บทที่ 6

การทดสอบการทำงาน

การทดสอบความเร็วในการเข้ารหัสของ DES ในโหมดต่าง ๆ

เพื่อให้ทราบถึงเวลาที่ต้องใช้ในการเข้ารหัสและถอดรหัสสำหรับ DES ในโหมดต่าง ๆ

1. รูปแบบการทดสอบ

การทดสอบนี้จะใช้ไฟล์ขนาดต่าง ๆ ที่มีขนาดประมาณ 5 กิโลไบท์ ถึง 40 กิโลไบท์ มาเป็นตัวอย่างในการทดสอบ โดยทำการทดสอบขณะเข้ารหัสในโหมดต่าง ๆ และบันทึกค่าเวลาที่ใช้ในการเข้ารหัสจริง โดยการจับเวลาเปรียบเทียบกับเวลาโดยประมาณที่แสดงผลทางโปรแกรม

2. ผลการทดสอบ

ผลการทดสอบแสดงดังตาราง 6.1-6.4

ตาราง 6.1 ผลการทดสอบเวลาที่ใช้ในการเข้ารหัสในโหมด ECB

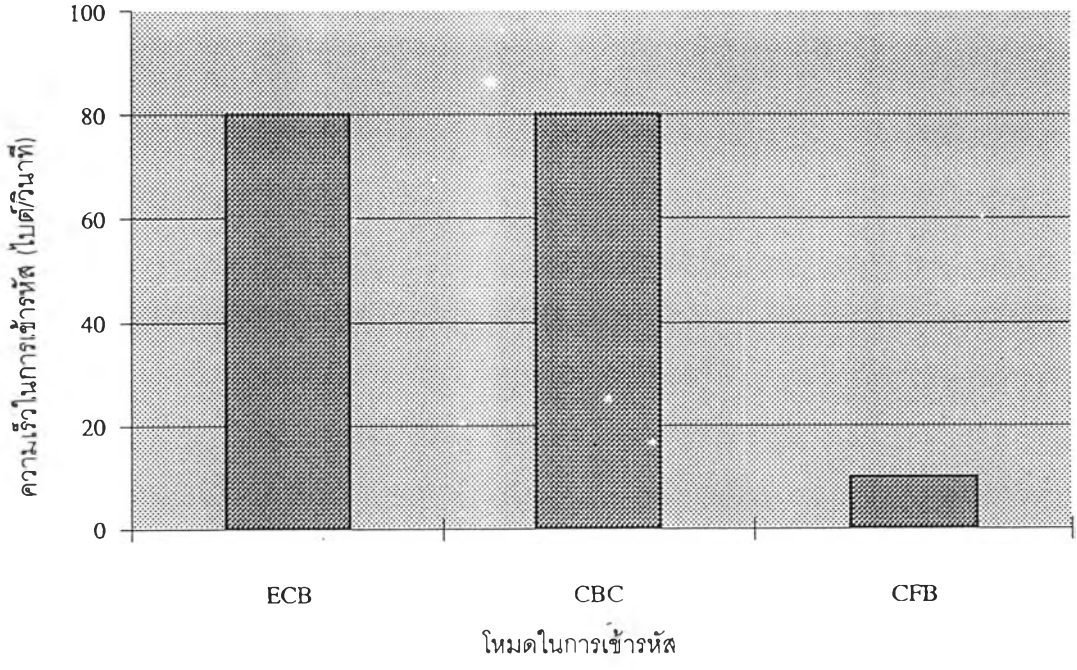
ECB			
ขนาด (กิโลไบต์)	**เวลาที่แสดง** (วินาที)	**เวลาจากการจับเวลา** (วินาที)	**ความเร็วในการเข้ารหัส** (ไบต์/วินาที)
5	64	64.2	79.8
10	128	128.9	79.4
15	192	193.4	79.4
20	256	258.8	79.1
25	320	324.4	79.9
30	384	386.6	79.5
35	448	451.6	79.4
40	512	515.5	79.5
		เฉลี่ย	79.4

ตาราง 6.2 ผลการทดสอบเวลาที่ใช้ในการเข้ารหัสในโหมด CBC

CBC			
ขนาด (กิโลไบต์)	**เวลาที่แสดง** (วินาที)	**เวลาจากการจับเวลา** (วินาที)	**ความเร็วในการเข้ารหัส** (ไบต์/วินาที)
5	64	64.6	79.3
10	128	129.2	79.3
15	192	193.8	79.3
20	256	259.1	79
25	320	326.8	78.3
30	384	390.1	78.7
35	448	453.4	79
40	512	516.9	79.2
		เฉลี่ย	79

ตาราง 6.3 ผลการทดสอบเวลาที่ใช้ในการเข้ารหัสในโหมด CFB

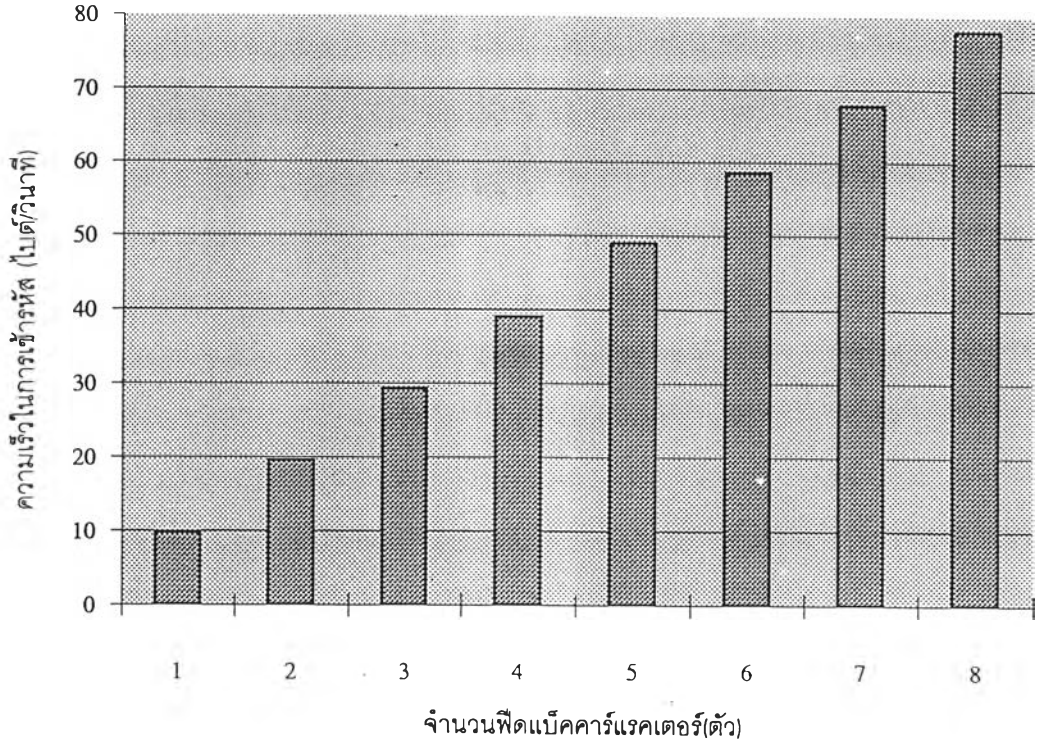
CFB			
ขนาด (กิโลไบต์)	**เวลาที่แสดง** (วินาที)	**เวลาจากการเวลา** (วินาที)	**ความเร็วในการเข้ารหัส** (ไบต์/วินาที)
0.5	51.2	52.4	9.8
1	102.4	105.6	9.7
1.5	153.6	159.4	9.6
2	204.8	210.4	9.7
2.5	256	267.1	9.6
3	307.2	320.4	9.6
3.5	358.4	371.2	9.7
4	409.6	421.3	9.7
		เฉลี่ย	9.7



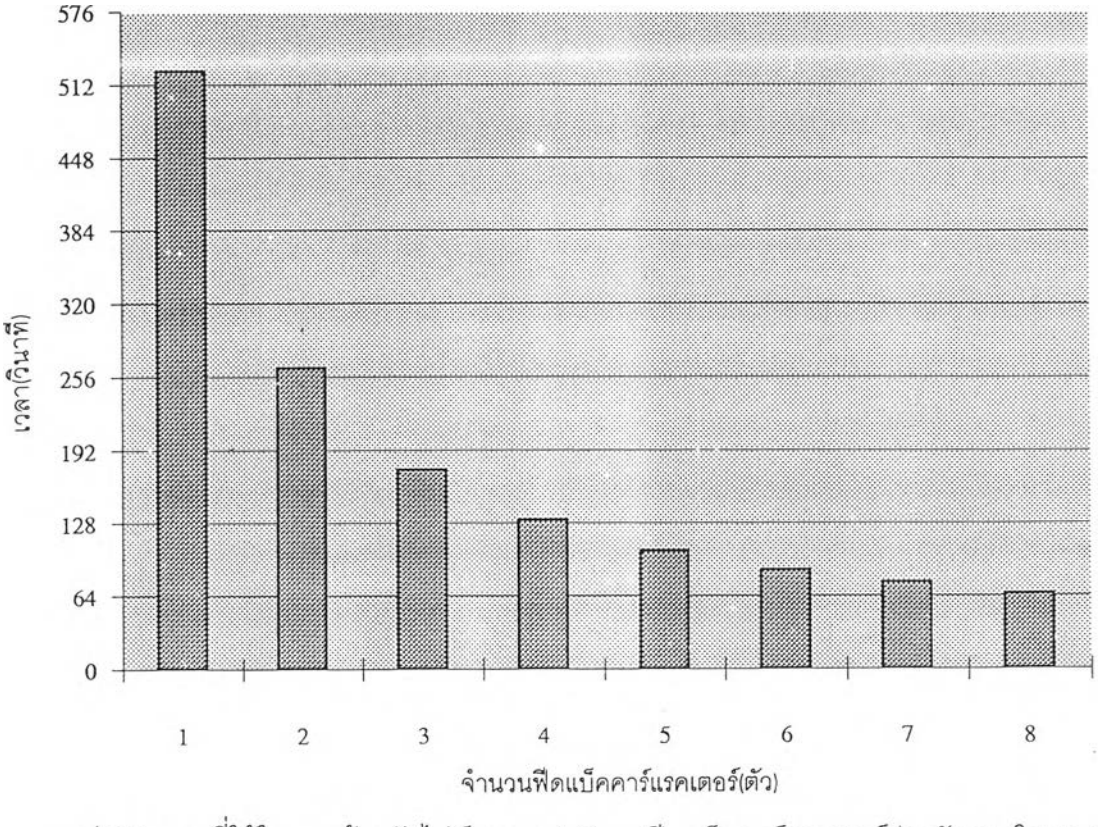
รูป 6.1 ความเร็วในการเข้ารหัสของโหมด EBC,CBC และ CFB

ตาราง 6.4 ผลการทดสอบเวลาที่ใช้ในการเข้ารหัสในโหมด OFB

OFB				
ขนาด (กิโลไบต์)	**จำนวนที่ป้อนกลับ** (ไบต์)	**เวลาที่แสดง** (วินาที)	**เวลาจากการจับเวลา** (วินาที)	**ความเร็วในการเข้ารหัส** (ไบต์/วินาที)
5	1	512	524.4	9.7
5	2	256	261.9	19.5
5	3	170.7	174.8	29.3
5	4	128	131.4	39
5	5	102.4	104.4	49
5	6	85.3	87.4	58.6
5	7	73.1	75.5	67.8
5	8	64	65.6	78



รูป 6.2 ความเร็วในการเข้ารหัสของโหมด OFB ที่ป้อนกลับด้วยฟีดแบ็คคาร์แรคเตอร์ค่าต่างๆ



รูป 6.3 เวลาที่ใช้ในการเข้ารหัสไฟล์ขนาดเท่ากันแต่ฟีดแบ็คคาร์แรคเตอร์ต่างกันของโหมด OFB

จากตารางจะเห็นว่าเวลาที่ใช้ในการเข้ารหัสในโหมด ECB และ CBC มีค่าประมาณ 80 ไบท์ต่อวินาที ในโหมด CFB ประมาณ 10 ไบท์ต่อวินาทีเท่านั้น เนื่องจากจะต้องมีการฟีดแบ็คไซเฟอร์เท็กซ์ กลับมาเข้ารหัสถึง 8 ครั้งต่อ 1 บล็อคของเพลนเท็กซ์ (64 บิต) ทำให้ความเร็วลดลง 8 เท่า ในส่วนของ OFB นั้น ความเร็วของการเข้ารหัสขึ้นอยู่กับจำนวนของฟีดแบ็คคาร์แรคเตอร์ที่เราป้อนเข้าไป ถ้าหากว่าฟีดแบ็คคาร์แรคเตอร์มีค่าเท่ากับ 1 หมายความว่าจะฟีดแบ็ค เอาท์พุท เข้าทำการเข้ารหัสทีละไบต์ ดังนั้นจึงต้องทำการเข้ารหัส 8 ครั้ง เช่นเดียวกับ CFB

ความเร็วของการเข้ารหัสในโหมด OFB หาได้จาก

$$\text{ความเร็วของการเข้ารหัส} = \frac{\text{จำนวนของฟีดแบ็คคาร์แรคเตอร์} * 80}{8} \quad \text{ไบท์ต่อวินาที}$$

สำหรับเวลาที่ใช้จริงมีค่ามากกว่าเวลาที่แสดงผลตามโปรแกรม เนื่องจากเวลาที่แสดงผลในโปรแกรมนั้นหาได้จากการที่นำเอาค่าความเร็วในการเข้ารหัส ซึ่งบอกไว้ในคู่มือการใช้งาน IC 8294 ซึ่งมีค่า 80 ไบท์ต่อวินาทีเป็นตัวหารขนาดไฟล์แต่ในการใช้งานจริงนั้นจะต้องมีการอ่านและเขียนข้อมูล ของฟลอปปีดิสค์และฮาร์ดดิสค์ทำให้ต้องใช้เวลามากขึ้น อย่างไรก็ตามจากผลการทดสอบสามารถสรุปได้ว่าความเร็วในการเข้ารหัสมีค่าใกล้เคียงกับความสามารถสูงสุดของ IC 8294

<u>การทดสอบการทำงานต่อเนื่อง</u>

เป็นการทดสอบความสามารถในการทำงานแบบต่อเนื่อง เพื่อให้ทราบถึงเสถียรภาพของเครื่องเข้ารหัส ในกรณีที่ไฟล์ที่จะทำการทดสอบมีขนาดใหญ่ ซึ่งต้องใช้เวลาในการเข้ารหัสนาน จึงจำเป็นต้องการมีการทดสอบคุณสมบัตินี้

1. รูปแบบในการทดสอบ

วิธีการทดสอบทำได้โดยการทดสอบเข้ารหัสรหัสไฟล์ที่มีขนาดประมาณ 32 กิโลไบต์ เป็นจำนวน 20 ครั้ง โดยใช้ทุกโหมดการทำงาน แล้วบันทึกเวลาที่ใช้และข้อผิดพลาดที่เกิดขึ้น

2. ผลการทดสอบ

ตาราง 6.5 แสดงผลการทดสอบการทำงานต่อเนื่อง

ครั้งที่	โหมด							
	ECB		CBC		CFB*		OFB**	
	เวลา	ผิดพลาด***	เวลา	ผิดพลาด	เวลา	ผิดพลาด	เวลา	ผิดพลาด
1	410.2	-	412.4	-	412.8	-	414.4	-
2	411.1	-	412.8	-	412.6	-	414.2	-
3	411.8	-	413.3	-	413.4	-	414.8	-
4	410.8	-	412.8	-	413.3	-	414.5	-
5	411.3	-	414.1	-	412.6	-	415.6	-
6	410.4	-	412.5	-	413.1	-	414.8	-
7	410.3	-	413.4	-	413.2	-	xxx	x
8	410.8	-	413.8	-	414.4	-	414.6	-
9	411.2	-	414.1	-	xxx	x	415.2	-
10	411.4	-	413.8	-	413.2	-	414.8	-

* MODE CFB ใช้ไฟล์ขนาด 4 กิโลไบท์

** MODE OFB ใช้ไฟล์ขนาด 4 กิโลไบท์ และฟีดแบ็คคาร์แรคเตอร์เท่ากับ 1

*** เครื่องเข้ารหัสข้อมูลทำงานต่อเนื่องแล้วทำให้คอมพิวเตอร์ค้าง (Hang)

จากตาราง 6.5 จะเห็นว่าการทำงานต่อเนื่องของคาร์ดในโหมดของ ECB และ CBC จะไม่เกิดข้อผิดพลาดขึ้น แต่ในโหมด CFB และ OFB จะเกิดข้อผิดพลาดขึ้นในครั้งที่ 9 และ 7 ตามลำดับ สาเหตุเนื่องจาก ใน 2 โหมด นี้มีการประมวลผลข้อมูลภายใน IC 8294 เป็นจำนวนมากกว่าใน ECB และ CBC ดังนั้นโอกาสที่จะเกิดข้อผิดพลาดของวงจรควบคุมทิศทางการส่งถ่ายข้อมูลหรือสัญญาณการรับและส่งข้อมูลระหว่างคอมพิวเตอร์และเครื่องเข้ารหัสข้อมูลทำงานไม่เข้าเข้าจังหวะกันจึงมีมากกว่า กล่าวโดยสรุปคือ ไฟล์ที่มีขนาดประมาณ 32 กิโลไบต์เมื่อนำมาเข้ารหัสในโหมด CFB และ OFB จะมีโอกาสผิดพลาดประมาณ 10 %

การทดสอบความเชื่อถือได้ (Reliability) ของเครื่องเข้ารหัส

เป็นการทดสอบความเชื่อถือได้ของการเข้าและถอดรหัสของเครื่องเข้ารหัส เพื่อให้เกิดความมั่นใจว่าทุก ๆ ครั้งเมื่อเข้ารหัสแล้ว สามารถที่จะถอดรหัสกลับออกมาเป็นข้อความเดิมได้

1. รูปแบบการทดสอบ

จะทำการเข้าและถอดรหัสไฟล์ที่มีขนาดประมาณ 2 กิโลไบท์ เป็นจำนวน 30 ครั้ง

2. ผลการทดสอบ

ตาราง 6.6 ผลการทดสอบความเชื่อถือได้ของเครื่องเข้ารหัส

ครั้งที่ทดสอบ	จำนวนที่ผิดพลาด			
	ECB	CBC	CFB*	OFB**
1-5	-	-	-	-
6-10	-	-	1	-
11-15	-	-	-	-
16-20	-	-	-	-
21-25	-	-	-	1
26-30	-	-	-	-

* CFB ใช้ไฟล์ขนาด 1 กิโลไบท์

** OFB ใช้ไฟล์ขนาด 2 กิโลไบท์ และฟีดแบ็คคาร์แรคเตอร์เท่ากับ 8

จากตาราง 6.6 จะพบการผิดพลาดขึ้นในโหมด CFB 1 ครั้ง และ OFB 1 ครั้ง ลักษณะของการผิดพลาดคือเมื่อถอดรหัสแล้วได้ข้อมูลไม่ตรงกับข้อมูลก่อนการเข้ารหัสจากการทดสอบถ้าหากว่าลดขนาดของไฟล์ให้เล็กลงเหลือขนาดไม่เกิน1 กิโลไบต์จะทำให้การผิดพลาดในการถอดรหัสลดลงอย่างมาก

การทดสอบหาขนาดของไฟล์

เป็นการทดสอบเพื่อเปรียบเทียบขนาดของไฟล์ก่อนและหลังการเข้าหรือถอดรหัส

1. รูปแบบของการทดสอบ

ทำได้โดยการเข้าและถอดรหัสไฟล์ขนาดต่าง ๆ และบันทึกค่าเพื่อเปรียบเทียบขนาด

2. ผลการทดสอบ

ตาราง 6.7 แสดงขนาดไฟล์ก่อนและหลังการเข้ารหัส

โหมด	ขนาด		
	ก่อนเข้ารหัส	หลังเข้ารหัส	หลังถอดรหัส
ECB	326	328	328
CBC	326	328	328
CFB	326	326	326
OFB*	326	326	326
FILE REG.	326	336	-
AUTHEN.	336	344	344

* ฟีดแบ็คคาร์แรคเตอร์เท่ากับ 8

จากตาราง 6.7 ไฟล์ที่ใช้ทดสอบมีขนาด 326 ไบต์ หลังจากการเข้ารหัสในโหมด ECB และ CBC จะมีขนาด 328 ไบต์ เนื่องจาก ECB และ CBC เป็นการเข้ารหัสแบบบล็อคไซเฟอร์ ดังนั้นข้อมูลที่ได้จากการเข้ารหัส จึงเป็นจำนวนเต็มของ 8 สำหรับในโหมด CFB และ OFB นั้นเป็นสตรีมไซเฟอร์ ซึ่งเป็นการเข้ารหัสแบบไบต์ต่อไบต์ ดังนั้นขนาดของไฟล์จึงเท่าเดิม นอกจากนี้เมื่อถอดรหัสแล้วขนาดของไฟล์ก็ยังเท่าเดิมด้วยสำหรับ File Registration นั้น หลังจากเข้ารหัสแล้วขนาดเพิ่มจาก 326 ไบต์ เป็น 336 ไบต์ เนื่องจากใช้โหมดในการเข้ารหัสแบบ CBC ดังนั้นขนาดไฟล์ที่ได้จากการเข้ารหัสคือ 328 ไบต์ อีก 8 ไบต์ คือส่วนที่เป็น AC หลังจากนั้นก็นำไฟล์นี้มาทำ Message Authentication ทำ

ให้ขนาดเพิ่มจาก 336 ไบต์ เป็น 344 ไบต์ สรุปได้ว่าเมื่อเข้ารหัสและถอดรหัสข้อมูลด้วยเครื่องเข้ารหัสที่สร้างขึ้นจะทำให้ขนาดของไฟล์เพิ่มขึ้นไม่เกิน 8 ไบต์

การทดสอบคุณลักษณะเฉพาะของแต่ละโหมด

เป็นการทดสอบเพื่อหาคุณสมบัติต่างๆของโหมดการเข้ารหัสทุกๆโหมดซึ่งมีคุณสมบัติต่างกันไป เช่น การแพร่กระจายความผิดพลาด,การคงความมีรูปแบบของไซเฟอร์เท็กซ์ , การมีคุณสมบัติเซลฟ์ซินโคไนซ์ และอื่น ๆ

1. รูปแบบการทดสอบ

1.1 สร้างไฟล์ทดสอบชื่อ SFORM.DAT แล้วเข้ารหัสในโหมด ECB, CBC, CFB, และ OFB ด้วยคีย์ ใดๆ

1.2 บันทึกไซเฟอร์ไฟล์ที่ได้ไว้ใน ECB.CIP, CBC.CIP, CFB.CIP และ OFB.CIP ตามลำดับเพื่อแสดงถึงคุณสมบัติการคงความมีรูปแบบของไซเฟอร์เท็กซ์ในการเข้ารหัสแต่ละโหมด

1.3 สร้างไฟล์ทดสอบชื่อDES.DOCแล้วนำมาเข้ารหัสโดยโหมดต่างๆภายใต้คีย์ '12345678' และเวกเตอร์เริ่มต้น '12345678'

1.4 ไซเฟอร์ไฟล์ของการเข้ารหัสในโหมด ECB, CBC, CFB และ OFB จะตั้งชื่อว่า DES1.CIP,DES2.CIP, DES3.CIP และ DES4.CIP ตามลำดับ

1.5 ถอดรหัสด้วยคีย์เดียวกับตอนเข้ารหัส แต่เปลี่ยนเวกเตอร์เริ่มต้นเป็น '1234567X' แล้วเก็บเพลนไฟล์ที่ถอดรหัสในโหมด ECB, CBC, CFB และ OFB ไว้ในชื่อ DES2IVC.PLN, DES3IVC.PLN และ DES4IVC.PLN ตามลำดับ

1.6 แก้ไขไซเฟอร์ไฟล์โดยการเปลี่ยนข้อมูลในไฟล์ในตำแหน่งไบต์ที่ 8แล้วถอดรหัสโดยใช้คีย์และเวกเตอร์เริ่มต้นเดียวกับตอนเข้ารหัสแล้วตั้งชื่อDES1TXTC.PLN,DES2TXTC.PLN , DES3TXTC.PLNและ DES4TXTC.PLN

1.7 แก้ไขไซเฟอร์ไฟล์จากข้อ 4 โดยการตัดข้อมูลในตำแหน่งไบต์ที่ 301 ออกแล้วถอดรหัสโดยใช้คีย์และเวกเตอร์เริ่มต้นเดียวกับตอนเข้ารหัสโดยใช้ชื่อDES1TXTD.PLN,DES2TXTD.PLN, DES3TXTD.PLN และ DES4TXTD.PLN ตามลำดับ

2. ผลการทดสอบ

2.1 ผลการทดสอบข้อ 1.1 - 1.3

ผลจากการทดสอบในข้อ1.1 และข้อ 1.2 แสดงไว้ในรูป6.4 - รูป6.8 ซึ่งจะเห็นได้ว่าการเข้ารหัสในโหมดECBนั้นไซเฟอร์ไฟล์ที่ได้จะยังคงมีลักษณะของความมีรูปแบบอยู่มาก สำหรับในโหมดอื่นๆจะไม่มีลักษณะดังกล่าวซึ่งถือเป็นคุณสมบัติที่ดีข้อหนึ่งในการเข้ารหัส

```
File : c:\sform.dat          Date : 31/08/1994    Time : 16:56    Page :    1
================================================================================
aaaaaaaaaaaaaaaaaaaa                                                        1
bbbbbbbbbbbbbbbbbbbb                                                        2
cccccccccccccccccccc                                                        3
dddddddddddddddddddd                                                        4
eeeeeeeeeeeeeeeeeeee                                                        5
ffffffffffffffffffff                                                        6
gggggggggggggggggggg                                                        7
                          EXAMPLE OF STRUCTURAL FILE
================================================================================
                        END OF File : c:\sform.dat
```

รูป 6.4 ตัวอย่างของเพลนเท็กซ์ที่มีความมีรูปแบบ

```
File : c:\ecb.cip            Date : 31/08/1994    Time : 16:57    Page :    1
================================================================================
```

(ไซเฟอร์เท็กซ์ที่ได้จากการเข้ารหัสเพลนเท็กซ์ในรูป6.4ด้วยโหมด ECB)

```
================================================================================
                        END OF File : c:\ecb.cip
```

รูป 6.5 ไซเฟอร์เท็กซ์ที่ได้จากการเข้ารหัสเพลนเท็กซ์ในรูป6.4ด้วยโหมด ECB

```
File : c:\cbc.cip              Date : 31/08/1994     Time : 16:58     Page :     1
================================================================================
iO1≥çNk=;╠'.úó╤kOkst.A"iD$╧P¬òQæ╒..bv.╡èʃ╝?αa.ß▌'Tg┐M€╥.. .x0.,.»O┐Ä├'vhvp....p6
R╩╩ ₤rCθ€.6¿₤é╛.┤3b.∫∫A>$aC½1∫.;.¡≤6I∫DΩ┤╠ê╕5€ ¦≡» µ3∫ú∫iU)N!.╘N≤─╩╙O∫.Φ.P╪1Mà½e
+û╬╜ ⌐{─a.¿╙╤è_uø╝∫╥ë..;à▐Ω≤┘o╟.j÷Ló2╬* m╟..╤b∫T ╬╜π≤ ä═╠n.äà╥kvFéU.F┤ C∞è┐.∫gMA
b¢)ä.¨Ωh╙;₤├.∫¦j╖¥ß₤_m╟I ╒╪╘D½▌╕EΩ.N¨╫≡úα%.≥Bú.µ─m,⌠.ç¿ÿá≥Uë▐GπÇΦ(dù╬.äB<.OΓ?:.
a±a╝╒ê.σ˜£X€Ω╝¡LQFuYçM╤.J├·┌.*.├╞/\èΓ.í∑&.]$:«|■Φòé Φ.éró|E)K┌ï.π╥╩(N_.?« .ß┴R
O¨τ@>.(╧.x.2=1¡µα·..\Xö² .Oa.|╣I.y.[╔?O≤V1¿.)«Çú.xè╪€D;┤Σ.h..@±.<╔!(.JF≤ó≈Çà .rq
.┬═┤R√¬..u.ï.ù╤╣Çòm∫─σ£σ≈.Γ9ZN╥MF±¿╛v.1qqN.¡╡€╘.¥è.╘¬δO.d.ΦΩè«├2┴s'\ΠúM.S■¢ÿa
».·á.;G.Äè..ET┤O Ä.Ç²s├k¦i±M&π..C.·\ïç...WÄ(┴θPë-.X■ñ1¨a╧ä;<Ωôδθ*.3(.à.1

================================================================================
                      END OF File : c:\cbc.cip
```

รูป 6.6 ไซเฟอร์เท็กซ์ที่ได้จากการเข้ารหัสเพลนเท็กซ์ในรูป6.4ด้วยโหมด CBC

```
File : c:\cfb.cip              Date : 31/08/1994     Time : 16:59     Page :     1
================================================================================
JWHk *µèH>.OYA O\.N¼'.«√zq╣[.╡╞≡(.╖. G_U@Φe.┤τüÇ@c.«├.J.∞∞s╛≡┬.(.AW▐]θ p╫ó;o╤J¬(
Γ..┘i86.OΓ╙▌ .3¬M≥╩8à,.äÖ(┐bXΩi.(╛ Tó≥=╙■Σ╙.≥»┤.╝E.ùä3.O).ßN.½i]y╬■äU╙udXπ.$≥╡Hw
P∫Γ.╧..┬s"Oè.!╩˜≈0xêää┤<▐τÄ.¡┤2Q\a£ .¨┼≈ ╬óq.;┐╩Γ<T .vy·wΩ8¢+ï:≈ë.MΣ.æ€3q Ω╣k
6╣9≈r═┐╣Tn.ïë≤¿┘ääKLß≤╥Aé"J9Nri─.äòí.ÇªO.äöWäö|M½J<&V╘.é6─∞/Z╩"+≈&╛■.äEvdM∞╝a═ö
=t²X.T. G.╘"|"B·╥╘¦╝i.1ú5Σç.┬½Aèt╪.╞¿ñθ┐1OÇ.╙╪.ò¦½N/A┤ñä£Rez≥·╜╣╙I¬ZΣU.&/T┴8tüu
kΩ⌐.Γ¢.O¦.Y ╒╣Yi.Ns1'¦C╟.╜≡═ï!ú r₤─4─X .Ωàm≈ço.2.┤┴⌐[FäPJ5ü╫1£· ⌠.i>ò─ôy/8╟çΣTg.
.┤_╚.╣<¢tK.▐■*R|J..=y¨iN..#C┴¨²╟....·σ┌╩vèJL.≈θ¢...jKÇY7ú.▐..┤.r£.┴┴θ·z>╔y.*k.╟
.f&₤╚NmΓo╖┼i╖┬ö⌐─yäio'ö€δ.4.ó2..(]╔P)&╘U6┤ù╣Ä╬(D.vR┴júTΦ≈.ò¨c┴╘..╟╙6·╘╤
================================================================================
                      END OF File : c:\cfb.cip
```

รูป 6.7 ไซเฟอร์เท็กซ์ที่ได้จากการเข้ารหัสเพลนเท็กซ์ในรูป6.4ด้วยโหมด CFB

```
File : c:\ofb.cip              Date : 31/08/1994     Time : 17:00     Page :      1
==============================================================================
J√:<. %.╛ø9–ōpe┬.ℝPi.0..╦¥=&I9▌J.Σ"w╔∫X·∈ik¦├.╕}«≈∫.äëC.┼‖..δqÇ╕╕ .╕MB┼√@;O..¨╒Σ
º3a≈╪w┬ßℝ‖1&FCAf&╣δ≈C.▀╝£Ü ┬▌/··▀p.7OΦ.XY╣»17?="╒i╛..÷mãAü╔nãε.XGεO┼╠UαNJδ╧╤¨«╧
«└ø*'à¿θō"üeæ²┤µA┘╞∩ ╔r·<I¢:.╔∫╒«n∞╠|µY╠_)╔Ma8 \y.\δ!▌=≠m..╒X&uæ‖.'.oGJDI┤╒üoc½Z
ëS ë.. ÷Eα■5δτÇ▄╒5∩├.DwΦa▌–G÷..ë╗Γr=╕╕E╗..ō.U.,S*1╪╤≈ë┤u╘≈┴Y.?╫/e.δ9╕–╞╙O.üGirxë
ëΓ╔z╦O·╗R1AΠ≡E.Js..=h.xANi½± ".d¼¬NhN.α«;y't.╜=U;q¨\┴├wy.N¿R.j╕"3┤«@╒■ß )╫Ω≤_ay
læö˜rih.▌Eg╞≡∈1┬[.6R;GF;[.j5|EG%Φk┴.N1┼½/gÿtō.÷e ).x£╗¨¨Jt¬PC┤a?B|¼(.¨╠t.ºE└n–└u
O=╒┤.èh(∈[∞ÿ╠U■/8 UV¨18y|ō╧N.╒╕U.TC((dI▀Qu╗æ1.j_uō]┬o!+1Uü╪ß1CU1=╞╒uHrΣ..,1.é√eo
∩B¿.Γ–√A`.6w£;┼Ke=±≤┼ ...¿'╛.[¼=.'╗@`.╠_£┴)..w.qōÇ├╕KNSæë7ō[[m£.@|Iä; oD



==============================================================================
                          END OF File : c:\ofb.cip
```

รูป 6.8 ไซเฟอร์เท็กซ์ที่ได้จากการเข้ารหัสเพลนเท็กซ์ในรูป6.4ด้วยโหมด OFB

2.2 ผลการทดสอบข้อ 1.3 - 1.7

```
File : c:\des.doc              Date : 16/09/1994     Time : 17:27     Page :      1
==============================================================================
" The Data Encryption Standard (DES) shall consist of the following Data Encryp-
tion  Algorithm to be  implemented in special purpose electronics devices. These
devices shall be designed in  such a way that they  may  be used  in a  computer
system or network to provide  cryptographic protection to binary coded data. The
method of implementation will depend on the application and environment. The de-
vices shall be implemented in such a  way  that they may be tested and validated
as accurately performing the transformations specified in a following algorithm

==============================================================================
                          END OF File : c:\des.doc
```

รูป 6.9 ไฟล์ทดสอบ DES.DOC ที่ใช้ทดสอบการเข้ารหัส

รูป 6.9 คือไฟล์ที่ใช้ทดสอบการเข้ารหัสในโหมดต่างๆโดยใช้คีย์และเวกเตอร์เริ่มต้นคือ'12345678'เมื่อถอดรหัสด้วยเวกเตอร์เริ่มต้นที่แตกต่างจากตอนเข้ารหัส จะได้ผลดังรูป 6.10 ถึงรูป6.12

```
File : c:\des2ivc.pln          Date : 16/09/1994    Time : 17:28    Page :    1
================================================================================
" The D!ta Encryption Standard (DES) shall consist of the following Data Encryp-
tion  Algorithm to be  implemented in special purpose electronics devices. These
devices shall be designed in  such a way that they  may  be used  in a  computer
system or network to provide  cryptographic protection to binary coded data. The
method of implementation will depend on the application and environment. The de-
vices shall be implemented in such a  way  that they may be tested and validated
as accurately performing the transformations specified in a following algorithm"

================================================================================
                    END OF File : c:\des2ivc.pln
```

รูป 6.10 ผลของการถอดรหัสด้วยโหมด CBCโดยใช้เวกเตอร์เริ่มต้น'1234567X'

```
File : c:\des3ivc.pln          Date : 16/09/1994    Time : 17:29    Page :    1
================================================================================
9=ñ╬╣ä7¿ta Encryption Standard (DES) shall consist of the following Data Encryp-
tion  Algorithm to be  implemented in special purpose electronics devices. These
devices shall be designed in  such a way that they  may  be used  in a  computer
system or network to provide  cryptographic protection to binary coded data. The
method of implementation will depend on the application and environment. The de-
vices shall be implemented in such a  way  that they may be tested and validated
as accurately performing the transformations specified in a following algorithm"

================================================================================
                    END OF File : c:\des3ivc.pln
```

รูป 6.11 ผลของการถอดรหัสด้วยโหมด CFCโดยใช้เวกเตอร์เริ่มต้น'1234567X'

รูป 6.12 ผลของการถอดรหัสด้วยโหมด OFB โดยใช้เวกเตอร์เริ่มต้น'1234567X'

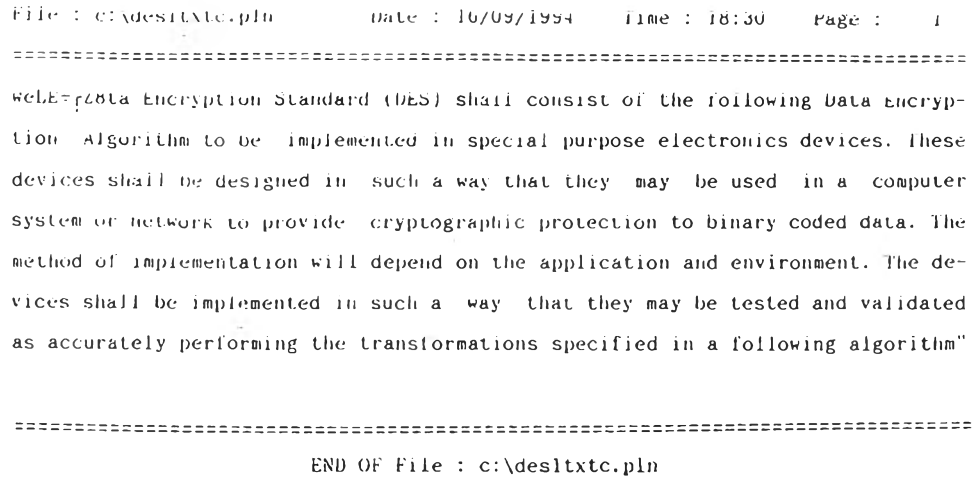
จะเห็นว่าการถอดรหัสที่เวกเตอร์เริ่มต้นไม่ตรงกับตอนเข้ารหัสตามรูป 6. 10 ถึงรูป 6.12 จะทำให้เกิดผลดังนี้คือ

1. ในโหมด CBC (DES2IVC.PLN) จะเกิดการผิดพลาดขึ้นที่ตำแหน่งที่เวกเตอร์เริ่มต้น ไม่ตรงจากตอนเข้ารหัสเท่านั้น (ตำแหน่งที่ 8 ในการทดสอบ) หลังจากนั้นจะไม่มีการผิดพลาดเกิดขึ้นอีก เนื่องจากเวกเตอร์เริ่มต้นที่ผิดพลาดจะถูกใช้เพียงรอบเดียวนรอบต่อไปของการถอดรหัสก็จะใช้ไซเฟอร์เท็กซ์ที่รับมาได้เป็นเวกเตอร์เริ่มต้น (ดูรูป 5.1 ประกอบ)

2. ในโหมด CFB (DES3IVC.PLN) การผิดพลาดจะเริ่มต้นจากตำแหน่งที่ 1 ถึงตำแหน่งที่เวกเตอร์เริ่มต้นไม่ตรงกับตอนเข้ารหัสจากการทดสอบเราใช้เวกเตอร์เริ่มต้นที่ผิดที่ตำแหน่งที่ 8 ดังนั้นเพลนเท็กซ์ที่ได้จึงผิดพลาดไป 8 ตัวอักษร เนื่องจากตัวที่ผิดพลาดในเวกเตอร์เริ่มต้นจะถูกเลื่อนผ่านชิพท์รีจิสเตอร์ถึง 8 ครั้ง หลังจากนั้นค่าที่อยู่ในชิพท์รีจิสเตอร์จะถูกต้องอีกครั้งหนึ่ง (ดูรูป 5.2 ประกอบ)

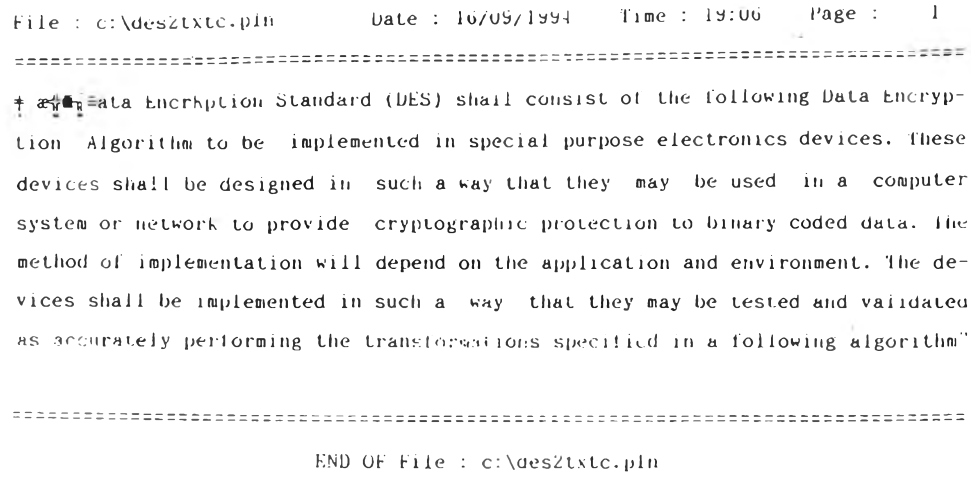
3. ในโหมด OFB (DES4IVC.PLN) จะผิดพลาดทั้งหมด เนื่องจากเวกเตอร์เริ่มต้นจะถูกเข้ารหัส และได้ค่าที่ไม่ตรงกับตอนเข้ารหัส เมื่อนำมาบวกแบบโมดูโล-2 กับไซเฟอร์เท็กซ์ ผลออกมาก็ไม่ถูกต้อง นอกจากนั้นค่าที่ผิดพลาดยังถูกป้อนกลับไปเป็นเวกเตอร์เริ่มต้นในรอบต่อไปอีกในทุก ๆ รอบตลอดทั้งไฟล์ (ดูรูป 5.3 ประกอบ)

ในรูป 6.13 ถึงรูป 6.16 จะแสดงผลของของการแก้ไขไซเฟอร์เท็กซ์ไฟล์ของโหมดต่างๆในตำแหน่งไบต์ที่ 8 แล้วทำการถอดรหัส



```
File : c:\desltxtc.pln          Date : 16/09/1994     Time : 18:30     Page :    1
================================================================================
WELE-Data Encryption Standard (DES) shall consist of the following Data Encryp-
tion  Algorithm to be  implemented in special purpose electronics devices. These
devices shall be designed in  such a way that they  may  be used  in a  computer
system or network to provide  cryptographic protection to binary coded data. The
method of implementation will depend on the application and environment. The de-
vices shall be implemented in such a  way  that they may be tested and validated
as accurately performing the transformations specified in a following algorithm"

================================================================================
                        END OF File : c:\desltxtc.pln
```

รูป 6.13 ผลการถอดรหัสด้วยโหมด ECB ที่ไซเฟอร์ไฟล์ถูกแก้ไขโดยการเปลี่ยนแปลงค่า



```
File : c:\desztxtc.pln          Date : 16/09/1994     Time : 19:06     Page :    1
================================================================================
▯ æ▯▯▯ata Encrhption Standard (DES) shall consist of the following Data Encryp-
tion  Algorithm to be  implemented in special purpose electronics devices. These
devices shall be designed in  such a way that they  may  be used  in a  computer
system or network to provide  cryptographic protection to binary coded data. The
method of implementation will depend on the application and environment. The de-
vices shall be implemented in such a  way  that they may be tested and validated
as accurately performing the transformations specified in a following algorithm"

================================================================================
                        END OF File : c:\desztxtc.pln
```

รูป 6.14 ผลการถอดรหัสด้วยโหมด CBC ที่ไซเฟอร์ไฟล์ถูกแก้ไขโดยการเปลี่ยนแปลงค่า

```
File : c:\des3txtc.pln        Date : 16/09/1994     Time : 18:47     Page :     1
================================================================================
" The DJã2<"6T zption Standard (DES) shall consist of the following Data Encryp-
tion  Algorithm to be  implemented in special purpose electronics devices. These
devices shall be designed in  such a way that they  may  be used  in a  computer
system or network to provide  cryptographic protection to binary coded data. The
method of implementation will depend on the application and environment. The de-
vices shall be implemented in such a  way  that they may be tested and validated
as accurately performing the transformations specified in a following algorithm"

================================================================================
                        END OF File : c:\des3txtc.pln
```

รูป 6.15 ผลการถอดรหัสด้วยโหมด CFB ที่ไซเฟอร์ไฟล์ถูกแก้ไขโดยการเปลี่ยนแปลงค่า

```
File : c:\des4txtc.pln        Date : 16/09/1994     Time : 18:33     Page :     1
================================================================================
" The D$ta Encryption Standard (DES) shall consist of the following Data Encryp-
tion  Algorithm to be  implemented in special purpose electronics devices. These
devices shall be designed in  such a way that they  may  be used  in a  computer
system or network to provide  cryptographic protection to binary coded data. The
method of implementation will depend on the application and environment. The de-
vices shall be implemented in such a  way  that they may be tested and validated
as accurately performing the transformations specified in a following algorithm

================================================================================
                        END OF File : c:\des4txtc.pln
```

รูป 6.16 ผลการถอดรหัสด้วยโหมด OFB ที่ไซเฟอร์ไฟล์ถูกแก้ไขโดยการเปลี่ยนแปลงค่า

จากการทดสอบการแก้ไขข้อมูลในไซเฟอร์ไฟล์ในตำแหน่งที่ 8 แล้วถอดรหัสผลที่ได้เป็นดังนี้

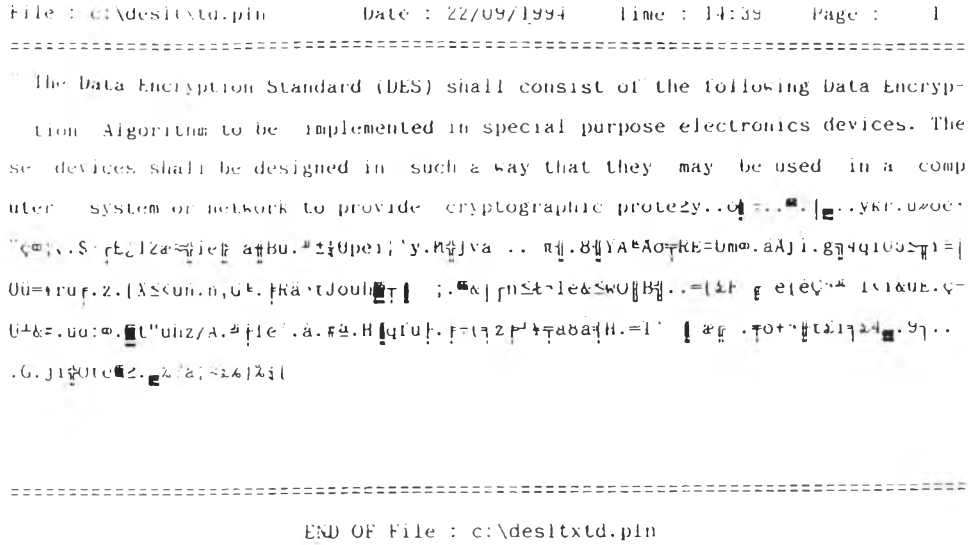
1. ในโหมด ECB (DES1TXTC.PLN)จะเกิดการผิดพลาดขึ้นเพียง8ตัวแรกเนื่องจากข้อมูลที่ถูกนำมาถอดรหัสจะผิดเพียงบล็อคแรกเท่านั้นไม่มีการป้อนกลับหรือมีผลต่อเนื่องไปสู่ข้อมูลชุดอื่น ๆ

2. ในโหมด CBC (DES2TXTC.PLN) ข้อมูลจะผิดพลาด 9 ตัวอักษร 8 บิตแรกจากการถอดรหัสไซเฟอร์ไฟล์ที่ผิดพลาด และอีก 1 ตัวคือ ตำแหน่งที่ 8 ในบล็อคที่ 2 ซึ่งเกิดจากการบวกไซเฟอร์เท็กซ์ที่ถูกแก้ไขเข้ากับข้อมูลที่ถูกถอดรหัสออกมา (ดูรูป 5.1)

3. ในโหมด CFB (DES3TXTC.PLN) จะเกิดผิดพลาดขึ้น9 ตัวอักษร โดยมีรายละเอียดคือ ตัวแรกที่ถอดรหัสได้ผิดพลาด คือในตำแหน่งที่ 8 เนื่องจากการนำเอาไซเฟอร์เท็กซ์ที่ผิดพลาด (ที่ถูกแก้ไข) มาบวกแบบโมดูโล-2 กับข้อมูลที่เกิดจากเวกเตอร์เริ่มต้น หลังจากนั้นก็จะถอดรหัสผิดพลาดอีก 8 ตัวต่อมา เนื่องจากไซเฟอร์เท็กซ์ที่ถูกแก้ไขถูกป้อนเข้าสู่รีจิสเตอร์เริ่มต้น แล้วสร้างข้อมูลที่ผิดพลาดขึ้นมาอีก 8 ชุด เมื่อนำไปบวกกับไซเฟอร์เท็กซ์ในตำแหน่งที่ 9-16 จึงได้ข้อมูลที่ผิดพลาดขึ้น (ดูรูป 5.2 ประกอบ) ซึ่งลักษณะเช่นนี้เราเรียกว่า การเกิดการขยายความผิดพลาด (Error Extension)

4. ในโหมด OFB (DES4TXTC.PLN) จะผิดพลาดเฉพาะตำแหน่งที่ 8 สาเหตุเพราะไซเฟอร์เท็กซ์ที่ถูกแก้ไขถูกใช้ในการบวกกับข้อมูลที่เกิดจากการเข้ารหัสเวกเตอร์เริ่มต้นเพียงครั้งเดียว แล้วหลังจากนั้นไม่มีผลต่อเนื่อง หรือถูกป้อนกลับไปยังข้อมูลบล็อคอื่นๆ อีก หรือไม่มีการขยายความผิดพลาด ซึ่งถือเป็นข้อดีเมื่อเทียบกับโหมด CFB

ในรูป 6.17 จะแสดงผลของการแก้ไขไซเฟอร์ไฟล์โดยการตัดข้อมูลบางส่วนทิ้งในการทดสอบนี้ได้ตัดข้อมูลออกเพียง 1 ไบต์คือที่ตำแหน่ง 301



รูป 6.17 ผลการถอดรหัสด้วยโหมด ECB ที่ไซเฟอร์ไฟล์ถูกแก้ไขโดยการตัดออกบางส่วน

```
File : c:\des2txtd.pln        Date : 22/09/1994     Time : 14:48     Page :     1
================================================================================
" The Data Encryption Standard (DES) shall consist of the following Data Encryp-
  tion  Algorithm to be  implemented in special purpose electronics devices. The
se  devices shall be designed in  such a way that they  may  be used  in a  comp
uter   system or network to provide  cryptographic proteH▌╥.┤C╩..U╞u├Wσ ╬U ħ$╜gm
.N.├┐.÷Ni di╤>)Æ.H╫e.'√.óÆ_≥Wv1D[Σk╛ʃΓ,=_kÆY&.Γk.√&.σæP└luux╚H@ÏA┴\<ä╣.pÿ1a'/┤vo
ç£.╬╝?.╝.z÷a>╥:╟(¢2╥ !▌╬Jçnø╝çn ├é.àèıJ9k2£Kt┘cΩ.ıWN.V╪2F.2╬T3±a.╣╞uJa¬\╜≥M-ĦkΓ
╛o8\=V.■v.`.┐æi.╤┌µvūpj.╫.¡1є.¡5.GJe3V╬┴rcD.H▄._D%.█t. m┤Φ D╧4╫╜.╫x)E┤bՈ┤..ue_.
Ä─OΓ.╚dΣ;¦⌐≥╥╞æ▐k,π*P┤i╛


================================================================================
                      END OF File : c:\des2txtd.pln
```

รูป 6.18 ผลการถอดรหัสด้วยโหมด CBC ที่ไซเฟอร์ไฟล์ถูกแก้ไขโดยการตัดออกบางส่วน

```
File : c:\des3txtd.pln        Date : 22/09/1994     Time : 14:50     Page :     1
================================================================================
" The Data Encryption Standard (DES) shall consist of the following Data Encryp-
tion  Algorithm to be  implemented in special purpose electronics devices. These
devices shall be designed in  such a way that they  may  be used  in a  computer
system or network to provide  cryptographic protectio╓liöL╣ Æry coded data. The
method of implementation will depend on the application and environment. The de-
vices shall be implemented in such a  way  that they may be tested and validated
as accurately performing the transformations specified in a following algorithm"

================================================================================
                      END OF File : c:\des3txtd.pln
```

รูป 6.19 ผลการถอดรหัสด้วยโหมด CFB ที่ไซเฟอร์ไฟล์ถูกแก้ไขโดยการตัดออกบางส่วน

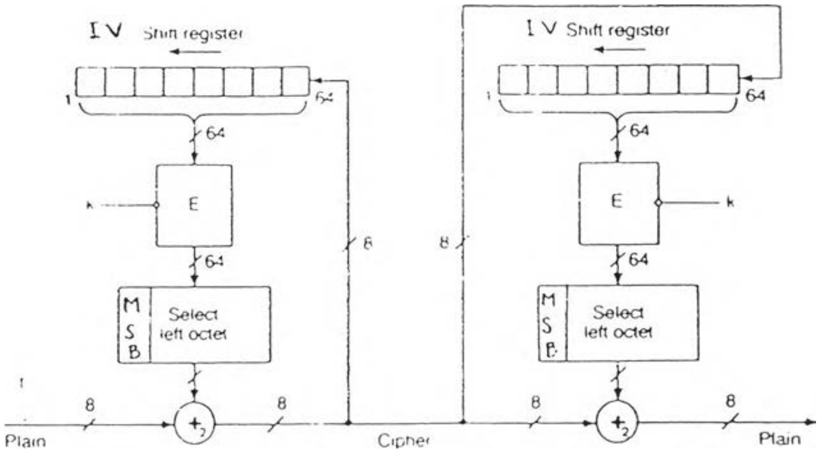
```
File : c:\des4txtd.pln        Date : 22/09/1994     Time : 14:49     Page :    1
================================================================================
" The Data Encryption Standard (DES) shall consist of the following Data Encryp-
  tion  Algorithm to be  implemented in special purpose electronics devices. The
se  devices shall be designed in  such a way that they  may  be used  in a  comp
uter   system or network to provide  cryptographic protectio8då╤╬6'æ-└#D.ū'óh┘n-
|H¬ª.béê±.!uáèδ.╒Tïë )╫ū"┤ïEáªs┼J┐╥\.Hüe.αT@±?╝úπ█=æy'O¥┼<oä6╒m..£aµ-ªy┤H.ΣΩ.i√¼
╝'=x∩è«U╝~öìú ╤█4 ₧H┐Ü~╬Jí╒@..₧e.±_@±9╝úΣπ;┘8q╒╤█>w=kF.╥q«--/ |.¬σ.'√τ∩.0y∩ÅÑ.
Ɛ.āē⌐!├Å"┘■) █oï.½╪E..çe.".Tè"┤∞σ√10¥Ozé>╫pA.Çh≗<ᵗ'|IF·≈.dµΣJ.1=ªÇδ.Ɛ.iè¼*╒Æ
)╜■E┐█ s┘.╝ª|Be·.sz┼█.»-S

================================================================================
                          END OF File : c:\des4txtd.pln
```

รูป 6.20 ผลการถอดรหัสด้วยโหมด OFB ที่ไซเฟอร์ไฟล์ถูกแก้ไขโดยการตัดออกบางส่วน

จากการทดสอบการแก้ไขข้อมูลในไซเฟอร์ไฟล์ โดยการลบข้อมูลในตำแหน่งที่ 301 ออก ตามรูป 6.17ถึงรูป 6.20 ผลการถอดรหัสจะเป็นดังนี้คือ

1. ในโหมดECB,CBC และ OFB (DES1TXTD.PLN, DES2TXTD.PLN และ DES4TXTD.PLN) จะให้ผลในลักษณะเดียวกันคือ ข้อมูลหลังจากตำแหน่งที่ถูกลบออกจะผิดพลาดหมดเนื่องจากสูญเสียการซินโครไนซ์ของข้อมูลทางด้านรับและด้านส่ง

2. ในโหมด CFB (DES3TXTD.PLN) ไฟล์ที่ถอดรหัสได้จะผิดพลาดเพียง 8 ตัวอักษร หลังจากนั้นจะถูกต้อง ซึ่งเรียกว่ามีคุณสมบัติเซลฟ์ซินโครไนซ์ ซึ่งแสดงรายละเอียด ไว้ในรูป 6.21



รูป 6.21 การเกิดเซลฟ์ซินโครไนซ์ในโหมด CFB

Initialization Vector : 12345678

Plaintext : ABCDEFGHIJKL .....

Ciphertext : กขคงจฉชฃฌญฎฏ .....

Round	IV(Encrypt)	Plain	MSB*	Cipher	IV(Decrypt)	Cipher	MSB*	Plain
1	12345678	A	Aก	ก	12345678	ก	Aก	A
2	234567ก	B	Bข	ข	2345678ก	ค	Bข	*Y1*
3	345678กข	C	Cค	ค	345678กค	ง	X1	*Y2*
4	45678กขค	D	Dง	ง	45678กคง	จ	X2	*Y3*
5	5678กขคง	E	Eจ	จ	5678กคงจ	ฉ	X3	*Y4*
6	678กขคงจ	F	Fฉ	ฉ	678กคงจฉ	ช	X4	*Y5*
7	78กขคงจฉ	G	Gช	ช	78กคงจฉช	ช	X5	*Y6*
8	8กขคงจฉช	H	Hช	ช	8กคงจฉชช	ฌ	X6	*Y7*
9	กขคงจฉชช	I	Iฌ	ฌ	กคงจฉชชฌ	ญ	X7	*Y8*
10	ขคงจฉชชฌ	J	Jญ	ญ	**คงจฉชชฌญ**	ฎ	Kฎ	K
11	**คงจฉชชฌญ**	K	Kฎ	ฎ	งจฉชชฌญฎ	ฎ	Lฎ	L
12	งจฉชชฌญฎ	L	Lฎ	ฎ	จฉชชฌญฎฎ	ฐ	Mฐ	M

* Aก,Bข,...และ X1,X2,...,X8 เป็นค่าใดๆที่เกิดจากบล็อคของการเข้ารหัสโดยสมมติให้มีค่าดังกล่าว เพื่อให้สอดคล้องกับการนำไปบวกแบบโมดูโล-2กับเพลนเท็กซ์ในการเข้ารหัสหรือไซเฟอร์เท็กซ์ในการถอดรหัสแล้วได้ผลลัพธ์ที่เข้าใจง่าย

รูป 6.21(ต่อ) การเกิดเซลฟ์ซินโครไนซ์ในโหมด CFB

จากรูป 6.21 เมื่อเข้ารหัสเพลนเท็กซ์ ABCDEFGHIJKL .... แล้วทำให้ได้ไซเฟอร์เท็กซ์ กขคงจฉชฃฌญฎฏ .... แต่ไซเฟอร์เท็กซ์บางตัว (ข) ถูกลบออก ดังนั้นทางด้านรับจึงรับได้แต่ กคงจฉชฃฌญฎฏ .... ซึ่งจะทำให้เพลนเท็กซ์ที่ถูกถอดรหัสกลับมาผิดพลาดไปเพียง 8 ตำแหน่ง (Y1,Y2,...,Y8)หลังจากนั้นก็จะรับได้ถูกต้องเหมือนเดิม

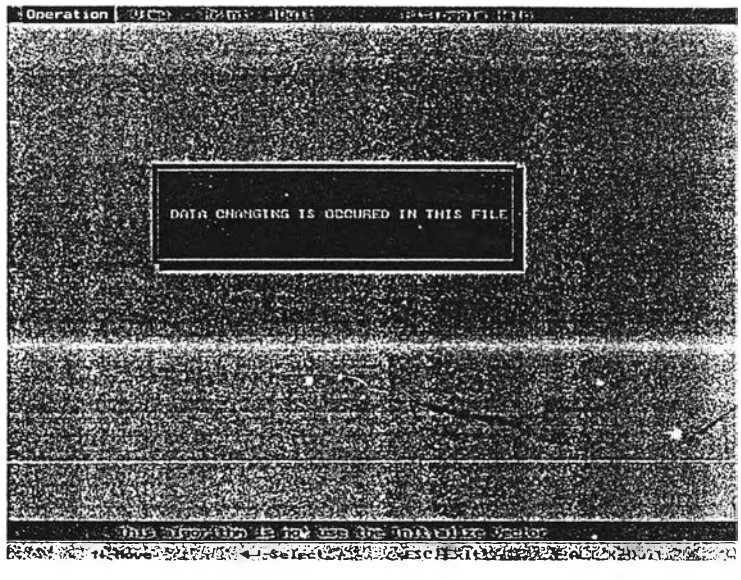
<u>การทดสอบการลงทะเบียนไฟล์</u>

เป็นการทดสอบความสามารถในการรักษาความปลอดภัยของวิธีการลงทะเบียนไฟล์

1. รูปแบบในการทดสอบ

ทำการลงทะเบียนไฟล์แล้วแก้ไขข้อมูลที่เป็นเพลนเท็กซ์ในไฟล์นั้น โดยแก้ไขในตำแหน่งบิตเดียวกันของบล็อคข้อมูลที่แตกต่างกันแล้วทำการรับรองข้อความไฟล์นั้นเพื่อส่งออกช่องสื่อสาร

2. ผลการทดสอบ



รูป 6.22 การตรวจพบไฟล์ที่ลงทะเบียนแล้วถูกแก้ไข

เมื่อทำการแก้ไขข้อมูลที่อยู่ในไฟล์ที่ลงทะเบียนแล้ว ถึงแม้ว่าจะแก้ไขในตำแหน่งบิตเดียวกันก็ตาม $AC_R(AC_R^{'}$ ในสมการ 5.10) ที่ถูกสร้างขึ้นมาใหม่มีโอกาสที่จะเปลี่ยนแปลงไปจาก AC_R เดิมถึง $1\text{-}2^{-64}$ ดังนั้นเมื่อตรวจพบว่า AC_R มีค่าแตกต่างจากเดิมก็จะแสดงผลดังรูป 6.22 และจะไม่อนุญาตให้ทำการรับรองข้อความนี้ส่งออกไปยังผู้รับทางช่องสื่อสารได้

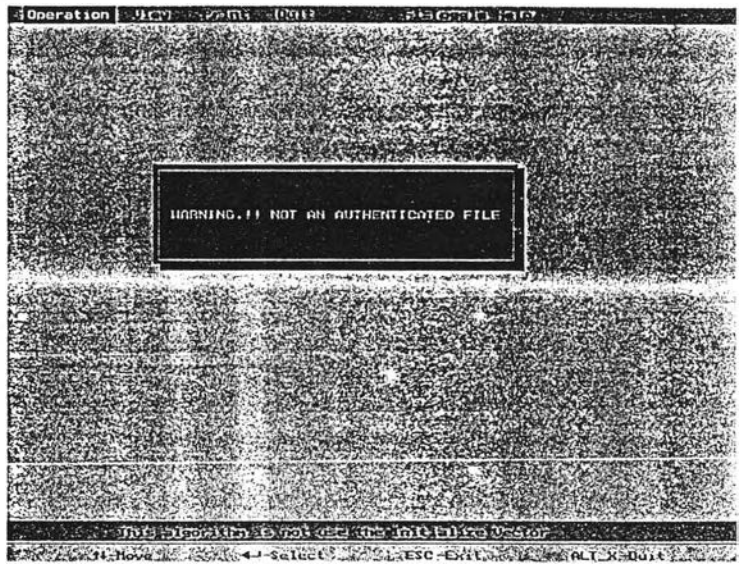
การทดสอบการรับรองข้อความ

เพื่อทดสอบความสามารถในการรับรองข้อความโดยการลงทะเบียนไฟล์ก่อน

1. รูปแบบการทดสอบ

นำไฟล์ที่ลงทะเบียนแล้วมาทำการรับรองข้อความแล้วส่งผ่านช่องสื่อสารไปในรูปของไซเฟอร์เท็กซ์ Y_A เราจะแก้ไข Y_A ในตำแหน่งบิตเดียวกันของบล็อคข้อมูลที่แตกต่างกัน แล้วถอดรหัสทางด้านผู้รับ

2. ผลการทดสอบ



รูป 6.23 แสดงการตรวจพบการแก้ไขในไฟล์ที่ผ่านการรับรองข้อความ

จากรูป 5.14เมื่อผู้รับ รับข้อมูลมาแล้ว จะคำนวนหา AC_A จาก Y_A และ AC_R โดยการบวกแบบโมดูโล-2ของข้อมูลในแต่ละบล็อค แต่เนื่องจาก Y_A ถูกแก้ไขในตำแหน่งบิตเดียวกัน ดังนั้น AC_A ที่คำนวนได้จะมีค่าเท่ากับที่รับมา ในขั้นนี้โปรแกรมจะยอมรับว่าข้อมูลดังกล่าวถูกต้อง

อย่างไรก็ตามเมื่อนำมาถอดรหัสในขั้นต่อไปเพื่อให้ได้เพลนเท็กซ์ X_R แต่เนื่องจาก Y_A ถูกเปลี่ยนแปลงไปเป็น Y_A' X_R ก็จะเปลี่ยนเป็น X_R' เมื่อนำ X_R' มาทำการเข้ารหัสเพื่อคำนวนหาค่า AC_R ไปเปรียบเทียบกับ AC_R ที่รับมาได้ ถ้าหากไม่เท่ากันซึ่งมีโอกาสถึง $1\text{-}2^{-64}$ ผู้รับก็จะไม่ยอมรับว่าเป็นข้อความที่ถูกต้องและแจ้งให้ทราบทางจอแสดงผลดังรูป 6.23