บทที่ 5

สรุปผล

โครงงานนี้แสดงให้เห็นถึงประสิทธิผลของการนำหลักการวิทยาการเข้ารหัสลับ เพื่อเขียนโปรแกรมในการเข้ารหัสในการส่งข้อมูลของโปรแกรม Cryptie และนำมาตรฐานในการเข้ารหัสลับและถอดรหัสลับมาศึกษา 6 อัลกอริทึม คือ อัลกอริทึมแบบ AES, Serpent, RC2, CAST6, Blowfish และ Twofish เป็นการเข้ารหัสโดยมีการแบ่งข้อมูลเป็นบล็อกข้อมูลเพื่อให้การเข้ารหัสเป็นไปอย่างง่าย รวดเร็ว สามารถเข้ารหัสข้อมูลขนาดใหญ่ๆ ได้ เพื่อให้เข้าใจถึงหลักการและวิธีในการเข้ารหัสและถอดรหัสลับอย่างแท้จริง และได้นำโปรแกรมที่พัฒนาขึ้นมาทดลองในการเข้ารหัสลับข้อมูลประเภทต่างๆ แล้วนำผลการทดลองมาวิเคราะห์ผลทางสถิติเพื่อให้ได้บทสรุปที่มีความน่าเชื่อถือซอฟต์แวร์ที่ใช้ในการเขียนโปรแกรมนั้น กลุ่มผู้ศึกษาได้พัฒนาโดยใช้ภาษา Java โดยใช้ Library คือ Bouncycastle ในการพัฒนาโปรแกรมการเข้ารหัส

5.1 สรุป และอภิปรายผล

จากการศึกษาและเขียนโปรแกรมการเข้ารหัสและถอดรหัสไฟล์ข้อมูล 3 ประเภท คือ Plan Text, Semi Binary file และ Pure Binary file ด้วยอัลกอริทึมต่างๆ ได้แก่ AES, Serpent, RC2, CAST6, Blowfish และ Twofish สามารถสรุปได้ว่า หลังจากการเข้ารหัสและการถอดรหัสนั้นในแต่ละอัลกอริทึมจะทำให้ขนาดของข้อมูลเปลี่ยนแปลงไปเล็กน้อย เนื่องมาจากมีการเข้ารหัสแบบบล็อกข้อมูลเมื่อข้อมูลมีขนาดน้อยกว่าขนาดบล็อกแล้วจะมีการเพิ่มข้อมูลที่เป็น Blank ต่อท้ายเพื่อให้ครบตามขนาดบล็อก ดังนั้นข้อมูลที่ถอดรหัสออกมาแล้วนั้นยังคงเป็นข้อความเดิม แต่ส่งผลให้เวลาในการเข้ารหัสนั้นใช้เวลามากกว่าเวลาในการถอดรหัส นอกจากนั้นขนาดคีย์ยังส่งผลต่อเวลาในการเข้ารหัสคือ การใช้คีย์ขนาดใหญ่จะใช้เวลาในการเข้ารหัสมากกว่าคีย์ขนาดเล็กกว่า

ในการเปรียบเทียบประสิทธิภาพของแต่ละอัลกอริทึมจะเห็นว่าเวลาในการเข้ารหัสและถอดรหัสของอัลกอริทึมแบบ Twofish จะใช้เวลามากกว่าอัลกอริทึมอื่นๆที่ใช้เปรียบเทียบ เนื่องจากกระบวนการในการเข้ารหัสมีความซับซ้อนมากกว่า ทำให้ในการเข้ารหัสมีความปลอดภัยมากกว่าอัลกอริทึมอื่นๆ ที่ใช้ทดสอบ และอัลกอริทึมที่ใช้น้อยลงมาได้แก่ Serpent, RC2, AES, Blowfish และ CAST6 ตามลำดับ ซึ่งหากผู้ใช้ต้องการเข้ารหัสข้อมูลภายในเวลาสั้นก็ควรเลือกอัลกอริทึมแบบ CAST6 และจะสามารถสรุปความปลอดภัยของแต่ละอัลกอริทึมได้ดังตารางต่อไปนี้

ตารางที่ 5.1 เปรียบเทียบประสิทธิภาพของแต่อัลกอริทึม

อัลกอริทึม	ความเร็ว	ความปลอดภัย	ความซับซ้อน
AES	เร็ว	ปานกลาง	มาก
Serpent	ปานกลาง	มาก	มาก
RC2	ปานกลาง	ปานกลาง	ปานกลาง
CAST6	เร็วมาก	น้อย	น้อย
Blowfish	เร็วมาก	ปานกลาง	ปานกลาง
Twofish	ช้า	มาก	มาก

5.2 ปัญหาที่พบ

1. เนื่องจากเอกสารอ้างอิงที่ใช้ในการค้นคว้าในเรื่องการเข้ารหัส และถอดรหัสยังไม่มีบทความที่เป็นภาษาไทยฉบับสมบูรณ์จึงจำเป็นต้องทำการศึกษาจากแหล่งอ้างอิงที่เป็นภาษาต่างประเทศ และต้องค้นหาจากแหล่งข้อมูลที่หลากหลาย เพื่อให้ได้ข้อมูลที่สมบูรณ์ที่สุด
2. ไฟล์บางประเภทไม่สามารถนำมาทดสอบเพื่อหาข้อจำกัดทางด้านขนาดได้ เนื่องจากไม่สามารถสร้างไฟล์ที่มีขนาดใหญ่ตามต้องการได้

5.3 ข้อเสนอแนะ

1. ในการใช้งานของโปรแกรมเนื่องจากขนาดของคีย์ที่ใช้จะใช้ขนาดเดียวกับขนาดรหัสผ่านที่ใช้เข้ารหัส ซึ่งทำให้ไม่มีความยืดหยุ่นต่อการใช้งานของผู้ใช้ ซึ่งหากมีการพัฒนาต่อไปโดยให้มีการจัดการกับขนาดของรหัสผ่าน เพื่อให้สามารถใช้ได้ทุกขนาดในการเข้ารหัสของผู้ใช้ เพื่อไม่เป็นการจำกัดขอบเขตของการใช้ และยังเป็นการเพิ่มความปลอดภัยในการกรอกรหัสผ่านอีกด้วย