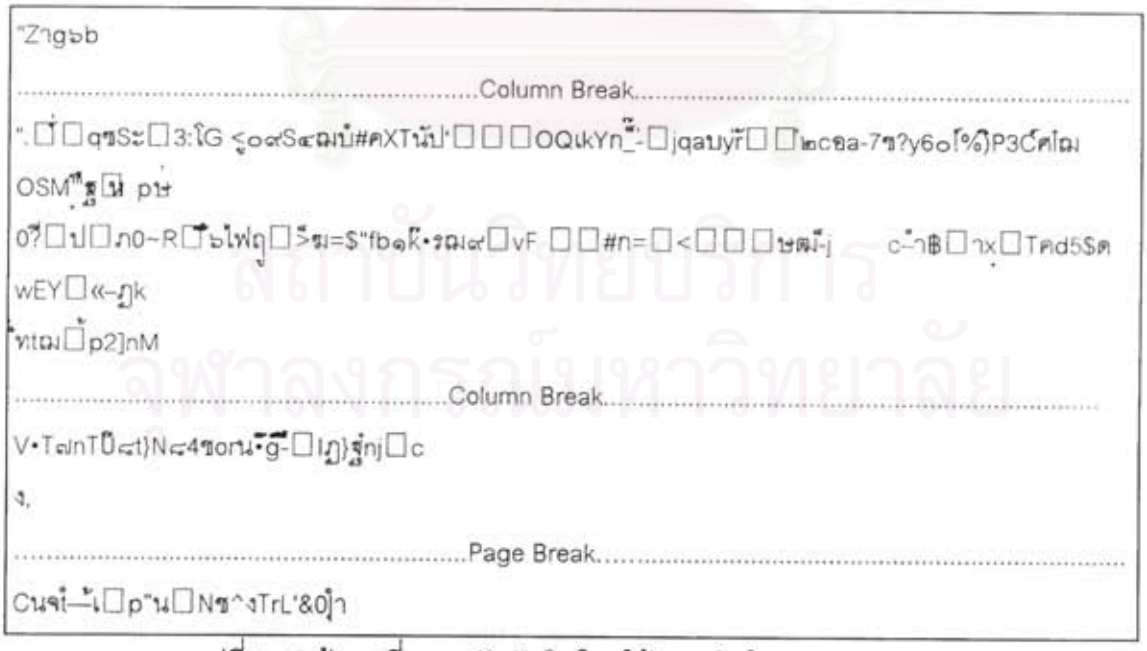
รูปที่ 4.9 ข้อมูลที่ถอดรหัสลับผิดโดยใช้ key ผิดใน 8 key mode



รูปที่ 4.9 ข้อมูลที่ถอดรหัสลับผิดโดยใช้ key ผิดใน 8 key mode (ต่อ)

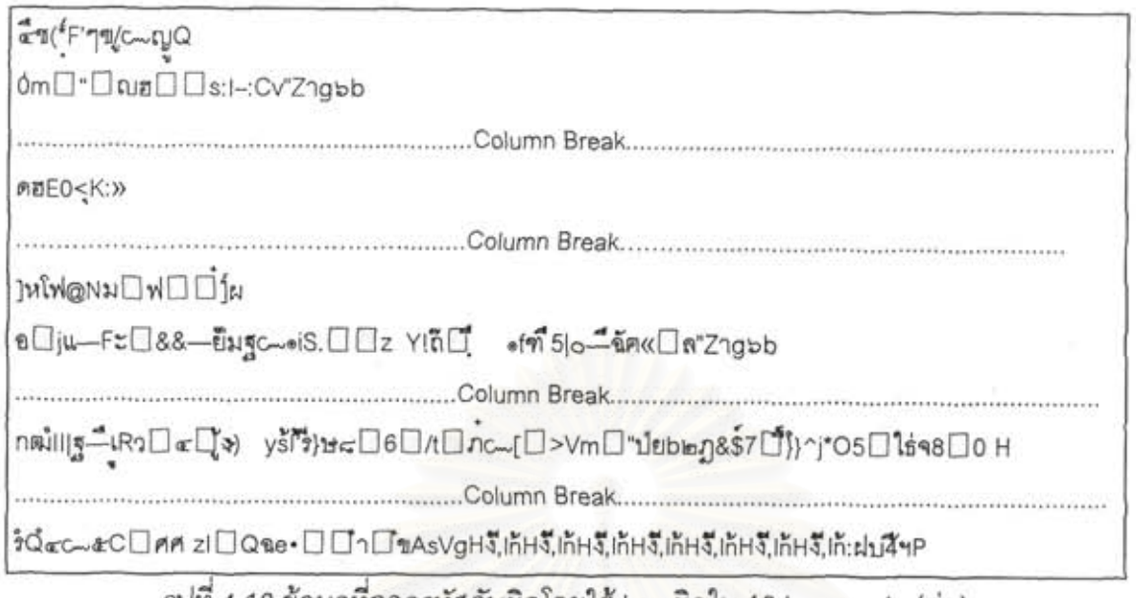


รูปที่ 4.9 ข้อมูลที่ถอดรหัสลับผิดโดยใช้ key ผิดใน 8 key mode (ต่อ)



รูปที่ 4.10 ข้อมูลที่ถอดรหัสลับผิดโดยใช้ key ผิดใน 16 key mode

รูปที่ 4.10 ข้อมูลที่ถอดรหัสลับผิดโดยใช้ key ผิดใน 16 key mode (ต่อ)



รูปที่ 4.10 ข้อมูลที่ถอดรหัสลับผิดโดยใช้ key ผิดใน 16 key mode (ต่อ)

จากข้อมูลในรูปจะพบว่า การเข้ารหัสลับใน key mode อื่นๆ สามารถให้ความปลอดภัยต่อข้อมูลได้ เพราะการใช้ key ที่ผิดในการถอดรหัสลับจะไม่สามารถถอดรหัสลับข้อมูลเดิมออกมาได้ นอกจากนี้แม้ key ต่างไปจากเดิมเพียงเล็กน้อย ข้อมูลที่ได้จากการถอดรหัสลับก็ไม่เหมือนเดิม และไม่มีส่วนคล้ายหรือเกี่ยวข้องกับข้อมูลเดิมด้วย ส่วนในแต่ละ key mode นั้น แม้ว่า key จะมีข้อผิดพลาดเท่ากันแต่การนำ key ไปใช้จะไม่เหมือนกัน ดังนั้นข้อมูลที่ถอดรหัสลับ (หรือเข้ารหัสลับ) ก็จะไม่เหมือนกันด้วย ซึ่งแสดงว่าการทำงานในแต่ละ key mode ตรงตามที่กำหนดไว้

จากผลการทดสอบแสดงให้เห็นว่า DES software สามารถทำการเข้ารหัสลับและถอดรหัสลับข้อมูลด้วย key ที่กำหนดขึ้นเอง และให้ความปลอดภัยของข้อมูลโดยขึ้นอยู่กับความปลอดภัยของ key ตราบใดที่ key ยังคงถูกรักษาไว้เป็นความลับได้ ข้อมูลก็ยังคงมีความปลอดภัยอยู่ ซึ่งตรงตามคุณสมบัติของการเข้ารหัสลับแบบ DES

4.3 การทดสอบการเข้ารหัสลับและถอดรหัสลับข้อมูลภาษาไทยใน 1 key mode

ในการทดสอบนี้ ได้นำข้อมูลภาษาไทยที่เตรียมไว้มาทำการเข้ารหัสลับและถอดรหัสลับด้วย key 2 ชุด ใน 1 key mode โดยทั้งสองชุดมี key ต่างกันดังนี้

1. key ชุดที่ 1 "software"
2. key ชุดที่ 2 "1-*^%#|@"

นำ keyมาเข้ารหัสลับโดยใช้ข้อมูลเดียวกัน ซึ่งข้อมูลที่ใช้ในการทดสอบเป็นดังนี้

ความรู้ทางวิทยาศาสตร์และเทคโนโลยี มีบทบาทสำคัญยิ่งต่อการพัฒนาเศรษฐกิจและอุตสาหกรรมของประเทศ และในการวางรากฐานความรู้ทางวิทยาศาสตร์และเทคโนโลยีเพื่อเตรียมบุคลากรให้มีความพร้อมสำหรับรองรับการพัฒนาดังกล่าวจำเป็นต้องอาศัยสื่อที่มีประสิทธิภาพ ทั้งนี้ หนังสือ ตำรา นับเป็นสื่ออันสำคัญอย่างหนึ่ง แต่ปัญหาก็คือ เรายังขาดแคลนตำราทางวิทยาศาสตร์และเทคโนโลยีที่เป็นภาษาของเราเอง จริงอยู่ แม้ในปัจจุบันเราจะมีตำราภาษาไทยมากขึ้นมากกว่าเมื่อสิบปีที่แล้ว แต่ก็ยังนับว่าไม่มากพอ เมื่อเทียบกับความก้าวหน้าทางวิทยาการที่รุดหน้าไปอย่างไม่หยุดยั้ง

รูปที่ 4.11 ข้อมูลที่ใช้ในการทดสอบ

เมื่อทำการเข้ารหัสลับข้อมูลจะได้เป็นข้อมูลซึ่งเมื่อไปแสดงใน Microsoft Word ใน Windows โดยแสดงข้อมูลแบบ textfile จะได้ดังรูปที่ 4.12 และ 4.13 ซึ่งเป็นการเข้ารหัสลับโดยใช้ key ชุดที่ 1 และ key ชุดที่ 2 ตามลำดับ แต่เนื่องจากแฟ้มข้อมูลที่ได้มีขนาดใหญ่มาก จึงจะแสดงข้อมูลเพียงบางส่วน

{น่ทรมMฮษ□iKลื@...□iKลื@...๔""Z٦gbb

□iKว13๗ฆ □ □"sYuฦธ[s+หบบฌฌ...□]N

<<ณ๋ก3..ZR มj ณใ ๔ RG

"onข]N

....Column Break...

เ÷ปฐุOณ•ญรต□ด๊า□ฒi4(ญ□ฤั»   )qZv̄nsฺiM\Dขต"Z٦gbb

....Column Break...

-ๆ

B•□ีขทภ @๕`□ □ีqV"ฆY-□ี_bั□แ ษัสDNHจี,เก้Hจี,เก้Hจี,เก้Hจี,เก้Hจี,เก้Hจี,เก้Hจี,เก้Hจี,เก้

....Page

Break..

□iKล์@...□iKล์@...□iKล์@...□iKล์@...□iKล์@...□iKล์@...□iKล์@...□iKล์@...

□iKล์@...□iKล์@...□iKล์@...□iKล์@...□iKล์@...□iKล์@...□iKล์@...□iKล์@...

□iKล์@...□iKล์@...□iKล์@...□iKล์@...□iKล์@...□iKล์@...□iKล์@...□iKล์@...

□iKล์@...□iKล์@...□iKล์@...□iKล์@...□iKล์@...□iKล์@...□iKล์@...□iKล์@...

□iKล์@...□iKล์@...□iKล์@...□iKล์@...

รูปที่ 4.12 ข้อมูลบางส่วนที่ได้จากการเข้ารหัสลับโดย key ชุดที่ 1

๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ

๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦

}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ

. □QIฤ

....Page Break...

>_P2 oo{□□#□Pฉแถสฤนศม{@๑

□□ฒไปงT>LG๔

....Page Break...

๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ

๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ}๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ๒٦}rฉ

รูปที่ 4.13 ข้อมูลบางส่วนที่ได้จากการเข้ารหัสลับข้อมูลโดย key ชุดที่ 2

จากข้อมูลในรูปจะเห็นได้ว่า ข้อมูลที่ได้มีลักษณะที่ไม่เหมือนข้อมูลเดิม และไม่สามารถตีความออกมาได้ นอกจากนี้ข้อมูลที่เข้ารหัสลับด้วย key ที่ต่างกันก็ไม่เหมือนกัน จากผลอันนี้แสดงให้เห็นว่า DES software สามารถเข้ารหัสลับข้อมูลได้ และการเข้ารหัสลับด้วย key ที่ต่างกันก็จะให้ผลที่ต่างกันด้วย ซึ่งได้ผลตามที่ต้องการ

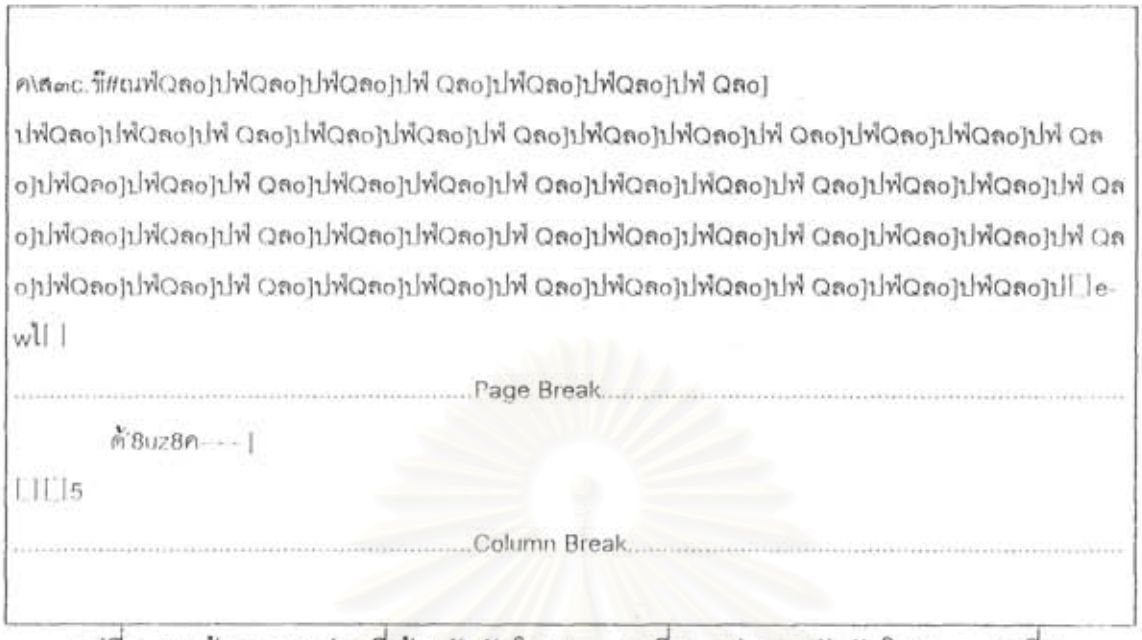
หลังจากนั้นได้นำข้อมูลมาถอดรหัสลับ โดยใช้ key เดิม และ key สลับกัน :ซึ่งเมื่อใช้ key เดิมถอดรหัสลับจะได้ข้อมูลเหมือนกัน ดังแสดงในรูปที่ 4.14 แต่เมื่อใช้ key สลับกัน คือใช้ key ชุดที่ 2 ถอดรหัสลับข้อมูลที่เข้ารหัสลับด้วย key ชุดที่ 1 และใช้ key ชุดที่ 1 ถอดรหัสลับข้อมูลที่เข้ารหัสลับด้วย key ชุดที่ 2 จะได้ผลดังในรูปที่ 4.15 และ 4.16 ตามลำดับ

ความรู้ทางวิทยาศาสตร์และเทคโนโลยี มีบทบาทสำคัญยิ่งต่อการพัฒนาเศรษฐกิจและอุตสาหกรรมของประเทศ และในการวางรากฐานความรู้ทางวิทยาศาสตร์และเทคโนโลยีเพื่อเตรียมบุคลากรให้มีความพร้อมสำหรับรองรับการพัฒนาดังกล่าวจำเป็นต้องอาศัยสื่อที่มีประสิทธิภาพ ทั้งนี้ หนังสือ ตำรา นับเป็นสื่ออันสำคัญอย่างหนึ่ง แต่ปัญหาก็คือ เรายังขาดแคลนตำราทางวิทยาศาสตร์และเทคโนโลยีที่เป็นภาษาของเราเอง จริงอยู่ แม้ในปัจจุบันเราจะมีตำราภาษาไทยมากขึ้นมากกว่าเมื่อสิบปีที่แล้ว แต่ก็ยังนับว่าไม่มากพอ เมื่อเทียบกับความก้าวหน้าทางวิทยาการที่รุดหน้าไปอย่างไม่หยุดยั้ง

รูปที่4.14 ข้อมูลที่ถอดรหัสลับออกมาโดยใช้ key เดิม

□&n#□&n#□&n#□&n#□&n#□&n#□&n#□&n#□&n#□&n#□&n#□&n#□&n#□&n#
n#□&n#□&n#□&n#□&n#□&n#□&n#□&n#□&n#□&n#□&n#□&n#□&n#□&n##□&n
#□&n#□&n#□&n#□&n#□&n#□&n#□&n#□&n#□&n#□&n#□&n#□&n##□&n#□&n
#□&n#□&n#□&n#□&n#□&n#□&n#□&n#□&n#□&n#□&n#□&n###□&u□
.....Page Break.....
ญฎฎ&๔/ฝ=ถ6ศีi>>□นcF>>□นcF>>□นcF>>□นcF>>□นcF>>□นcF>>□นcF>>□นc
F>>□นcF>>□นcF>>□นcF>>□นcF>>□นcF>>□นcF>>□นcF>>□นcF>>□นcF>>□นc

รูปที่ 4.15 ข้อมูลบางส่วนที่เข้ารหัสลับโดย key ชุดที่ 1 แต่ถอดรหัสลับโดย key ชุดที่ 2



รูปที่ 4.16 ข้อมูลบางส่วนที่เข้ารหัสลับโดย key ชุดที่ 2 แต่ถอดรหัสลับโดย key ชุดที่ 1

จากผลในรูปที่ 4.14 4.15 และ 4.16 แสดงให้เห็นว่า DES software สามารถถอดรหัสลับข้อมูลได้ถูกต้องได้เป็นข้อมูลเดิมกลับมา ในขณะที่การใช้ key ผิดๆ จะทำให้ไม่สามารถถอดรหัสลับกลับคืนมาได้ แสดงว่าข้อมูลมีความปลอดภัย ถ้า key ยังถูกรักษาไว้เป็นความลับได้

ในการเข้ารหัสลับนั้น ข้อมูลหลังการเข้ารหัสลับแล้วจะมีขนาดใหญ่ขึ้น ซึ่งได้แสดงข้อมูลบางส่วนไว้ ทั้งนี้เนื่องมาจากในขั้นตอนการเข้ารหัสลับจะทำการดึงข้อมูลมาเข้ารหัสลับครั้งละ 8 ไบต์ (64บิต) ถ้าข้อมูลไม่ครบ 8 ไบต์ DES software จะทำการเติมข้อมูลด้วยตัวว่างจนครบ 8 ไบต์ ดังนั้นขนาดของแฟ้มข้อมูลจึงอาจเพิ่มขึ้นได้ และจะเพิ่มเป็นขนาดที่หารด้วยเลข 8 ลงตัว

4.4 การทดสอบการเข้ารหัสลับและถอดรหัสลับข้อมูลภาษาไทยใน key mode อื่นๆ

การเข้ารหัสลับและถอดรหัสลับข้อมูลที่เป็นภาษาไทยในกรณีที่ใช้ 1 key mode นั้น สามารถกระทำได้เช่นเดียวกับข้อมูลที่เป็นภาษาอังกฤษดังที่ได้แสดงให้ดูแล้วในหัวข้อที่ผ่านมา ในหัวข้อนี้จะแสดงผลของการเข้ารหัสลับและถอดรหัสลับข้อมูลที่เป็นภาษาไทย ใน key mode อื่นๆของโปรแกรม อันได้แก่แบบ 4, 8 และ 16 key mode ซึ่งจะได้ผลเป็นดังตัวอย่างต่อไปนี้ คือ

สมมติว่าข้อมูลที่ต้องการจะทำการเข้ารหัสลับเป็นดังรูปที่ 4.17 โดยถูกเก็บไว้ในแฟ้มข้อมูลชื่อ DEARN.TXT เมื่อสั่งให้โปรแกรมทำการเข้ารหัสลับข้อมูลโดยใช้ 4 key mode อันได้แก่

DEARN1 , DEARN2 , DEARN3 และ DEARN4 แล้วเก็บข้อมูลที่ถูกเข้ารหัสลับแล้ว ไว้ในแฟ้มข้อมูลชื่อ DEARN.DES จะได้ส่วนหนึ่งของข้อมูลในแฟ้มข้อมูลนี้แสดงอยู่ในรูปที่ 4.18

เดิน เดิน เถิดเรานิสิตมหาจุฬาลงกรณ์
เดิน เดิน พร้อมหน้าเพื่อนำชัยมาจุฬาลงกรณ์
ชโย ชโยจุฬาฯ สถานศึกษาสง่าพระนาม
ใครจะหยามเหยียดจุฬาฯ เราอย่ายอม เราอย่ายอม
ชิงเถิดชิงเอาชัยชิงด้วยน้ำใจเป็นนักกีฬา
เชียร์เถิดเราเชียร์ให้บำรุงน้ำใจพวกเราจุฬาฯ
พลีเถิดพลีกายพร้อมเลือดเนื้อเรายอมยกให้จุฬาฯ
จงมุ่งหน้าพาเอาชัยให้จุฬาฯ ให้จุฬาฯ

รูปที่ 4.17 ข้อมูลที่ต้องการจะทำการเข้ารหัสลับ

~สีHtNq-
~สีHtNq-
.....Column Break.....
~สีHtNq-
~บ๓ฑ~Cๆม
.....Page Break.....
QคZ[—CdZ~แ~)
~สีHtNq-" ~■ขkที่ลๆZ4ถZX~iA~—\Hฤ
~/~ต~~l'ฺ ~0%Q□"๒ผม.ร-M]'~c□~e
c~ฎkl ผ~ภกฯ•ฎ~&!&D=-)ภๆwใ
.....Column Break.....
~Yฯ%Mc~ฒZฎๆภ
H'ทณ~B๑หทTญoYฬ
.....Column Break .....
J;Ã๒kC•ฯ

รูปที่ 4.18 ส่วนหนึ่งของแฟ้มข้อมูล DEARN.DES

ซึ่งจะเห็นว่าข้อมูลที่ถูกเข้ารหัสลับแล้วมีความปลอดภัยตามต้องการ และแม้ว่าแฟ้มข้อมูลนี้จะมีขนาดหลายร้อยหน้า แต่ก็ใช้เนื้อที่ในหน่วยความจำเพียง 7,168 bytes เช่นเดียวกับแฟ้มข้อมูล DEARN.TXT ส่วนเมื่อต้องการถอดรหัสลับข้อมูลก็สามารถทำได้โดยใช้ key 4 ตัวเดิม โดยเรียงลำดับอย่างเดิม ซึ่งจะทำให้ได้ข้อมูลที่ต้องการเหมือนเดิมทุกประการดังแสดงในรูปที่ 4.19

เดิน เดิน เถิดเรานิ สิตมหาจุฬาลงกรณ์
เดิน เดิน พร้อมหน้าเพื่อนำชัยมาจุฬาลงกรณ์
ชโย ชโยจุฬาฯ สถานศึกษาสง่าพระนาม
ใครจะหยามเหยียดจุฬาฯ เราอย่ายอม เราอย่ายอม
ชิงเถิดชิงเอาชัยชิงด้วยน้ำใจเป็นนักกีฬา
เชียร์เถิดเราเชียร์ให้บำรุงน้ำใจพวกเราจุฬาฯ
พลีเถิดพลีกายพร้อมเลือดเนื้อเรายอมยกให้จุฬาฯ
จงมุ่งหน้าพาเอาชัยให้จุฬาฯ ให้จุฬาฯ

รูปที่ 4.19 ข้อมูลที่ได้จากการถอดรหัสลับด้วยวิธีที่ถูกต้อง

โดยการเรียงลำดับ key ที่ใช้ในการถอดรหัสลับ จะต้องเหมือนกับตอนที่ทำการเข้ารหัสลับข้อมูลด้วย มิเช่นนั้นแล้วข้อมูลที่ได้จะไม่ใช่ข้อมูลที่ต้องการ ตัวอย่างเช่น หากทำการถอดรหัสลับด้วย key เป็น DEARN1 DEARN2 DEARN4 และ DEARN3 ตามลำดับ จะทำให้ได้ข้อมูลที่ถูกถอดรหัสลับโดยรวมแล้วเป็นดังรูปที่ 4.20

#ฒ9~&yเ๊Fฎvl$□UW]□:ภูภ฿iFy]gู๋#□' o8W๔ ด๒="pE□ไ^ฑOOก »kE-□oq-~ť□ฎp๔
"ฑ—ฎฮ

....Page Break..

[=ฤ`ทฯ□ู๊□ฟบ์□ฒๆฟ□□3-ะ่ว"T`6ะ□vq9ษมฮ~พ'น๊!jข4ไ๑ค"—@9□@□-ำ 0-ล□ีำดF
..-#ล๊ เขส๓ต่ฯ□?k□ภ(@□Qฤ7แtฉ๙ไ<>ฒ่ำ3-\□W□น๔?+รPu|ฎ้4฿v
ฎธ;Nด□+จmวกี•□'๓ธdy

....Column Break..

ฝโPอt๒□'โPอt๒

....Column Break..

□'โPอt๒

□'โPอt๒

....Column Break..

□'โPอt๒

□'โPอt๒

□'โPอt๒

□'โPอt๒

□'โPอt๒

□'โPอt๒

□'โPอt๒

□'ร"ฒม□กKคN» !ซไ5□ซว!O>พc~ง□J้ก□ห;~ศ» ธข&"□□

....Page Break..

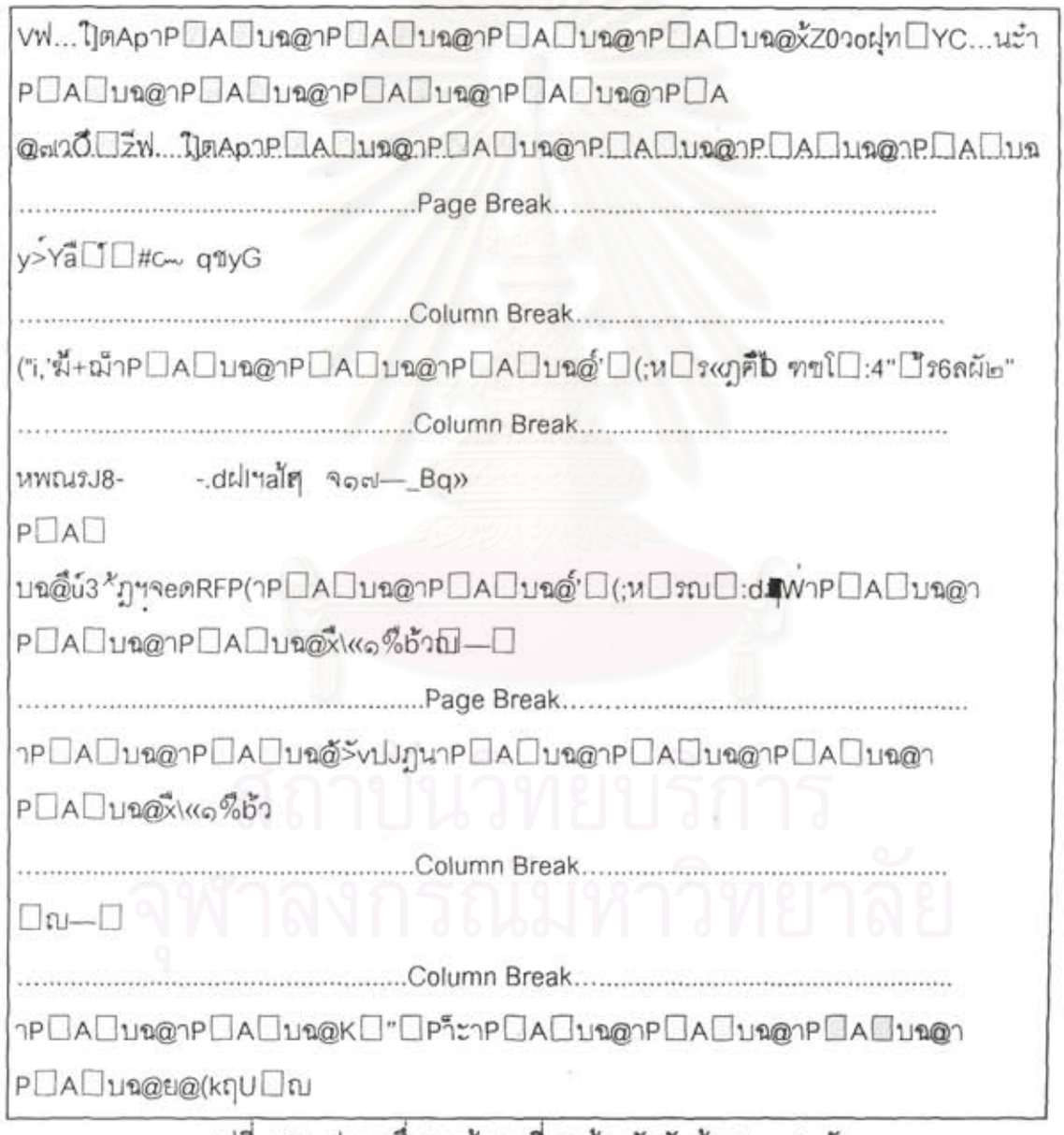
C้มษป้ฒ]6;h๑tฎ□X6า□฿□๖prศฑlษ฿hฎ<ล่ร□ม%ข๊ฮXต2ม่□โด A □ฟ
FM3□□□

....Column Break..

3□* □า□pooฒจ๔๑ฌภมศ□□จ□-ถ□+ฝดี๒ O ตฉไf๖ฌwv-ถ□+ผ"zK(\X ถ□ +ผ-
ถ□+ผถ□ +ผ-

รูปที่ 4.20 ส่วนหนึ่งของข้อมูลที่ได้จากการเรียงลำดับ key ผิด

สำหรับ key mode ที่เหลือคือแบบ 8 และ 16 key mode นั้นก็สามารถใช้ในการเข้ารหัสข้อมูลลับได้ด้วยวิธีการเดียวกันกับแบบ 4 key mode เช่นกัน โดยที่จะทำให้ข้อมูลที่ถูกเข้ารหัสลับมีความปลอดภัยมากขึ้นตามลำดับ ส่วนหนึ่งของข้อมูลที่เข้ารหัสลับแล้วด้วยการใช้ key 8 และ 16 ตัว จะเป็นดังแสดงในรูปที่ 4.21 และรูปที่ 4.22 ตามลำดับ โดยแฟ้มข้อมูลที่เก็บข้อมูลทั้งสองนี้ก็มีขนาด 7,168 bytes เช่นเดียวกัน และเมื่อถูกถอดรหัสลับด้วย key ลำดับที่ถูกต้องแล้ว ก็จะได้ข้อมูลที่เหมือนกับข้อมูลเดิมทุกประการตามต้องการ



รูปที่ 4.21 ส่วนหนึ่งของข้อมูลที่ถูกเข้ารหัสลับด้วย key 8 ตัว

w* _cฬ:ฆแจฺ\j5ใ๏

....Column Break...

ษซ41ฒง 0...นa-? □pไA๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□

....Page Break...

๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถ

!ฬ«ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ

□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถ

!ฬ«ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ

□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□๊ัถฬ «ฎ□

๊ัถฬ «ฎ□๊ัถ -ห;ดเ□--ศี□"□IJJป□k□E□ñuUพ□#ฦA—:Uพ□#ฦA—:Uพ□#ฦA—:Uพ

□#ฦA—:Uพ□

....Page Break...

#ฦA—:5̈ ̃ดซ๋+>zlหิ"̧

....Page Break...

๓'ยค}5□ไ งUพ□#ฦA—:-̇☑ พ่G ์ั่ไม่ ฐณ ̃า;ภḄ□cปnธฒง3□Cฦ ค๋ Uพ□#ฦA—:Uพ

□#ฦA—:Uพ□#ฦA—:Uพ□#ฦA—:Uพ□#ฦA—:Uพ□#ฦA—:ฆh%L]]Fxฬ«ฎ□๊ัถUพ

□#ฦA—:Uพ□#ฦA—:Uพ□#ฦA—:Uพ□#ฦA—:Uพ□#ฦA—:ฌม□ ฯฉ\\bฆ1;□ḳ

....Column Break...

□P□ม5□ดยไ

....Column Break...

`Uพ□#ฦA—:Uพ□#ฦA—:Uพ□#ฦA—:Uพ□#ฦA—:Uพ□#ฦA—̄:T□□q<□□N๒G&ถ

:ฤ่Uพ□#ฦA—:Uพ□#ฦA—:Uพ□#ฦA—:Uพ□#ฦA—:ไ□"pJฒ7โYภ□Kďc̈:p๑h_ฝฺ๑ฎ

Ė๑ฮส้j□

Uพ□#ฦA—:Uพ□#ฦA—:Uพ□#ฦA—:Uพ□#ฦA—:Uพ□#ฦA—:VMHิto๖ฆ่xห์—□t\Uพ

□#ฦA—:U

....Page Break...

รูปที่ 4.22 ส่วนหนึ่งของข้อมูลที่ถูกเข้ารหัสลับด้วย key 16 ตัว

4.5 สรุปผลการทดสอบโปรแกรม

ผลการทดสอบโปรแกรมนั้นอาจจะสรุปได้ดังนี้

1. การทดสอบการเข้ารหัสลับและถอดรหัสลับใน 1 key mode

จากผลการทดสอบแสดงให้เห็นว่า

1.1 โปรแกรมใน 1 key mode สามารถทำการเข้ารหัสลับข้อมูลที่เป็น textfile ภาษาอังกฤษและภาษาไทยได้ และทำการถอดรหัสลับข้อมูลกลับคืนมาได้อย่างถูกต้อง

1.2 ในการเข้ารหัสลับ การใช้ key ที่แตกต่างกันจะให้ข้อมูลที่เข้ารหัสลับแล้วไม่เหมือนกัน ซึ่งแสดงว่าโปรแกรมนำ key ไปใช้ในการเข้ารหัสลับ ทำให้มีผลต่อข้อมูลที่เข้ารหัสลับแล้ว

1.3 การถอดรหัสลับข้อมูลโดยใช้ key ที่สลับกันจะไม่สามารถถอดรหัสลับกลับคืนมาได้ถูกต้อง แสดงว่าการเข้ารหัสลับโดยโปรแกรมสามารถให้ความปลอดภัยแก่ข้อมูลได้

2. การทดสอบการเข้ารหัสลับและถอดรหัสลับใน key mode อื่นๆ

จากการทดสอบตอนแรก แสดงให้เห็นว่าใน 1 key mode โปรแกรมสามารถเข้ารหัสลับและถอดรหัสลับข้อมูลได้ถูกต้อง จึงใช้ข้อมูลที่ผ่านการเข้ารหัสลับในตอนที่ 1 ในการเปรียบเทียบผลในการทดสอบนี้ ซึ่งอาจสรุปผลได้ดังนี้

2.1 จากการทดสอบโดยใช้ key ที่เหมือนกันทั้งหมดในการเข้ารหัสลับในแต่ละ key mode จะได้ข้อมูลที่เข้ารหัสลับแล้วเหมือนกัน แสดงให้เห็นว่า ทุก key mode สามารถนำ key ที่รับเข้ามาไปใช้ทำการเข้ารหัสลับได้อย่างถูกต้องเหมือนกับใน 1 key mode

2.2 เมื่อทำการถอดรหัสลับโดยใช้ key เดิมจะสามารถถอดรหัสลับข้อมูลออกมาได้อย่างถูกต้อง แต่เมื่อใช้ key ผิดไป 1 ตัวอักษร(ในทุก key mode) จะไม่สามารถถอดรหัสลับข้อมูลออกมาได้อย่างถูกต้อง แสดงว่าการเข้ารหัสลับโดยใช้โปรแกรม DES software สามารถให้ความปลอดภัยกับข้อมูลได้ ไม่ว่าจะเป็น key mode ใดก็ตาม ข้อมูลที่เข้ารหัสลับแล้วจะมีความปลอดภัยตราบเท่าที่ key ยังถูกเก็บรักษาไว้เป็นความลับได้

2.3 จากการที่เมื่อใช้ key เหมือนกันหมดในการเข้ารหัสลับ ทำให้ได้ข้อมูลที่เข้ารหัสลับแล้วเหมือนกัน ทำให้พบข้อสังเกตที่น่าสนใจคือการใช้ key mode เช่น 16 key mode ซึ่งจะใช้ key ในการเข้ารหัสถึง 16 ตัว ถ้าใช้ key ที่เหมือนกันหมดทุกชุด ก็จะให้ผลที่เหมือนกับการใช้ 1 key mode หรือ key เดียวในการเข้ารหัสลับ นั่นคือข้อมูลก็จะมีความปลอดภัยน้อยลงกว่าที่ควร

จะเป็น ใน key mode อื่นๆ ก็เช่นเดียวกัน ดังนั้นการที่จะเข้ารหัสลับโดยใช้ key หลายๆ ตัว จะให้ความปลอดภัยได้สูงที่สุดเมื่อใช้ key ในการเข้ารหัสลับที่ต่างกันทั้งหมดทุก key

นอกจากนี้ในระหว่างทำการทดสอบนั้น จะใช้โปรแกรมทดสอบโดยตรง ทำให้สามารถเห็นการทำงาน การรับคำสั่งและการแสดงผลให้ผู้ใช้ทราบ ซึ่งหลังจากผ่านการทดสอบและแก้ไขข้อผิดพลาดแล้ว โปรแกรมสามารถทำงาน โต้ตอบกับผู้ใช้ได้ดี รวมทั้งเวลาในการเข้ารหัสลับและถอดรหัสลับข้อมูล textfile ขนาดใหญ่ (เช่น 15,000 ไบต์ขึ้นไป) โปรแกรมสามารถทำได้โดยใช้เวลาเพียงเล็กน้อย แสดงว่าการทำงานของโปรแกรมเป็นไปอย่างถูกต้องตามที่กำหนดไว้

บทที่ 5
บทสรุปและข้อเสนอแนะ

จากผลการทดสอบการเข้ารหัสลับและถอดรหัสลับของโปรแกรมนั้น แสดงให้เห็นว่า DES software ที่สร้างขึ้น สามารถเข้ารหัสลับและถอดรหัสลับข้อมูลที่เป็น textfile ภาษาไทยและภาษาอังกฤษได้อย่างถูกต้อง ข้อมูลที่เข้ารหัสลับแล้วมีลักษณะที่ต่างไปจากข้อมูลเดิมและไม่สามารถตีความได้ การถอดรหัสลับโดยใช้ key ผิดไปจากเดิมแม้เพียงตัวอักษรเดียว ก็ทำให้ไม่สามารถถอดรหัสลับข้อมูลออกมาได้ ข้อมูลจึงมีความปลอดภัยตราบเท่าที่ key ยังถูกเก็บรักษาไว้เป็นความลับ ตรงกับคุณสมบัติของ algorithm การเข้ารหัสลับแบบ Data Encryption Standard หรือ DES

สำหรับในส่วนของการแสดงผลและติดต่อกับผู้ใช้นั้น โปรแกรมสามารถทำงานได้อย่างถูกต้อง ซึ่งอาจดูได้จากการที่สามารถรับคำสั่งจากผู้ใช้และทำการเข้ารหัสลับและถอดรหัสลับข้อมูลได้ตามต้องการ DES software จึงสามารถทำงานได้ตามเป้าหมายที่ตั้งไว้

อย่างไรก็ตามก็ยังมีข้อจำกัดบางประการใน DES software release 1.0 นี้ ซึ่งอาจจะสรุปเป็นข้อๆ พร้อมกับแนวทางในการปรับปรุงได้ดังนี้

1. ใน DES software release 1.0 นี้ ได้ทำการกำหนดให้สามารถเข้ารหัสลับข้อมูลได้เฉพาะที่เป็น textfile อย่างเดียวเท่านั้น แต่อันที่จริงสามารถใช้งานกับข้อมูลในลักษณะอื่นๆ ได้ ไม่จำกัดเฉพาะข้อมูลที่เป็น textfile อย่างเดียวเท่านั้น ซึ่งที่ได้ทำการกำหนดเช่นนี้ไว้เพราะ การเข้ารหัสลับข้อมูลประเภทอื่นนั้น จะเห็นผลของการเข้ารหัสลับว่าถูกต้องหรือไม่ได้ยาก ต่างไปจากข้อมูลที่เป็น textfile ที่สามารถแสดงออกมาให้เห็นได้ แต่ถ้าเราสามารถทำการตรวจสอบการเข้ารหัสลับในข้อมูลชนิดอื่นว่าถูกต้องหรือไม่ ก็จะสามารถพัฒนาให้โปรแกรมใช้งานกับข้อมูลประเภทอื่นๆ ได้อีก ซึ่งโดยตัวของ algorithm ในการเข้ารหัสลับนั้นสามารถทำได้อยู่แล้ว

2. เนื่องจาก DES software นั้นเป็นโปรแกรมที่ทำงานบน DOS ใน Text Mode ดังนั้นรูปแบบของโปรแกรมจึงยังอยู่ในรูปที่ไม่สะดวก ทั้งต่อการใช้งานและการพัฒนาโปรแกรมต่อไป ยกตัวอย่างเช่น ไม่สามารถแสดงข้อมูลที่เป็นภาษาไทยได้ ดังนั้นถ้าสามารถพัฒนาให้ทำงานใน Graphic Mode ได้ ก็จะเป็นประโยชน์มากกว่านี้ ยกตัวอย่างเช่น ถ้าสามารถทำการปรับปรุงให้ใช้บนโปรแกรม Windows ได้ ก็จะสามารถแสดงข้อความเป็นภาษาไทยได้ การใช้งานก็จะง่ายขึ้น

นอกจากนี้ยังอาจจะนำเข้าไปเป็นส่วนหนึ่งของระบบการทำงาน ที่มีการส่งข้อมูลระหว่างระบบโครงข่าย เช่น การส่ง E-mail หรือ โปรแกรม application ต่างๆ ในระบบ Internet ก็จะช่วยให้การส่งข้อมูลผ่านโครงข่ายมีความปลอดภัยมากขึ้น

3. ในส่วนของการแสดงข้อมูลใน Display mode ของโปรแกรม ยังใช้ประโยชน์ได้ไม่เต็มที่ เพราะยังไม่สามารถแสดงข้อมูลที่มีขนาดใหญ่เกินกว่า 7,000 ไบต์ได้ จึงอาจจะต้องมีการปรับปรุงให้สามารถแสดงข้อมูลที่ใหญ่กว่านี้ได้ และอาจจะเพิ่มให้สามารถทำการแก้ไขข้อมูลได้ด้วย

4. อาจจะทำการเพิ่มเติมส่วนที่ช่วยอำนวยความสะดวกแก่ผู้ใช้มากขึ้น เป็นต้นว่า สามารถพิมพ์ key ที่ใช้ในการเข้ารหัสลับออกมาให้ผู้ใช้ได้ หรือสามารถพิมพ์ข้อมูลที่ทำการถอดรหัสลับแล้ว ออกมาให้ผู้ใช้ได้เป็นต้น

เอกสารอ้างอิง

1. Charles P. Pfleeger, Security in Computing , Prentice-Hall International Editions , U.S.A., 1989
2. มนตรี พจนารถลาวัณย์ , การเขียนโปรแกรมคอมพิวเตอร์ด้วยเทอร์โบซี , บริษัท ซีเอ็ดยูเคชั่น จำกัด , ไทย , 2535
3. Hervert Schildt, Teach Yourself C++ , Osborne/McGraw-Hill , U.S.A., 1992