บทที่ 4

ผลการทดลอง

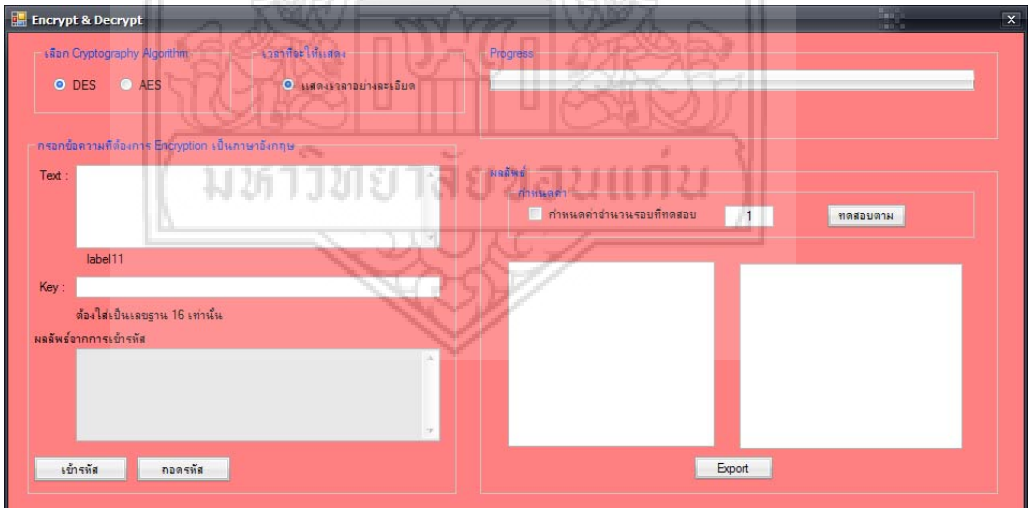
เนื้อหาในบทนี้กล่าวถึงการทดลองและวิเคราะห์ผล ในส่วนแรกจะอธิบายถึงการดำเนินการทดลองคือ วิธีทดสอบ และผลการทดสอบ ส่วนที่สองจะกล่าวถึงการวิเคราะห์ผลการทดสอบ

1. การดำเนินการทดลอง

1.1 วิธีทดสอบ

งานวิจัยครั้งนี้ได้ทำการสร้างโปรแกรมประยุกต์เพื่อเข้าและถอดรหัสคำไทย ด้วยภาษา C# โดยการใช้ Microsoft Visual Studio 2008 และทำการทดสอบการทำงานบนเครื่องคอมพิวเตอร์รุ่น Intel® Core™ 2 Duo Duo CPU T6500 @ 2.10 GHz ใช้ RAM ขนาด 2GB ประกอบกับ Hard disk ความจุขนาด 320 GB ทำงานบนระบบปฏิบัติการ Window XP SP2 ลักษณะข้อมูลที่นำเข้ามาประมวลผลเป็นแบบ ข้อความที่มีขนาดความยาว (plaintexts sizes) คือ 4kb 10kb และ 14kb ตามลำดับ โดยแต่ละขนาดความยาวจะใช้ชุดข้อความคำไทยอย่างละ 5 ชุด โดยแต่ละชุดนั้นจะมีความหลากหลายของคำในภาษาไทย

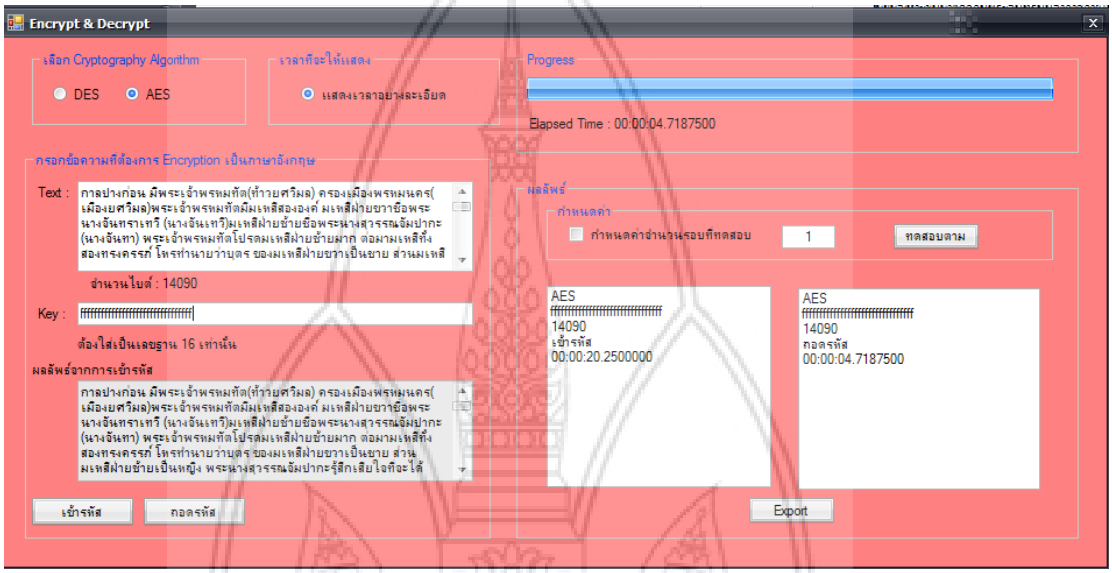
จากการออกแบบส่วนติดต่อกับผู้ใช้สำหรับการเข้าและถอดรหัสคำภาษาไทย นั้นมีองค์ประกอบดังภาพด้านล่างนี้



ภาพที่ 31 แสดงหน้าจอส่วนประกอบของซอฟต์แวร์ที่สร้าง

1.2 ผลการทดสอบ

ในการทดสอบได้แบ่งประเด็นการทดสอบออกเป็น สองประเด็นคือ ประเด็นแรกจะทดสอบความถูกต้องในการเข้าและถอดรหัสข้อความ และประเด็นที่สองจะทดสอบถึงความเร็วในการเข้าและถอดรหัสข้อความด้วยอัลกอริทึม DES และ AES โดยในการทดสอบแต่ละครั้งนั้นจะทำการบันทึกเวลาในการเข้าและถอด แล้วนำค่าเวลาเหล่านั้นมาทำการหาค่าเฉลี่ย



ภาพที่ 32 ตัวอย่างการเข้าและถอดรหัสข้อความภาษาไทยขนาด 14 kb ด้วยอัลกอริทึม AES

ตารางที่ 18 แสดงค่าเวลาที่ใช้ในการเข้าและถอดรหัสชุดข้อความภาษาไทยที่ขนาด 4 kb โดย DES Algorithm และคำนวณค่าเวลาเฉลี่ย

Time (milliseconds)	**ข้อความภาษาไทยที่ขนาดความยาวประมาณ 4 กิโลไบท์**				
	ชุดที่ 1	ชุดที่ 2	ชุดที่ 3	ชุดที่ 4	ชุดที่ 5
Encrypt Time	2.3437500	2.1406250	2.0312500	2.2500000	1.4843750
Decrypt Time	0.4531250	0.4218750	0.5468750	0.7656250	1.2968750
Average	**1.39844**	**1.28125**	**1.28906**	**1.50781**	**1.39063**
Totals Average	**1.37344**				

ตารางที่ 19 แสดงค่าเวลาที่ใช้ในการเข้าและถอดรหัสชุดข้อความภาษาไทยที่ขนาด 10 kb โดย DES Algorithm และคำนวณค่าเวลาเฉลี่ย

Time (milliseconds)	**ข้อความภาษาไทยที่ขนาดความยาวประมาณ 10 กิโลไบท์**				
	ชุดที่ 1	ชุดที่ 2	ชุดที่ 3	ชุดที่ 4	ชุดที่ 5
Encrypt Time	9.437500	8.5781256	8.1250000	7.9375000	7.2500000
Decrypt Time	0.812500	1.1718750	1.1406250	1.2500000	1.1093750
Average	**5.12500**	**4.87500**	**4.63281**	**4.59375**	**4.17969**
Totals Average	**4.68125**				

ตารางที่ 20 แสดงค่าเวลาที่ใช้ในการเข้าและถอดรหัสชุดข้อความภาษาไทยที่ขนาด 14 kb โดย DES Algorithm และคำนวณค่าเวลาเฉลี่ย

Time (milliseconds)	**ข้อความภาษาไทยที่ขนาดความยาวประมาณ 14 กิโลไบท์**				
	ชุดที่ 1	ชุดที่ 2	ชุดที่ 3	ชุดที่ 4	ชุดที่ 5
Encrypt Time	15.1406250	15.3906250	15.3281250	15.2031250	14.4375000
Decrypt Time	1.7656250	0.9062500	1.5156250	1.1718750	1.2656250
Average	**8.45313**	**8.14844**	**8.42188**	**8.18750**	**7.85156**
Totals Average	**8.21250**				

ตารางที่ 21 แสดงค่าเวลาที่ใช้ในการเข้าและถอดรหัสชุดข้อความภาษาไทยที่ขนาด 4 kb โดย AES Algorithm และคำนวณค่าเวลาเฉลี่ย

Time (milliseconds)	**ข้อความภาษาไทยที่ขนาดความยาวประมาณ 4 กิโลไบท์**				
	ชุดที่ 1	ชุดที่ 2	ชุดที่ 3	ชุดที่ 4	ชุดที่ 5
Encrypt Time	3.2812500	2.9687500	2.5781250	2.9375000	3.1562500
Decrypt Time	2.2031250	1.8431500	1.9843750	2.1406250	1.8593750
Average	**2.74219**	**2.40595**	**2.28125**	**2.53906**	**2.50781**
Totals Average	**2.49525**				

ตารางที่ 22 แสดงค่าเวลาที่ใช้ในการเข้าและถอดรหัสชุดข้อความภาษาไทยที่ขนาด 10 kb โดย AES Algorithm และคำนวณค่าเวลาเฉลี่ย

Time (milliseconds)	**ข้อความภาษาไทยที่ขนาดความยาวประมาณ 10 กิโลไบท์**				
	ชุดที่ 1	ชุดที่ 2	ชุดที่ 3	ชุดที่ 4	ชุดที่ 5
Encrypt Time	11.8281250	11.7187500	11.3906250	11.4531250	10.0468750
Decrypt Time	3.7968750	3.3125000	3.3593750	4.1562500	3.3437500
Average	**7.81250**	**7.51563**	**7.37500**	**7.80469**	**6.69531**
Totals Average	**7.44063**				

ตารางที่ 23 แสดงค่าเวลาที่ใช้ในการเข้าและถอดรหัสชุดข้อความภาษาไทยที่ขนาด 14 kb โดย AES Algorithm และคำนวณค่าเวลาเฉลี่ย

Time (milliseconds)	**ข้อความภาษาไทยที่ขนาดความยาวประมาณ 14 กิโลไบท์**				
	ชุดที่ 1	ชุดที่ 2	ชุดที่ 3	ชุดที่ 4	ชุดที่ 5
Encrypt Time	20.2500000	19.5468750	19.687500	19.6250000	18.3281250
Decrypt Time	4.7187500	4.5625000	4.8750000	4.8437500	4.5312500
Average	**12.48438**	**12.05469**	**12.28125**	**12.23438**	**11.42969**
Totals Average	**12.09688**				

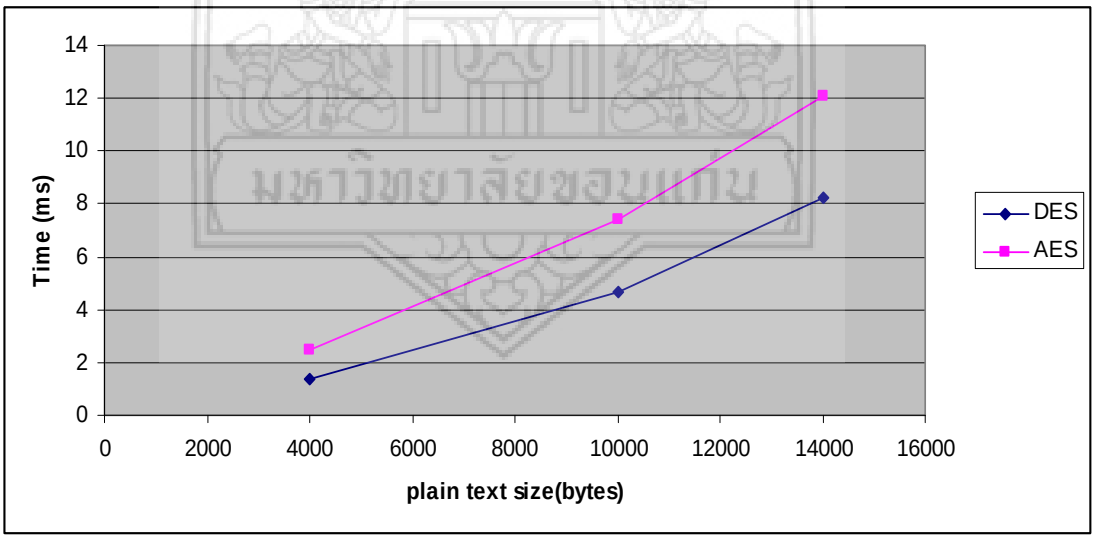
2. วิเคราะห์ผลการทดสอบ

จากการทดสอบทำงานของโปรแกรมประยุกต์ที่สร้างสำหรับการเข้าและถอดรหัส ข้อความภาษาไทยที่มีขนาดความยาวที่แตกต่างกัน และมีความหลากหลายของคำภาษาไทย ด้วยอัลกอริทึม DES และ AES ซึ่งแบ่งประเด็นการทดสอบออกเป็น สองประเด็นคือ ประเด็นแรกจะทดสอบความถูกต้องในการเข้าและถอดรหัสข้อความ ผลปรากฏว่า โปรแกรมประยุกต์ที่สร้างมีความสามารถในการถอดรหัสออกมาได้อย่างถูกต้องแม่นยำตรงตามต้นฉบับข้อความแต่ละชุดที่นำเข้ามา และในส่วนประเด็นที่สองนั้นจะทดสอบถึงความเร็วในการเข้าและถอดรหัสข้อความด้วยอัลกอริทึม DES และ AES ซึ่งในการทดสอบแต่ละครั้งนั้นจะทำการบันทึกเวลาในการเข้าและถอดรหัสของแต่ละชุดข้อความของแต่ละความยาว แล้วนำค่าเวลาเหล่านั้นมาทำการหา

ค่าเฉลี่ย แล้วค่าเฉลี่ยเหล่านั้นมาคำนวณหาค่าเฉลี่ยดังตารางที่ 29 ผลปรากฏว่าค่าเวลาที่ได้สำหรับ DES อัลกอริทึมนั้น มีแนวโน้มเพิ่มขึ้นตามขนาดข้อความที่นำเข้ามา ส่วน AES อัลกอริทึมนั้น ค่าเวลาที่ใช้ในการเข้าและถอดรหัสก็มีแนวโน้มเพิ่มขึ้นตามขนาดข้อความที่นำเข้ามาเช่นกันหากพิจารณาในแง่ของความเร็ว DES อัลกอริทึมจะคำนวณได้เร็วกว่า เพราะมีความซับซ้อนและจำนวนบิตที่น้อยกว่า AES อัลกอริทึม หากพิจารณาในแง่ของความปลอดภัย AES อัลกอริทึมจะมีความปลอดภัยมากกว่าเพราะมีความซับซ้อนในการคำนวณมากกว่าและจำนวนบิตของกุญแจที่ยาวกว่า และเมื่อนำค่าเวลาเหล่านั้น มาทำการสร้างกราฟความสัมพันธ์ของแต่ละอัลกอริทึมจะได้ดังภาพที่ 33

ตารางที่ 24 แสดงค่าเวลาเฉลี่ยที่ใช้ในการเข้าและถอดรหัสข้อความภาษาไทยที่มีขนาดที่แตกต่างกันสำหรับ อัลกอริทึม DESและAES

Plaintext sizes (bytes)	DES	AES
4000	**1.37344**	**2.49525**
10000	**4.68125**	**7.44063**
14000	**8.21250**	**12.09688**



ภาพที่ 33 กราฟแสดงความสัมพันธ์ขนาดของข้อความที่นำเข้าเทียบกับเวลาที่ใช้ในการประมวลของแต่ละอัลกอริทึม