บทที่ 1
บทนำ

1. ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันการแลกเปลี่ยนข้อมูลข่าวสารได้มีการประยุกต์ใช้งานกว้างขวางมากขึ้นไม่ว่าจะเป็นการสื่อสารบนระหว่างเครื่องคอมพิวเตอร์ เอง หรือ โทรศัพท์เคลื่อนที่โดยมีการคำนึงถึงความปลอดภัยในระหว่างการใช้งานแลกเปลี่ยนข้อมูล วิธีการป้องกันไม่ให้ข้อความที่ต้องการสื่อสารนั้นมีการเปลี่ยนแปลงแก้ไขหรือเปิดเผยข้อมูลก่อนถึงมือผู้รับจึงได้มีการเพิ่มวิธีการเข้ารหัสข้อมูล (Encryption) จึงเป็นทางเลือกหนึ่งของการเพิ่มความปลอดภัยข้อมูลยิ่งขึ้น รูปแบบการเข้ารหัสข้อมูลแบ่งเป็น 2 กลุ่มหลัก คือ การเข้ารหัสแบบสมมาตร (Symmetric Encryption หรือ Secret Key) และการเข้ารหัสแบบอสมมาตร (Asymmetric Encryption หรือ Public-Key Encryption)โดยนำข้อความ (Plain Text) ที่ต้องการส่งมาทำการเข้ารหัสด้วยลูกกุญแจ (Encryption) จะได้ข้อความที่ถูกเข้ารหัส (Cipher Text) หากมีการเข้ารหัสโดยใช้กุญแจแบบสมมาตร เป็นการเข้ารหัสและถอดรหัสโดยการใช้กุญแจดอกเดียวกัน (Secret-Key) โดยอัลกอริทึมในการเข้ารหัสแบบสมมาตร ไม่ว่าจะเป็น DES ขนาด 56 บิต และ AES ขนาด 128 บิต ซึ่งการเข้ารหัสเหล่านี้สามารถทำงานได้บนฮาร์ดแวร์และซอฟแวร์ เพราะความสามารถในการประมวลผลอันรวดเร็วและเปิดเผยอัลกอริทึมจึงเป็นที่นิยมอย่างแพร่หลาย อัลกอริทึมเหล่านี้นั้นที่ใช้ตัวอักษรภาษาอังกฤษเป็นมาตรฐานในการเข้ารหัส ดังนั้นหากต้องการนำอัลกอริทึมเหล่านี้มาใช้เพื่อสนับสนุนการใช้ตัวอักษรภาษาไทยนั้นจำเป็นอย่างยิ่งที่ต้องเพิ่มขั้นตอนบางอย่างในการทำงานเพื่อให้สามารถเข้ารหัสและถอดรหัสออกมาเป็นภาษาไทยได้

การใช้มาตรฐานเข้ารหัสภาษาไทยนั้นมีอยู่หลากหลายไม่ว่าจะเป็น window-874 ซึ่งเป็นมาตรฐานการเข้ารหัสบนระบบปฏิบัติการของวินโดวส์ tis-620 หรือ มอก.620 เป็นมาตรฐานของรหัสตัวอักษร ซึ่งกำหนดโดยสำนักงานมาตรฐานอุตสาหกรรมหรือ สมอ.(TISI : Thai Industrial Standard Institute) Unicode เป็นมาตรฐานการเข้ารหัสของ Unicode Consortium สามารถที่จะรองรับการเก็บอักษรทุกภาษาทั่วโลกได้ โดยอาศัยรหัสเพียงชุดเดียวเพราะเป็นรหัสอักษรแบบ 16 บิต ซึ่งมีค่าอ้างอิงเป็นตารางเลขฐานสิบหกซึ่งเป็นมาตรฐานของ ภาษาไทย ใน Unicode

ในการดำเนินการวิจัยครั้งนี้ ได้ทำการสร้างโปรแกรมประยุกต์ทดสอบการทำงานของอัลกอริทึมพื้นฐานในการเข้าและถอดรหัสคือDES และ AES สำหรับการใช้งานกับตัวอักษรภาษาไทย โดยการเพิ่มขั้นตอนการจับคู่กับตาราง Unicode ฐานสิบหก สำหรับภาษาไทย ประกอบกับ

แบ่งประเด็นการทดสอบออกเป็น สองประเด็นคือ ประเด็นแรกจะทดสอบความถูกต้องในการเข้าและถอดรหัสข้อความ และในส่วนประเด็นที่สองนั้นจะทดสอบถึงความเร็วในการเข้าและถอดรหัสโดยการนำเข้าข้อความภาษาไทยที่ขนาดความยาวต่างๆ กันและบันทึกเวลาในการประมวลผลและนำมาหาค่าเฉลี่ย สร้างกราฟวิเคราะห์ถึงความสัมพันธ์

2. **จุดประสงค์ของงานวิจัย**

2.1 ศึกษาการทำงานของอัลกอริทึม DES ขนาด 56 บิต และ AES ขนาด 128 บิต

2.2 ออกแบบและพัฒนาซอฟต์แวร์สำหรับใช้ในการเข้ารหัสภาษาไทยโดยใช้วิธีการเทียบชุดข้อความที่นำเข้ากับตารางเลขฐานสิบหกซึ่งเป็นมาตรฐานของ ภาษาไทย ใน Unicode

2.3 ทดสอบความถูกต้องและความเร็วของโปรแกรมที่สร้าง โดยนำเข้าชุดของข้อความภาษาไทยที่มีขนาดแตกต่างกันสำหรับการ เข้าและถอดรหัสด้วยอัลกอริทึม DES ขนาด 56 บิต และ AES ขนาด 128 บิต

2.4 สร้างโปรแกรมประยุกต์ที่สามารถประยุกต์ใช้ในการเข้าและถอดรหัสภาษาไทยโดยใช้อัลกอริทึม DES ขนาด 56 บิต และ AES ขนาด128 บิต ได้อย่างถูกต้อง

3. ขอบเขตของงานวิจัย

3.1 ศึกษาทฤษฎีและขั้นตอนของอัลกอริทึมDESขนาด 56 บิตและAES ขนาด 128 บิต

3.2 ออกแบบขั้นตอนการเข้าและถอดรหัสภาษาไทยด้วยวิธีการเทียบค่าเลขฐานสองที่นำเข้ากับตารางเลขฐานสิบหกซึ่งเป็นมาตรฐานของภาษาไทยใน Unicode ก่อนทำการเข้าและถอด รหัสด้วยอัลกอริทึม DES ขนาด 56 บิต และ AES ขนาด 128 บิต

3.3 ทดสอบความถูกต้องในการเข้าและถอดรหัสการทำงานอัลกอริทึม DES ขนาด 56 บิต และ AES ขนาด 128 บิต

3.4 เพิ่มทางเลือกในการใช้ซอฟต์แวร์เข้าและถอดรหัสภาษาไทย ด้วยอัลกอริทึม DES ขนาด 56 บิต และ AES ขนาด 128 บิต ได้อย่างถูกต้อง

4. ประโยชน์ที่คาดว่าจะได้รับจากงานวิจัย

4.1 โปรแกรมประยุกต์สำหรับใช้ในการเข้ารหัสภาษาไทย โดยใช้อัลกอริทึม DES ขนาด 56 บิต และ AES ขนาด 128 บิต

4.2 เป็นแนวทางในการประยุกต์การสร้างรหัสลับสำหรับภาษาไทยได้

เนื้อหาของการศึกษาอิสระนี้ แบ่งเนื้อหาออกเป็น 4 บท บทต่อไปที่จะกล่าวถึงคือ บทที่ 2 ซึ่งอธิบายเกี่ยวกับทฤษฎีที่ใช้และงานวิจัยที่เกี่ยวข้อง ได้แก่ การทำงานอัลกอริทึม DES, AES และ Unicode , ขั้นตอนวิธีในการสร้างรหัสลับภาษาไทย, การเปรียบเทียบประสิทธิภาพการทำงานของอัลกอริทึมในการเข้ารหัสข้อมูล บทที่ 3 จะกล่าวถึงวิธีการดำเนินการวิจัย โดยการออกแบบขั้นตอนการทำงานของซอฟต์แวร์สำหรับใช้ในการเข้ารหัสภาษาไทยโดยใช้วิธีการเทียบชุดข้อความที่นำเข้ากับตารางเลขฐานสิบหกซึ่งเป็นมาตรฐานของภาษาไทยใน Unicode บทที่ 4 ผลการทดลอง และบทที่ 5 สรุปผลการศึกษา