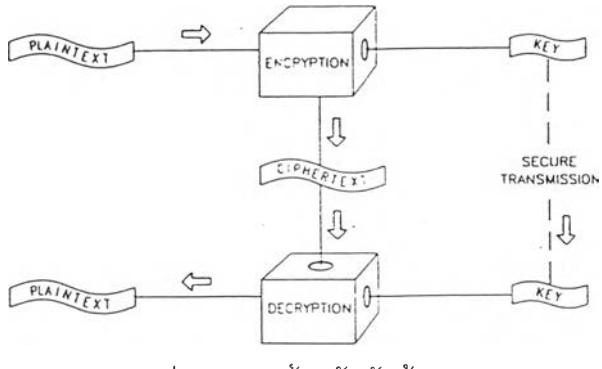
บทที่ 1

บทนำ

ความเบื้องต้น

ในปัจจุบัน ข้อมูลข่าวสารนับว่ามีความสำคัญอย่างยิ่งในทุกวงการ รูปแบบของการให้ข้อมูลข่าวสารก็มีมากมายหลายรูปแบบไม่ว่าจะเป็นทางโทรทัศน์ วิทยุ โทรศัพท์ หรือข่าย สื่อสารข้อมูลต่างๆ ข่าวสารที่มีการให้แก่กันก็มีทั้งในรูปของภาพ เสียง และข้อมูลทางคอมพิวเตอร์ (Computer Data) การส่งข่าวสารเหล่านี้ก็มีพัฒนาการขึ้นมาจากที่ส่งกันตัวต่อตัวส่งกันในกลุ่มเล็กๆ ที่มีช่องทางการสื่อสารของตัวเองหรือส่งกันในข่ายสื่อสารสาธารณะขนาดใหญ่ที่มีผู้ใช้บริการเป็นจำนวนมากข้อมูลที่ส่งกันในข่ายสื่อสารก็จะมีทั้งข้อมูลที่ต้องการจะเผยแพร่ให้แก่สาธารณชนได้ทราบได้ และข้อมูลที่ต้องการรักษาไว้เป็นความลับรู้กันแต่เฉพาะในบุคคลที่เราต้องการให้รู้ ในกรณีของการส่งข่าวสารความลับที่ต้องการให้เฉพาะผู้ที่เราตั้งใจจะส่งข่าวสารให้เท่านั้นคนอื่นไม่สามารถรับข่าวสารได้ เราก็อาจจะใช้วิธีการส่งผ่านช่องสื่อสารที่เป็นเฉพาะของเราเองซึ่งก็จะเป็นการปลอดภัยในระดับหนึ่งแต่ถ้าหากว่าช่องสื่อสารนั้นถูกเชื่อมต่อด้วยอุปกรณ์รับข้อมูลของผู้ไม่ประสงค์ดีข้อมูลที่เป็นความลับนั้นก็จะมีการรั่วไหลออกไปในกรณีที่ต้องการส่งข้อมูลความลับแต่ไม่มีช่องสื่อสารที่เป็นของตัวเองจำเป็นต้องส่งข้อมูลความลับนั้นผ่านข่ายสื่อสารสาธารณะที่มีผู้ใช้งานคนอื่นร่วมอยู่ด้วยในข่ายเป็นจำนวนมากก็ไม่สามารถกระทำได้ดังนั้นทางออกวิธีหนึ่งสำหรับปัญหาเหล่านี้คือการทำการเข้ารหัสลับข้อมูล (Data Encryption) ก่อนที่จะส่งออกไปเพื่อป้องกันมิให้ผู้อื่นรับข่าวสารนั้นได้นอกจากผู้ที่เราต้องการเท่านั้น ดังแสดงไว้ในรูปที่ 1.1



รูป 1.1 การเข้ารหัสลับข้อมูล [Caelli,1991]

โดยที่เพลนเท็กซ์(Plaintext)คือข้อความก่อนที่จะถูกเข้ารหัสหรือหลังจากที่ถูกถอดรหัสแล้วและไซเฟอร์เท็กซ์(Ciphertext) คือข้อความหลังจากที่ถูกเข้ารหัส

วิธีการเข้ารหัสลับก็มีหลายวิธี เช่น การสลับตำแหน่งของตัวอักษร (Transposition) ในข้อความนั้น การแทนที่ตัวอักษร (Substitution) เดิมด้วยชุดของตัวอักษรใหม่หรือ อาจจะใช้ทั้ง 2 วิธีร่วมกันเพื่อเพิ่มความปลอดภัยอย่างไรก็ตามเพื่อให้การส่งข้อความที่เป็นรหัสลับไม่จำกัดอยู่ในวงผู้สนทนาเพียงผู้ใดผู้หนึ่งที่มีช่องสื่อสารส่วนตัวอยู่ในข่ายสื่อสารขนาดเล็กที่มีวิธีการเข้ารหัสแบบสลับตำแหน่งหรือแทนที่ตำแหน่งด้วยวิธีการที่แล้วแต่คู่สนทนาจะคิดขึ้นมาเองซึ่งไม่เป็นมาตรฐานทาง NBS(National Bureau of Standard) จึงได้กำหนดมาตรฐานสำหรับการเข้ารหัสลับข้อมูลขึ้นมาเรียกว่า DES (Data Encryption Standard) เพื่อเป็นระบบรักษาความปลอดภัยของข้อมูล ทั้งทางด้านการพาณิชย์ การเงินการธนาคาร

DES จะมีอัลกอริธึ่มในการเข้ารหัสลับที่ประกอบด้วยการแทนที่และการสลับตำแหน่งข้อมูลการใช้คีย์ (Key) เป็นตัวแปรสำคัญในการนำเข้าหรือถอดรหัสซึ่งผู้รับและผู้ส่งข้อมูลจะต้องใช้คีย์ให้ตรงกันจึงจะสามารถถอดรหัสได้ถูกต้อง DES ใช้คีย์ซึ่งมีความยาว 56 บิทดังนั้นผู้ที่จะพยายามถอดรหัสโดยไม่ทราบคีย์จะต้องทำการสุ่มค่าคีย์ถึง 2^{56} ครั้ง ซึ่งนับว่ายากมากที่จะทำการสำเร็จในเวลาที่จำกัด อย่างไรก็ตามถึงแม้ว่าความปลอด ภัยในด้านจำนวนคีย์ที่มีมากนั้น จะทำให้ DES เป็นที่นิยมใช้กันแพร่หลาย แต่ถ้าข้อมูลที่เรานำมาเข้ารหัสเป็นข้อมูลที่มีความมีรูปแบบอยู่มาก เช่น ข้อมูลประเภทที่เป็นตารางแสดงค่าหรือเปรียบเทียบค่าต่าง ๆ เหล่านี้เมื่อใช้ DES ในการเข้ารหัสข้อมูลแล้วไซเฟอร์เท็กซ์จะยังคงลักษณะความมีรูปแบบของข้อมูลอยู่ซึ่งจะเป็นประโยชน์สำหรับผู้ที่ต้องการข้อมูลส่วนนั้นแต่ไม่ทราบคีย์ นอกจากนี้ในกรณีที่ไซเฟอร์เท็กซ์ถูกเพิ่มเติมหรือลดขนาดลงไปเพลนเท็กซ์ที่ถอดรหัสออกมาได้จะผิดพลาดทั้งหมดตั้งแต่จุดที่ถูกเพิ่มหรือลดข้อมูลนั้นซึ่งลักษณะเช่นนี้เรียกว่าการแพร่กระจายของการผิดพลาด (Error Propagation) จากปัญหาเหล่านี้ทำให้มีการคิดวิธีการในการเข้ารหัสเพื่อแก้ไขโดยยังคงใช้ DES วิธีการที่สร้างขึ้นมานี้เรียกว่า ไซเฟอร์บล็อกเชนนิ่ง (Cipher Block Chaining)ซึ่งสามารถแก้ปัญหาการเข้ารหัสข้อมูลที่มีลักษณะความมีรูปแบบได้แต่ปัญหาการแพร่กระจายของความผิดพลาดจะยังคงมีอยู่

<u>วัตถุประสงค์ของการวิจัย</u>

1. เพื่อสร้างเครื่องเข้ารหัสข้อมูล(Data Encryptor)ที่ใช้ DES โดยมีโหมดในการเข้ารหัสแบบ ECB,CBC, CFB และ OFB อยู่บนเครื่องเดียวกัน

2. สามารถใช้เครื่องเข้ารหัสข้อมูลนี้เป็นเครื่องออเทนธิเคเตอร์(Authenticator)โดยไม่ต้องเพิ่มฮาร์ดแวร์ส่วนอื่น

3. สร้างโปรแกรมใช้งานและควบคุมดาต้าเอนคริปเตอร์และออเทนธิเคเตอร์ให้สะดวกกับการใช้งาน

4. เพื่อเป็นเครื่องต้นแบบที่จะใช้สำหรับงานพัฒนาโหมดในการเข้ารหัสข้อมูลแบบอื่นๆ

ประโยชน์ที่คาดว่าจะได้รับ

1. สามารถใช้ดาต้าเอนคริปเตอร์ในการเข้าและถอดรหัสเพื่อรักษาความปลอดภัยของข้อมูลได้หลายโหมดบนเครื่องเดียวกัน

2. สามารถใช้ออเทนธิเคเตอร์ในการตรวจสอบข้อมูลที่รับได้ว่าเป็นข้อมูลที่แท้จริง ไม่ถูกแก้ไขเปลี่ยนแปลงในระหว่างการส่งผ่านช่องสื่อสาร

3. เป็นการสร้างพื้นฐานความเข้าใจเกี่ยวกับการเข้ารหัสจากคีย์ส่วนตัว (Private Key) สู่คีย์สาธารณะ (Public Key) ซึ่งมีแนวโน้มว่าจะเกิดขึ้นในระบบสื่อสารข้อมูลในอนาคต

4. เป็นแนวทางในการพัฒนาเอนคริปเตอร์และออเทนธิเคเตอร์ไปสู่เชิงพาณิชย์ เนื่องจากยังไม่มีสินค้าประเภทนี้มากนักในตลาดภายในประเทศ