บทที่ 1

บทนำ

1.1 ความเป็นมาของปัญหา

ในสังคมยุคแห่งข่าวสารทุกวันนี้ ข้อมูล มีความสำคัญมากในการดำเนินงานขององค์กร ทั้งของรัฐบาลและธุรกิจเอกชน ตั้งแต่องค์กรขนาดใหญ่ ขนาดกลาง ไปจนกระทั่งองค์กรขนาดเล็ก นั่นคือข้อมูลได้กลายเป็นปัจจัยสำคัญที่ถูกนำมาใช้เพื่อการบริหาร เช่น ช่วยในการวางแผนและพัฒนา ช่วยในการตัดสินใจ ช่วยในการแก้ปัญหา ช่วยเพิ่มผลผลิต และเพิ่มประสิทธิภาพของการทำงานขององค์กร คอมพิวเตอร์ถูกนำมาใช้ในการประมวลผลข้อมูลเพื่อให้ได้ข้อมูลที่ถูกต้องรวดเร็ว และทันสมัยอยู่เสมอ ข้อมูลเหล่านี้จะถูกเก็บเอาไว้ในลักษณะที่เป็นข้อมูลดิจิตอลบนสื่อต่าง ๆ เช่น พวกจานแม่เหล็ก เทปแม่เหล็ก เป็นต้น แทนการเก็บข้อมูลไว้บนกระดาษดังที่เคยเป็นมา และเมื่อมีการนำความเจริญก้าวหน้าทางด้านเทคโนโลยีการสื่อสารมาเชื่อมโยงเข้ากับระบบคอมพิวเตอร์ กลายเป็นระบบเครือข่ายสื่อสารมีขอบเขตครอบคลุมไปทั่วโลก ทำให้ผู้คนในส่วนต่าง ๆ ของโลกสามารถติดต่อสื่อสารเข้าถึงข้อมูลได้ สามารถใช้แหล่งข้อมูลเดียวกันได้ภายในเวลาอันรวดเร็ว แต่ปัญหาที่สำคัญ ก็คือ การควบคุมและป้องกันข้อมูลเหล่านี้ให้ปลอดภัยและถูกต้องอยู่ตลอดเวลา เนื่องจากข้อมูลมีโอกาสที่จะถูกเข้าถึงจากผู้ไม่มีสิทธิ หรือ ข้อมูลอาจจะถูกดักจับ แก้ไข หรือปลอมแปลง ทำให้ข้อมูลไม่ถูกต้องและมีผลเสียหายต่อผู้ที่นำข้อมูลเหล่านี้ไปใช้ได้

การกระทำอันจะก่อให้เกิดเสียหายกับระบบคอมพิวเตอร์ ซึ่งประกอบด้วย ฮาร์ดแวร์ ซอฟต์แวร์ และ ข้อมูล สามารถแบ่งได้เป็น 4 ลักษณะ คือ (Pfleeger, Charles P.,1989)

1. การดักจับข้อมูล (Interception) ตัวอย่างเช่น อาจจะมีบุคคล หรือองค์กรอื่น ที่พยายามจะดักจับข้อมูล โดยการพยายามเข้าถึงข้อมูล (access) ที่อยู่ในระบบคอมพิวเตอร์ หรือการดักจับข้อมูล ในขณะที่ข้อมูลถูกส่งไปตามสายสื่อสารของเครือข่ายสื่อสาร ด้วยการแอบต่อสาย

2. การเปลี่ยนแปลงแก้ไขข้อมูล (Modification) อาจจะเป็นในลักษณะที่มีองค์กรอื่น หรือ บุคคลอื่น ๆ ที่ไม่ประสงค์ดี พยายามเปลี่ยนแปลงแก้ไขข้อมูลในระบบฐานข้อมูล หรือ เป็นการเปลี่ยนแปลงโปรแกรม โดยการเพิ่มการคำนวณบางส่วนลงไป หรือเป็นในลักษณะ

ที่แอบแก้ไขข้อมูลที่ถูกส่งมาตามสายสื่อสาร ทำให้ข้อมูลผิดไปจากความเป็นจริง อันจะก่อให้เกิดความเสียหายได้

3. การปลอมแปลงข้อมูล (Fabrication) อาจจะเป็นในลักษณะที่แอบเพิ่มข้อมูลเข้าไปในระบบฐานข้อมูล หรือเพิ่มข้อมูลเข้าไปในสายสื่อสาร

4. การขัดจังหวะการทำงานของคอมพิวเตอร์ (Interruption) ตัวอย่างการขัดจังหวะ เช่น การทำลายฮาร์ดแวร์ การลบโปรแกรม หรือข้อมูลต่าง ๆ ของระบบปฏิบัติการ ซึ่งมีผลทำให้ระบบคอมพิวเตอร์ทำงานไม่ได้ หรือข้อมูลเกิดการสูญหาย

ถึงแม้ว่าระบบคอมพิวเตอร์ในปัจจุบันจะมีระบบการป้องกันขั้นพื้นฐานอยู่แล้ว คือ มีระบบการควบคุมการทำงานของซอฟต์แวร์ ฮาร์ดแวร์ และ ระบบข้อมูล เช่น อนุญาตให้เฉพาะผู้มีสิทธิรู้ข้อมูลจึงจะเข้าถึงข้อมูลได้เท่านั้น โดยต้องบอกรหัสผ่าน (password) ให้ถูกต้องเสียก่อน แต่อย่างไรก็ตาม ระบบการป้องกันข้อมูลขั้นพื้นฐานยังไม่เพียงพอสำหรับข้อมูลที่มีความสำคัญมาก ๆ เช่น ข้อมูลที่เกี่ยวกับความมั่นคงของชาติ ถ้าข้อมูลเหล่านี้รั่วไหลไปถึงศัตรูของชาติ หรือถูกแก้ไขปลอมแปลง ก็จะก่อให้เกิดความเสียหายต่อความมั่นคงของชาติได้ หรือในกรณีข้อมูลที่สำคัญของบริษัทรั่วไหลไปถึงบริษัทคู่แข่ง ก็จะทำให้เกิดผลเสียต่อการดำเนินกิจการของบริษัทได้

1.2 การเข้ารหัสลับ (Cryptography)

จากเหตุผลที่กล่าวมาข้างต้น จึงมีความจำเป็นที่จะต้องเพิ่มมาตรการเพื่อป้องกันข้อมูลที่มีความสำคัญเป็นพิเศษ วิธีการหนึ่งที่สามารถกระทำได้ ก็คือ การแปลงข้อมูลเหล่านั้นให้อยู่ในรูปแบบอื่นที่แตกต่างไปจากเดิม เพื่อปกปิดเนื้อหาที่แท้จริง ซึ่งเรียกว่า การเข้ารหัสลับข้อมูล (Cryptography) โดยจะนำข้อมูลที่มีความสำคัญมาเข้ารหัสลับก่อนที่จะเก็บข้อมูลเหล่านั้นลงในสื่อบันทึกข้อมูล หรือส่งออกไปยังที่อื่น ๆ โดยผ่านเครือข่ายสื่อสาร

ในการเข้ารหัสลับนี้จะต้องมีอัลกอริทึมสำหรับเข้ารหัสลับ ซึ่งเป็นขั้นตอนการแปลงข้อมูลให้มีรูปแบบที่เปลี่ยนไป และมีคีย์สำหรับเข้ารหัสลับ ซึ่งอาจจะเป็นตัวเลข หรือ ข้อความ ซึ่งถูกเก็บเป็นความลับ และเมื่อต้องการเข้ารหัสลับข้อมูลก็จะนำข้อมูลและคีย์สำหรับการเข้ารหัสลับผ่านเข้าไปทำงานในอัลกอริทึม ก็จะได้ผลลัพธ์เป็นข้อมูลที่เข้ารหัสแล้ว จะมีเพียงเจ้าของและผู้มีสิทธิที่รู้ค่าคีย์สำหรับเข้ารหัสลับเท่านั้น ที่จะถอดรหัสข้อมูลให้อยู่ในรูปเดิมได้ โดยวิธีการเข้ารหัสลับนี้จะทำให้ข้อมูลมีความปลอดภัย เพราะถ้าข้อมูลนี้ตกไปอยู่ในมือของผู้อื่นที่ไม่มีสิทธิหรือฝ่ายตรงข้ามก็จะไม่มีประโยชน์เพราะข้อมูลอยู่ในรูปแบบที่ไม่อาจอ่านเข้าใจได้ ไม่ได้มีความหมาย

หมายที่แท้จริงและไม่สามารถที่จะถอดรหัสข้อมูลได้ เนื่องจากไม่ทราบค่าคีย์สำหรับเข้ารหัสลับ หรือไม่ทราบขั้นตอนการทำงานของอัลกอริทึมที่ใช้ในการถอดรหัส

จะเห็นว่า สิ่งที่สำคัญสำหรับการเข้ารหัสลับ ก็คือ คีย์สำหรับการเข้ารหัสลับ ซึ่งจะต้องเก็บเป็นความลับไม่ให้ผู้ที่ไม่มีส่วนเกี่ยวข้องรู้ และอัลกอริทึมที่ใช้สำหรับการเข้ารหัส จะต้องมีการทำงานที่มีประสิทธิภาพ มีขั้นตอนการทำงานที่ซับซ้อน สามารถป้องกันข้อมูลให้มีความปลอดภัยได้ ทำให้ผู้ที่สามารถดักจับข้อมูลได้จะไม่สามารถที่จะหาค่าคีย์หรือข้อมูลที่แท้จริงได้

1.3 การปรับเปลี่ยนอัลกอริทึมสำหรับการเข้ารหัสลับ

เนื่องจากความเจริญก้าวหน้าทางด้านเทคโนโลยี ทำให้อัลกอริทึมสำหรับการเข้ารหัสลับที่มีการใช้กันอยู่แต่เดิมอาจจะให้ความปลอดภัยไม่เพียงพอ นั่นคือ มีความเป็นไปได้ที่ผู้ไม่หวังดีจะค้นหาว่าคีย์ที่ใช้สำหรับเข้ารหัสลับคืออะไรและสามารถถอดรหัสข้อมูลได้

ดังนั้น การวิจัยนี้มีจุดประสงค์เพื่อศึกษาหาอัลกอริทึมสำหรับการเข้ารหัสลับที่มีประสิทธิภาพ มีความซับซ้อนในการทำงาน โดยจะทำการศึกษาอัลกอริทึมสำหรับการเข้ารหัสลับแบบต่าง ๆ ที่มีการใช้กันอยู่ในปัจจุบัน และได้พบว่า อัลกอริทึมเดส (Data Encryption Standard : DES) ซึ่งเป็นอัลกอริทึมที่ได้รับความนิยมอย่างสูง และเป็นอัลกอริทึมที่ได้รับการยอมรับให้เป็นมาตรฐานจาก National Bureau of Standard (NBS) เป็นอัลกอริทึมที่มีประสิทธิภาพสูง มีความซับซ้อนในการทำงาน ยังสามารถที่จะปรับเปลี่ยนการทำงานของอัลกอริทึมนี้ในบางส่วนให้มีความซับซ้อนยิ่งขึ้นได้ ทำให้เมื่อนำอัลกอริทึมนี้มาเข้ารหัสแล้ว จะทำให้ข้อมูลมีความปลอดภัย การวิจัยนี้จะเน้นการศึกษาขั้นตอนการทำงานของอัลกอริทึมเดส และแนวทางในการปรับเปลี่ยนอัลกอริทึมเดสให้มีการทำงานที่ซับซ้อนยิ่งขึ้น และเพื่อความสะดวกจะเรียกอัลกอริทึมเดส ที่ได้ปรับเปลี่ยนแล้วว่า **อัลกอริทึมไอเดส (Improved DES)**

1.4 วัตถุประสงค์ของการวิจัย

เพื่อทำการปรับเปลี่ยนอัลกอริทึมเดสให้มีประสิทธิภาพ มีความซับซ้อนในการทำงานมากขึ้น ทำให้ข้อมูลมีความปลอดภัย สามารถป้องกันข้อมูลได้ดีกว่าอัลกอริทึมเดสแบบเดิม

1.5 ขอบเขตการวิจัย

1. การวิจัยนี้จะเน้นศึกษาในเรื่องของอัลกอริทึมเดส
2. การสร้างและการพัฒนาโปรแกรมจะใช้ภาษา C
3. ในการวิจัยนี้จะทดสอบโปรแกรมบนไมโครคอมพิวเตอร์ ประเภท IBM PC

1.6 ขั้นตอนและวิธีการดำเนินการวิจัย

1. ศึกษาค้นคว้าแนวความคิดพื้นฐานของการเข้ารหัสลับข้อมูล
2. ศึกษาค้นคว้าอัลกอริทึมเดส (Data Encryption Standard Algorithm หรือ DES)
3. ทำการพัฒนาปรับเปลี่ยนอัลกอริทึมเดส
4. พัฒนาโปรแกรมเพื่อใช้ในการทดสอบ
5. ทำการทดสอบเปรียบเทียบประสิทธิภาพระหว่างอัลกอริทึมเดสและอัลกอริทึมที่ได้ปรับเปลี่ยนแล้ว หรือ อัลกอริทึมไอเดส โดยจะใช้วิธีการวิเคราะห์ความสัมพันธ์ของข้อมูลเข้ารหัสและข้อมูลเนื้อแท้ และพิสูจน์โดยใช้วิธีการทางคณิตศาสตร์และสถิติ
6. สรุปผลวิจัยและข้อเสนอแนะ

1.7 ประโยชน์ที่คาดว่าจะได้รับ

1. ได้อัลกอริทึมใหม่ที่มีขั้นตอนการทำงานที่ซับซ้อนขึ้นยากแก่การทำลาย และมีประสิทธิภาพมากขึ้นกว่าการใช้อัลกอริทึมเดส
2. สามารถนำอัลกอริทึมนี้ไปใช้สำหรับเข้ารหัสข้อมูลที่มีความสำคัญ ซึ่งจะทำให้ข้อมูลมีปลอดภัยยิ่งขึ้น
3. เป็นแนวทางในการศึกษาในเรื่องการเข้ารหัสลับต่อไปในอนาคต