เอกสารประกอบการสอน

204505

ความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ

ธรา อั่งสกุล

เทคโนโลยีสารสนเทศ

มหาวิทยาลัยเทคโนโลยีสุรนารี

คำนำ

รายวิชา 204505 ความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ เป็นหนึ่งในรายวิชาบังคับของหลักสูตรวิทยาการสารสนเทศมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีสุรนารี ที่มุ่งเน้นให้นักศึกษา มีความรู้ความเข้าใจเกี่ยวกับ แนวคิดเกี่ยวกับความมั่นคงปลอดภัยในระบบคอมพิวเตอร์ ความปลอดภัยในไปรษณีย์อิเล็กทรอนิกส์และระบบปฏิบัติการต่างๆ การตรวจสอบความถูกต้องของข้อความ การเข้ารหัสและการถอดรหัสชนิดต่างๆ คณิตศาสตร์ทางด้านความปลอดภัย กุญแจสาธารณะ เทคนิคการโจมตีและการป้องกันด้านความปลอดภัยของระบบเครือข่าย ความปลอดภัยของโปรแกรมประยุกต์ ประเด็นกฎหมายและจริยธรรมที่เกี่ยวข้อง แนวโน้ม และการประยุกต์งานด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ

ผู้เขียนหวังว่าเอกสารประกอบการสอนเล่มนี้จะ มีส่วนช่วยให้นักศึกษาสามารถบรรลุวัตถุประสงค์ของรายวิชาดังกล่าว และสามารถใช้ความรู้ด้วยจริยธรรมกำกับอย่างมีประสิทธิภาพ

สารบัญ

บทที่ 1

ความรู้พื้นฐานเกี่ยวกับความมั่นคง

- ประวัติศาสตร์
- เป้าหมาย
- การโจมตี
- การให้บริการและกลไก
- เทคนิค

บทที่ 1

ความรู้พื้นฐานเกี่ยวกับความมั่นคง

ซุนวูได้กล่าวในตำราพิชัยสงครามว่า *''จงอย่าวางใจว่าข้าศึกจะไม่มาราวี เราต้องเตรียมพร้อมรับมือ''* ประโยคนี้ถือเป็นหัวใจสำคัญของการทำสงคราม การทำสงครามกับภัยคุกคามต่างๆ ในโลกคอมพิวเตอร์ก็เช่นเดียวกัน เราจำเป็นที่จะต้องต้องเตรียมพร้อมรับมือกับการโจมตีในทุกรูปแบบ

ในปัจจุบัน คำว่า *''แฮกเกอร์''* * เริ่มพบเห็นมากขึ้นในสื่อข่าวต่างๆ ซึ่งแสดงให้เห็นถึงภัยคุกคามและการโจมตีในโลกคอมพิวเตอร์ที่ใกล้ตัวและเพิ่มมากขึ้น ดังนั้นทุกคนโดยเฉพาะอย่างยิ่ง บุคลากรทางด้านเทคโนโลยีสารสนเทศทุกคน จะต้องตระหนักถึงภัยคุกคามต่างๆ และเตรียมพร้อมรับมือ ซึ่งเหตุผลสำคัญที่ทำให้เกิดภัยคุกคามในโลกคอมพิวเตอร์เพิ่มมากขึ้น เนื่องจากเกือบทุกสิ่งทุกอย่างในชีวิตประจำวันนั้น ถูกควบคุมหรือจัดเก็บด้วยระบบคอมพิวเตอร์ เช่น ระบบควบคุมการจราจร สาธารณูปโภคต่างๆ สถาบันทางการเงิน ข้อมูลของบริษัทต่างๆ หรือ แม้กระทั่งเกรดของนักศึกษาในวิชานี้ก็ถูกจัดเก็บและควบคุมอยู่ในระบบคอมพิวเตอร์เช่นเดียวกัน

1.1 ประวัติศาสตร์

ประวัติศาสตร์ด้านความมั่นคงปลอดภัยมีมานานก่อนสมัยพุทธกาล เริ่มตั้งแต่การเข้ารหัสแบบต่างๆ ซึ่งการเข้ารหัสส่วนใหญ่ถูกคิดค้นสำหรับ ใช้ในการส่งความลับระหว่างการทำสงคราม ในยุคถัดมา เมื่อมีการนำเทคโนโลยี ต่างๆ มาใช้ เช่น โทรเลข โทรศัพท์ เครื่องคอมพิวเตอร์ส่วนบุคคล และ ระบบเครือข่ายเทคโนโลยีต่างๆ เหล่านี้ก็ถูกเป็นเป้าหมายของการโจมตีด้วยวิธีการต่างๆ ซึ่งตัวอย่างของเหตุการณ์ด้านความมั่นคงปลอดภัยเหล่านี้ได้แสดงไว้ในตารางที่ 1.1

* คำว่า แฮกเกอร์ จริงๆ แล้วหมายถึงบุคคลที่ชอบค้นหาสิ่งต่างๆ มิได้มีความหมายในเชิงผู้บุกรุกแต่ประการใด สำหรับผู้บุกรุกซึ่งทำให้ผู้อื่นเสียหายนั้น ควรจะใช้คำว่า แครกเกอร์ มากกว่า

ตารางที่ 1.1: ตัวอย่างของเหตุการณ์ด้านความมั่นคงปลอดภัย

ปีพุทธศักราช	เหตุการณ์ด้านความมั่นคง
ประมาณ 1350 ปีก่อน พ.ศ.	การเข้ารหัสครั้งแรก ชาวสุมาเรียนได้ประดิษฐ์ตัวอักษรแบบคูเนฟอร์ม ซึ่งเป็นยุคเดียวกับที่ชาวอียิปต์ได้ประดิษฐ์ ตัวอักษรแบบไฮโรไกลฟิกส์
43	การเข้ารหัสของชาวฮิบบรู ซึ่งเป็นการเข้ารหัสด้วยการแทนที่ตัวอักษร เช่น การเข้ารหัสแบบแอทแบช
493	การเข้ารหัสของซีซ่า ซึ่งตั้งชื่อตามจูเลียส ซีซ่า ผู้นำทางทหารของชาวโรมัน ซึ่งเป็นผู้ใช้การแทนที่ตัวด้วยตัวอักษรที่ถัดไป 3 ตัวอักษร ในการส่งข้อความลับของทหารโรมัน
2387	การดักฟังโทรเลข
2443	การดักฟังวิทยุสื่อสาร
2466	กำเนิดเครื่องเข้ารหัสอีนิกมา ซึ่งถูกคิดค้นโดยวิศวกรชาวเยอรมันในช่วงหลังสงครามโลก ครั้งที่ 1 ซึ่งเครื่องดังกล่าวได้มีบทบาทอย่างมากในช่วงการทำสงครามโลกครั้งที่ 2 และเป็นส่วนหนึ่งที่ทำให้เยอรมันแพ้สงคราม เนื่องจากโปแลนด์และอังกฤษสามารถ ถอดรหัสเครื่องดังกล่าวได้
2517	การเข้ารหัสด้วยดีอีเอส เป็นมาตรฐานการเข้ารหัสแบบสมมาตร (ซึ่งจะกล่าวรายละเอียดในหัวข้อที่ 3.2)
2519	การเข้ารหัสด้วยกุญแจสาธารณะ เป็นการเข้ารหัสแบบอสมมาตร (ซึ่งจะกล่าวรายละเอียดในหัวข้อที่ 5.2)
2528	การดักฟังเครือข่าย
2531	การโจมตีอินเตอร์เน็ตด้วยหนอนมอริส ซึ่งมีผลกระทบกับเครื่อง 10ของอินเทอร์เน็ต ในยุคนั้น
2534	การเข้ารหัสด้วยพีจีพี ซึ่งเป็นโปรแกรมประยุกต์ที่ออกแบบสำหรับการส่งข้อความลับ และ ลายมือชื่อดิจิทัล
2537	การโจมตีด้วยรูทคิท ซึ่งเป็นโปรแกรมที่สามารถทำให้ผู้โจมตีกลายเป็นผู้ดูแลระบบ ของเครื่องที่ถูกโจมตี
2538	การใช้งานเอสเอสแอล ซึ่งเป็นลำดับชั้นที่ทำให้โปรแกรมเมอร์สามารถ เขียนโปรแกรมเพื่อส่งข้อความลับได้ง่าย
2543	การใช้งานเออีเอส (เรนดอล) ซึ่งเป็นมาตรฐานการเข้ารหัสแบบสมมาตรชั้นสูง (ซึ่งจะกล่าวรายละเอียดในหัวข้อที่ 4.1)
2543	การโจมตีด้วยเทคนิคดีดอส ซึ่งเป็นการใช้เครื่องคอมพิวเตอร์หลายเครื่องช่วยกันรุมโจมตีเครื่องเหยื่อด้วยการส่งข้อมูลมหาศาลจนเครื่องเหยื่อไม่สามารถใช้งานได้
2552 (วันที่ 23 พฤศจิกายน)	เว็บไซต์หน้าแรกของมหาวิทยาลัยเทคโนโลยีสุรนารี โดนโจมตีด้วยมัลแวร์

1.2 เป้าหมาย

ในอดีตเมื่อกล่าวถึงความมั่นคงปลอดภัย องค์กรต่างๆ ก็จะนึกถึงการป้องกันทางกายภาพ เพื่อป้องกันการโจรกรรมข้อมูล หรือขโมยของต่างๆ จากการเดินเข้ามาขโมย ซึ่งสามารถป้องกันได้ด้วย การใช้กำแพงหรือรั้วที่แน่นหนา การติดตั้งอุปกรณ์ป้องกันและตรวจจับขโมยต่างๆ เช่น อุปกรณ์ตรวจจับความเคลื่อนไหว กล้องวงจรปิด เป็นต้น แต่อย่างไรก็ตามการป้องกันดังกล่าวสามารถใช้ได้เฉพาะกับจารกรรมจากภายนอกองค์กร ดังนั้น การป้องกันการโจมตีจากบุคลากรภายในองค์กรเองก็เป็นเรื่องที่สำคัญ ซึ่งสามารถป้องกันได้ด้วย การคัดเลือกพนักงานที่มีคุณธรรมและจริยธรรมเข้าทำงาน เนื่องจากองค์กรในปัจจุบันเป็นองค์กรที่อยู่ในยุคดิจิทัล หรือกล่าวอีกนัยหนึ่งว่าเป็น องค์กรซึ่งประยุกต์ใช้เทคโนโลยีสารสนเทศมากขึ้น ดังนั้น การป้องกันจึงต้องคำนึงถึง การป้องกันระบบคอมพิวเตอร์และเครือข่ายจากการโจมตีในรูปแบบต่างๆ ด้วย เพื่อไม่ให้ข้อมูลและสารสนเทศขององค์กรถูกโจมตี

เป้าหมายของความมั่นคงปลอดภัย มีจุดประสงค์หลัก 3 ข้อ คือ การรักษาความลับ, บูรณภาพ และสภาพพร้อมใช้งาน

- **การรักษาความลับ** หมายถึง การป้องกันไม่ให้เข้าถึงข้อมูลจากคนที่ไม่มีสิทธิ์ หรือการรักษาความลับของข้อมูล ทั้งข้อมูลที่ถูกจัดเก็บอยู่และ ข้อมูลที่กำลังรับส่งอยู่ เช่น การป้องกันความลับทางการทหาร การป้องกันข้อมูลสำคัญรั่วไหลจากองค์กรไปยังคู่แข่ง การรักษาความลับของบัญชีลูกค้าธนาคาร เป็นต้น
- **บูรณภาพ** หมายถึง การป้องกันการเปลี่ยนแปลงข้อมูลจากคนที่ไม่มีสิทธิ์ เช่น ธนาคาร จำเป็นต้องมีการป้องกันการเปลี่ยนแปลงข้อมูลที่สื่อสาร กันระหว่างตู้เอทีเอ็มและธนาคาร เป็นต้น
- **สภาพพร้อมใช้งาน** หมายถึง การให้คนที่มีสิทธิสามารถเข้าถึงข้อมูลได้ตลอดเวลาที่ต้องการ เช่น ลูกค้าธนาคารต้องสามารถเข้าถึงข้อมูลบัญชีของตัวเองได้ตลอดเวลา เป็นต้น

1.3 การโจมตี

การโจมตีในโลกคอมพิวเตอร์นั้นส่วนใหญ่แล้วจะเกิดจากบุคคล ภายในองค์กรนั่นเอง เพราะเป็นผู้ที่สามารถเข้าถึงข้อมูลได้ง่ายที่สุด ดังนั้นผู้ดูแลป้องกันระบบจึงจำเป็นต้อง ตระหนักถึงความจริงดังกล่าว นอกจากนั้นการโจมตียังอาจเกิดจากอาชญากรหรือผู้ก่อการร้าย ซึ่งโจมตีระบบคอมพิวเตอร์เพื่อต้องการจารกรรมข้อมูล ตั้งแต่ข้อมูลส่วนบุคคล เช่น ข้อมูลบัตรเครดิต ไปจนถึง ข้อมูลทางการค้าของบริษัท การโจมตีระบบคอมพิวเตอร์นั้น อาจจะไม่ได้ถูกกระทำโดยมืออาชีพเพียงอย่างเดียว แต่ยังอาจถูกกระทำโดยมือสมัครเล่น เช่น นักศึกษาที่มีความรู้ด้านความมั่นคงปลอดภัยของ เทคโนโลยีสารสนเทศแต่ใช้ความรู้ในทางที่ผิด (หวังว่าคงจะไม่ใช่ผู้อ่าน) เป็นต้น สำหรับเหตุผลของการโจมตีของผู้โจมตีแต่ละคนนั้น อาจจะแตกต่างกันไป ตั้งแต่ เรื่องเงินหรือความโลภ, การเมือง, การทหาร, ความผิดปกติทางจิต

ไปจนถึงการแข่งขันในเชิงของกีฬา ซึ่งการโจมตีเหล่านี้เป็นสิ่งที่กระทำได้ง่าย แต่ตรวจจับและลงโทษได้ยากมาก ซึ่งโดยทั่วไปแล้วการโจมตีต่างๆ สามารถแบ่งประเภทได้เป็น 2 ประเภท คือ การโจมตีอกัมมันต์และการโจมตีกัมมันต์

- **การโจมตีอกัมมันต์** เป็นการโจมตีเพื่อมีจุดประสงค์ในการได้มาซึ่งข้อมูล โดยไม่มีการเปลี่ยนแปลงหรือทำลายข้อมูล การโจมตีดังกล่าวส่วนใหญ่แล้วเหยื่อจะไม่รู้ตัว ทำให้ตรวจสอบการถูกโจมตีได้ยาก แต่อย่างไรก็ตามวิธีการโจมตีดังกล่าวสามารถป้องกันได้ด้วยการเข้ารหัสข้อมูล ตัวอย่างของการโจมตีอกัมมันต์ได้แก่ การดักจับข้อความที่ส่งรับกันด้วยโปรแกรมรับส่งข้อความ เช่น โปรแกรมเอ็มเอสเอ็น การขโมยข้อมูลส่วนตัวจากถังขยะ การหลอกถามข้อมูลด้วยการปลอมเป็นบุคคลอื่น เป็นต้น

- **การโจมตีกัมมันต์** เป็นการโจมตีดังกล่าวมีวัตถุประสงค์เพื่อการเปลี่ยนแปลงหรือทำลายข้อมูล ซึ่งจะสามารถตรวจสอบได้ง่าย เนื่องจากเหยื่อจะรู้ตัวแต่ป้องกันได้ยาก ตัวอย่างของการโจมตีกัมมันต์ ได้แก่ การโจมตีด้วยไวรัส หนอนอินเตอร์เน็ต ม้าโทรจันและโปรแกรมประสงค์ร้ายชนิดอื่นๆ การโจมตีด้วยเทคนิคดีดอส เป็นต้น

นอกจากนั้นรูปแบบการโจมตียังสามารถแบ่งตามผลกระทบต่อเป้าหมายความมั่นคง ได้เป็น 3 ประเภท คือ การโจมตีซึ่งส่งผลต่อการรักษาความลับ การโจมตีซึ่งส่งผลต่อบูรณภาพ และ การโจมตีซึ่งส่งผลต่อสภาพพร้อมใช้งาน

- **การโจมตีซึ่งส่งผลต่อการรักษาความลับ** ได้แก่ การดักจับหรือขโมยข้อมูล ซึ่งสามารถป้องกันได้ด้วยการเข้ารหัสซึ่งทำให้ถึงแม้ข้อมูลจะถูกดักจับหรือถูกขโมย แต่ผู้ดักจับจะไม่สามารถเข้าใจข้อมูลดังกล่าวได้หากไม่มีการถอดรหัส แต่อย่างไรก็ตาม หากผู้โจมตีวิเคราะห์การจราจรของเครือข่ายก็สามารถทราบข้อมูลอื่นๆ เช่น ที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ ของทั้งผู้ส่งและผู้รับ นอกจากนั้นผู้โจมตียังสามารถวิเคราะห์การส่งและรับข้อมูล เช่น ถ้าผู้ส่งส่งข้อมูลแบบหนึ่งแล้วผู้รับจะตอบอย่างไร ทำให้ทราบรูปแบบการรับส่งข้อมูล เป็นต้น

- **การโจมตีซึ่งส่งผลต่อบูรณภาพ** สามารถทำได้หลายรูปแบบ ได้แก่ การแก้ไขข้อมูลโดยการดักจับข้อมูลจากการส่งแล้วเปลี่ยนแปลงข้อมูลก่อนจะส่งไปให้ผู้รับ (ฤๅษีแปลงสาร) การสวมรอยเป็นบุคคลอื่น (เช่น สร้างเว็บไซต์สวมรอยว่าเป็นเว็บไซต์ธนาคาร เพื่อหลอกรู้ค้าของธนาคารนั้น) การส่งข้อมูลซ้ำโดยการดักจับข้อมูลที่ส่งจริงแล้วส่งข้อมูลดังกล่าวอีกรอบ (เช่น การส่งข้อมูลการถอนเงินซ้ำเพื่อจะได้เงินสองเท่า) การปฏิเสธความรับผิดชอบ เช่น ผู้รับปฏิเสธว่าไม่เคยรับข้อมูล หรือ ผู้ส่งปฏิเสธว่าไม่เคยส่งข้อมูล

- **การโจมตีซึ่งส่งผลต่อสภาพพร้อมใช้งาน** สามารถกระทำโดย เทคนิคที่เรียกว่า ดอส หรือการทำให้ผู้ให้บริการปฏิเสธการให้บริการ เช่น ผู้โจมตีส่งข้อมูลมหาศาลไปให้เหยื่อจนเหยื่อไม่สามารถ

ให้บริการได้ ซึ่งการโจมตีดังกล่าวถือว่าเป็นวิธีที่นิยมมาก เช่น ผู้โจมตีส่งข้อมูลมหาศาลไปยังเว็บเซิฟเวอร์ จนเครื่องดังกล่าวไม่สามารถให้บริการอื่นได้

รูปแบบการโจมตีทั้งหมดที่ได้กล่าวไปแล้วสามารถสรุปได้ดังตาราง 1.2

ตารางที่ 1.2: รูปแบบการโจมตี

การโจมตี	ประเภท	ผลกระทบ
การดักจับข้อมูล การวิเคราะห์การจราจร	อกัมมันต์	การรักษาความลับ
การแก้ไขข้อมูล การสวมรอย การส่งข้อมูลซ้ำ การปฏิเสธความรับผิดชอบ	กัมมันต์	บูรณภาพ
การปฏิเสธการให้บริการ	กัมมันต์	สภาพพร้อมใช้งาน

1.4 การให้บริการและกลไก

หน่วยมาตรฐานโทรคมนาคมของสหภาพการสื่อสารทางไกลนานาชาติ (ไอทียู-ที) ได้เสนอการให้บริการและกลไกด้านความมั่นคงและกำหนดไว้ในมาตรฐาน ไอทียู-ที(เอ็กซ์.800) ดังนี้

1.4.1 การให้บริการด้านความมั่นคง

การให้บริการด้านความมั่นคงมี 5 ด้าน ได้แก่ ความลับของข้อมูล บูรณภาพของข้อมูล การพิสูจน์ตัวจริง การป้องกันการปฏิเสธความรับผิดชอบ และการควบคุมการเข้าถึง

- **ความลับของข้อมูล** การให้บริการรักษาความลับของข้อมูลได้ถูกออกแบบไว้สำหรับการป้อนกันการโจมตี ด้วยวิธีการดักจับข้อมูล และ การวิเคราะห์การจราจรของเครือข่าย
- **บูรณภาพของข้อมูล** การให้บริการบูรณภาพของข้อมูลได้ถูกออกแบบไว้สำหรับการป้องกันข้อมูลจาก การแก้ไข การแทรก การลบ และ การส่งข้อมูลซ้ำ
- **การพิสูจน์ตัวจริง** การพิสูจน์ตัวจริงสามารถแบ่งเป็น 2 ชนิด คือ ในกรณีการสื่อสารที่มีการกำหนดการเชื่อมต่อ จะมีการพิสูจน์ตัวจริงของทั้งผู้ส่งและผู้รับ สำหรับกรณีการสื่อสารแบบไม่กำหนดการเชื่อมต่อ จะมีเฉพาะการพิสูจน์ตัวจริงของผู้ส่งข้อมูล
- **การป้องกันการปฏิเสธความรับผิดชอบ** การป้องกันการปฏิเสธความรับผิดชอบหมายถึง การที่ผู้รับสามารถยืนยันได้ว่าผู้ส่งได้ส่งข้อมูลมาให้ตนจริง ถึงแม้ว่าผู้ส่งจะปฏิเสธการส่งก็ตาม และการที่ผู้ส่งสามารถยืนยันว่าได้ส่งข้อมูลให้ผู้รับจริง ถึงแม้ว่าผู้รับจะปฏิเสธการรับข้อมูลก็ตาม

- **การควบคุมการเข้าถึง** การควบคุมการเข้าถึง หมายถึง การควบคุมการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต เช่น การควบคุมการอ่าน การเขียน การแก้ไข การกระทำการของโปรแกรม เป็นต้น

1.4.2 กลไกด้านความมั่นคง

กลไกด้านความมั่นคงเพื่อสนับสนุนการให้บริการด้านความมั่นคงนั้นมีหลายวิธี อาทิเช่น

- **การเข้ารหัส** การเข้ารหัสเป็นวิธีการหนึ่งที่ใช้ในการรักษาความลับของข้อมูล ซึ่งปัจจุบันมีเทคนิคที่นิยมกันสองวิธี คือ การเข้ารหัสข้อความ และ การซ่อนข้อความ
- **บูรณภาพของข้อมูล** กลไกบูรณภาพของข้อมูล คือ กลไกที่ช่วยรักษาบูรณภาพของข้อมูลด้วยการที่ ฝ่ายผู้ส่งคำนวณรหัสตรวจสอบจากข้อมูล และ ส่งรหัสตรวจสอบดังกล่าวไปพร้อมกับข้อมูล ฝ่ายผู้รับจะคำนวณรหัสตรวจสอบจากข้อมูลที่ได้รับและเปรียบเทียบรหัสดังกล่าวกับรหัสตรวจสอบที่ได้รับจากผู้ส่ง หากรหัสตรวจสอบทั้งสองมีค่าตรงกัน จะถือว่าข้อมูลดังกล่าวมีบูรณภาพ คือ มิได้ถูกแก้ไขดัดแปลงระหว่างทาง
- **ลายมือชื่อดิจิทัล** ลายมือชื่อดิจิทัลเป็นกลไกที่ผู้ส่งสามารถเซ็นลายมือชื่อแบบอิเล็กทรอนิกส์ ซึ่งผู้รับสามารถตรวจสอบลายมือชื่อของผู้ส่งดังกล่าวได้ว่าเป็นของจริง
- **การแลกเปลี่ยนการพิสูจน์ตัวจริง** การแลกเปลี่ยนการพิสูจน์ตัวจริงเป็นกลไกที่ทั้งผู้ส่งและผู้รับแลกเปลี่ยนเอกลักษณ์ของแต่ละฝ่าย โดยการพิสูจน์ว่าผู้นั้นรู้สิ่งที่ควรจะรู้
- **การเสริมเต็มการจราจร** กลไกการเสริมเต็มการจราจรเป็นกลไกหนึ่งซึ่งแทรกข้อมูลลวงไว้ในการจราจรของระบบเครือข่าย เพื่อป้องกันการวิเคราะห์จราจร
- **การควบคุมเส้นทาง** กลไกการควบคุมเส้นทางเป็นการเลือกหรือเปลี่ยนเส้นทางการสื่อสารหรือหว่างผู้ส่งและผู้รับ เพื่อป้องกันการดักจับข้อมูลในเส้นทางใดเส้นทางหนึ่ง
- **การรับรอง** การรับรองเป็นกลไกที่อาศัยบุคคลที่สามที่เชื่อถือได้ในการเป็นผู้รับรองว่าผู้ส่งได้ส่งข้อมูลจริง เพื่อป้องกันการปฏิเสธความลับผิดชอบของผู้ส่งในภายหลัง
- **การควบคุมการเข้าถึง** การควบคุมการเข้าถึงเป็นกลไกที่ควบคุมการใช้งานของสิ่งต่างๆ เช่น การถามรหัสผ่าน

การให้บริการและกลไกความมั่นคงสามารถสรุปได้ดังตารางที่ 1.3

ตารางที่ 1.3: การให้บริการและกลไกด้านความมั่นคง

การให้บริการ	กลไก
ความลับของข้อมูล	การเข้ารหัส, การควบคุมเส้นทาง
บูรณภาพของข้อมูล	การเข้ารหัส, ลายมือชื่อดิจิทัล, กลไกบูรณภาพของข้อมูล
การพิสูจน์ตัวจริง	การเข้ารหัส, ลายมือชื่อดิจิทัล, การแลกเปลี่ยนการพิสูจน์ตัวจริง
การป้องกันการปฏิเสธความรับผิดชอบ	ลายมือชื่อดิจิทัล, กลไกบูรณภาพของข้อมูล, การรับรอง
การควบคุมการเข้าถึง	กลไกควบคุมการเข้าถึง

1.5 เทคนิค

1.5.1 การเข้ารหัส

เทคนิคการเข้ารหัสแบ่งเป็น 3 รูปแบบใหญ่ๆ คือ การเข้ารหัสด้วยกุญแจแบบสมมาตร การเข้ารหัสด้วยกุญแจแบบอสมมาตร และ การแฮช

การเข้ารหัสด้วยกุญแจแบบสมมาตร

การเข้ารหัสด้วยกุญแจแบบสมมาตร เป็นรูปแบบการเข้ารหัสซึ่งผู้ส่งและผู้รับข้อมูลจะเข้ารหัสและถอดรหัสด้วยกุญแจดอกเดียวกัน ซึ่งทั้งสองฝ่ายจะต้องหาวิธีตกลงเรื่องกุญแจดอกดังกล่าว

การเข้ารหัสด้วยกุญแจแบบอสมมาตร

การเข้ารหัสด้วยกุญแจแบบอสมมาตร เป็นรูปแบบการเข้ารหัสซึ่งผู้ส่งและผู้รับข้อมูลแต่ละฝ่ายจะมีกุญแจสองดอก ที่ใช้คู่กัน เรียกว่า กุญแจส่วนตัว และ กุญแจสาธารณะ กุญแจส่วนตัวจะเป็นกุญแจซึ่งเก็บเป็นความลับ ในขณะที่กุญแจสาธารณะจะประกาศให้ทุกคนรู้ การเข้ารหัสจะกระทำโดยผู้ส่งจะเข้ารหัสด้วยกุญแจสาธารณะของผู้รับ และ ผู้รับจะถอดรหัสด้วยกุญแจส่วนตัวของผู้รับเอง

การแฮช

การแฮชคือการใช้ข้อมูลฉบับย่อความยาวคงที่สั้นๆ เพื่อใช้แทนข้อความจริงความยาวเท่าใดก็ได้ซึ่งปกติแล้ว ความยาวของข้อมูลฉบับย่อจะสั้นกว่าข้อความจริงมาก การแฮชจะถูกใช้งานเพื่อบูรณภาพของข้อมูล ด้วยการคำนวณหาข้อความฉบับย่อจากข้อมูลจริงเพื่อใช้เป็นรหัสตรวจสอบว่าข้อมูลจริงมิได้ถูกแก้ไข

1.5.2 การซ่อนข้อความ

การซ่อนข้อความ เป็นเทคนิคในด้านความมั่นคงโดยการปกปิดข้อความด้วยสิ่งอื่น เช่น การซ่อนข้อความไว้ในข้อความอื่น ซ่อนไว้ในรูป เป็นต้น เทคนิคนี้ได้ถูกใช้กันมานาน เช่น การกลืนยาเสพติดซ่อนไว้ในคน การซ่อนข้อความด้วยการขูดไม้เป็นตัวอักษรเคลือบด้วยขี้ผึ้ง การเขียนด้วยหมึกล่องหนซึ่งตัวอักษรจะปรากฏเมื่อได้รับความร้อนหรือผสมกับสารบางชนิด การเขียนข้อความด้วยตัวอักษรขนาดเล็กมากซ่อนในข้อความปกติ การซ่อนลายน้ำในธนบัตรชนิดต่างๆ การแฝงข้อความในคำแรกหรือคำสุดท้ายของประโยค เช่น ‘‘อยากกินข้าวกับไข่ใส่กุ้งสับ ให้สำรับมีผัดผักอีกสักนิด เธอคงคิดจะกินต้มปลากรอบ รู้ว่าชอบฉันเลยทำมาให้ ว่าไปแล้วอยากกินยำหมูย่าง ฉันยังว่างมีเวลาพอทำได้ รักห้องครัวยิ่งกว่าห้องใดใด เธอจำไว้หาฉันได้ในห้องครัว’’ นอกจากนั้นยังมีการใช้วิธีการพิมพ์ข้อความที่ต้องการจะซ่อนให้มีขนาดเล็กเท่าจุด แล้วพิมพ์แทนที่จุดมหัพภาค ทุกจุดของข้อความที่ใช้ปกปิด

ในปัจจุบัน สามารถซ่อน ข้อความ รูปภาพ แฟ้มข้อมูลต่างๆ ด้วยการเก็บอยู่ในรูปดิจิทัล (ข้อมูลบิต 0 และบิต 1 หรือที่เรียกว่าทวิภาค) ซึ่งสามารถซ่อนได้หลายวิธี เช่น การแทนที่บิต 0 ด้วยเว้นวรรค 1 เคาะ และบิต 1 ด้วยเว้นวรรค 2 เคาะในข้อความที่ใช้ปกปิด การแทนที่ทวิภาคด้วยคำที่กำหนด ด้วยการจัดคำให้อยู่ในรูปแบบบางอย่าง เช่น คำนำหน้านาม-คำนาม-คำกริยา-คำนำหน้านาม-คำนาม ซึ่งหากมีคำนำหน้านาม 2 คำ (แทนข้อมูล 1 บิต) คำนาม 32 คำ (แทนข้อมูล 5 บิต) คำกริยา 16 คำ (แทนข้อมูล 4 บิต) จะทำให้สามารถแทนที่ข้อมูล 16 บิตด้วยข้อความรูปแบบดังกล่าว การแทนที่ทวิภาคในรูปสี 24 บิต (แดง-เขียว-น้ำเงิน สีละ 8 บิต) โดยแทนที่บิตที่มีนัยสำคัญต่ำสุดของแต่ละจุดภาพ (1 จุดภาพแทรกข้อมูลได้ 3 บิต) การแทรกข้อมูลทวิภาคในแฟ้มข้อมูลเสียง เป็นต้น

1.6 สรุป

บทนี้ได้กล่าวถึงความรู้พื้นฐานเกี่ยวกับความมั่นคง โดยเริ่มตั้งแต่ประวัติศาสตร์ความเป็นมา ที่เกี่ยวข้องกับความมั่นคง เป้าหมายของความมั่นคง การโจมตีในรูปแบบต่างๆ การให้บริการความมั่นคง กลไกด้านความมั่นคง รวมถึงเทคนิคต่างๆ ที่เกี่ยวข้องกับความมั่นคง

1.7 แบบฝึกหัด

1. กรณีต่อไปนี้ถือว่าเป็นการโจมตีในลักษณะใด

   (a) การที่นักศึกษาขโมยข้อสอบจากห้องพักของอาจารย์

   (b) นักศึกษาส่งไปรษณีย์อิเล็กทรอนิกส์ให้เพื่อเป็นร้อยฉบับต่อวันไปให้เพื่อนคนหนึ่งโดยไม่ระบุที่อยู่ตอบกลับ

   (c) การที่มีบุคคลแอบอ้างว่าเป็นเจ้าหน้าที่กรมสรรพากรเพื่อหลอกให้ไปโอนเงินคืนภาษี

   (d) การชุมนุมต่อต้านรัฐบาลจนทำให้รัฐบาลทำงานไม่ได้

   (e) การที่ตำรวจปฏิเสธความรับผิดชอบผลกระทบของการสลายการชุมนุม

2. กรณีต่อไปนี้ถือว่าเป็นกลไกด้านความปลอดภัยอย่างไร

   (a) การที่เครื่องให้บริการลงทะเบียนเรียน ถามชื่อผู้ใช้และรหัสผ่าน

   (b) การที่เครื่องให้บริการลงทะเบียนเรียน ให้ออกจากระบบเมื่อไม่ใช้งานเกิน 15 นาที

   (c) การที่อาจารย์รับการบ้านทางไปรษณีย์อิเล็กทรอนิกส์จากที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ของนักศึกษาที่กำหนดไว้เท่านั้น

   (d) การที่ผู้คุมห้องสอบขอดูบัตรนักศึกษาและให้นักศึกษาลงลายมือชื่อผู้เข้าสอบ

   (e) การที่หน่วยรักษาความปลอดภัยของนายกรัฐมตรีเปลี่ยนเส้นทางการเดินทางอยู่เสมอเพื่อป้องกันการทำร้ายของกลุ่มผู้ประท้วงรัฐบาล

3. เทคนิคการเข้ารหัสข้อมูลและการซ่อนข้อมูลต่างกันอย่างไร

4. กรณีต่อไปนี้จัดว่าเป็นเทคนิคการเข้ารหัสข้อมูลหรือการซ่อนข้อมูล

   (a) นักศึกษาแอบเอากระดาษจดสูตรใส่ไว้ในปากกาเข้าห้องสอบ

   (b) การส่งข้อความทางทหารด้วยเครื่องอินิกมาของทหารเยอรมนีในสงครามโลกครั้งที่สอง

   (c) การใส่ลายน้ำในธนบัตรเพื่อป้องกันการปลอม

บทที่ 2

การเข้ารหัสด้วยกุญแจแบบสมมาตรในอดีต

- คณิตศาสตร์ที่เกี่ยวข้อง
- การเข้ารหัสด้วยกุญแจแบบสมมาตร
- การเข้ารหัสด้วยการแทนที่
- การเข้ารหัสด้วยการสลับที่
- การเข้ารหัสแบบกระแสและบล็อก

บทที่ 2

การเข้ารหัสด้วยกุญแจแบบสมมาตรในอดีต

ในบทนี้จะกล่าวถึงวิธีการเข้ารหัสด้วยกุญแจแบบสมมาตรในอดีตซึ่งเป็นวิธีการที่สามารถโดนโจมตีได้ง่าย และไม่มีความซับซ้อนมากนัก โดยเริ่มกล่าวถึงตั้งแต่คณิตศาสตร์ที่เกี่ยวข้อง ไปจนถึงการเข้ารหัสด้วยกุญแจแบบสมมาตรในรูปแบบต่างๆที่ใช้กันในอดีต ได้แก่ การเข้ารหัสด้วยการแทนที่และการสลับที่ การเข้ารหัสแบบกระแสและบล็อก

2.1 คณิตศาสตร์ที่เกี่ยวข้อง

ในหัวข้อนี้จะเป็นการทบทวนคณิตศาสตร์พื้นฐานที่เกี่ยวข้องกับการเข้ารหัสด้วยกุญแจแบบสมมาตร ได้แก่เรื่อง เลขคณิตจำนวนเต็ม เลขคณิตมอดุลาร์ และ เมทริกซ์

2.1.1 เลขคณิตจำนวนเต็ม

เลขจำนวนเต็ม คือ เลขที่ไม่มีทศนิยม ที่มีค่าตั้งแต่ลบอนันต์ ($-\infty$) ถึง อนันต์ (∞) ดังแสดงได้ในเซต $\mathbb{Z} = \{-\infty, ..., -3, -2, -1, 0, 1, 2, 3, ..., \infty\}$ โดยที่ในศาสตร์ของการเข้ารหัสจะสนใจ ตัวดำเนินการแบบทวิภาค กล่าวคือ ตัวดำเนินการซึ่งรับข้อมูลนำเข้าสองค่าและมีข้อมูลนำออกหนึ่งค่า เช่น ตัวดำเนินการบวก ($+$) ตัวดำเนินการลบ ($-$) และ ตัวดำเนินการคูณ ($\times$) ซึ่งข้อมูลนำเข้าและข้อมูลนำออกเป็นเซตของเลขคณิตจำนวนเต็ม

การหารเลขคณิตจำนวนเต็มนั้นแตกต่างจากตัวดำเนินการชนิดอื่นๆ เนื่องจากมีข้อมูลนำออกสองค่า คือ ผลลัพธ์ของการหาร และ เศษของการหาร กล่าวคือ *ตัวตั้ง=(ตัวหาร×ผลหาร)+เศษ* ซึ่งในทางปฏิบัติแล้ว การหาผลหารและการหาเศษที่เป็นจำนวนเต็มด้วยการเขียนโปรแกรมสามารถ กระทำได้ง่าย เช่น ในภาษาซีใช้ตัวดำเนินการ '/' เพื่อการหาผลหาร และ '%' เพื่อการหาเศษจากการหาร

สำหรับในศาสตร์ของการเข้ารหัสจะสนใจเฉพาะการหารกรณีที่ตัวหารเป็นจำนวนเต็มบวก และเศษเป็นจำนวนเต็มซึ่งมากกว่าหรือเท่ากับศูนย์เท่านั้น กรณีที่เศษมีค่าเท่ากับศูนย์จะเรียกว่า *การหารลงตัว* ซึ่งใช้สัญลักษณ์ (ตัวหาร|ตัวตั้ง) หากหารไม่ลงตัวจะใช้สัญลักษณ์ (ตัวหาร∤ตัวตั้ง)

การหารร่วมมาก (หรม.) ของเลขจำนวนเต็มสองจำนวน คือ เลขจำนวนเต็มที่มากที่สุดซึ่งสามารถหารเลขทั้งสองลงตัว หาก หรม. ของเลขทั้งสองมีค่าเท่ากับ หนึ่ง จะเรียกเลขทั้งสองว่าเป็น *จำนวนเฉพาะสัมพัทธ์* สำหรับการหารค่า หรม. สามารถใช้ขั้นตอนวิธีของยูคลิด ซึ่งนิยามว่า หรม.(a,0) = a และ หรม.(a,b) = หรม.(b,r) โดยที่ r คือเศษของการหารตัวตั้ง a ด้วยตัวหาร b ตัวอย่างเช่น หรม.(16,12) = หรม.(12,4) = หรม.(4,0) = 4

2.1.2 เลขคณิตมอดุลาร์

คำว่า ''มอดุลาร์'' หมายถึง การหาเศษของการหารซึ่งจะใช้ตัวดำเนินการที่เรียกว่า mod โดยไม่สนใจผลลัพธ์ของการหาร ซึ่งเป็นตัวดำเนินการแบบทวิภาค คล้ายกับตัวดำเนินการ บวก ลบ และ คูณ ซึ่งมีข้อมูลนำเข้าสองค่า และ ข้อมูลนำออกเพียงหนึ่งค่า เช่น 37 mod 4 = 1 (37 หารด้วย 4 ได้ผลลัพธ์เท่ากับ 9 และเหลือเศษ 1 แต่การมอดุลาร์นั้นไม่สนใจผลลัพธ์ของการหาร)

ในศาสตร์ด้านการเข้ารหัสนั้นนิยมใช้เครื่องหมายสมภาค (≡) แทน เครื่องหมายเท่ากับ (=) ตัวอย่างเช่น ผลลัพธ์ของ (2 mod 10) = (12 mod 10) = (22 mod 10) จะนิยมเขียนว่า $2 \equiv 12 \equiv 22 \equiv \pmod{10}$

เลขคณิตมอดุลาร์มีคุณสมบัติที่น่าสนใจ 3 ประการคือ

- $(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$
- $(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$
- $(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

นอกจากนั้นในศาสตร์ด้านการเข้ารหัสจะนิยามค่าที่เกี่ยวข้องกับ มอดุลาร์ อีก 2 คือ เรียกว่า ตัวผกผันการบวก และ ตัวผกผันการคูณ เลขจำนวนเต็ม a และ b จะเรียกว่า ตัวผกผันการบวก ก็ต่อเมื่อ $a + b \equiv 0 \bmod n$ เลขจำนวนเต็ม a และ b จะเรียกว่า ตัวผกผันการคูณ ก็ต่อเมื่อ $a \times b \equiv 1 \bmod n$ เลขจำนวนเต็ม a จะสามารถหาค่า ตัวผกผันการคูณ ได้ก็ต่อเมื่อ a และ n เป็น จำนวนเฉพาะสัมพัทธ์ กล่าวคือ หรม.(a, n) มีค่าเท่ากับ 1

2.1.3 เมทริกซ์

เมทริกซ์ คือ การจัดเรียงตัวเลขให้อยู่ในรูปของสี่เหลี่ยมขนาด $m \times n$ เมื่อ m เป็นจำนวนแถว และ n คือ จำนวนสดมภ์ ดังแสดงในรูปที่ 2.1

เมทริกซ์มีคุณสมบัติดังต่อไปนี้

$$M_{m\times n} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

รูปที่ 2.1: ตัวอย่างของเมทริกซ์

- การเท่ากันของเมทริกซ์ เมทริกซ์สองเมทริกซ์จะเท่ากันก็ต่อเมื่อ เมทริกซ์ทั้งสองมีขนาดเท่ากัน และสมาชิกทุกตัวของทั้งสองเมทริกซ์เหมือนกัน
- การบวกลบของเมทริกซ์ เมทริกซ์สองเมทริกซ์จะบวกลบกันได้ก็ต่อเมื่อ เมทริกซ์ทั้งสองมีขนาดเท่ากัน ซึ่งผลลัพธ์ของการบวกลบคือการบวกลบแต่ละค่าของสมาชิก แต่ละตัวในเมทริกซ์ ดังแสดงในรูปที่ 2.2
- การคูณเมทริกซ์ เมทริกซ์สองเมทริกซ์จะคูณกันได้ก็ต่อเมื่อจำนวนสดมภ์ของเมทริกซ์แรก เหมือนกับจำนวนแถวของเมทริกซ์ที่สอง ซึ่งเมทริกซ์ผลลัพธ์จะมีขนาดเท่ากับ จำนวนแถวของเมทริกซ์แรก คูณ จำนวนสดมภ์ของเมทริกซ์ที่สอง กล่าวคือ $A_{m\times n} = B_{m\times k} \times C_{k\times n}$ โดยที่ผลลัพธ์ของแต่ละค่า $a_{ij} = b_{i1} \times c_{1j} + b_{i2} \times c_{2j} + \cdots + b_{ik} \times c_{kj}$ จากรูปที่ 2.3 เป็นตัวอย่างการคูณเมทริกซ์ โดย ค่า 14 (a_{11}) สามารถคำนวณจาก $(1 \times 1) + (2 \times 2) + (3 \times 3)$ ค่า 77 (a_{22}) สามารถคำนวณจาก $(4 \times 4) + (5 \times 5) + (6 \times 6)$ เป็นต้น แต่หากเป็นการคูณเมทริกซ์ด้วยตัวเลขให้นำเลขนั้นไปคูณทุกค่าของเมทริกซ์

$$\begin{bmatrix} 5 & 7 & 9 \\ 5 & 7 & 9 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} + \begin{bmatrix} 4 & 5 & 6 \\ 1 & 2 & 3 \end{bmatrix}$$

$$\begin{bmatrix} -3 & -3 & -3 \\ 3 & 3 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} - \begin{bmatrix} 4 & 5 & 6 \\ 1 & 2 & 3 \end{bmatrix}$$

รูปที่ 2.2: ตัวอย่างของการบวกลบเมทริกซ์

2.2 การเข้ารหัสด้วยกุญแจแบบสมมาตร

การเข้ารหัสด้วยกุญแจแบบสมมาตรนั้นเป็นการเข้ารหัสซึ่งผู้ส่งและผู้รับใช้กุญแจดอกเดียวกัน ในการเข้ารหัสและถอดรหัส โดยที่ผู้ส่งจะสร้างข้อความที่ถูกเข้ารหัสจากการเข้ารหัสของข้อความด้วยกุญแจ หลังจากนั้นข้อความที่ถูกเข้ารหัสดังกล่าวสามารถส่งไปในช่องทางที่ปลอดภัยหรือไม่ก็ได้เนื่องจากผู้โจมตี

$$\begin{bmatrix} 14 & 32 \\ 32 & 77 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \times \begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix}$$

รูปที่ 2.3: ตัวอย่างของการคูณเมทริกซ์

ไม่สามารถถอดรหัสข้อความดังกล่าวได้เนื่องจากไม่มีกุญแจ เมื่อข้อความที่เข้ารหัสดังกล่าวเดินทางมาถึงผู้รับ ผู้รับจะสามารถถอดรหัสข้อความดังกล่าวด้วยกุญแจดอกเดียวกับผู้ส่งดังแสดงในรูปที่ 2.4

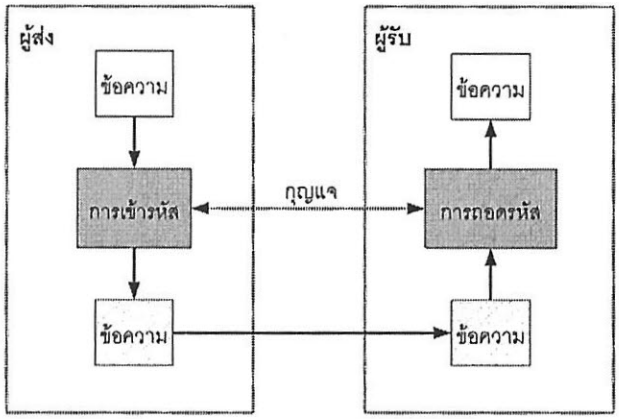
เมื่อผู้รับต้องการที่จะเป็นผู้ส่งบ้างบุคคลดังกล่าวจะสามารถใช้กุญแจดอกเดิมในการเข้ารหัส (ซึ่งเป็นที่มาของชื่อ ''สมมาตร'') วิธีการเข้ารหัสและถอดรหัสนั้นสามารถเปิดเผยสู่สาธารณะได้ แต่กุญแจนั้นจะต้องถูกเก็บความลับซึ่งรู้แค่เพียงผู้ส่งและผู้รับ โดยที่ผู้ส่งและผู้รับจำเป็นต้องตกลงการใช้กุญแจในช่องทางที่ปลอดภัยก่อนที่จะใช้งานกุญแจดังกล่าว หากคนหนึ่งต้องการสื่อสารกับอีก k คน คนนั้นจำเป็นต้องมีกุญแจ ทั้งหมด k ดอก ดังนั้นหากมีบุคคล n คนต้องการสื่อสารด้วยวิธีนี้แบบพบกันหมดจะมีกุญแจในระบบทั้งหมด $n \times (n-1)/2$ ดอก เนื่องจากแต่ละคนต้องมีกุญแจ n-1 ดอก ทั้งระบบมี n คน และกุญแจแต่ละดอกใช้ระหว่างคน 2 คน

วิธีการเข้ารหัสแบบสมมาตรดังกล่าวสามารถถูกโจมตีด้วยวิธีการพื้นฐาน 4 วิธี คือ การโจมตีข้อความหลังการเข้ารหัส การโจมตีเมื่อรู้คู่ของข้อความก่อนและหลังการเข้ารหัส การโจมตีผู้ส่งโดยการเลือกข้อความก่อนเข้ารหัส และ การโจมตีผู้รับโดยการเลือกข้อความหลังการเข้ารหัส

- การโจมตีข้อความหลังการเข้ารหัส เป็นการโจมตีโดยที่ผู้โจมตีรู้เพียงข้อความหลังการเข้ารหัส เพื่อที่จะหากุญแจและข้อความก่อนเข้ารหัส ซึ่งการโจมตีดังกล่าวสามารถกระทำได้หลายวิธี เช่น วิธีการทดลองทุกกุญแจที่เป็นไปได้เพื่อใช้ในการถอดรหัส ซึ่งสามารถป้องกันได้โดยการกำหนดให้กุญแจที่เป็นไปได้มีจำนวนมหาศาล วิธีการใช้เทคนิคทางสถิติเข้าช่วย เช่น เรารู้ว่าตัวอักษรที่ใช้บ่อยที่สุด ในภาษาอังกฤษคือ ตัวอักษร E ดังนั้นเราสามารถดูจากความถี่ของข้อความที่ถูกเข้ารหัสว่าอักขระใด พบมากที่สุด ซึ่งเราสามารถคาดเดาได้ว่าอักขระดังกล่าวคือตัวอักษร E วิธีการหารูปแบบต่างๆจากข้อความที่ถูกเข้ารหัส เป็นต้น

- การโจมตีเมื่อรู้คู่ของข้อความก่อนและหลังการเข้ารหัส สามารถกระทำได้โดยเทคนิค เดียวกับการโจมตีเมื่อรู้ข้อความหลังการเข้ารหัสเพียงอย่างเดียว แต่สามารถกระทำได้เร็วขึ้น เนื่องจากมีข้อมูลมากขึ้น แต่อย่างไรก็ตามโอกาสที่จะรู้คู่ของข้อความก่อนและหลังเข้ารหัสนั้น เป็นได้ได้น้อยมากในความเป็นจริง

- การโจมตีผู้ส่งโดยการเลือกข้อความก่อนเข้ารหัส การโจมตีนี้สามารถกระทำได้ โดยผู้โจมตีสามารถเข้าถึงเครื่องผู้ส่งและสามารถเลือกข้อความก่อนเข้ารหัสเอง เพื่อที่จะหากุญแจของผู้ส่ง



รูปที่ 2.4: การเข้ารหัสด้วยกุญแจแบบสมมาตร

- การโจมตีผู้รับโดยการเลือกข้อความหลังการเข้ารหัส การโจมตีนี้จะกระทำโดยผู้โจมตีสามารถเข้าถึงเครื่องผู้รับโดยการเลือกข้อความที่ถูกเข้ารหัสเอง เพื่อที่จะใช้หากุญแจของผู้รับ

วิธีการเข้ารหัสด้วยกุญแจแบบสมมาตรที่จะกล่าวต่อไปนี้เป็นการเข้ารหัสอย่างง่ายซึ่งไม่นิยมใช้ในปัจจุบัน แต่อย่างไรก็ตามวิธีการดังกล่าวนั้นเป็นพื้นฐานที่สำคัญของการเข้ารหัสที่ซับซ้อนซึ่งใช้ในปัจจุบัน การเข้ารหัสด้วยกุญแจแบบสมมาตรในอดีตนั้นสามารถแบ่งตามวิธีการเข้ารหัสได้สองวิธี คือ การเข้ารหัสด้วยการแทนที่ และ การเข้ารหัสด้วยการสลับที่

2.3 การเข้ารหัสด้วยการแทนที่

การเข้ารหัสด้วยการแทนที่เป็นวิธีการแทนที่อักขระหนึ่งด้วยอีกอักขระหนึ่งโดยไม่สนใจ ตำแหน่งของอักขระดังกล่าว ยกตัวอย่างเช่น การแทนตัวอักษร A ด้วย C ของทั้งข้อความ ซึ่งวิธีการเข้ารหัสด้วยการแทนที่นี้สามารถแบ่งเป็นสองกลุ่ม คือ กลุ่มการแทนที่ด้วยอักขระเดิมเสมอ และ กลุ่มการเปลี่ยนอักขระแทนที่ในแต่ละครั้ง เช่น หากแทนที่คำว่า THARA ด้วย SIBSB เป็นการ แทนที่ด้วยตัวอักขระเดิมเสมอ สังเกตได้จากตัวอักษร A ทั้งสองตัว แทนด้วยตัวอักษร B ทั้งคู่ แต่หากแทนที่ คำว่า THARA ด้วยคำว่า RJSKM ซึ่งตัวอักษร A ทั้งสองตัวถูกแทนด้วยตัวอักษรที่ต่างกัน จะจัดเป็นกลุ่มการเปลี่ยนอักขระแทนที่ในแต่ละครั้ง

2.3.1 การแทนที่ด้วยอักขระเดิมเสมอ

การแทนที่ด้วยวิธีนี้มีด้วยการหลายเทคนิค เช่น การแทนที่ด้วยการเลื่อนตัวอักษร หรือที่เรียกว่า การเข้ารหัสแบบซีซ่า * วิธีการดังกล่าวเป็นวิธีการแทนที่ด้วยการเลื่อนตัวอักษร k ตัว หากต้องการเข้ารหัสภาษาอังกฤษ โดยให้ตัวอักษร A มีค่าเท่ากับ 0 และ Z มีค่าเท่ากับ 25 ดังแสดงในตารางที่ 2.1

ตารางที่ 2.1: ตัวอย่างการแทนที่ตัวอักษรด้วยตัวเลข

ตัวอักษร	A	B	C	D	E	F	G	H	I	J	K	L	...	V	W	X	Y	Z
ตัวเลข	0	1	2	3	4	5	6	7	8	9	10	11	...	21	22	23	24	25

ผู้ส่งสามารถเข้ารหัสด้วยการคำนวณ ''ตัวอักษรใหม่ = (ตัวอักษรเดิม + k) mod 26'' และผู้รับสามารถถอดรหัสด้วยการคำนวณ ''ตัวอักษรเดิม = (ตัวอักษรใหม่ - k) mod 26'' ซึ่งจำนวนตัวอักษรที่เลื่อน (k) ก็คือกุญแจ สำหรับวิธีการดังกล่าวนั่นเอง ยกตัวอย่างเช่น หากต้องการเข้ารหัสคำว่า THARA โดยเลื่อนตัวอักษร 3 ตัว (กุญแจมีค่า k=3) สามารถทำได้โดยแปลงตัวอักษรเป็นตัวเลข T=19, H=7, A=0, R=17, A=0 จากนั้น คำนวณด้วยการบวกด้วย 3 แล้ว mod ด้วย 26 ดังนั้นผลลัพธ์คือ (19+3) mod 26 = 22 = W, (7+3) mod 26 = 10 = K, (0+3) mod 26 = 3 = D, (17+3) mod 26 = 20 = U และ (0+3) mod 26 = 3 = D ดังนั้นคำว่า THARA จะถูกเข้ารหัสเป็นคำว่า WKDUD ด้วยวิธีการดังกล่าว

การโจมตีวิธีการนี้สามารถทำได้ง่ายมากเพียงแค่การลองทุกกุญแจซึ่งมีเพียง 26 กุญแจที่เป็นไปได้ (จริงๆ ลองเพียง 25 ครั้งเนื่องจาก k=0 จะทำให้ข้อความทั้งก่อนและหลังเข้ารหัสเหมือนกัน) นอกจากนั้นวิธีการดังกล่าวยังสามารถถูกโจมตีด้วยการวิเคราะห์ความถี่ของตัวอักษร (อาจเป็นตัวอักษรเดียว, สองตัว, สามตัวก็ได้) เนื่องจากความถี่การใช้งานของตัวอักษรนั้นแตกต่างกัน ตัว E ใช้มากที่สุด ในขณะที่ตัว Z ใช้น้อยที่สุดเป็นต้น

การเข้ารหัสวิธีนี้ยังสามารถเปลี่ยนวิธีการดังกล่าวเป็นการคูณแทนการบวก กล่าวคือ ผู้ส่งสามารถเข้ารหัสด้วยการคำนวณ ''ตัวอักษรใหม่ = (ตัวอักษรเดิม $\times$ k) mod 26'' และผู้รับสามารถถอดรหัสด้วยการคำนวณ ''ตัวอักษรเดิม = (ตัวอักษรใหม่ $\times k^{-1}$) mod 26'' โดยค่า k และ 26 จะต้องเป็น จำนวนเฉพาะสัมพัทธ์กัน หรือ หรม.(k,26) = 1 เพื่อที่จะทำให้สามารถคำนวณหาค่าตัวผกผันการคูณ(k^{-1})ได้ ซึ่งมีกุญแจ (ค่า k) ที่เป็นไปได้ทั้งหมด 12 ค่า หากเราใช้ทั้งการบวกและการคูณ (เรียกว่าการเข้ารหัสแบบ สัมพรรค) จะทำให้กุญแจที่เป็นได้ทั้งหมดเพิ่มเป็น 26 $\times$ 12 โดยที่ ผู้ส่งสามารถเข้ารหัสด้วยการคำนวณ ''ตัวอักษรใหม่ = (ตัวอักษรเดิม $\times k_1 + k_2$) mod 26'' และผู้รับสามารถถอดรหัสด้วยการคำนวณ ''ตัวอักษรเดิม = ((ตัวอักษรใหม่ - k_2) $\times k_1^{-1}$) mod 26''

*การเข้ารหัสแบบซีซ่า มีที่มาจากวิธีการที่จูเลียส ซีซ่าใช้เข้ารหัสเพื่อการติดต่อกับทหารของตน ด้วยการเลื่อนตัวอักษรไป 3 ตัว เช่น ตัว A แทนด้วยตัว D, ตัว B แทนด้วยตัว E เป็นต้น

การเข้ารหัสด้วยวิธีการแทนที่ดังกล่าวข้างต้นนั้นมีจำนวนกุญแจที่เป็นไปได้ทั้งหมดน้อยมาก ทำให้เสี่ยงต่อการถูกโจมตีด้วยการลองทุกกุญแจที่เป็นไปได้ ดังนั้น หากเราสามารถทำให้ตัวอักษรแต่ละตัวเป็นอิสระจากกัน ดังเช่น ตารางที่ 2.2 จะทำให้กุญแจที่เป็นไปได้ทั้งหมดมีค่าเป็น 26! (ประมาณ 4×10^{26}) ซึ่งยากที่จะลองทุกวิธี แต่อย่างไรก็ตามวิธีการดังกล่าวก็ยังคงเสี่ยงต่อการใช้วิธีทางสถิติ โดยดูจากความถี่ของตัวอักษร

ตารางที่ 2.2: ตัวอย่างการแทนที่ตัวอักษรแบบอิสระจากกัน

ก่อนเข้ารหัส	A	B	C	D	E	F	G	H	I	J	K	L	...	V	W	X	Y	Z
หลังเข้ารหัส	U	O	V	N	C	Q	W	Y	S	P	T	A	...	E	F	B	D	H

2.3.2 การเปลี่ยนอักขระแทนที่ในแต่ละครั้ง

กลุ่มการเปลี่ยนอักขระแทนที่ในแต่ละครั้ง หมายถึง การที่ตัวอักขระเดียวกันอาจแทนที่ด้วยตัวอักษร ที่ต่างกันหากตำแหน่งของตัวอักษร เช่น การแทนที่ คำว่า THARA ด้วยคำว่า RJSKM ซึ่งตัวอักษร A ทั้งสองตัวถูกแทนด้วยตัวอักษรที่ต่างกัน A ตัวแรกถูกแทนที่ด้วย S และ A ตัวที่สอง ถูกแทนที่ด้วย M ซึ่งการเปลี่ยนอักขระแทนที่ในแต่ละครั้งนั้นสามารถทำได้หลายวิธี ได้แก่ การเข้ารหัสโดยใช้กุญแจอัตโนมัติ การเข้ารหัสแบบเฟลย์แฟร์ การเข้ารหัสแบบไวเจเนียร์ การเข้ารหัสแบบฮิลล์ แพดครั้งเดียว การเข้ารหัสแบบโรเตอร์ เครื่องอินิกม่า เป็นต้น

การเข้ารหัสโดยใช้กุญแจอัตโนมัติ

การเข้ารหัสโดยใช้กุญแจอัตโนมัติ คือ การที่มองข้อความเป็นสายของตัวอักษร (เรียกว่า $P_1, P_2, ..., P_n$) โดยที่กุญแจสำหรับตัวอักษรแรกเป็นกุญแจที่ตกลงกันทั้งผู้ส่งและผู้รับ กุญแจดอกที่สองจะใช้ตัวอักษรตัวแรก (P_1) กุญแจดอกที่สามจะใช้ตัวอักษรตัวที่สอง และทำแบบนี้ไปเรื่อยๆ โดยที่ตัวอักษรที่เข้ารหัสแต่ละตัวสามารถคำนวณได้จาก ''ตัวอักษรใหม่ = (ตัวอักษรเดิม + k) mod 26'' และผู้รับสามารถถอดรหัสด้วยการคำนวณ ''ตัวอักษรเดิม = (ตัวอักษรใหม่ - k) mod 26'' ซึ่งค่า k ก็คือกุญแจแบบอัตโนมัติ ซึ่งจะเปลี่ยนค่าในทุกตัวอักษรที่เข้ารหัส ตัวอย่างเช่น หากต้องการเข้ารหัสคำว่า THARA โดยกุญแจค่าแรกมีค่าเท่ากับ 3 สามารถทำได้โดยแปลงตัวอักษรเป็นตัวเลข T=19, H=7, A=0, R=17, A=0 จากนั้น คำนวณตัวอักษรตัวแรกด้วยการบวกด้วย 3 แล้ว mod ด้วย 26 ตัวอักษรใหม่ตัวแรก คือ (19+3) mod 26 = 22 = W, กุญแจดอกที่สองคือตัวอักษรตัวแรก (19) ดังนั้นตัวอักษรใหม่ตัวที่สอง คือ (7+19) mod 26 = 0 = A, ตัวอักษรใหม่ตัวที่สาม คือ (0+7) mod 26 = 7 = H, ตัวอักษรใหม่ตัวที่สี่ คือ (17+0) mod 26 = 17 = R และตัวอักษรใหม่ตัวสุดท้าย คือ (0+17) mod 26 = 17 = R ดังนั้นคำว่า THARA จะถูกเข้ารหัสเป็นคำว่า WAHRR ด้วยวิธีการดังกล่าว ซึ่งจะสามารถสังเกตได้ว่า A ตัวแรกถูกแทนที่ด้วยตัว H และตัวที่สองถูกแทนที่ด้วยตัว R ซึ่งวิธีการดังกล่าวปลอดภัยจากการ

โจมตีด้วยสถิติแต่ยังคงเสี่ยงต่อการลองทุกวิธี เนื่องจากกุญแจที่เป็นไปได้ของตัวอักขระแรกมีเพียง 25 วิธี

การเข้ารหัสแบบเพลย์แฟร์

การเข้ารหัสแบบเพลย์แฟร์เป็นการเข้ารหัสที่ใช้ในสงครามโลกครั้งที่ 1 โดยกองทัพอังกฤษ ซึ่งการเข้ารหัสวิธีนี้เริ่มต้นโดยการสร้างตารางขนาด 5×5 ดังแสดงในตารางที่ 2.3 โดยตารางดังกล่าวสร้างโดยการกำหนดกุญแจ (เช่น คำว่า SUT) จากนั้นนำตัวอักขระในกุญแจไปไว้ที่ใดก็ได้ในตาราง หลังจากนั้นให้เติมตัวอักษร A ถึง Z ให้เต็มตารางตามลำดับโดยข้ามตัวอักษรที่อยู่ในกุญแจ โดยที่ตัวอักษร I และ J อยู่ในช่องเดียวกันเสมอ

ตารางที่ 2.3: ตัวอย่างตารางเพลย์แฟร์

S	U	T	A	B
C	D	E	F	G
H	I/J	K	L	M
N	O	P	Q	R
V	W	X	Y	Z

S	A	B	C	D
E	U	F	G	H
I/J	K	T	L	M
N	O	P	Q	R
V	W	X	Y	Z

การเข้ารหัสด้วยเพลย์แฟร์นั้นจะเข้ารหัสครั้งละ 2 ตัวอักษร โดยก่อนที่จะเริ่มการเข้ารหัสหากมีตัวอักษรที่ซ้ำกัน 2 ตัวในคำที่ต้องการเข้ารหัส จะต้องแทรกตัวอักษรอื่น ระหว่างกลาง เช่น HELLO ต้องเปลี่ยนเป็น HE LX LO จากนั้นให้นับจำนวนตัวอักษร หากจำนวนตัวอักษรในคำดังกล่าวเป็นเลขคี่ ให้เพิ่มตัวอักษรแทรกอีกหนึ่งตัวเพื่อให้จำนวนรวมเป็นเลขคู่

การเข้ารหัสจะดำเนินการเข้ารหัสทีละคู่โดยดูตารางตามขั้นตอนต่อไปนี้

- กรณีที่ตัวอักษรทั้งสองอยู่ในแถวเดียวกันจะแทนที่ด้วยตัวอักษรทางด้านขวาของแต่ละตัว (หากเป็นตัวขวาสุดให้แทนที่ด้วยตัวซ้ายสุด) เช่น จากตารางที่ 2.3 ด้านซ้าย หากคู่ของตัวอักษร คือ DG จะถูกแทนที่ด้วย EC
- กรณีที่ตัวอักษรทั้งสองอยู่ในสดมภ์เดียวกันจะแทนที่ด้วยตัวอักษรทางด้านล่างของแต่ละตัว (หากเป็นตัวล่างสุดให้แทนที่ด้วยตัวบนสุด) เช่น จากตารางที่ 2.3 ด้านซ้าย หากคู่ของตัวอักษร คือ FY จะถูกแทนที่ด้วย LA
- กรณีที่ตัวอักษรทั้งสองไม่อยู่ในแถวและสดมภ์เดียวกันให้แทนที่ตัวอักษรในแถวเดียวกันที่มีสดมภ์ตรงกับตัวอักษรอีกตัวหนึ่งที่คู่กัน เช่น จากตารางที่ 2.3 ด้านซ้าย หากคู่ของตัวอักษร คือ ER จะถูกแทนที่ด้วย GP

ยกตัวอย่างเช่น หากต้องการเข้ารหัสคำว่า THARA สิ่งแรกที่ต้องทำคือ แบ่งคู่แล้วดูว่ามีคู่ที่ตัวอักษรเหมือนกันหรือไม่ เนื่องจากจำนวนตัวอักษรเป็นเลขคี่ จำเป็นต้องเติมตัวอักษรแทรก กลายเป็น TH AR AX จากนั้นเข้ารหัสทีละคู่ตามขั้นตอน หากใช้ตารางที่ 2.3 ด้านซ้ายจะได้ผลลัพธ์ คือ SK BQ TY หากใช้ตารางที่ 2.3 ด้านขวาจะได้ผลลัพธ์ คือ MF DO BW

การโจมตีการเข้ารหัสแบบเพลย์แฟร์ด้วยการลองทุกวิธีทำค่อนข้างยาก เนื่องจากมีกุญแจที่เป็นไปได้ทั้งหมด 25! และไม่สามารถใช้สถิติได้

การเข้ารหัสแบบไวเจเนียร์

การเข้ารหัสแบบไวเจเนียร์ ถูกคิดค้นโดยนักคณิตศาสตร์ชาวฝรั่งเศสในสมัยคริสตศักราชที่ 1600 ชื่อ เบลส เดอ ไวเจเนียร์ โดยกุญแจเรียงกันเป็นสายโดยการวนซ้ำกุญแจไปเรื่อยๆ จนความยาว ของกุญแจมีความยาวเท่ากับข้อความที่ต้องการเข้ารหัส หลังจากนั้นผู้ส่งจะเข้ารหัสด้วย โดยที่ตัวอักษรที่เข้ารหัสแต่ละตัวสามารถคำนวณได้จาก ‘‘ตัวอักษรใหม่ = (ตัวอักษรเดิม + k) mod 26’’ และผู้รับสามารถถอดรหัสด้วยการคำนวณ ‘‘ตัวอักษรเดิม = (ตัวอักษรใหม่ - k) mod 26’’ ยกตัวอย่าง เช่น หากต้องการเข้ารหัสคำว่า CRYPTOGRAPHY โดยอาศัยกุญแจ คือ คำว่า THARA จะสามารถเข้ารหัสได้ดังตารางที่ 2.4 การเข้ารหัสแบบไวเจเนียร์นั้นสามารถหาคำตอบโดยอาศัยตารางที่เรียกว่าตารางไวเจเนียร์ ดังแสดงในตารางที่ 2.5 โดยที่แถวบนสุดคือตัวอักษรที่ต้องการเข้ารหัส และ สดมภ์ซ้ายสุดของตารางคือกุญแจ

ตารางที่ 2.4: ตัวอย่างการเข้ารหัสด้วยวิธีไวเจเนียร์

ข้อความ	C	R	Y	P	T	O	G	R	A	P	H	Y
กุญแจ	T	H	A	R	A	T	H	A	R	A	T	H
ข้อความเข้ารหัส	V	Y	Y	G	T	H	N	R	R	P	A	F

แพดครั้งเดียว

แพดครั้งเดียว เป็น วิธีการเข้ารหัสโดยการสุ่มกุญแจซึ่งมีความยาวเท่ากับข้อความที่ต้องการเข้ารหัส วิธีการดังกล่าวถือเป็น*วิธีการที่ปลอดภัยที่สุด* แต่อย่างไรก็ตามเป็นวิธีที่ไปได้ยากในทางปฏิบัติเนื่องจากผู้ส่งและผู้รับต้องเปลี่ยนวิธี ส่งรับกุญแจกันตลอดเวลา

การเข้ารหัสแบบโรเตอร์

การเข้ารหัสแบบโรเตอร์เป็นวิธีการซึ่งอาศัยวงล้อโดยการแทนที่ตัวอักขระ โดยเปลี่ยนรูปแบบการแทนที่ในทุกอักขระที่ต้องการเข้ารหัสด้วยการหมุนวงล้อ ดังแสดงในตารางที่ 2.6 ซึ่งเป็นการสมมุติว่าวงล้อดังกล่าวเป็นวงล้อเข้ารหัสแบบห้าตัวอักษร (แต่ในความเป็นจริงวงล้อสามารถเข้ารหัสยี่สิบหกตัวอักษร)

ตารางที่ 2.5: ตารางไวเจเนียร์

	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
B	B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
C	C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
D	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
E	E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
F	F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
G	G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
H	H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
I	I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
J	J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
K	K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
L	L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
M	M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
N	N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
O	O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
P	P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
Q	Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
R	R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
S	S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
T	T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
U	U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
V	V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
W	W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
X	X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
Y	Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
Z	Z A B C D E F G H I J K L M N O P Q R S T U V W X Y

หากเข้ารหัสคำว่า DEAD จะเข้ารหัสได้เป็นคำว่า ABCE ซึ่งจะเห็นได้ว่าตัวอักขระ D ครั้งแรกจะถูกเข้ารหัสเป็นตัวอักขระ A และตัวอักขระ D ครั้งที่สองจะถูกเข้ารหัสเป็นตัว E

ตารางที่ 2.6: ตัวอย่างการแทนที่ด้วยการหมุนวงล้อ (หมุนลง)

ค่าเริ่มต้นของวงล้อ	หมุนครั้งแรก	หมุนครั้งที่สอง	หมุนครั้งที่สาม	...
A ⇒ B	A ⇒ D	A ⇒ C	A ⇒ B	...
B ⇒ E	B ⇒ C	B ⇒ E	B ⇒ D	...
C ⇒ D	C ⇒ A	C ⇒ D	C ⇒ A	...
D ⇒ A	D ⇒ E	D ⇒ B	D ⇒ E	...
E ⇒ C	E ⇒ B	E ⇒ A	E ⇒ C	...

เครื่องอินิกม่า

เครื่องอินิกม่าเป็นเครื่องเข้ารหัสซึ่งถูกใช้โดยทหารเยอรมนีในช่วงสงครามโลกครั้งที่สอง โดยอาศัยการเข้ารหัสแบบโรเตอร์ เครื่องอินิกม่าจะมีส่วนประกอบ ได้แก่ ปุ่มกดตัวอักษร (คีย์บอร์ด) หลอดไฟแสดงผลตัวอักษร วงจรเชื่อมสายไฟ และ วงล้อสามวงสำหรับการเข้ารหัส โดยที่วงแรกจะหมุนทุกตัวอักษร วงที่สองจะหมุนหนึ่งครั้งเมื่อวงล้อวงแรกหมุนครบรอบ วงล้อวงสุดท้ายจะหมุนก็ต่อเมื่อวงล้อวงที่สองหมุนครบรอบ การเข้ารหัสด้วยเครื่องอินิกม่าแต่ละครั้งจะต้องอาศัย สมุดสำหรับการเข้ารหัสซึ่งจะเก็บค่าเริ่มต้นของวงล้อแรก วิธีการเลือกวงล้อสามวงจากห้าวง การวางตำแหน่งของวงล้อทั้งสาม และวิธีการเชื่อมต่อสายไฟ

2.4 การเข้ารหัสด้วยการสลับที่

การเข้ารหัสด้วยวิธีการสลับที่ คือ การสลับตำแหน่งของตัวอักขระ เช่น หากต้องการเข้ารหัส คำว่า ELEVEN PLUS TWO อาจเข้ารหัสเป็น TWELVE PLUS ONE คำว่า DEBIT CARD อาจเข้ารหัสเป็น BAD CREDIT เป็นต้น การเข้ารหัสด้วยวิธีการสลับที่สามารถแบ่งได้เป็นสองแบบ คือ การเข้ารหัสแบบไม่ใช้กุญแจ และ การเข้ารหัสแบบใช้กุญแจ

2.4.1 การเข้ารหัสสลับที่แบบไม่ใช้กุญแจ

การเข้ารหัสสลับที่แบบไม่ใช้กุญแจสามารถแบ่งเป็นสองวิธี คือ เขียนตัวอักษรทีละสดมภ์แล้วส่งข้อความทีละแถว (เช่น การเข้ารหัสแบบเรียลเฟนซ์) และ การเขียนตัวอักษรทีละแถวแล้วส่งข้อความทีละสดมภ์ดังแสดง ในตารางที่ 2.7 ซึ่งเป็นตัวอย่างการเข้ารหัสคำว่า SURANAREE ในตารางขนาด 2×5 โดยที่หากเป็นการเข้ารหัสด้วยการเขียนตามสดมภ์และอ่านตามแถวจะได้ผลลัพธ์เป็น SRNREUAAE ในขณะที่หากเป็นการเข้ารหัสด้วยการเขียนตามแถวแล้วอ่านตามสดมภ์จะได้ผลลัพธ์เป็น SAURREAEN

หากตารางดังกล่าวมีจำนวนแถวและจำนวนสดมภ์เท่ากันวิธีการทั้งสองวิธีจะได้ผลลัพธ์เดียวกัน เช่น ตารางขนาด 3×3 จะได้ผลลัพธ์เป็น SARUNERAE ตารางขนาด 4×4 จะได้ผลลัพธ์เป็น SNEUAR-RAE เป็นต้น

ตารางที่ 2.7: ตัวอย่างการแทนที่สลับที่แบบไม่ใช้กุญแจ

เขียนตามสดมภ์อ่านตามแถว	เขียนตามแถวอ่านตามสดมภ์
S R N R E U A A E	S U R A N A R E E

2.4.2 การเข้ารหัสสลับที่แบบใช้กุญแจ

การเข้ารหัสด้วยการสลับที่แบบใช้กุญแจนั้นคล้ายกับวิธีการเข้ารหัสสลับที่แบบไม่ใช้กุญแจแต่ วิธีการอ่านนั้นไม่จำเป็นต้องอ่านจากแถวแรกไปจนถึงแถวสุดท้ายหรืออ่านจากสดมภ์แรกไปจนถึงสดมภ์สุดท้าย ซึ่งการเข้ารหัสวิธีนี้สามารถอ่านแถวใดหรือสดมภ์ใดก่อนก็ได้แบบไม่เรียงลำดับ ยกตัวอย่างเช่น จากตารางที่ 2.7 หากเป็นการเขียนตามแถวแล้วอ่านตามสดมภ์ โดยกำหนดกุญแจหรือลำดับการอ่านตามสดมภ์ คือ 3 1 2 4 5 ผลลัพธ์ของการเข้ารหัสคำว่า SURANAREE คือ คำว่า RESAURAEN ซึ่งสามารถมองวิธีการสลับที่แบบใช้กุญแจดังกล่าวเป็นการคูณเมทริกซ์ดังแสดง ในรูปที่ 2.5

$$\begin{bmatrix} S & U & R & A & N \\ A & R & E & E & \end{bmatrix} \times \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} R & S & U & A & N \\ E & A & R & E & \end{bmatrix}$$

รูปที่ 2.5: การมองวิธีการเข้ารหัสแบบสลับที่ด้วยการใช้กุญแจเป็นการคูณเมทริกซ์

2.5 การเข้ารหัสแบบกระแสและบล็อก

วิธีการเข้ารหัสที่กล่าวมาสามารถสรุปตามวิธีการเข้ารหัสได้เป็นสองประเภทใหญ่ ได้แก่ การเข้ารหัสแบบกระแส และ การเข้ารหัสแบบบล็อก การเข้ารหัสแบบกระแสหมายถึง การเข้ารหัสครั้งละหนึ่งอักขระ เช่น การเข้ารหัสแบบซีซ่า และ กลุ่มการเข้ารหัสด้วยการแทนที่ด้วยอักขระเดิมเสมอ ส่วนการเข้ารหัสแบบบล็อก หมายถึง การเข้ารหัสครั้งละมากกว่าหนึ่งอักขระ เช่น กลุ่มของการเข้ารหัสซึ่งเปลี่ยนอักขระแทนที่ในแต่ละครั้ง และ กลุ่มการเข้ารหัสแบบสลับที่

2.6 สรุป

บทนี้ได้กล่าวถึงการเข้ารหัสด้วยกุญแจแบบสมมาตร โดยเริ่มตั้งแต่คณิตศาสตร์ที่เกี่ยวข้อง การเข้ารหัสด้วยกุญแจแบบสมมาตรในอดีต เทคนิคการเข้ารหัสแบบต่างๆ ได้แก่ การแทนที่ การสลับที่ การเข้ารหัสแบบกระแสและบล็อก

2.7 แบบฝึกหัด

1. การเข้ารหัสต่อไปนี้เป็นการเข้ารหัสแบบกระแส หรือ การเข้ารหัสแบบบล็อก

   (a) การเข้ารหัสแบบเพลย์แฟร์

   (b) การเข้ารหัสแบบกุญแจอัตโนมัติ

   (c) การเข้ารหัสแบบแพดครั้งเดียว

   (d) การเข้ารหัสด้วยเครื่องอินิกม่า

2. หากนักศึกษาปริญญาโทมีจำนวน 30 คนต้องการส่งข้อความลับซึ่งกันละกันจงหาจำนวนกุญแจที่ต้องใช้

   (a) กรณีที่ทุกคนต้องการสื่อสารกันเองทุกคู่

   (b) กรณีที่ทุกคนเชื่อใจประธานรุ่นและสื่อสารกันผ่านประธานรุ่น

3. หากตัวอักขระก่อนเข้ารหัสเปลี่ยนหนึ่งตัว ตัวอักขระหลังเข้ารหัสแล้วจะเปลี่ยนสูงสุดกี่ตัวในกรณีต่อไปนี้

   (a) การเข้ารหัสด้วยวิธีการสลับที่

   (b) การเข้ารหัสด้วยวิธีการสลับที่สองครั้ง

   (c) การเข้ารหัสด้วยเพลย์แฟร์

4. จงเข้ารหัสคำว่า SURANAREE UNIVERSITY OF TECHNOLOGY (ไม่ต้องสนใจช่องว่าง) ด้วยวิธีการต่อไปนี้

   (a) การเข้ารหัสด้วยวิธีไวเจเนียร์โดยที่กุญแจคือ ชื่อภาษาอังกฤษของนักศึกษา

   (b) การเข้ารหัสด้วยวิธีเพลย์แฟร์โดยที่กุญแจคือ ชื่อภาษาอังกฤษของนักศึกษา เขียนทีละแถว โดยเขียนเรียงจากแถวบนไปล่างและเรียงตัวอักขระจากซ้ายไปขวา

   (c) การเข้ารหัสด้วยกุญแจอัตโนมัติ โดยที่กุญแจ คือ ความยาวของชื่อภาษาอังกฤษของนักศึกษา

บทที่ 3

การเข้ารหัสด้วยกุญแจแบบสมมาตรสมัยใหม่ขั้นพื้นฐาน

- การเข้ารหัสด้วยกุญแจแบบสมมาตรสมัยใหม่
- มาตรฐานการเข้ารหัสข้อมูล (ดีอีเอส)

บทที่ 3

การเข้ารหัสด้วยกุญแจแบบสมมาตรสมัยใหม่ขั้นพื้นฐาน

3.1 การเข้ารหัสด้วยกุญแจแบบสมมาตรสมัยใหม่

การเข้ารหัสด้วยกุญแจแบบสมมาตรสมัยใหม่สามารถแบ่งเป็น 2 ประเภท คือ การเข้ารหัสแบบบล็อก และ การเข้ารหัสแบบกระแส ซึ่งจะกล่าวในรายละเอียดในหัวข้อที่ 3.1.1 และ 3.1.2 ตามลำดับ

3.1.1 การเข้ารหัสแบบบล็อก

การเข้ารหัสแบบบล็อกเป็นเข้ารหัสหรือถอดรหัสข้อความครั้งละ n บิต โดยอาศัยกุญแจความยาว k บิต ในการเข้ารหัสและถอดรหัส หากข้อความมีความยาวมากกว่า n บิตจะต้องแบ่งเข้ารหัสครั้ง n บิต หากบล็อกสุดท้ายมีความยาวน้อยกว่า n บิตอาจต้องมีการเพิ่มบิตให้เต็ม n บิต ซึ่งการเพิ่มบิตดังกล่าวเรียกว่า ''การแพดดิ้ง'' โดยทั่วไปค่า n จะมีค่าเท่ากับ 64, 128, 256 หรือ 512 บิต ตัวอย่างเช่น หากต้องการเข้ารหัสแบบบล็อกครั้งละ 64 บิตของข้อความซึ่งมีความยาว 100 ตัวอักษร โดยที่ตัวอักษรหนึ่งตัวสามารถแทนด้วยข้อมูล 8 บิต (ข้อความมีความยาว 800 บิต) การเข้ารหัสดังกล่าว จะต้องเข้ารหัสข้อความครั้งละ 64 บิต 13 ครั้งโดยที่ครั้งสุดท้ายต้องเพิ่มแพดดิ้ง 32 บิต หลักการเข้ารหัสด้วยกุญแจแบบสมมาตรสมัยใหม่นั้นคล้ายกับการเข้ารหัสในอดีตกล่าวคือ อาศัยการแทนที่และสลับที่ เพียงแต่เป็นการแทนที่หรือสลับที่บิตของข้อมูลไม่ใช่ตัวอักษร การแทนที่บิต 1 หรือ บิต 0 จะทำให้ข้อความที่ถูกเข้ารหัสอาจมีจำนวนบิต 1 และบิต 0 ไม่เท่าเดิม ในขณะที่การสลับที่จะยังคงจำนวนบิต 1 และบิต 0 เพียงแต่สลับที่กันเท่านั้น ซึ่งจะสลับที่กันได้ 2^n วิธี เมื่อ n คือความยาวของบล็อกในการเข้ารหัสแต่ละครั้ง แต่อย่างไรก็ตาม การสลับที่สามารถถูกโจมตี ด้วยการลองเพียง $\frac{n!}{(n-r)!r!}$ เมื่อ r คือ จำนวนบิต 1 (หรือบิต 0) ซึ่งการลองดังกล่าวมีค่าน้อยกว่า 2^n มาก ดังนั้นการเข้ารหัสด้วยวิธีแทนที่จึงมีความปลอดภัยมากกว่า ซึ่งต้องลองโจมตีถึง 2^n วิธี

การเข้ารหัสด้วยกุญแจแบบสมมาตรสมัยใหม่อาศัยองค์ประกอบย่อยต่างๆ ดังต่อไปนี้

- **กล่องสลับที่ หรือ กล่องพี** เป็นกล่องซึ่งอาศัยการสลับที่ซึ่งแบ่งเป็นสามประเภท ได้แก่ ประเภทที่จำนวนบิตนำเข้าและส่งออกจากกล่องเท่ากัน ประเภทที่จำนวนบิตนำเข้ามากกว่าบิตส่งออก (ตัดบางบิตทิ้ง) และ ประเภทที่จำนวนบิตส่งออกมากกว่าจำนวนบิตนำเข้า (คัดลอกบางบิต)

- **กล่องแทนที่ หรือ กล่องเอส** เป็นกล่องซึ่งอาศัยการแทนที่ซึ่งจำนวนบิตนำเข้า และส่งออกจากกล่องไม่จำเป็นต้องเท่ากัน เช่น กล่องอาจจะกำหนดว่าบิตนำเข้าเป็น 101 บิตส่งออก เป็น 01 (บิตนำเข้า 3 บิต ส่งออก 2 บิต)

- **เอ็กซ์คลูซีฟ ออร์ หรือ เอ็กซ์ออร์** ($\oplus$) เป็นตัวดำเนินการ ทางตรรกศาสตร์ ซึ่งใช้มากในด้านการเข้ารหัสเนื่องจากมีคุณสมบัติหลายประการ เช่น ผลลัพธ์ของการเอ็กซ์ออร์เลขฐานสองความยาว n บิตสองจำนวนจะมีขนาด n บิต นอกจากนั้นการเอ็กซ์ออร์ยังมีคุณสมบัติการจัดหมู่ กล่าวคือ $a \oplus (b \oplus c) \leftrightarrow (a \oplus b) \oplus c$ คุณสมบัติการสลับที่ กล่าวคือ $a \oplus b \leftrightarrow b \oplus a$ และคุณสมบัติอื่นๆ เช่น $a \oplus 0 = a$, $a \oplus a = 0$, $a \oplus \bar{a} = 1$, $a \oplus 1 = \bar{a}$ และคุณสมบัติที่สำคัญก็คือ $a = b \oplus c \rightarrow b = a \oplus c$ ซึ่งหาก c คือกุญแจแล้ว นั่นหมายความว่า หากนำข้อความมาเอ็กซ์ออร์กับกุญแจแล้วจะได้ข้อความที่เข้ารหัส และเมื่อนำข้อความที่เข้ารหัสดังกล่าวแล้วมาเอ็กซ์ออร์กับกุญแจจะได้ข้อความเดิมก่อนเข้ารหัส

- **การเลื่อนวน** การเลื่อนวนดังกล่าวสามารถกระทำได้ทั้งวนด้านซ้ายและวนด้านขวา ยกตัวอย่างเช่น หากมีข้อมูล 8 บิต $b_7b_6b_5b_4b_3b_2b_1b_0$ แล้วเลื่อนวนด้านซ้าย 2 ตำแหน่งจะกลายเป็น $b_5b_4b_3b_2b_1b_0b_7b_6$ หากเลื่อนข้อมูลต้นฉบับดังกล่าววนด้านขวา 5 ตำแหน่งจะกลายเป็น $b_4b_3b_2b_1b_0b_7b$ หากการเลื่อนวนด้วยตำแหน่งครึ่งหนึ่ง ของความยาวคำ จะเรียกการเลื่อนวนดังกล่าวว่า ''การสลับที่'' เช่น ในกรณีข้อมูล 8 บิต 4 บิตซ้ายกับ 4 บิตขวาจะสลับที่กันกลายเป็น $b_3b_2b_1b_0b_7b_6b_5b_4$ เป็นต้น

- **การแยกและการรวม** การเข้ารหัสและถอดรหัสอาจทำด้วยการแยกและการรวม เช่น หากข้อมูล 8 บิตอาจแยกข้อมูลเป็นสองส่วน ครึ่งละ 4 บิตเพื่อการเข้ารหัส ส่วนการถอดรหัสคือการรวมข้อมูลดังกล่าวกลับเป็น 8 บิตดังเดิม

วิธีการเข้ารหัสแบบบล็อกในปัจจุบันส่วนใหญ่เกิดจากการรวมเทคนิคดังกล่าวข้างต้นไว้ด้วยกัน ซึ่งทำให้การเข้าแบบบล็อกมีคุณสมบัติที่สำคัญ 2 ประการ ซึ่งเรียกว่า ดิฟฟิวชั่น และ คอนฟิวชั่น

- **ดิฟฟิวชัน** หมายถึง การซ่อนความสัมพันธ์ระหว่างข้อความต้นฉบับกับข้อความที่เข้ารหัสแล้ว การที่ตัวอักขระเข้ารหัสหนึ่งตัว(บิต) ขึ้นอยู่กับตัวอักขระต้นฉบับหลายตัว(บิต) หรือพูดอีกนัยหนึ่งว่า การเปลี่ยนตัวอักขระต้นฉบับเพียงหนึ่งตัวจะทำให้ตัวอักขระที่เข้ารหัสแล้วเปลี่ยนหลายตัว

- **คอนฟิวชัน** หมายถึง การซ่อนความสัมพันธ์ระหว่างกุญแจกับข้อความที่เข้ารหัสแล้ว ซึ่งหมายถึง การที่กุญแจเปลี่ยนเพียงหนึ่งตัวทำให้ตัวอักขระที่เข้ารหัสแล้วเปลี่ยนหลายตัว

การซ่อนความสัมพันธ์ระหว่างข้อความหลังเข้ารหัสกับข้อความต้นฉบับและกุญแจ ดังกล่าวสามารถกระทำได้โดยการเข้ารหัสด้วยเทคนิคต่างๆ เช่น กล่องเอส กล่องพี การเอ็กซ์ออร์ ซ้ำๆ หลายๆ รอบ (ยิ่งมากรอบ ยิ่งซ่อนความสัมพันธ์) ซึ่งจะส่งผลให้การเปลี่ยนแปลงข้อความต้นฉบับหรือกุญแจเพียงหนึ่งบิตส่งผลต่อ ข้อความที่เข้ารหัสแล้วหลายบิต

การเข้ารหัสแบบบล็อกสมัยใหม่นั้นสามารถจัดกลุ่มได้เป็น 2 ประเภท คือ กลุ่มฟรีซเทล และ กลุ่มที่ไม่ใช่พรีซเทล

- **การเข้ารหัสกลุ่มฟรีซเทล** เช่น การเข้ารหัสแบบดีอีเอส (ดังจะกล่าวในรายละเอียดในหัวข้อ 3.2) เป็นกลุ่มการเข้ารหัสโดยอาศัยคุณสมบัติของเอ็กซ์ออร์ทำให้สามารถใช้ส่วนประกอบ ซึ่งเป็นฟังก์ชันทางเดียว ($y = f(x)$ แต่ $x \neq f(y)$) หรือ ฟังก์ชันสองทางก็ได้ ซึ่งการเอ็กซ์ออร์จะทำให้ฟังก์ชันดังกล่าวไม่มีผล เช่น หากต้องการเข้ารหัสข้อความ p_1 ด้วยกุญแจ k และผลลัพธ์การเข้ารหัสคือ c จะได้ว่า $c = p_1 \oplus f(k)$ ดังนั้นหากต้องการถอดรหัส c เพื่อหา p_2 สามารถกระทำได้โดย $p_2 = c \oplus f(k) = p_1 \oplus f(k) \oplus f(k) = p_1 \oplus 0 = p_1$ ยกตัวอย่าง เช่น หากเรามีฟังก์ชันทางเดียวซึ่งอาศัยกล่องพีซึ่งผลลัพธ์คือข้อมูลนำเข้าบิตเลขคี่ (จำนวนข้อมูลส่งออกไม่เท่ากับข้อมูลนำเข้า) โดยมีข้อความคือ 1001 และกุญแจคือ 1000100 เราสามารถหาข้อความที่เข้ารหัส แล้วได้จาก $1001 \oplus f(1000100) = 1001 \oplus 1010$ ซึ่งได้ผลลัพธ์ คือ 0011 หากเราต้องการถอดรหัสเราสามารถกระทำได้โดย $0011 \oplus f(1000100) = 0011 \oplus 1010$ ซึ่งได้ผลลัพธ์ คือ 1001 ในทางปฏิบัติฟังก์ชันดังกล่าวจะมีข้อมูลนำเข้าคือกุญแจและข้อความต้นฉบับครึ่งหนึ่ง โดยผลลัพธ์ของฟังก์ชันดังกล่าวจะสลับซ้ายขวากับข้อความต้นฉบับอีกครึ่งหนึ่งที่เหลือ ซึ่งกระทำการเข้ารหัสในลักษณะนี้หลายๆ รอบซึ่งกุญแจแต่ละรอบอาจไม่เหมือนกัน
- **การเข้ารหัสกลุ่มที่ไม่ใช่ฟรีซเทล** เช่น การเข้ารหัสแบบเออีเอส (ดังจะกล่าวรายละเอียดในหัวข้อ 4.1) เป็นการเข้ารหัสซึ่งใช้ฟังก์ชันสองทางเป็นส่วนประกอบเท่านั้น เช่น กล่องเอสและกล่องพี ซึ่งมีจำนวนข้อมูลนำเข้าเท่ากับส่งออก เป็นต้น โดยที่กระทำการเข้ารหัสในลักษณะนี้หลายๆ รอบซึ่งกุญแจแต่ละรอบอาจไม่เหมือนกัน

3.1.2 การเข้ารหัสแบบกระแส

การเข้ารหัสแบบกระแสเป็นการเข้ารหัสครั้งละหนึ่งอักขระ(บิต) ซึ่งสามารถเข้ารหัสได้รวดเร็วกว่าการเข้ารหัสแบบบล็อก และสามารถพัฒนาได้ง่ายด้วยฮาร์ดแวร์ โดยที่การเข้ารหัสแบบกระแสของคำความยาว n อักขระ(บิต) จะต้องใช้กุญแจความยาวเท่ากันในการเข้ารหัส โดยที่วิธีการเข้ารหัสแบบกระแส

สามารถแบ่งเป็นสองประเภทใหญ่ ๆ คือ การเข้ารหัสแบบกระแสชนิดซิงโครนัส และการเข้ารหัสแบบกระแสชนิดนอนซิงโครนัส

- **การเข้ารหัสแบบกระแสชนิดซิงโครนัส** เป็นการเข้ารหัสโดยที่กระแสของกุญแจนั้น ไม่ขึ้นอยู่กับข้อความต้นฉบับหรือข้อความที่เข้ารหัสแล้ว ตัวอย่างของการเข้ารหัสแบบกระแสชนิดซิงโครนัส คือ แพดครั้งเดียว ซึ่งเป็นการเข้ารหัสโดยอาศัยการสร้างกุญแจแบบสุ่ม ที่มีความยาวเท่ากับข้อความที่ต้องการเข้ารหัส การเข้ารหัสจะกระทำโดยการเอ็กซ์ออร์ข้อความต้นฉบับกับกุญแจครั้งละหนึ่งอักขระ(บิต) การเข้ารหัสด้วยวิธีนี้จะทำให้ผลลัพธ์เป็นการสุ่มเนื่องจาก $0 \oplus k_i = k_i$ และ $1 \oplus k_i = \bar{k_i}$ ดังนั้นหาก k_i คือกุญแจแบบสุ่มจะทำให้ผลลัพธ์ เป็นแบบสุ่มเช่นเดียวกัน การสร้างกุญแจแบบสุ่มนั้นสามารถทำได้ด้วยการเลื่อนตำแหน่ง และการไหลกลับ ยกตัวอย่าง เช่น การใช้บิตเรียงกัน 4 บิต คือ $b_3b_2b_1b_0$ และบิตพิเศษ b_4 โดยที่ $b_4 = b_1 \oplus b_0$ หากให้ค่าเริ่มต้น คือ 0001 ทำให้ ค่าที่เรียงกันของ $b_4b_3b_2b_1b_0$ (เรียกว่าซี้ด) คือ 10001 กุญแจของการเข้ารหัสแต่ละบิต คือ บิตขวาสุดเมื่อมีการเลื่อนขวาในแต่ละรอบ เช่น รอบแรกได้กุญแจ คือ 1 และค่าของ 5 บิตดังกล่าวกลายเป็น 01000 รอบแรกได้กุญแจ คือ 0 และค่าของ 5 บิตดังกล่าวกลายเป็น 00100 หากเข้ารหัสดังกล่าวหลายรอบจะได้ค่ากุญแจแบบสุ่มดังแสดงในตารางที่ 3.1 ซึ่งจะได้กุญแจแบบสุ่มแต่อย่างไรก็ตามกุญแจดังกล่าวจะเกิดการวนซ้ำ ซึ่งในทางทฤษฎีแล้ว หากมีบิตเรียงกัน m บิต อาจจะทำให้ไม่เกิดการวนซ้ำจนถึงรอบที่ $2^m - 1$ จากตัวอย่างนี้กุญแจจะวนซ้ำทุกๆ 15 รอบ กล่าวคือ 100010011010111 100010011010111 100010011010111 ...

ตารางที่ 3.1: ตัวอย่างการสร้างกุญแจแบบสุ่ม

รอบที่	$b_4 = b_1 \oplus b_0$	b_3	b_2	b_1	b_0	กุญแจ k_i
เริ่มต้น	1	0	0	0	1	ไม่มีค่า
1	0	1	0	0	0	1
2	0	0	1	0	0	0
3	1	0	0	1	0	0
4	1	1	0	0	1	0
5	0	1	1	0	0	1
6	1	0	1	1	0	0
7	0	1	0	1	1	0
8	1	0	1	0	1	1
9	1	1	0	1	0	1

- **การเข้ารหัสแบบกระแสชนิดนอนซิงโครนัส** เป็นการเข้ารหัสโดยที่กระแสของกุญแจนั้น ขึ้นอยู่กับข้อความต้นฉบับหรือข้อความที่เข้ารหัสแล้ว เช่น โหมดต่างๆ ในการเข้ารหัสแบบบล็อก ซึ่งจะกล่าวรายละเอียดในหัวข้อ 4.2.1

3.2 มาตรฐานการเข้ารหัสข้อมูล (ดีอีเอส)

มาตรฐานการเข้ารหัสข้อมูล (ดีอีเอส) เป็นการเข้ารหัสด้วยกุญแจสมมาตรแบบบล็อก ซึ่งกำหนดโดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติสหรัฐอเมริกา (นีสท์) โดยในปี พ.ศ. 2516 สถาบันดังกล่าวได้จัดประกวดการเข้ารหัสแบบสมมาตร และผู้ชนะคือ การเข้ารหัสซึ่งถูกดัดแปลงจากโครงการ ลูซีเฟอร์ของบริษัทไอบีเอ็ม และประกาศใช้ในฐานะมาตรฐานการเข้ารหัสข้อมูลในปี พ.ศ. 2520 แต่อย่างไรก็ตามมาตรฐานการเข้ารหัสดังกล่าวก็ถูกกล่าวหาว่าไม่ปลอดภัยเนื่องจากใช้กุญแจเพียง 56 บิต และอาจมีกับดักซ่อนอยู่ในกล่องเอส เพื่อทำให้องค์กรความมั่นคงแห่งชาติสหรัฐอเมริกา (เอ็นเอสเอ) สามารถถอดรหัสได้ ดีอีเอสได้รับความนิยมในโปรแกรมประยุกต์ที่ไม่ใช่ความลับ ซึ่งภายหลัง นีสท์ ได้แนะนำให้ใช้ ทริปเปิ้ลดีอีเอส (การเข้ารหัสดีอีเอสสามครั้ง) แทน และในปัจจุบันให้ใช้ มาตรฐานการเข้ารหัสขั้นสูง (เออีเอส) แทน

การเข้ารหัสแบบดีอีเอสเป็นการเข้ารหัสสมมาตรแบบบล็อกโดยการเข้ารหัสข้อความครั้งละ 64 บิต ด้วยกุญแจความยาว 56 บิต และ ผลลัพธ์ที่ได้เป็นข้อความที่เข้ารหัสแล้วความยาว 64 บิต ซึ่งจะกล่าวรายละเอียดในหัวข้อถัดไป

3.2.1 โครงสร้างของดีอีเอส

การเข้ารหัสดีอีเอสเริ่มต้นด้วยการผ่านกล่องพีหนึ่งครั้ง จากนั้นจะเป็นการเข้ารหัส แบบฟรีซเทลจำนวน 16 รอบโดยแต่ละรอบจะใช้กุญแจที่แตกต่างกัน ซึ่งกุญแจดังกล่าวมีความยาว 48 บิต ซึ่งกุญแจแต่ละรอบถูกสร้างจากกุญแจ 56 บิตต้นฉบับ หลังจากผ่านฟรีซเทลรอบสุดท้าย แล้วข้อความจะผ่านกล่องพีอีกครั้ง จึงจะได้ผลลัพธ์สุดท้ายของการเข้ารหัสดีอีเอส

กล่องพีแรกและกล่องพีสุดท้าย

กล่องพีแรกและสุดท้ายจะมีลักษณะตรงกันข้าม เช่น กล่องแรกข้อมูลนำเข้าบิต 58 จะกลาย เป็นบิตที่ 1 ในขณะที่กล่องสุดท้ายข้อมูลบิตที่ 1 จะกลายเป็นบิต 58 เป็นต้น ดังแสดงในตารางที่ 3.2 ซึ่งตัวเลขในตารางแทนตำแหน่งบิตข้อมูลขาเข้าในขณะที่ตำแหน่งของตัวเลขดังกล่าว แสดงข้อมูลขาออก ตัวอย่าง เช่น หากข้อมูลนำเข้าของกล่องพีกล่องแรกมีค่าเป็น 0x8000400020001000 ซึ่งมีบิต 1 จำนวน 4 บิต (คือ บิตที่ 1, 18, 35 และ 52) ซึ่งจะได้ผลลัพธ์ คือ 0x0440000001100000 ซึ่งมีบิต 1 จำนวน 4 บิต (คือ บิตที่ 40, 6, 44 และ 10) เช่นเดียวกันกับข้อมูลนำเข้า และหากนำผลลัพธ์ของกล่องพีกล่องแรกเป็นข้อมูลนำเข้าของกล่องพีกล่องสุดท้าย ผลลัพธ์ที่ออกมาจากกล่องพีกล่องสุดท้าย คือ ข้อมูลนำเข้าของกล่องพีกล่องแรก ซึ่งจะเห็นได้ว่า กล่องพีกล่องสุดท้ายมีคุณสมบัติตรงข้ามกับกล่องพีกล่องแรกนั่นเอง

ตารางที่ 3.2: กล่องพีของดีอีเอส

กล่องพีกล่องแรก								กล่องพีกล่องสุดท้าย							
58	50	42	34	26	18	10	02	40	08	48	16	56	24	64	32
60	52	44	36	28	20	12	04	39	07	47	15	55	23	63	31
62	54	46	38	30	22	14	06	38	06	46	14	54	22	62	30
64	56	48	40	32	24	16	08	37	05	45	13	53	21	61	29
57	49	41	33	25	17	09	01	36	04	44	12	52	20	60	28
59	51	43	35	27	19	11	03	35	03	43	11	51	19	59	27
61	53	45	37	29	21	13	05	34	02	42	10	50	18	58	26
63	55	47	39	31	23	15	07	33	01	41	09	49	17	57	25

การเข้ารหัสในแต่ละรอบ

การเข้ารหัสในแต่ละรอบ (ทั้ง 16 รอบ) จะเป็นการเข้ารหัสแบบฟรีซเทล โดยที่ข้อมูล 64 บิตจะแบ่งเป็น 2 ฝั่งซ้ายและขวาฝั่งละ 32 บิต ข้อมูล 32 บิตครึ่งขวาจะถูกสลับไปเป็นข้อมูล 32 บิตครึ่งซ้ายของผลลัพธ์ ในขณะที่ข้อมูลนำเข้า 32 บิตครึ่งซ้ายจะถูกนำไปเข้ารหัสด้วยการนำไปเอ็กซ์ออร์ กับ ดีอีเอสฟังก์ชัน ซึ่งผลลัพธ์ของการเอ็กซ์ออร์ดังกล่าวจะถูกเก็บในข้อมูล 32 บิตครึ่งขวาของผลลัพธ์

ดีอีเอสฟังก์ชัน

ดีอีเอสฟังก์ชัน ถือเป็นหัวใจของดีอีเอสซึ่งเป็นการเข้ารหัสข้อมูล 32 บิตขวาสุดด้วยกุญแจ 48 บิต โดยได้ผลลัพธ์ 32 บิต ดีอีเอสฟังก์ชันนี้ประกอบด้วย 4 ขั้นตอนย่อยๆ คือ กล่องพีแบบขยายซึ่งข้อมูลส่งออก มีจำนวนบิตมากกว่าข้อมูลนำเข้า การผสมกุญแจ (ไวท์เทนเนอร์) กลุ่มของกล่องเอส และ กล่องพีแบบตรง ซึ่งจำนวนบิตของข้อมูลนำเข้าและส่งออกเท่ากัน

- **กล่องพีขยาย** จะเป็นกล่องพีซึ่งนำเข้าข้อมูล 32 บิตและได้ผลลัพธ์ 48 บิต โดยที่กล่องดังกล่าวจะแบ่งข้อมูลนำเข้าเป็นกลุ่ม กลุ่มละ 4 บิตจำนวน 8 กลุ่ม โดยที่แต่ละกลุ่มจะให้ผลลัพธ์กลุ่มละ 6 บิตกล่าวคือ ผลลัพธ์บิตแรก คือ บิตนำเข้าบิตสุดท้ายของกลุ่มก่อนหน้า ผลลัพธ์บิตที่ 2 ถึง 5 คือ บิตนำเข้าทั้ง 4 บิตเรียงตามลำดับ ผลลัพธ์บิตสุดท้ายของกลุ่ม คือ บิตนำเข้าบิตแรกของกลุ่มถัดไปดังแสดงในตารางที่ 3.3 ซึ่งตัวเลขในตาราง คือ ตำแหน่งของบิตนำเข้า ในขณะที่ตำแหน่งของตัวเลขดังกล่าว คือ ตำแหน่งของบิตส่งออกในแต่ละกลุ่ม

- **ไวท์เทนเนอร์** หลังจากที่ข้อมูล 32 บิต ถูกขยายเป็น 48 บิตด้วยการผ่านกล่องพีในขั้นตอนแรกแล้ว ข้อมูล 48 บิตดังกล่าวจะถูกนำมาเอ็กซ์ออร์กับกุญแจประจำรอบซึ่งมีความยาว 48 บิต

- **กล่องเอส** ดีอีเอสใช้กล่องเอส 8 กล่องโดยที่แต่ละกล่องจะรับข้อมูลนำเข้า 6 บิตและส่งออกข้อมูล 4 บิต กล่องเอสดังกล่าวจะอยู่ในรูปของตารางโดยที่บิตที่ 1 และ 6 จะใช้เลือกแถวของตาราง (แถวที่ 0 ถึง 3) ส่วนบิตที่ 2 ถึงบิตที่ 5 จะใช้เลือกสดมภ์ของตาราง (สดมภ์ที่ 0 ถึง

ตารางที่ 3.3: กล่องพีแบบขยายในดีอีเอสฟังก์ชัน

กลุ่มที่ 1	32	01	02	03	04	05
กลุ่มที่ 2	04	05	06	07	08	09
กลุ่มที่ 3	08	09	10	11	12	13
กลุ่มที่ 4	12	13	14	15	16	17
กลุ่มที่ 5	16	17	18	19	20	21
กลุ่มที่ 6	20	21	22	23	24	25
กลุ่มที่ 7	24	25	26	27	28	29
กลุ่มที่ 8	28	29	30	31	32	01

15) โดยที่ค่าในตารางคือผลลัพธ์ 4 บิต (0 ถึง 15) กล่องเอสทั้ง 8 กล่องแสดงในตารางที่ 3.4 ตัวอย่างเช่น หากข้อมูลนำเข้ากล่องเอส 1 คือ 111101 (ซึ่งบิต 1 และ 6 คือ 11 (แถว 3) และบิต 2 ถึง 5 คือ 1110 (สดมภ์ 14)) จะได้ผลลัพธ์ คือ 6 (0110) หากข้อมูลนำเข้ากล่องเอส 4 คือ 101010 จะได้ผลลัพธ์ คือ 1011 เป็นต้น

- **กล่องพีแบบตรง** กล่องพีดังกล่าวจะเป็นการสลับที่ของข้อมูล 32 บิต ดังแสดงในตารางที่ 3.5 ยกตัวอย่าง เช่น ข้อมูลนำเข้าบิตที่ 16 จะกลายเป็นผลลัพธ์บิตที่ 1 ข้อมูลนำเข้าบิตที่ 25 จะกลายเป็นผลลัพธ์บิตที่ 32 เป็นต้น

วิธีการถอดรหัสของดีอีเอสสามารถทำตรงกันข้ามกับการเข้ารหัส กล่าวคือรอบที่ 1 จะกลายเป็นรอบที่ 16 ข้อมูลนำเข้าจะกลายเป็นส่งออก เป็นต้น ซึ่งรอบสุดท้ายของการเข้ารหัสไม่จำเป็นต้องมีการสลับครึ่ง (หรือเพิ่มการสลับครึ่งอีกครั้ง) เพื่อให้สามารถย้อนกลับในการถอดรหัสได้

การสร้างกุญแจในแต่ละรอบ

กุญแจในแต่ละรอบมีขนาด 48 บิตซึ่งถูกสร้างมาจากกุญแจ 56 บิต โดยปกติแล้วกุญแจจะถูกนำเข้าด้วยกุญแจขนาด 64 บิตซึ่งประกอบไปด้วยกุญแจจริงๆ 56 บิตและ พาริตี้บิตอีก 8 บิต (ซึ่งอยู่ในบิตที่ 8, 16, 24, ..., 64) ซึ่งพาริตี้บิตเหล่านี้จะต้องถูกเอาออกก่อนโดยการใช้กล่องพีดังแสดงในตารางที่ 3.6 หลังจากผ่านกล่องพีแล้ว กุญแจจะถูกแบ่งเป็นสองส่วนส่วนละ 28 บิต โดยหากเป็นการสร้างกุญแจในรอบที่ 1,2,9 และ 16 จะวนแต่ละส่วนไปทางซ้าย 1 บิต หากเป็นรอบอื่นๆ จะวนแต่ละส่วนไปทางซ้าย 2 บิต หลังจากนั้นในรอบต่างๆ จะนำกุญแจทั้งสองส่วนรวมกลับเป็น 56 บิต แล้วผ่านกล่องพีแบบบีบอัดเพื่อให้ได้ผลลัพธ์เป็นกุญแจ 48 บิตดังแสดงในตารางที่ 3.7

ตารางที่ 3.4: กล่องเอสทั้ง 8 กล่องของดีอีเอส

กล่องเอส 1	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
00	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
01	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
02	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
03	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13
กล่องเอส 2	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
00	15	01	08	14	06	11	03	04	09	07	02	13	12	00	05	10
01	03	13	04	07	15	02	08	14	12	00	01	10	06	09	11	05
02	00	14	07	11	10	04	13	01	05	08	12	06	09	03	02	15
03	13	08	10	01	03	15	04	02	11	06	07	12	00	05	14	09
กล่องเอส 3	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
00	10	00	09	14	06	03	15	05	01	13	12	07	11	04	02	08
01	13	07	00	09	03	04	06	10	02	08	05	14	12	11	15	01
02	13	06	04	09	08	15	03	00	11	01	02	12	05	10	14	07
03	01	10	13	00	06	09	08	07	04	15	14	03	11	05	02	12
กล่องเอส 4	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
00	07	13	14	03	00	06	09	10	01	02	08	05	11	12	04	15
01	13	08	11	05	06	15	00	03	04	07	02	12	01	10	14	09
02	10	06	09	00	12	11	07	13	15	01	03	14	05	02	08	04
03	03	15	00	06	10	01	13	08	09	04	05	11	12	07	02	14
กล่องเอส 5	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
00	02	12	04	01	07	10	11	06	08	05	03	15	13	00	14	09
01	14	11	02	12	04	07	13	01	05	00	15	10	03	09	08	06
02	04	02	01	11	10	13	07	08	15	09	12	05	06	03	00	14
03	11	08	12	07	01	14	02	13	06	15	00	09	10	04	05	03
กล่องเอส 6	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
00	12	01	10	15	09	02	06	08	00	13	03	04	14	07	05	11
01	10	15	04	02	07	12	09	05	06	01	13	14	00	11	03	08
02	09	14	15	05	02	08	12	03	07	00	04	10	01	13	11	06
03	04	03	02	12	09	05	15	10	11	14	01	07	10	00	08	13
กล่องเอส 7	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
00	04	11	02	14	15	00	08	13	03	12	09	07	05	10	06	01
01	13	00	11	07	04	09	01	10	14	03	05	12	02	15	08	06
02	01	04	11	13	12	03	07	14	10	15	06	08	00	05	09	02
03	06	11	13	08	01	04	10	07	09	05	00	15	14	02	03	12
กล่องเอส 8	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
00	13	02	08	04	06	15	11	01	10	09	03	14	05	00	12	07
01	01	15	13	08	10	03	07	04	12	05	06	11	10	14	09	02
02	07	11	04	01	09	12	14	02	00	06	10	10	15	03	05	08
03	02	01	14	07	04	10	08	13	15	12	09	09	03	05	06	11

ตารางที่ 3.5: กล่องพีแบบตรงในดีอีเอสฟังก์ชัน

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

ตารางที่ 3.6: กล่องพีสำหรับการสร้างกุญแจในแต่ละรอบ

57	49	41	33	25	17	09	01
58	50	42	34	26	18	10	02
59	51	43	35	27	19	11	03
60	52	44	36	63	55	47	39
31	23	15	07	62	54	46	38
30	22	14	06	61	53	45	37
29	21	13	05	28	20	12	04

ตารางที่ 3.7: กล่องพีบีบอัดสำหรับการสร้างกุญแจในแต่ละรอบ

14	17	11	24	01	05	03	28
15	06	21	10	23	19	12	04
26	08	16	07	27	20	13	02
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

3.2.2 ตัวอย่างการเข้ารหัสด้วยดีอีเอส

หากต้องการเข้ารหัสคำว่า thara sut (แปลงเฉพาะตัวอักษรเป็นรหัสแอสกี จะได้ 0x7468617261737574) โดยใช้กุญแจ คำว่า security (แปลงตัวอักษรเป็นรหัสแอสกี จะได้ 0x7365637572697479) จะได้ผลลัพธ์เป็น 0x7BB6210C734B3A1D เป็นต้น ซึ่งมีขั้นตอนการทำงานโดยเริ่มจาก การนำข้อความที่ต้องการเข้ารหัสมาผ่านกล่องพีกล่องแรกจะได้ผลลัพธ์ คือ 0xFFE9C17400FF0228 ซึ่งสามารถแยกเป็นข้อมูลก่อนเข้ารอบที่ 1 เป็นฝั่งซ้าย คือ 0xFFE9C174 และ ฝั่งขวาคือ 0x00FF0228 หลังจากนั้นจะผ่านเข้ารหัส 16 รอบ ดังแสดงในตารางที่ 3.8 ผลลัพธ์ที่ได้จากการเข้ารหัสรอบที่ 16 จะนำไปผ่าน

ตารางที่ 3.8: ตัวอย่างการทำงานของดีอีเอส

รอบที่	ฝั่งซ้าย	ฝั่งขวา	กุญแจประจำรอบ
1	0x00FF0228	0x19F7085F	0xF0BE6E752830
2	0x19F7085F	0x93036AC9	0xF0BEF682C285
3	0x93036AC9	0xF7A77599	0xF4F676D20781
4	0xF7A77599	0x2314B244	0xE6D7769A0309
5	0x2314B244	0x224881E7	0xEED377527300
6	0x224881E7	0x9674BB86	0xAFD37B702128
7	0x9674BB86	0x4D8D86FF	0xAF53FBE0380A
8	0x4D8D86FF	0x2E64EAC5	0xBF5BD964323A
9	0x2E64EAC5	0x29EF4D76	0x3F59DB8AC501
10	0x29EF4D76	0x64D9648E	0x3F69DD4A4704
11	0x64D9648E	0x39F52637	0x1F6D9DD84188
12	0x39F52637	0x066A9E61	0x5F2DBDC05209
13	0x066A9E61	0xC1703185	0xDFACADD23228
14	0xC1703185	0x3797D329	0xDBAEAEB01B28
15	0x3797D329	0x0257E973	0xF8BEAE103A32
16	0x0257E973	0x31D38AB5	0xF1BEA68841C5

กล่องพีกล่องสุดท้าย ซึ่งจะได้คำตอบ คือ 0x7BB6210C734B3A1D

3.2.3 ทริปเปิ้ลดีอีเอส

การเพิ่มความมั่นคงปลอดภัยให้กับดีอีเอสสามารถกระทำได้ด้วยวิธีการที่เรียกว่า ทริปเปิ้ลดีอีเอส โดยการเข้ารหัสด้วยดีอีเอสสามขั้นตอนทั้งการเข้ารหัสและการถอดรหัสโดยที่ขั้นตอนที่สองจะทำตรงกันข้าม เช่น หากเป็นการเข้ารหัส ขั้นตอนแรกคือ การเข้ารหัส ขั้นตอนที่สอง คือ การถอดรหัส และขั้นตอนที่สาม คือ การเข้ารหัส สำหรับวิธีการทริปเปิ้ลดีอีเอสยังสามารถแบ่งเป็นสองชนิดย่อย คือ แบบใช้กุญแจสองดอก (ขั้นตอนแรกและขั้นตอนที่สองจะใช้กุญแจดอกเดียวกัน) และ กุญแจสามดอกซึ่งแต่ละขั้นตอนจะใช้กุญแจหนึ่งดอก ตัวอย่างเช่น หากต้องการเข้ารหัสคำว่า thara sut (แปลงเฉพาะตัวอักษรเป็นรหัสแอสกี จะได้ 0x7468617261737574) โดยใช้กุญแจ สองดอก ดอกแรก คือ คำว่า security (แปลงตัวอักษรเป็นรหัสแอสกี จะได้ 0x7365637572697479) และดอกที่สอง คือ คำว่า computer (แปลง

ตัวอักษรเป็นรหัสแอสกี จะได้ 0x636F6D7075746572) ซึ่งผลลัพธ์ที่ได้ คือ 0xD1D3077AB03618E8 เป็นต้น ในปัจจุบันวิธีการเข้ารหัสดังกล่าวได้ถูกนำมาใช้ในการรับส่งข้อมูลระหว่างตู้เอทีเอ็มกับธนาคาร

3.3 สรุป

บทนี้ได้กล่าวถึง การเข้ารหัสด้วยกุญแจแบบสมมาตรสมัยใหม่ ได้แก่ การเข้ารหัสแบบบล็อก และการเข้ารหัสแบบกระแส นอกจากนั้นยังกล่าวถึงรายละเอียดของมาตรฐานการเข้ารหัสด้วยกุญแจแบบสมมาตร (ดีอีเอส)

3.4 แบบฝึกหัด

1. จงคำนวณหาค่าต่อไปนี้

   (a) 01101011 $\oplus$ 10101001

   (b) วนซ้าย 3 บิตของข้อมูล 10101001

   (c) วนขวา 3 บิตของผลลัพธ์ของข้อก่อนหน้านี้

   (d) การสลับที่ (เลื่อนวนครึ่งของความยาว) ของ 01101011

2. หากต้องการเข้ารหัสข้อมูล 1000 ตัวอักษรด้วยวิธีการเข้ารหัสซึ่งอ่านข้อมูลครั้งละ 64 บิต จงหาว่าจะต้องเข้ารหัสทั้งหมดกี่รอบ

3. การสลับที่หรือการแทนที่ปลอดภัยกว่ากัน เพราะเหตุใด

4. จงคำนวณหาว่า กล่องพีต่อไปนี้เป็นกล่องพีชนิดใด (แบบขยาย แบบตรง หรือ แบบบีบอัด)

   (a) 1 2 5 7 8 9

   (b) 1 1 2 3 4 4

   (c) 1 2 3 4 5 6

5. จงหาผลลัพธ์ของกล่องเอส 4 ในดีอีเอส ที่มีข้อมูลนำเข้า คือ 111111

6. จงหาผลลัพธ์ของกล่องพีแรกในดีอีเอส ที่ข้อมูลนำเข้า คือ 0xABCDABCDABCDABCD

7. จงหาผลลัพธ์ของกล่องพีกล่องสุดท้ายในดีอีเอส ที่ข้อมูลนำเข้า คือ ผลลัพธ์ของข้อก่อนหน้า

8. หากกุญแจ 64 บิตมีค่า 0xDEADDEADDEADDEAD จงหากุญแจรอบแรกของดีอีเอส

9. ข้อมูลและกุญแจ คือ 0x0000000000000000 จงหาผลลัพธ์หลังสิ้นสุดรอบแรกของดีอีเอส

บทที่ 4

การเข้ารหัสด้วยกุญแจแบบสมมาตรสมัยใหม่ขั้นสูง

- มาตรฐานการเข้ารหัสขั้นสูง (เออีเอส)
- การใช้งานการเข้ารหัสด้วยกุญแจแบบสมมาตรสมัยใหม่

บทที่ 4

การเข้ารหัสด้วยกุญแจแบบสมมาตรสมัยใหม่ขั้นสูง

ในบทนี้จะกล่าวถึงการเข้ารหัสด้วยกุญแจแบบสมมาตรสมัยใหม่ขั้นสูง ได้แก่ มาตรฐานการเข้ารหัสขั้นสูง วิธีการใช้งานการเข้ารหัสด้วยกุญแจแบบสมมาตรสมัยใหม่แบบบล็อก เพื่อเข้ารหัสข้อความที่มีความยาวมากกว่าหรือน้อยกว่าบล็อกของการเข้ารหัส วิธีการใช้งานการเข้ารหัสด้วยกุญแจแบบสมมาตรสมัยใหม่แบบกระแส เป็นต้น

4.1 มาตรฐานการเข้ารหัสขั้นสูง (เออีเอส)

มาตรฐานการเข้ารหัสชั้นสูง หรือ เออีเอส เป็นการเข้ารหัสด้วยกุญแจสมมาตรแบบบล็อก ซึ่งกำหนดโดย สถาบันมาตรฐานและเทคโนโลยีแห่งชาติสหรัฐอเมริกา (นีสท์) สถาบันดังกล่าวได้จัดประกวดการเข้ารหัสแบบสมมาตร เพื่อใช้ทดแทน ดีอีเอส (ดังรายละเอียดในหัวข้อ 3.2) ในปี พ.ศ. 2540 โดยกำหนดว่าการเข้ารหัสแบบเออีเอสต้องเป็นการเข้ารหัสแบบบล็อกโดยอ่านข้อมูลบล็อกละ 128 บิต โดยใช้กุญแจความยาว 128 บิต, 192 บิต และ 256 บิต ในปี พ.ศ. 2541 มีผู้ผ่านการคัดเลือกรอบแรกจำนวน 15 จาก 21 โครงการ หลังจากนั้น ในปี พ.ศ. 2542 มีโครงการที่ผ่านการเข้ารอบครั้งที่สองจำนวน 5 จาก 15 โครงการ คือ มาร์, อาร์ซี 6, เรนดอล, เซอเป็น และ ทูฟิช หลังจากนั้น ในปี พ.ศ. 2542 สถาบันนีสท์ได้ประกาศว่า ผู้ชนะ คือ ''เรนดอล'' ซึ่งถูกออกแบบโดย นักวิจัยชาวเบลเยี่ยมสองคน คือ โจน เดม่อน และ วินเซนต์ เรนเม็นท์ และประกาศใช้เออีเอสอย่างเป็นทางการในปี พ.ศ. 2544 หลักเกณฑ์ในการคัดเลือกเออีเอส มีสามด้าน คือ ด้านความมั่นคงปลอดภัย ต้นทุน (ประสิทธิภาพในการคำนวณ จัดเก็บ ทั้งในซอฟต์แวร์ และ ฮาร์ดแวร์) และ ความสามารถในการประยุกต์ใช้ (ความง่ายและสามารถใช้ได้ในทุกอุปกรณ์) ซึ่งเรนดอล ก็ทำได้ดีทั้งสามด้าน

เออีเอสจัดได้ว่าเป็นการเข้ารหัสแบบมิใช่ฟรีซเทล ซึ่งเป็นการเข้ารหัสข้อมูลแบบบล็อก ครั้งละ 128 บิต ซึ่งสามารถเข้ารหัสแบบ 10, 12 และ 14 รอบ โดยมีกุญแจความยาว 128, 192 และ 256 บิต ขึ้นกับจำนวนรอบตามลำดับ เรียกว่า เออีเอส-128, เออีเอส-192 และ เออีเอส-256 แต่อย่างไรก็ตาม กุญแจประจำรอบในแต่ละรอบนั้นมีขนาดคงที่ 128 บิตเสมอ โดยที่กุญแจประจำรอบจะมีจำนวนเท่ากับ จำนวนรอบ + 1 โดยที่กุญแจอีกดอกที่เพิ่มขึ้นมาจะถูกใช้ในขั้นตอนก่อนรอบแรก

4.1.1 รูปแบบข้อมูลของเออีเอส

เออีเอสมีรูปแบบข้อมูลอยู่ 5 รูปแบบ ได้แก่ บิต ไบต์ เวิร์ด บล็อก และ สเตท โดยที่บิตคือข้อมูลที่เล็กที่สุด ซึ่งประกอบไปด้วยบิต 0 และบิต 1 ในขณะที่ หนึ่งไบต์มีขนาด 8 บิต ซึ่งอาจจะเขียนอยู่ในรูปของเมตริกซ์ 1×8 หรือ 8×1 ก็ได้) หนึ่งเวิร์ด มีขนาด 4 ไบต์ ซึ่งอาจจะเขียนอยู่ในรูปของเมทริกซ์ 1×4 หรือ 4×1 ก็ได้ หนึ่งบล็อกมีขนาด 16 ไบต์ซึ่งถูกเขียนอยู่ในรูปของเมทริกซ์ 1×16 ในขณะที่ สเตท คือ สถานะ ของข้อมูลขนาด 16 ไบต์ซึ่งถูกเขียนอยู่ในรูปของเมทริกซ์ 4×4 ทีละสดมภ์ ยกตัวอย่าง เช่น หากเรามีข้อมูล ''We love Suranaree.'' เราสามารถแปลงเป็นรหัสแอสกี (โดยไม่สนใจเว้นวรรค) ได้เป็น 57 65 6C 6F 76 65 53 75 72 61 6E 61 72 65 65 2E ซึ่งสามารถแสดงเป็นบล็อกและสเตทได้ดังรูปที่ 4.1

บล็อก

$$\begin{bmatrix} 57 & 65 & 6C & 6F & 76 & 65 & 53 & 75 & 72 & 61 & 6E & 61 & 72 & 65 & 65 & 2E \end{bmatrix}$$

สเตท

$$\begin{bmatrix} 57 & 76 & 72 & 72 \\ 65 & 65 & 61 & 65 \\ 6C & 53 & 6E & 65 \\ 6F & 75 & 61 & 2E \end{bmatrix}$$

รูปที่ 4.1: ตัวอย่างของการแปลงระหว่างบล็อกกับสเตท

4.1.2 โครงสร้างของเออีเอส

ในแต่ละรอบของเออีเอสเป็นการแปลงจากสเตทหนึ่งไปยังอีกสเตทหนึ่งด้วยขั้นตอนย่อยๆ ซึ่งประกอบด้วย 4 ขั้นตอนย่อย ได้แก่ การแทนที่ไบต์ การเลื่อนแถว การผสมสดมภ์ และ การผสมกุญแจ โดยปกติแล้วในแต่ละรอบของเออีเอสทำงานครบทั้ง 4 ขั้นตอนย่อย ยกเว้น ขั้นตอนก่อนรอบแรกจะประกอบด้วย การผสมกุญแจเพียงอย่างเดียว และ รอบสุดท้ายจะประกอบไปด้วย 3 ขั้นตอนย่อยโดยไม่มีการผสมสดมภ์

การแทนที่ไบต์

การแทนที่ไบต์ของเออีเอสจะเป็นการแทนที่ครั้งละ 1 ไบต์ ซึ่งทุกไบต์จะใช้ตารางเดียวกัน โดยที่ 4 บิตซ้ายสุดของไบต์นำเข้าจะชี้ที่แถว และ 4 บิตขวาสุดของไบต์นำเข้าจะชี้ที่สดมภ์ ส่วนค่าในตารางคือไบต์ส่งออกที่ใช้แทนที่ กล่องเอสที่ใช้ในการแทนที่ไบต์ ของขั้นตอนในการเข้ารหัสและถอดรหัส แสดงในตารางที่ 4.1 และ 4.2 ตามลำดับ

ตารางที่ 4.1: กล่องเอสเพื่อใช้ในการแทนที่ไบต์ในการเข้ารหัส

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	CB	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

รูปที่ 4.2 แสดงการแปลงระหว่างสเตทโดยใช้กล่องเอส จากสเตท A ไปยัง สเตท B จะใช้กล่องเอสสำหหรับการเข้ารหัส ในขณะที่สเตท B กลับไปยัง สเตท A จะใช้กล่องเอสสำหรับการถอดรหัส ซึ่งจะสังเกตได้ว่ากล่องเอสทั้งสองตรงข้ามกัน

การสลับที่ไบต์

การสลับที่ไบต์ในเออีเอสจะกระทำด้วยการเลื่อนไบต์ในแต่ละแถว หากเป็นการเข้ารหัสจะเป็นการเลื่อนไปทางซ้าย ในขณะที่การถอดรหัสจะเป็นการเลื่อนไปทางขวา จำนวนไบต์ของการเลื่อนแต่ละครั้งคือตำแหน่งของแถว เช่น แถวที่ 0 จะไม่มีการเลื่อน แถวที่ 1 จะเป็นการเลื่อน 1 ไบต์ แถวที่ 2 จะเป็นการเลื่อน 2 ไบต์ และ แถวที่ 3 จะเป็นการเลื่อน 3 ไบต์

รูปที่ 4.3 แสดงการแปลงระหว่างสเตทโดยการเลื่อนไบต์ในแต่ละแถว จากสเตท A ไปยัง สเตท B จะเป็นการเข้ารหัส (เลื่อนไปทางซ้าย) ในขณะที่สเตท B กลับไปยัง สเตท A จะเป็นการถอดรหัส (เลื่อนไปทางขวา)

ตารางที่ 4.2: กล่องเอสเพื่อใช้ในการแทนที่ไบต์ในการถอดรหัส

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

$$State_A = \begin{bmatrix} 57 & 76 & 72 & 72 \\ 65 & 65 & 61 & 65 \\ 6C & 53 & 6E & 65 \\ 6F & 75 & 61 & 2E \end{bmatrix} State_B = \begin{bmatrix} 5B & 38 & 40 & 40 \\ 4D & 4D & EF & 4D \\ 50 & ED & 9F & 4D \\ A8 & 9D & EF & 31 \end{bmatrix}$$

รูปที่ 4.2: ตัวอย่างการแทนที่ไบต์ระหว่างสเตทด้วยกล่องเอส

$$State_A = \begin{bmatrix} 57 & 76 & 72 & 72 \\ 65 & 65 & 61 & 65 \\ 6C & 53 & 6E & 65 \\ 6F & 75 & 61 & 2E \end{bmatrix} State_B = \begin{bmatrix} 57 & 76 & 72 & 72 \\ 65 & 61 & 65 & 65 \\ 6E & 65 & 6C & 53 \\ 2E & 6F & 75 & 61 \end{bmatrix}$$

รูปที่ 4.3: ตัวอย่างการสลับที่ไบต์ระหว่างสเตทด้วยการเลื่อนไบต์ในแต่ละแถว

การผสมสดมภ์

ขั้นตอนการแทนที่ไบต์และการเลื่อนไบต์ในแต่ละแถวที่กล่าวมานั้นเป็นการเปลี่ยนข้อมูลทั้งไบต์ แต่ข้อมูลแต่ละบิตในไบต์ยังคงเหมือนเดิม ดังนั้นจึงจำเป็นต้องคละข้อมูลในแต่ละบิตใหม่ ด้วยวิธีการที่เรียกว่า การผสมสดมภ์ ด้วยการคูณแต่ละสดมภ์ด้วยเมทริกซ์ค่าคงที่ซึ่งจะได้สดมภ์ใหม่ โดยเมทริกซ์ค่าคงที่ดังกล่าวแสดงดังรูปที่ 4.4 โดยที่ $M_{Encoding}$ คือ เมทริกซ์ค่าคงที่สำหรับการเข้ารหัส และ $M_{Decoding}$ คือ เมทริกซ์ค่าคงที่สำหรับการถอดรหัส หากค่าเดิมในแต่ละสดมภ์เป็น $Old_0, Old_1, Old_2, Old_3$ เมื่อคูณด้วยเมทริกซ์ค่าคงที่จะได้ผลลัพธ์เป็น $New_0, New_1, New_2, New_3$ ซึ่งวิธีการคูณเมทริกซ์สามารถแสดงได้ดังสมการที่ 4.1, 4.2, 4.3 และ 4.4 ตามลำดับ

$$New_0 = (2 \cdot Old_0) \oplus (3 \cdot Old_1) \oplus Old_2 \oplus Old_3 \tag{4.1}$$

$$New_1 = Old_0 \oplus (2 \cdot Old_1) \oplus (3 \cdot Old_2) \oplus Old_3 \tag{4.2}$$

$$New_2 = Old_0 \oplus Old_1 \oplus (2 \cdot Old_2) \oplus (3 \cdot Old_3) \tag{4.3}$$

$$New_3 = (3 \cdot Old_0) \oplus Old_1 \oplus Old_2 \oplus (2 \cdot Old_3) \tag{4.4}$$

การคูณเมทริกซ์ดังกล่าวคล้ายกับการคูณเมทริกซ์ปกติแต่หากเป็นการคูณเมทริกซ์ซึ่งผลลัพธ์อยู่ใน จีเอฟ(2^8) ซึ่งสามารถคำนวณได้ดังนี้

- **การบวกใน จีเอฟ(2^8)** จะได้ผลลัพธ์เหมือนกับการเอ็กซ์ออร์ ($\oplus$) ทีละบิต กล่าวคือ $0 \oplus 0 = 0, 0 \oplus 1 = 1, 1 \oplus 0 = 1, 1 \oplus 1 = 1$ ยกตัวอย่างเช่น $AB_{16}(10101011_2) \oplus CD_{16}(11001101_2) = 66_{16}(01100110_2)$ เป็นต้น

$$M_{Encoding} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \quad M_{Decoding} = \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix}$$

รูปที่ 4.4: เมตริกซ์ค่าคงที่สำหรับการเข้ารหัสและถอดรหัสในเออีเอส

- **การคูณใน จีเอฟ**(2^8) จะเป็นการคูณของพหุนาม ซึ่งการแปลงจากเลขฐานสอง n บิตเป็นพหุนามสามารถกระทำโดย บิตซึ่งมีนัยสำคัญต่ำสุด (บิตขวาสุด) จะเป็นสัมประสิทธิ์ของ x^0 ในขณะที่บิตซึ่งมีนัยสำคัญสูงสุด (บิตซ้ายสุด) จะเป็นสัมประสิทธิ์ของ x^{n-1} ตัวอย่าง เช่น 10011110 $= 1x^7 + 0x^6 + 0x^5 + 1x^4 + 1x^3 + 1x^2 + 1x^1 + 0x^0 = x^7 + x^4 + x^3 + x^2 + x$ การคูณจะเป็นการลดรูปพหุนามให้อยู่ในรูป x เช่น $x^2 \cdot P_2 = (x \cdot (x \cdot P_2))$ การคูณกับ x จะอยู่ในรูปของสมการที่ 4.5 ซึ่งสามารถกระทำโดยการเลื่อนบิตไปทางซ้าย 1 บิต และหากบิตที่ 7 ของข้อมูลเดิมเป็นบิต 1 จะต้องนำค่าที่เลื่อนไปทางซ้ายแล้วมาเอ็กซ์ออร์กับค่ามอดุลาร์ซึ่งตัดบิตที่มีนัยสำคัญสูงสุด สำหรับค่ามอดุลาร์ของเออีเอส คือ 100011011 (เออีเอสจะใช้ 00011011 ในการเอ็กซ์ออร์)

$$x \cdot B = \begin{cases} (b_6 b_5 b_4 b_3 b_2 b_1 b_0 0), \text{ กรณีที่ } b_7 = 0 \\ (b_6 b_5 b_4 b_3 b_2 b_1 b_0 0) \oplus (\text{มอดุลาร์ตัดบิตแรก}), \text{ กรณีที่ } b_7 = 1 \end{cases} \tag{4.5}$$

ตัวอย่างเช่น หากต้องการคูณ $P_1 = 26_{16}(00100110_2)$ ด้วย $P_2 = 9E_{16}(10011110_2)$ โดยมี 100011011 เป็นค่ามอดุลาร์จะได้ผลลัพธ์เป็น $P_1 \cdot P_2 = 2F_{16}(00101111_2)$ ดังแสดงในตารางที่ 4.3

ตารางที่ 4.3: ตัวอย่างการคูณในจีเอฟ(2^8)

การคูณ	ผลลัพธ์
$x^0 \cdot P_2$	10011110
$x^1 \cdot P_2$	(00111100) $\oplus$ (00011011) = *00100111*
$x^2 \cdot P_2$	*01001110*
$x^3 \cdot P_2$	10011100
$x^4 \cdot P_2$	(00111000) $\oplus$ (00011011) = 00100011
$x^5 \cdot P_2$	*01000110*
$P_1 \cdot P_2 = (x^5 + x^2 + x^1) \cdot P_2$	(*00100111*) $\oplus$ (*01001110*) $\oplus$ (*01000110*) = **00101111**

รูปที่ 4.5 แสดงตัวอย่างการผสมสดมภ์จากเมทริกซ์ต้นฉบับ $M_{Original}$ ผ่านการผสมสดมภ์จะได้ผลลัพธ์เป็นเมทริกซ์ $M_{MixColumns}$

$$M_{Original} = \begin{bmatrix} 87 & C9 & FE & 30 \\ 6E & 63 & 26 & F2 \\ 46 & D4 & C9 & C9 \\ A6 & FA & 63 & 82 \end{bmatrix} M_{MixColumns} = \begin{bmatrix} 47 & 02 & 27 & 26 \\ 37 & 92 & 91 & 0D \\ 94 & 0C & F4 & D6 \\ ED & 18 & 30 & 74 \end{bmatrix}$$

รูปที่ 4.5: ตัวอย่างการผสมสดมภ์ในเออีเอส

จากตัวอย่างการผสมสดมภ์ดังกล่าว ค่าในสดมภ์แรกสามารถคำนวณได้จาก

$47 = (02 \cdot 87) \oplus (03 \cdot 6E) \oplus 46 \oplus A6$

$37 = 87 \oplus (02 \cdot 6E) \oplus (03 \cdot 46) \oplus A6$

$94 = 87 \oplus 6E \oplus (02 \cdot 46) \oplus (03 \cdot A6)$

$ED = (03 \cdot 87) \oplus 6E \oplus 46 \oplus (02 \cdot A6)$

หากพิจารณาสมการแรก จะพบว่า $(02 \cdot 87) = 00010101$, $(03 \cdot 6E) = 10110010$, 46 = 01000110 และ A6 = 10100110 ซึ่งหากเอ็กซ์ออร์ค่าทั้งหมด (00010101⊕10110010⊕01000110⊕10100110) จะได้ผลลัพธ์เป็น 01000111 = 47

สังเกตได้ว่าข้อมูลไบต์เดียวกัน เมื่อผ่านการผสมสดมภ์แล้วจะให้ผลลัพธ์ที่แตกต่างกัน เช่น ไบต์ C9 ในแถวแรกจะได้ผลลัพธ์เป็น 02 ในขณะที่แถวที่สามในสองสดมภ์สุดท้ายจะได้ผลลัพธ์ เป็น F4 และ D6 ตามลำดับ

การผสมกุญแจ

กุญแจในแต่ละรอบของเออีเอสมีความยาว 128 บิตเสมอซึ่งสามารถมองเป็น 4 เวิร์ด โดยที่การผสมกุญแจ คือ การเอ็กซ์ออร์ค่ากุญแจแต่ละเวิร์ดเข้ากับค่าแต่ละสดมภ์ของสเตท

4.1.3 การสร้างกุญแจประจำรอบ

จำนวนกุญแจในแต่ละรอบที่ต้องสร้าง คือ จำนวนรอบ + 1 โดยกุญแจในแต่ละรอบต้องใช้ 4 เวิร์ด ดังนั้น เออีเอส-128 ต้องการกุญแจทั้งหมด 44 เวิร์ด ((10 รอบ + 1) × 4) เออีเอส-192 ต้องการกุญแจทั้งหมด 52 เวิร์ด ((12 รอบ + 1) × 4) และ เออีเอส-256 ต้องการกุญแจทั้งหมด 60 เวิร์ด ((14 รอบ + 1) × 4) นั่นคือ กุญแจก่อนรอบแรก คือ เวิร์ด w_0, w_1, w_2, w_3, กุญแจรอบแรก คือ เวิร์ด w_4, w_5, w_6, w_7 กุญแจรอบสุดท้าย (รอบที่ N) คือ เวิร์ด $w_{4N}, w_{4N+1}, w_{4N+2}, w_{4N+3}$

ขั้นตอนการสร้างกุญแจประกอบไปด้วยการสร้างเวิร์ด 3 ขั้นตอน

1. สร้างเวิร์ดชุดแรกจากกุญแจที่ใส่เข้ามา

   (a) เออีเอส-128: สร้างกุญแจ 4 เวิร์ดแรก $(w_0, w_1, ..., w_3)$

(b) เออีเอส-192: สร้างกุญแจ 6 เวิร์ดแรก $(w_0, w_1, ..., w_5)$

(c) เออีเอส-256: สร้างกุญแจ 8 เวิร์ดแรก $(w_0, w_1, ..., w_7)$

2. สร้างเวิร์ดจากเวิร์ดก่อนหน้าเอ็กซ์ออร์เวิร์ดชุดด้านบน

(a) เออีเอส-128: กรณีตำแหน่งของเวิร์ด (i) mod $4 \neq 0, w_i = w_{i-1} \oplus w_{i-4}$

(b) เออีเอส-192: กรณีตำแหน่งของเวิร์ด (i) mod $6 \neq 0, w_i = w_{i-1} \oplus w_{i-6}$

(c) เออีเอส-256: กรณีตำแหน่งของเวิร์ด (i) mod $8 \neq 0, w_i = w_{i-1} \oplus w_{i-8}$ ยกเว้นกรณีที่ตำแหน่งของเวิร์ด (i) mod 4 = 0, $w_i = SWord(w_{i-1}) + w_{i-8}$

3. สร้างเวิร์ดจากเวิร์ดพิเศษเอ็กซ์ออร์เวิร์ดชุดด้านบน

(a) เออีเอส-128: กรณีตำแหน่งของเวิร์ด (i) mod $4 = 0, w_i = t \oplus w_{i-4}$

(b) เออีเอส-192: กรณีตำแหน่งของเวิร์ด (i) mod $6 = 0, w_i = t \oplus w_{i-6}$

(c) เออีเอส-256: กรณีตำแหน่งของเวิร์ด (i) mod $8 = 0, w_i = t \oplus w_{i-8}$

โดยที่มีเงื่อนไขดังนี้

- ค่า t คือ $SWord(RWord(w_{i-1})) \oplus RC$
- SWord คือ การแทนที่ 4 ไบต์ในเวิร์ดด้วย 4 ไบต์ใหม่โดยใช้ตารางที่ 4.1
- RWord คือ การเลื่อนวนไบต์ไปทางซ้ายหนึ่งไบต์ โดยที่ไบต์ซ้ายสุดจะวนมาไบต์ขวาสุด
- RC คือ ค่าคงที่ประจำรอบซึ่งมีขนาด 4 ไบต์โดย 3 ไบต์ขวาสุดมีค่าเป็น 0 เสมอและไบต์ซ้ายสุด (RC_j) มีค่าเท่ากับ $2 \cdot RC_{j-1}$ และ $RC_1 = 1$ ซึ่งผลลัพธ์อยู่ใน จีเอฟ(2^8) ซึ่งค่าคงที่ประจำรอบทั้งหมดสามารถแสดงได้ดังตารางที่ 4.4

ตารางที่ 4.4: ค่าคงที่ประจำรอบ

รอบที่	ค่าคงที่	รอบที่	ค่าคงที่	รอบที่	ค่าคงที่
1	0x01000000	6	0x20000000	11	0x6C000000
2	0x02000000	7	0x40000000	12	0xD8000000
3	0x04000000	8	0x80000000	13	0xAB000000
4	0x08000000	9	0x1B000000	14	0x4D000000
5	0x10000000	10	0x36000000		

ตัวอย่างเช่น หากมีกุญแจ ''We love Suranaree.'' กุญแจดังกล่าวสามารถแปลงเป็นรหัสแอสกี (โดยไม่สนใจเว้นวรรค) ได้เป็น 57 65 6C 6F 76 65 53 75 72 61 6E 61 72 65 65 2E กุญแจ

นำเข้า 128 บิตดังกล่าวสามารถสร้างกุญแจประจำรอบได้ดังขั้นตอนในตารางที่ 4.5 หากพิจารณาการหาค่า t ค่าแรก จะเริ่มจาก RWord(7265652E) = 65652E72 หลังจากนั้นหาค่า SWord(65652E72) = 4D4D3140 เมื่อนำค่าดังกล่าวไปเอ็กซ์ออร์กับค่าคงที่ประจำรอบ (01000000) จะได้ 4C4D3140

ตารางที่ 4.5: การสร้างกุญแจประจำรอบ

รอบ	ค่า t	เวิร์ดที่ 1	เวิร์ดที่ 2	เวิร์ดที่ 3	เวิร์ดที่ 4
-	-	w_{00}=57656C6F	w_{01}=76655375	w_{02}=72616E61	w_{03}=7265652E
1	4C4D3140	w_{04}=1B285D2F	w_{05}=6D4D0E5A	w_{06}=1F2C603B	w_{07}=6D490515
2	396B593C	w_{08}=22430413	w_{09}=4F0E0A49	w_{10}=50226A72	w_{11}=3D6B6F67
3	7BA88527	w_{12}=59EB8134	w_{13}=16E58B7D	w_{14}=46C7E10F	w_{15}=7BAC8E68
4	99194521	w_{16}=C0F2C415	w_{17}=D6174F68	w_{18}=90D0AE67	w_{19}=EB7C200F
5	00B776E9	w_{20}=C045B2FC	w_{21}=1652FD94	w_{22}=868253F3	w_{23}=6DFE73FC
6	9B8FB03C	w_{24}=5BCA02C0	w_{25}=4D98FF54	w_{26}=CB1AACA7	w_{27}=A6E4DF5B
7	299E3924	w_{28}=72543BE4	w_{29}=3FCCC4B0	w_{30}=F4D66817	w_{31}=5232B74C
8	A3A92900	w_{32}=D1FD12E4	w_{33}=EE31D654	w_{34}=1AE7BE43	w_{35}=48D5090F
9	18017652	w_{36}=C9FC64B6	w_{37}=27CDB2E2	w_{38}=3D2A0CA1	w_{39}=75FF05AE
10	206BE49D	w_{40}=E997802B	w_{41}=CE5A32C9	w_{42}=F3703E68	w_{43}=868F3BC6

4.1.4 ตัวอย่างการทำงานของเออีเอส

หากเราต้องการเข้ารหัสข้อมูลคำว่า ''long live the king.'' ซึ่งสามารถแปลงเป็นรหัสแอสกี (โดยไม่สนใจเว้นวรรค) ได้เป็น 6C 6F 6E 67 6C 69 76 65 74 68 65 6B 69 6E 67 2E โดยใช้กุญแจ ''We love Suranaree.'' กุญแจดังกล่าวสามารถแปลงเป็นรหัสแอสกี (โดยไม่สนใจเว้นวรรค) ได้เป็น 57 65 6C 6F 76 65 53 75 72 61 6E 61 72 65 65 2E ด้วยเออีเอส-128 ซึ่งเป็นการเข้ารหัสด้วยกุญแจขนาด 128 บิตจำนวน 10 รอบ ผลลัพธ์ที่ได้ คือ 39 4A 85 26 5E 57 23 48 3A 08 E3 39 6D 02 4C 27

ตารางที่ 4.6 แสดงการเข้ารหัสก่อนรอบแรก ซึ่งมีเพียงขั้นตอนในการผสมกุญแจ ในขณะที่ตาราง 4.7 แสดงการเข้ารหัสในรอบแรกถึงรอบที่สิบ ซึ่งมีครบทั้ง 4 ขั้นตอนในแต่ละรอบ คือ การแทนที่ไบต์ การเลื่อนแถว การผสมสดมภ์ และ การผสมกุญแจ ยกเว้นในรอบที่สิบซึ่งขาดขั้นตอนการผสมสดมภ์

4.2 การใช้งานการเข้ารหัสด้วยกุญแจแบบสมมาตรสมัยใหม่

4.2.1 การใช้งานแบบบล็อก

การใช้งานวิธีการเข้ารหัสแบบสมมาตรสมัยใหม่ เช่น ดีอีเอส และ เออีเอส ถูกออกแบบสำหรับ การเข้ารหัสเป็นบล็อกโดยที่ดีอีเอสทำงานด้วยการเข้ารหัสข้อมูลครั้งละ 64 บิต และ เออีเอส เป็นการเข้ารหัสข้อมูลครั้งละ 128 บิต แต่ในทางปฏิบัติแล้วข้อมูลที่ต้องการเข้ารหัสนั้น มีความยาวมากกว่าบล็อก

ตารางที่ 4.6: ตัวอย่างการเข้ารหัสเออีเอสก่อนรอบแรก

รอบ	สเตทนำเข้า	แทนที่ไบต์	เลื่อนแถว	ผสมสดมภ์	ผสมกุญแจ	กุญแจรอบ
0	6C6C7469				3B1A061B	57767272
	6F69686E				0A0C090B	65656165
	6E766567				02250B02	6C536E65
	67656B2E				08100A00	6F75612E

ดังกล่าวมาก ซึ่งการเข้ารหัสข้อความยาวๆ ดังกล่าวสามารถ ใช้วิธีการเข้ารหัสแบบบล็อกทั้งดีอีเอส และเออีเอส จำนวน 5 แบบ ได้แก่ อีซีบี ซีบีซี ซีเอฟบี โอเอฟบี และ ซีทีอาร์

การใช้งานแบบอีซีบี

อีซีบีเป็นวิธีการเข้ารหัสที่ง่ายที่สุด โดยการแบ่งข้อมูลเป็นบล็อกขนาดเท่ากับข้อมูลนำเข้าของวิธีการเข้ารหัสนั้น โดยบล็อกสุดท้ายอาจจะมีการเติมเต็มข้อมูล (แพดดิ้ง) เพื่อทำให้ข้อมูลเต็มบล็อก โดยใช้กุญแจดอกเดียวกันในการเข้ารหัสและถอดรหัสข้อมูลในแต่ละบล็อก การใช้งานแบบอีซีบีถือว่ามีจุดอ่อนด้านความปลอดภัย เนื่องจากแต่ละบล็อกอิสระจากกัน และด้วยเหตุผลที่การทำงานของแต่ละบล็อกอิสระจากกันนี้ทำให้การใช้งานแบบอีซีบีสามารถ เข้ารหัสแบบขนานได้ เช่น การเข้ารหัสในฐานข้อมูลขนาดใหญ่ และหากมีข้อผิดพลาดภายในบล็อก การผิดพลาดดังกล่าวจะไม่กระทบกับบล็อกอื่นๆ

การใช้งานแบบซีบีซี

ซีบีซี คือ การที่นำข้อความที่เข้ารหัสแล้วของบล็อกก่อนหน้ามาเอ็กซ์ออร์กับข้อความที่ยังไม่ได้เข้ารหัสก่อนที่จะถูกนำไปเข้ารหัส ยกเว้นบล็อกแรกสุด (ไม่มีบล็อกก่อนหน้า) จะนำไปเอ็กซ์ออร์กับไอวี ซึ่งไอวีคือค่าที่ตกลงกันระหว่างผู้ส่งและผู้รับ เนื่องจากการเข้ารหัสในแต่ละบล็อกนั้นขึ้นกับบล็อกก่อนหน้า ดังนั้นจะไม่สามารถเข้ารหัสแบบขนานกันได้ และเมื่อเกิดข้อผิดพลาดขึ้นข้อผิดพลาดดังกล่าวจะถูกส่งต่อไปยัง บล็อกถัดไปที่ติดกัน

การใช้งานแบบซีเอฟบี

การเข้ารหัสด้วยวิธีการแบบ อีซีบี และ ซีบีซี ถูกออกแบบให้กับการเข้ารหัสที่มีความยาวมากกว่าหรือเท่ากับ ขนาดของบล็อก (เช่น ดีอีเอสมีขนาด 64 บิต เออีเอสขนาด 128 บิต) แต่อย่างไรก็ตาม บางครั้งจำเป็นต้องมีการเข้ารหัสข้อมูลที่สั้นกว่าขนาดของบล็อก ซึ่งกรณีดังกล่าวควรจะใช้วิธีการที่เรียกว่าซีเอฟบี วิธีการเข้ารหัสแบบนี้จะมิได้เข้ารหัสข้อความโดยตรงแต่หากเป็นการเข้ารหัสข้อความเทียม ซึ่งมีความยาวเท่ากับบล็อก ตัวอย่างเช่น ข้อความที่ต้องการเข้ารหัส มีความยาว r บิต โดยที่ขนาดของบล็อกของการเข้ารหัสมีขนาด n บิต ซึ่ง $r \leq n$ ข้อความเทียมความยาว n บิตจะถูกเข้ารหัสด้วยวิธีการเข้ารหัสซึ่งจะได้ผลลัพธ์ n บิต จากนั้นจะเลือก r บิตซ้ายสุดจากผลลัพธ์ n บิตเพื่อมาเอ็กซ์ออร์กับข้อความซึ่งมี

ตารางที่ 4.7: ตัวอย่างการเข้ารหัสเออีเอสรอบแรกถึงรอบที่สิบ

รอบ	สเตทนำเข้า	แทนที่ไบต์	เลื่อนแถว	ผสมสดมภ์	ผสมกุญแจ	กุญแจรอบ
1	3B1A061B	E2A26FAF	E2A26FAF	8E1B1EB4	957601D9	1B6D1F6D
	0A0C090B	67FE012B	FE012B67	1B096A47	3344460E	284D2C49
	02250B02	773F2B77	2B77773F	EF1DEF1F	B2138F1A	5D0E6005
	08100A00	30CA6763	6330CA67	2EEB627C	01B15969	2F5A3B15
2	957601D9	2A387C35	2A387C35	F340E182	D10FB1BF	224F503D
	3344460E	C31B5AAB	1B5AABC3	700DA0E4	3303828F	430E226B
	B2138F1A	377D73A2	73A2377D	C7B9FA4A	C3B39025	040A6A6F
	01B15969	7CC8CBF9	F97CC8CB	FF48936C	EC01E10B	13497267
3	D10FB1BF	3E76C808	3E76C808	BA284CDB	E33E0AA0	5916467B
	3303828F	C37B1373	7B1373C3	43DF20DA	A83AE776	EBE5C7AC
	C3B39025	2E6D603F	603F2E6D	F8526302	79D9828C	818BE18E
	EC01E10B	CE7CF82B	2BCE7CF8	0F31E65D	3B4CE935	347D0F68
4	E33E0AA0	11B267E0	11B267E0	3C5E19AD	FC888946	C0D690EB
	A83AE776	C2809438	809438C2	A9CFFF3E	5BD82F42	F217D07C
	79D9828C	B6351364	1364B635	16D3536A	D29CFD4A	C44FAE20
	3B4CE935	E2291E96	96E2291E	97E275F0	828A12FF	1568670F
5	FC888946	B0C4A75A	B0C4A75A	9A69EAE8	5A7F6C85	C016866D
	5BD82F42	3961152C	61152C39	989C4598	DDCEC766	455282FE
	D29CFD4A	B5DE54D6	54D6B5DE	43537884	F1AE2BF7	B2FD5373
	828A12FF	137EC916	16137EC9	D2B29780	2E26647C	FC94F3FC
6	5A7F6C85	BED25097	BED25097	00B7A3CA	5BFA686C	5B4DCBA6
	DDCEC766	C18BC633	8BC633C1	ABCC397A	6154239E	CA981AE4
	F1AE2BF7	A1E4F168	F168A1E4	FC973840	FE68949F	02FFACDF
	2E26647C	31F74310	1031F743	83A19701	43F5305A	C054A75B
7	5BFA686C	392D4550	392D4550	8EF1CACB	FCCE3E99	723FF452
	6154239E	EF20260B	20260BEF	A10D635E	F5C1B56C	54CCD632
	FE68949F	BB4522DB	22DBBB45	84881239	BF4C7A8E	3BC468B7
	43F5305A	1AE604BE	BE1AE604	2EBEA852	CA0EBF1E	E4B0174C
8	FCCE3E99	B08BB2EE	B08BB2EE	5B042CD7	8AEA369F	D1EE1A48
	F5C1B56C	E678D550	78D550E6	4765A14A	BA54469F	FD31E7D5
	BF4C7A8E	0829DA19	DA190829	F1F01442	E326AA4B	12D6BE09
	CA0EBF1E	74AB0872	7274AB08	8DA2D8F6	69F69BF9	E454430F
9	8AEA369F	7E8705DB	7E8705DB	A9B12F49	6096123C	C9273D75
	BA54469F	F4205ADB	205ADBF4	4804D93E	B4C9F3C1	FCCD2AFF
	E326AA4B	11F7ACB3	ACB311F7	ADB03AE6	C90236E3	64B20C05
	69F69BF9	F9421499	99F94214	2792415D	9170E0F3	B6E2A1AE
10	6096123C	D090C9EB	D090C9EB		395E3A6D	E9CEF386
	B4C9F3C1	8DDD0D78	DD0D788D		4A570802	975A708F
	C90236E3	DD770511	0511DD77		8523E34C	80323E3B
	9170E0F3	8151E10D	0D8151E1		26483927	2BC968C6

ความยาว r บิต ผลลัพธ์ที่ได้จากการเอ็กซ์ออร์ คือ ผลลัพธ์ของซีเอฟบี ข้อความเทียมดังกล่าว ถูกสร้างโดยการเลื่อนข้อความเทียมเดิมไปทางซ้ายเท่ากับความยาวของข้อความที่ต้องการเข้ารหัส (r บิต) แล้วต่อท้ายทางขวาด้วยผลลัพธ์ของซีเอฟบีของรอบก่อนหน้า ยกเว้นรอบแรกซึ่งไม่มีการเลื่อนเนื่องจากไม่มีรอบก่อนหน้า

การเข้ารหัสด้วยวิธีนี้ส่วนใหญ่ใช้กับการเข้ารหัสขนาดคงที่สั้นๆ เช่น การเข้ารหัสครั้งละหนึ่งไบต์ ซึ่งไม่ต้องการแพดดิ้ง แต่การเข้ารหัสแบบนี้มีข้อเสียคือความเร็วในการเข้ารหัสค่อนข้างช้า เมื่อเทียบกับอีซีบีและซีบีซี เนื่องจากการเข้ารหัสในแต่ละบล็อกนั้นขึ้นกับบล็อกก่อนหน้า ดังนั้นจะไม่สามารถเข้ารหัสแบบขนานกันได้ และเมื่อเกิดข้อผิดพลาดขึ้นข้อผิดพลาดดังกล่าวจะถูกส่งต่อไปยัง บล็อกถัดไปที่ติดกัน

การใช้งานแบบโอเอฟบี

โอเอฟบีมีการทำงานคล้ายกับซีเอฟบีมาก แต่แตกต่างกันตรงที่ข้อความเทียม ถูกสร้างโดยการเลื่อนข้อความเทียมเดิมไปทางซ้ายเท่ากับความยาวของข้อความที่ต้องการเข้ารหัส (r บิต) แล้วต่อท้ายทางขวาด้วย r บิตซ้ายสุดของผลลัพธ์ n บิตที่เกิดจากการเข้ารหัส (ในขณะที่ซีเอฟบีจะต้อท้ายด้วยผลลัพธ์หลังจากการเอ็กซ์ออร์ข้อความแล้ว) ทำให้ข้อผิดพลาดไม่ถูกส่งไปยัง บล็อกถัดไป

การใช้งานแบบซีทีอาร์

การทำงานของซีทีอาร์เป็นการทำงานโดยไม่มีการส่งข้อความย้อนกลับ กล่าวคือ การเข้ารหัสข้อมูล ด้วยการเอ็กซ์ออร์ข้อความกับผลลัพธ์ของการเข้ารหัสตัวนับด้วยกุญแจ ตัวนับดังกล่าวเปรียบเสมือนค่าสุ่มซึ่งเปลี่ยนทุกครั้งในแต่ละบล็อก การทำงานของซีทีอาร์สามารถเปรียบเทียบได้กับโอเอฟบีและอีซีบี โดยที่ซีทีอาร์คล้ายกับโอเอฟบี ในแง่ที่การสร้างกุญแจซึ่งอิสระจากข้อความที่เข้ารหัสแล้วบล็อกก่อนหน้า แต่ซีทีอาร์ไม่มีการส่งข้อความย้อนกลับ ซีทีอาร์นั้นคล้ายกับอีซีบีในแง่ของการสร้างข้อความเข้ารหัสที่อิสระจะบล็อกก่อนหน้าซึ่งการเข้ารหัสดังกล่าว จะขึ้นอยู่ค่าของตัวนับ ซึ่งไม่เหมาะกับการเข้ารหัสแบบเรียลไทม์เหมือนกับอีซีบี เนื่องจากต้องรอการเข้ารหัสให้ครบทั้งบล็อก

4.2.2 การใช้งานแบบกระแส

การใช้งานแบบบล็อกชนิด อีซีบี ซีบีซี ซีทีอาร์ เหมาะสำหรับการเข้ารหัสข้อมูลขนาดใหญ่ ในขณะที่ ซีเอฟบีและโอเอฟบี เหมาะสำหรับการเข้ารหัสข้อมูลขนาดเล็ก แต่อย่างไรก็ตามการใช้งาน เหล่านี้ได้ถูกออกแบบสำหรับการเข้ารหัสทีละบล็อก ไม่เหมาะกับการเข้ารหัสแบบเรียลไทม์ ซึ่งควรจะใช้การเข้ารหัสแบบกระแส การใช้งานแบบกระแสที่จะกล่าวในบทนี้ คือ อาร์ซี4 และ เอ5/1

อาร์ซี 4

การเข้ารหัสแบบอาร์ซี 4 ถูกคิดค้นในปี พ.ศ. 2527 ซึ่งปัจจุบันนิยมใช้ในการสื่อสารข้อมูลด้วยคอมพิวเตอร์ เช่น ใช้ในการเข้ารหัส เอสเอสแอล/ทีแอลเอส (ดังจะกล่าวรายละเอียดในหัวข้อที่ 8.2) การเข้ารหัสในเครือข่ายแลนแบบไร้สาย การเข้ารหัสแบบอาร์ซี 4 จะเข้ารหัสข้อมูลครั้งละ 1 ไบต์ด้วยการเอกซ์ออร์กับกุญแจ 1 ไบต์ ซึ่งจะได้ผลลัพธ์ความยาว 1 ไบต์เช่นเดียวกัน โดยที่กุญแจ 1 ไบต์จะเป็นการเลือกสุ่ม ในทุกไบต์ของการเข้ารหัส

เอ 5/1

การเข้ารหัสแบบเอ 5/1 เป็นการเข้ารหัสที่ใช้ในการสื่อสารของโทรศัพท์เคลื่อนที่จีเอสเอ็ม ซึ่งเป็นการเข้ารหัสเฟรมข้อมูล ครั้งละ 228 บิต โดยอาศัยกุญแจ 64 บิต ซึ่งกุญแจดังกล่าว จะถูกสร้างเป็นกุญแจชั่วคราวความยาว 228 บิตเพื่อนำมาเอ็กซ์ออร์กับข้อมูลขนาดเดียวกัน

4.3 สรุป

บทนี้ได้กล่าวถึง มาตรฐานการเข้ารหัสขั้นสูง (เออีเอส) วิธีการใช้งานการเข้ารหัสด้วยกุญแจแบบสมมาตรสมัยใหม่แบบบล็อก เพื่อเข้ารหัสข้อความที่มีความยาวมากกว่าหรือน้อยกว่าบล็อกของการเข้ารหัส 5 รูปแบบ ได้แก่ อีซีบี ซีบีซี ซีเอฟบี โอเอฟบี และ ซีทีอาร์ วิธีการใช้งานการเข้ารหัสด้วยกุญแจแบบสมมาตรสมัยใหม่แบบกระแส 2 รูปแบบ คือ อาร์ซี 4 และ เอ 5/1

4.4 แบบฝึกหัด

1. หากข้อมูลก่อนเข้ารหัสเปลี่ยน 1 บิตจงหาว่าหลังจากผ่านขั้นตอนต่อไปนี้ของเออีเอส จะมีผลลัพธ์เปลี่ยนกี่บิต

   (a) การแทนที่ไบต์

   (b) การเลื่อนแถว

   (c) การผสมสดมภ์

   (d) การผสมกุญแจ

2. จงระบุว่าขั้นตอนใดของเออีเอสที่ทำให้ข้อมูลในแต่ละไบต์เกิดการเปลี่ยนแปลง

3. หากการเข้ารหัสแบบเออีเอส n รอบจะมีการแทนที่ การเลื่อนแถว การผสมสดมภ์ และ การผสมกุญแจ อย่างละกี่ครั้ง และต้องใช้กุญแจทั้งหมดกี่ดอก

4. จงแบ่งกลุ่มการใช้งานแบบบล็อกทั้ง 5 แบบเป็น 2 กลุ่ม คือ กลุ่มที่ต้องการแพดดิ้ง และ กลุ่มที่ไม่ต้องการ

5. จงแบ่งกลุ่มการใช้งานแบบบล็อกทั้ง 5 แบบเป็น 2 กลุ่ม คือ กลุ่มที่ใช้กุญแจดอกเดียวกันทุกบล็อก และ กลุ่มที่ใช้กุญแจแบบกระแส

6. การใช้งานแบบบล็อกแบบใดบ้างที่สามารถคำนวณแต่ละบล็อกแบบขนานได้

บทที่ 5

การเข้ารหัสด้วยกุญแจแบบอสมมาตร

- คณิตศาสตร์ที่เกี่ยวข้อง
- การเข้ารหัสด้วยกุญแจแบบอสมมาตร

บทที่ 5

การเข้ารหัสด้วยกุญแจแบบอสมมาตร

ในบทนี้จะกล่าวถึง คณิตศาสตร์พื้นฐานที่จำเป็นในการเรียนรู้เรื่องการเข้ารหัสด้วยกุญแจแบบอสมมาตร อาทิเช่น จำนวนเฉพาะ การแยกตัวประกอบเฉพาะ เป็นต้น การเข้ารหัสแบบสมมาตรด้วยวิธีต่างๆ ได้แก่ การเข้ารหัสแบบถุงเป้ การเข้ารหัสแบบอาร์เอสเอ และการเข้ารหัสแบบราบิน

5.1 คณิตศาสตร์ที่เกี่ยวข้อง

การเข้ารหัสด้วยกุญแจแบบอสมมาตรนั้นอยู่บนพื้นฐานการทำงานของเลขจำนวนเฉพาะ รวมถึงทฤษฎีต่างๆ ที่เกี่ยวข้อง เช่น ออยเลอร์ฟีฟังก์ชัน ทฤษฎีของเฟอร์แมทและออยเลอร์ การแยกตัวประกอบเฉพาะ เอ็กซ์โปเนนเชียล และลอการิทึม

5.1.1 เลขจำนวนเฉพาะ

เลขจำนวนเต็มบวก (จำนวนเต็มที่มากกว่า 0) สามารถแบ่งออกเป็น 3 ชนิด ได้แก่ *เลข 1 เลขจำนวนเฉพาะ* และ*เลขจำนวนประกอบ* โดยที่นิยามของจำนวนเฉพาะ คือ เลขที่หารด้วยจำนวนเต็ม สองจำนวนลงตัวเท่านั้น คือ เลข 1 และเลขตัวเอง เลขจำนวนเฉพาะดังกล่าวจะอยู่ในรูปของ $4k+1$ หรือ $4k+3$ โดยที่ k คือจำนวนเต็มบวก หากมีเลขจำนวนเต็มที่หารลงตัวมากกว่าสองจำนวน จะเรียกเลขดังกล่าวว่า เลขจำนวนประกอบ ตัวอย่างเช่น จำนวนเฉพาะที่น้อยที่สุด คือ เลข 2 (เลข 1 มิใช่จำนวนเฉพาะ เนื่องจากต้องมีจำนวนเต็มที่หารลงตัวสองจำนวน ในขณะที่เลข 1 มีเพียงจำนวนเดียว คือ เลข 1) จำนวนเฉพาะที่มีค่าน้อยกว่า 10 คือ 2,3,5,7 เป็นต้น ซึ่งจำนวนของเลขจำนวนเฉพาะทั้งหมดนั้นมีค่าเป็นอนันต์ (มหาศาลไม่สิ้นสุด) หากเลขจำนวนเต็ม 2 จำนวน มี หรม. มีค่าเป็น 1 จะเรียกเลข 2 จำนวนดังกล่าวว่า *จำนวนเฉพาะสัมพัทธ์*

การคำนวณหาจำนวนของเลขจำนวนเฉพาะที่มีค่าน้อยกว่าหรือเท่ากับ n (เช่น จำนวนของเลขจำนวนเฉพาะที่มีค่าน้อยกว่า 10 มี 4 จำนวน) สามารถประมาณค่าโดย จำนวนของเลขจำนวนเฉพาะดังกล่าว

จะมีค่าอยู่ระหว่าง $[\frac{n}{ln(n)}]$ และ $[\frac{n}{ln(n)-1.08366}]$ (พิสูจน์โดย เกาส์และลากอง) เช่น จำนวนของเลขจำนวนเฉพาะที่มีค่าน้อยกว่า 1,000,000 มีค่าประมาณอยู่ระหว่าง 72,383 ถึง 78,543 จำนวน (ซึ่งจริงๆ แล้วมี 78,498 ตัว) เป็นต้น

การตรวจสอบว่าเลข n เป็นเลขจำนวนเฉพาะหรือไม่ สามารถทดลองทำด้วยการหารเลขดังกล่าวด้วยจำนวนเฉพาะที่มีค่าน้อยกว่า $\sqrt{n}$ (หากจำนวนประกอบ n จะมีตัวประกอบเฉพาะต่ำสุดเป็น a ดังนั้น $n \geq a^2$ ดังนั้น จึงสามารถทดสอบเพียง $a \leq \sqrt{n}$ ก็พอ) เช่น ต้องการตรวจสอบว่า เลข 89 เป็นจำนวนเฉพาะ หรือไม่ ให้ทดลองหารด้วย จำนวนเฉพาะที่มีค่าน้อยกว่า $\sqrt{89} = 9$ ซึ่งก็ คือ 2,3,5,7 ซึ่งหากหารไม่ลงตัวแสดงว่า 89 เป็นเลขจำนวนเฉพาะ ซึ่งวิธีการทดสอบว่า n เป็นเลขจำนวนเฉพาะดังกล่าว ต้องการการคำนวณเป็น เอ็กซ์โปเนนเชียล ($O(2^b)$) เมื่อ b คือจำนวนบิตของ n แต่เมื่อปี พ.ศ. 2543 ได้มีผู้คิดค้นขั้นตอนวิธีที่เรียกว่า เอเคเอส ซึ่งต้องการการคำนวณเพียง $O((log_2 b)^{12})$

5.1.2 ออยเลอร์ฟีฟังก์ชัน ($\phi(n)$)

ออยเลอร์ฟีฟังก์ชัน $\phi(n)$ เป็นฟังก์ชันในการคำนวณที่ใช้ในการเข้ารหัสในปัจจุบัน ซึ่ง $\phi(n)$ คือ ฟังก์ชันซึ่งใช้หาจำนวนของเลขจำนวนเต็มซึ่งมีค่าน้อยกว่า n และเป็นจำนวนเฉพาะสัมพัทธ์ กับ n ซึ่งมีคุณสมบัติเบื้องต้นดังนี้

- $\phi(1) = 0$
- $\phi(p) = p - 1$ เมื่อ p คือจำนวนเฉพาะ
- $\phi(p^e) = p^e - p^{e-1}$ เมื่อ p คือจำนวนเฉพาะ
- $\phi(m \times n) = \phi(m) \times \phi(n)$ เมื่อ m และ n เป็นจำนวนเฉพาะสัมพัทธ์

ตัวอย่างเช่น $\phi(89) = 89 - 1 = 88$ เนื่องจาก 89 เป็นจำนวนเฉพาะ $\phi(10) = \phi(5) \times \phi(2) = (5-1) \times (2-1) = 4$ และ $\phi(25) = 5^2 - 5^1 = 20$ เป็นต้น

5.1.3 ทฤษฎีของเฟอร์แมทและออยเลอร์

ทฤษฎีของเฟอร์แมทและออยเลอร์เป็นทฤษฎีที่อยู่เบื้องหลังการเข้ารหัสและถอดรหัส เช่น

- ถ้า p เป็นจำนวนเฉพาะ a เป็นจำนวนเต็มซึ่งหารด้วย p ไม่ลงตัวแล้ว $a^{p-1} \equiv 1 \bmod p$
- ถ้า p เป็นจำนวนเฉพาะ a เป็นจำนวนเต็มแล้ว $a^p \equiv a \bmod p$
- ถ้า a และ n เป็นจำนวนเฉพาะสัมพัทธ์แล้ว $a^{\phi(n)} \equiv 1 \bmod n$
- ถ้า $n = p \times q$ โดยที่ $a < n$ และ k เป็นจำนวนเต็มแล้ว $a^{k \times \phi(n)+1} \equiv a \bmod n$

5.1.4 การแยกตัวประกอบเฉพาะ

การแยกตัวประกอบเฉพาะ คือ การเขียนจำนวนเต็มบวก n ให้อยู่ในรูปของ $n = p_1^{e_1} \times p_2^{e_2} \times \ldots \times p_k^{e_k}$ โดยที่ $p_1, p_2, \ldots, p_k$ คือ จำนวนเฉพาะ และ $e_1, e_2, \ldots, e_k$ คือ จำนวนเต็ม ซึ่งหาก $a = p_1^{a_1} \times p_2^{a_2} \times \ldots \times p_k^{a_k}$ และ $b = p_1^{b_1} \times p_2^{b_2} \times \ldots \times p_k^{b_k}$ แล้ว หรม. (หารร่วมมาก) ของ a และ b คือ หรม.$(a,b) = p_1^{min(a_1,b_1)} \times p_2^{min(a_1,b_2)} \times \ldots \times p_k^{min(a_k,b_k)}$ ส่วน ครน. (คูณร่วมน้อย) ของ a และ b คือ ครน.$(a,b) = p_1^{max(a_1,b_1)} \times p_2^{max(a_1,b_2)} \times \ldots \times p_k^{max(a_k,b_k)}$ ซึ่ง ครน.$(a,b) \times$หรม.$(a,b) = a \times b$ การแยกตัวประกอบเฉพาะนั้นสามารถทำได้หลายวิธี เช่น การทดลองหารไปเรื่อยๆ ว่าตัวเลขใดหารลงตัว ซึ่งใช้เวลาเป็นเอ็กซ์โปเนนเชียล การหาด้วยวิธีการของเฟอร์แมต การหาด้วยวิธีการของโพหลาด และอื่นๆ ซึ่งในปัจจุบันยังไม่พบวิธีการแยกตัวประกอบที่เร็วสำหรับการแยกตัวประกอบตัวเลขขนาดใหญ่ ซึ่งนับว่าเป็นเรื่องที่ดีสำหรับศาสตร์ในการเข้ารหัสและถอดรหัส

5.1.5 เอ็กซ์โปเนนเชียลและลอการิทึม

เอ็กซ์โปเนนเชียลและลอการิทึมเป็นฟังก์ชันที่ตรงข้ามกัน กล่าวคือ ถ้า $y = a^x$ แล้ว $x = log_a y$ ซึ่งในเรื่องการเข้ารหัสและถอดรหัส นิยมหาค่า $y = a^x \bmod n$ ซึ่งสามารถคำนวณได้เร็ว ด้วยการมองเลข x เป็นฐาน 2 ซึ่งจะมีจำนวนรอบในการคำนวณเท่ากับจำนวนบิตของ x จากนั้นให้หาค่า y และ a ในแต่ละรอบ โดยค่า y เกิดจากค่า y ของรอบก่อนหน้าคูณค่า a ของรอบก่อนหน้าแล้ว mod ด้วย n ซึ่งค่า y จะถูกคำนวณเฉพาะรอบซึ่งค่า x มีบิตเป็น 1 ส่วนค่า a เกิดจากค่า a ของรอบก่อนหน้ายกกำลัง 2 แล้ว mod n ซึ่งคำนวณทุกรอบยกเว้นรอบสุดท้าย โดยผลลัพธ์ของการคำนวณ คือ ค่า y ของรอบสุดท้าย ยกตัวอย่าง เช่น หากต้องการคำนวณหาค่า $17^{22} \bmod 21$ จะได้ผลลัพธ์เป็น 4 ซึ่งสามารถแสดงขั้นตอนการคำนวณได้ดังตารางที่ 5.1 โดยที่เลข 22 สามารถเขียนเป็นเลขฐาน 2 คือ $(10110)_2$ สังเกตว่า ผลลัพธ์ของการหาค่า 17^{22} นั้นมีค่ามหาศาล แม้กระทั่งเครื่องคิดเลขบางรุ่นยังไม่สามารถคำนวณได้ จึงจำเป็นต้องใช้วิธีการดังกล่าว

ตารางที่ 5.1: ตัวอย่างการคำนวณหาค่า $17^{22} \bmod 21$

รอบที่	เลขฐาน 2	ค่า y (ค่าเริ่มต้น = 1)	ค่า a (ค่าเริ่มต้น = 17)
0	0		a = $17^2 \bmod 21 = 16$
1	1	y = $1 \times 16 \bmod 21 = 16$	a = $16^2 \bmod 21 = 4$
2	1	y = $16 \times 4 \bmod 21 = 1$	a = $4^2 \bmod 21 = 16$
3	0		a = $16^2 \bmod 21 = 4$
4	1	y = $1 \times 4 \bmod 21 = 4$	

5.2 การเข้ารหัสด้วยกุญแจแบบอสมมาตร

การเข้ารหัสด้วยกุญแจทั้งแบบสมมาตรและอสมมาตรนั้นมีข้อดีข้อเสียแตกต่างกัน การเข้ารหัสด้วยกุญแจแบบสมมาตรจะมีความเร็วสูงมากกว่าการเข้ารหัสด้วยกุญแจแบบอสมมาตร ในขณะที่การเข้ารหัสด้วยกุญแจแบบอสมมาตรนิยมใช้ในการและเปลี่ยนกุญแจ (ของการเข้ารหัสด้วยกุญแจแบบสมมาตร) การระบุตัวตน และลายเซ็นดิจิทัล ในเนื้อหาก่อนหน้านี้ได้กล่าวถึง การเข้ารหัสด้วยกุญแจแบบสมมาตรซึ่งจะใช้กุญแจดอกเดียวกันที่รู้ทั้งผู้ส่งและผู้รับ การเข้ารหัสและถอดรหัส จะอาศัยการแทนที่หรือการสลับที่ของข้อมูลซึ่งถูกมองเป็นสัญลักษณ์หรือตัวอักษร สำหรับบทนี้จะกล่าวถึงการเข้ารหัสด้วยกุญแจแบบสมมาตร ซึ่งจะใช้กุญแจสองดอกที่เรียกว่า ''กุญแจสาธารณะ'' และ ''กุญแจส่วนตัว'' กุญแจส่วนตัวเป็นกุญแจที่เก็บไว้คนเดียวไม่ต้องบอกให้ใครรู้ ในขณะที่กุญแจสาธารณะสามารถให้คนอื่นรู้ได้ หากกุญแจดอกหนึ่งใช้ในการเข้ารหัส กุญแจอีกดอกหนึ่งที่คู่กันจะใช้ในการถอดรหัส เช่น หากผู้ส่งต้องการส่งข้อความลับไปให้ผู้รับ ผู้ส่งจะใช้กุญแจสาธารณะของผู้รับในการเข้ารหัส แล้วส่งข้อความที่เข้ารหัสแล้วไปให้ผู้รับ และเมื่อผู้รับได้รับข้อความที่เข้ารหัสแล้ว ผู้รับจะสามารถถอดรหัสข้อความดังกล่าวได้โดยใช้กุญแจส่วนตัวของผู้รับ วิธีการเข้ารหัสและถอดรหัสจะอาศัยการคำนวณทางคณิตศาสตร์ โดยที่ข้อมูลทั้งหมดจะถูกมองเป็นตัวเลข โดยการคำนวณดังกล่าวจะอาศัยฟังก์ชั่นทางเดียว (ฟังก์ชั่นที่ $y = f(x)$ คำนวณได้ง่าย ในขณะที่ $x = f^{-1}(y)$ นั้นคำนวณได้ยากมาก เช่น การหาค่าตัวเลขจำนวนเต็มที่เกิดจาก การคูณของเลขจำนวนเฉพาะสองจำนวน $n = p \times q$ นั้นหาได้ง่าย ในขณะที่หากรู้ค่า n แล้วต้องการคำนวณหาว่าเกิดจากจำนวนเฉพาะ p และ q ไหนนั้นคำนวณได้ยากมาก) หากมีผู้ที่ต้องการเข้ารหัส n คน การเข้ารหัสด้วยกุญแจแบบสมมาตรจะต้องเก็บรักษากุญแจให้เป็นความลับ ทั้งหมด $\frac{n\times(n-1)}{2}$ ในขณะที่การเข้ารหัสด้วยกุญแจแบบอสมมาตรจะต้องรักษา กุญแจส่วนตัวเพียง n ดอก

5.2.1 การเข้ารหัสด้วยวิธีถุงเป้

การเข้ารหัสวิธีนี้เป็นการเข้ารหัสแบบง่ายซึ่งแสดงให้เห็นถึงพื้นฐานการเข้ารหัสด้วยกุญแจแบบ อสมมาตรในปัจจุบัน หลักการของการเข้ารหัสนี้ เปรียบเสมือนกับตัวเลขที่อยู่ในถุงเป้ แล้วต้องการคำนวณผลรวมของเลขดังกล่าว แต่หากทราบผลรวมแล้วการที่จะว่าเลขใดอยู่ในถุงเป้นั้นทำยาก โดยที่กำหนดให้ a คือชุดของตัวเลขจำนวนเต็ม $a = [a_1, a_2, \ldots, a_k]$ และ $x = [x_1, x_2, \ldots, x_k]$ คือชุดของตัวเลข 0 และ 1 ซึ่งระบุว่าค่า a ตัวใดอยู่ ในถุงเป้แล้ว s คือผลรวม ซึ่ง $s = Sum(a, x) = x_1a_1 + x_2a_2 + \ldots + x_ka_k$ การคำนวณ $s = Sum(a, x)$ นั้นกระทำได้ง่ายในขณะที่ $x = invSum(s, a)$ นั้นกระทำได้ยาก ซึ่งในที่นี้ a คือกุญแจสาธารณะ, x คือข้อความที่ต้องการส่ง ส่วน s คือข้อความที่เข้ารหัสแล้วนั่นเอง

ขั้นตอนการสร้างกุญแจ

1. สร้าง $b = [b_1, b_2, \ldots, b_k]$ โดยที่ $b_i \geq b_1 + b_2 + \ldots + b_{i-1}$

2. เลือกค่า n ซึ่ง $n > b_1 + b_2 + \ldots + b_k$

3. เลือกค่า r ซึ่งเป็นจำนวนเฉพาะสัมพัทธ์กับ n และ $1 \leq r \leq n-1$

4. สร้าง $t = [t_1, t_2, \ldots, t_k]$ โดยที่ $t_i = r \times b_i$ mod n

5. สลับที่ตำแหน่งของ t จะได้ $a = [a_1, a_2, \ldots, a_k]$

6. กำหนดชุดตัวเลข a คือ กุญแจสาธารณะ ส่วน ชุดตัวเลข b ค่า n และค่า r คือกุญแจส่วนตัว

ขั้นตอนการเข้ารหัส

1. แปลงค่าที่ต้องการส่งเป็น $x = [x_1, x_2, \ldots, x_k]$ โดยที่ x_i มีค่าเป็น 0 หรือ 1 เช่น การแปลงจากตัวอักษรเป็นรหัสแอสกี

2. คำนวณหาค่า s โดย $s = Sum(a, x)$

ขั้นตอนการถอดรหัส

1. คำนวณค่า $s' = r^{-1} \times$s mod n โดยที่ r^{-1} คือ การหาค่าซึ่ง $r^{-1} \times r$ mod n เท่ากับ 1

2. คำนวณหาค่า x' จาก ค่าผลรวมสมมุติ s' และ b โดยดูว่าค่าใดของ b ที่อยู่ในถุงเป้บ้าง ซึ่งสามารถคำนวณได้ง่ายเนื่องจาก ค่า b แต่ละตัวจะน้อยกว่าผลรวมของตัวก่อนหน้าอยู่แล้ว

3. สลับตำแหน่งของ x' ให้ถูกต้องจะได้ผลลัพธ์ x ซึ่งคือข้อความก่อนเข้ารหัส

5.2.2 การเข้ารหัสด้วยวิธีอาร์เอสเอ

อาร์เอสเอ เป็นการเข้ารหัสแบบกุญแจอสมมาตรที่นิยมที่สุดในปัจจุบัน ซึ่งตั้งชื่อตามนามสกุลของผู้คิดค้นวิธีการดังกล่าวทั้งสามคน คือ รอน ริเวสท์, เอดิ ชาร์เมีย และเลียวนาร์ด เอเดิลแมน อาร์เอสเอใช้คู่ของค่า e และ n เป็นกุญแจสาธารณะ และคู่ของค่า d กับ n เป็นกุญแจส่วนตัว หาก P คือข้อความก่อนเข้ารหัส C คือข้อความที่เข้ารหัสแล้ว ผู้ส่งจะใช้กุญแจสาธารณะของผู้รับ เพื่อสร้างข้อความที่เข้ารหัสจาก $C = P^e$ mod n แล้วผู้รับจะใช้กุญแจส่วนตัวของตนเองในการถอดรหัสด้วย $P = C^d$ mod n หากผู้ประสงค์ร้ายต้องการถอดรหัสจะต้องใช้สมการ $P = \sqrt[e]{C}$ mod n ซึ่งคำนวณได้ยาก

ขั้นตอนการสร้างกุญแจ

1. เลือกค่าจำนวนเฉพาะ 2 ค่า คือ p และ q (ควรมีขนาดอย่างน้อย 512 บิต)

2. คำนวณค่า n จาก p และ q (ควรมีผลคูณอย่างน้อย 1024 บิต)

3. คำนวณค่า $\phi(n)$ จาก $\phi(n) = (p-1) \times (q-1)$

4. เลือกค่า e ซึ่ง $1 < e < \phi(n)$ และ e เป็นจำนวนเฉพาะสัมพัทธ์กับ $\phi(n)$ (หรม. ของ e และ $\phi(n)$ มีค่าเป็น 1)

5. คำนวณหาค่า d ซึ่ง $d = e^{-1} \bmod \phi(n)$ หรือ ค่าจำนวนเต็มบวก d ที่น้อยที่สุดซึ่งทำให้ $d \times e \bmod \phi(n)$ มีค่าเท่ากับ 1

6. ประกาศค่า e และ n เป็นกุญแจสาธารณะ และเก็บค่า d กับ n ไว้เป็นกุญแจส่วนตัว

ขั้นตอนการเข้ารหัส

หาก P คือข้อความก่อนเข้ารหัส C คือข้อความที่เข้ารหัสแล้วซึ่งผู้ส่งสามารถ คำนวณจาก $C = P^e \bmod n$ โดยค่า e และ n เป็นกุญแจสาธารณะของผู้รับ การคำนวณหาค่ายกกำลังโดยตรงแล้ว mod n อาจคำนวณได้ยากเนื่องจากมีค่ามหาศาล แต่การคำนวณดังกล่าวสามารถแทนที่ด้วยคุณสมบัติ [(a mod n) × (b mod n)] mod n = (a × b) mod n ยกตัวอย่างเช่น หาก e มีค่า 7 และ P มีค่า 88 และ n มีค่า 187 การคำนวณ 88^7 ซึ่งมีค่า 40,867,559,636,992 แล้วนำมา mod 187 ซึ่งจะได้ผลลัพธ์เป็น 11 นั้นอาจทำไม่ได้จริงในทางปฏิบัติถึงแม้จะใช้เครื่องคิดเลขบางรุ่นก็ตาม ดังนั้นจึงควรคำนวณ $88^7 \bmod 187$ จาก $[(88^4 \bmod 187) \times (88^2 \bmod 187) \times (88^1 \bmod 187)] \bmod 187$ ซึ่งการคำนวณเลขยกกำลังจะน้อยกว่ามาก หรืออาจจะใช้วิธีการคำนวณที่กล่าวใน 5.1.5 ก็ได้

ขั้นตอนการถอดรหัส

ผู้รับถอดรหัสข้อความต้นฉบับจาก $P = C^d \bmod n$ โดยค่า d และ n เป็นกุญแจส่วนตัวของผู้รับ การคำนวณดังกล่าวสามารถใช้เทคนิคเดียวกับการเข้ารหัสได้

5.2.3 การเข้ารหัสด้วยวิธีราบิน

การเข้ารหัสแบบราบิน คล้ายกับการเข้ารหัสแบบอาร์เอสเอ โดยมีค่า e คือ 2 และ d คือ $\frac{1}{2}$

ขั้นตอนการสร้างกุญแจ

1. เลือกค่าจำนวนเฉพาะ 2 ค่า คือ p และ q ซึ่งอยู่ในรูป 4k+3

2. คำนวณหาค่า n ซึ่ง $n = p \times q$

3. ประกาศกุญแจสาธารณะ คือ ค่า n ส่วนค่า p กับ q คือ กุญแจส่วนตัว

ขั้นตอนการเข้ารหัส

หาก P คือ ข้อความก่อนเข้ารหัส C คือข้อความที่เข้ารหัสแล้ว ผู้ส่งจะเข้ารหัสด้วยการคำนวณ $C = P^2$ mod n

ขั้นตอนการถอดรหัส

ผู้รับจะไม่สามารถคำนวณค่า P ได้โดยตรง แต่ต้องเลือกจากค่า 4 ค่าที่เป็นไปได้ คือ P_1, P_2, P_3, P_4 โดยที่

- ค่า P_1 คือ ค่าซึ่งทำให้สมการ $+C^{\frac{(p+1)}{4}}$ mod p และ $+C^{\frac{(q+1)}{4}}$ mod q เป็นจริง
- ค่า P_2 คือ ค่าซึ่งทำให้สมการ $+C^{\frac{(p+1)}{4}}$ mod p และ $-C^{\frac{(q+1)}{4}}$ mod q เป็นจริง
- ค่า P_3 คือ ค่าซึ่งทำให้สมการ $-C^{\frac{(p+1)}{4}}$ mod p และ $+C^{\frac{(q+1)}{4}}$ mod q เป็นจริง
- ค่า P_4 คือ ค่าซึ่งทำให้สมการ $-C^{\frac{(p+1)}{4}}$ mod p และ $-C^{\frac{(q+1)}{4}}$ mod q เป็นจริง

หาก $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$, ..., $x \equiv a_k \pmod{m_k}$ แล้ว สามารถคำนวณหาค่า x ได้จากขั้นตอนต่อไปนี้

1. คำนวณหาค่า M จาก $m_1 \times m_2 \times \ldots \times m_k$
2. คำนวณหาค่า $M_1 = \frac{M}{m_1}, M_2 = \frac{M}{m_2}, \ldots, M_k = \frac{M}{m_k}$
3. คำนวณหาค่า $M_1^{-1}, M_2^{-1}, \ldots, M_k^{-1}$ โดยที่ค่า $M_i^{-1} \times M_i \bmod m_i = 1$
4. คำนวณหา $x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \ldots + a_k \times M_k \times M_k^{-1}) \bmod M$

5.2.4 การเข้ารหัสด้วยวิธีอื่นๆ

นอกจากการเข้ารหัสที่กล่าวมาแล้วยังมีวิธีการเข้ารหัสแบบอสมมาตรวิธีอื่นอีก เช่น การเข้ารหัสแบบเอลกามอล ซึ่งทุกวิธีที่กล่าวมามีข้อเสีย คือ กุญแจมีขนาดใหญ่ ซึ่งในปัจจุบัน มีความพยายามที่จะลดขนาดของกุญแจโดยยังคงความมั่นคงปลอดภัยไว้เหมือนเดิม เช่น การเข้ารหัสแบบอีซีซีซึ่งใช้ทฤษฎีของเส้นโค้งอีลิปติก

5.3 สรุป

ในบทนี้ได้กล่าวถึง การเข้ารหัสด้วยกุญแจแบบอสมมาตรซึ่งนิยมใช้ในการและเปลี่ยนกุญแจ (ของการเข้ารหัสด้วยกุญแจแบบสมมาตร) การระบุตัวตน และลายเซ็นดิจิทัล เนื้อหาบทนี้ครอบคลุม คณิตศาสตร์

พื้นฐานของการเข้ารหัสด้วยกุญแจแบบอสมมาตร อาทิเช่น จำนวนเฉพาะ การแยกตัวประกอบเฉพาะ เป็นต้น รวมถึงการเข้ารหัสแบบสมมาตรด้วยวิธีต่างๆ ได้แก่ การเข้ารหัสแบบถุงเป้ การเข้ารหัสแบบอาร์เอสเอ และการเข้ารหัสแบบราบิน

5.4 แบบฝึกหัด

1. จงหาอัตราส่วนของค่าจำนวนเฉพาะกับจำนวนเต็มทั้งหมดในช่วงของจำนวนเต็มต่อไปนี้

   (a) ช่วงจำนวนเต็ม ระหว่าง 1 ถึง 10

   (b) ช่วงจำนวนเต็ม ระหว่าง 100,000 ถึง 200,000

2. จงคำนวณหาค่าต่อไปนี้

   (a) $5^{15} \bmod 13$

   (b) $15^{18} \bmod 17$

   (c) $456^{17} \bmod 17$

   (d) $145^{102} \bmod 101$

3. จงหาค่า x ในกรณีต่อไปนี้

   (a) $x \equiv 2 \bmod 7$ และ $x \equiv 3 \bmod 9$

   (b) $x \equiv 4 \bmod 5$ และ $x \equiv 10 \bmod 11$

   (c) $x \equiv 7 \bmod 13$ และ $x \equiv 11 \bmod 12$

4. จงเข้ารหัสตัวอักษร a ด้วยวิธีการแบบถุงเป้ ซึ่งมีค่า b=[7,11,23,43,87,173,357] ค่า r=41 และ n=1001 โดยการสลับที่ซึ่งมีลำดับ 7,6,5,1,2,3,4

5. ในการเข้ารหัสแบบอาร์เอสเอ หาก n มีค่า 221 และ e มีค่าเป็น 5 จงหาค่า d

6. ในการเข้ารหัสแบบอาร์เอสเอ หาก p มีค่า 19 q มีค่า 23 และ e มีค่า 3 จงหากุญแจสาธารณะและกุญแจส่วนตัว

7. หากข้อความก่อนเข้ารหัส คือ 26 จงคำนวณหาข้อความหลังเข้ารหัสด้วยวิธีการเข้ารหัสแบบอาร์เอสเอ ด้วยข้อมูลของข้อก่อนหน้า

8. หากข้อความก่อนเข้ารหัส คือ 17 จงคำนวณหาข้อความหลังเข้ารหัสด้วยวิธีการเข้ารหัสแบบราบิน โดยค่า p = 47 และ q = 11 พร้อมทั้งคำนวณหาค่าที่ได้จากการถอดรหัสทั้ง 4 ค่า

บทที่ 6

บูรณภาพและการพิสูจน์ตัวจริงของสาร

- บูรณภาพและการพิสูจน์ตัวจริงของสาร
- แฮชฟังก์ชัน
- ลายมือชื่อดิจิทัล

บทที่ 6

บูรณภาพและการพิสูจน์ตัวจริงของสาร

ในบทที่ผ่านมาได้เน้นการเข้ารหัสของข้อความทั้งวิธีการแบบสมมาตรและอสมมาตร แต่สำหรับข้อความบางประเภท ไม่จำเป็นต้องการการเข้ารหัสแต่ต้องการพิสูจน์ตัวจริงว่าใครคือผู้ส่งหรือสร้างข้อความ และข้อความมิได้ถูกแก้ไข (เช่น พินัยกรรมอาจใช้ลายนิ้วมือของผู้เขียนในการระบุตัวตนของผู้เขียน และป้องกันการปลอมแปลงเอกสาร) ซึ่งบทนี้จะกล่าวถึงบูรณภาพและการพิสูจน์ตัวจริงของสาร แฮชฟังก์ชัน และ ลายมือชื่อดิจิทัล

6.1 บูรณภาพและการพิสูจน์ตัวจริงของสาร

6.1.1 บูรณภาพของสาร

การตรวจสอบบูรณภาพของสารหรือข้อความ หมายถึง การตรวจสอบว่าข้อความมิได้ถูกแก้ไข โดยอาศัยหลักการที่ผู้เขียนข้อความ สร้างข้อความฉบับย่อ (หรือ ไดเจสต์) โดยใช้ฟังก์ชัน ที่เรียกว่า ''แฮชฟังก์ชัน'' ผู้ส่งข้อความต้องส่งข้อความ พร้อมด้วยข้อความฉบับย่อของข้อความนั้น ซึ่งผู้รับสามารถตรวจสอบบูรณภาพของข้อความดังกล่าว โดยการนำข้อความที่ได้รับมาผ่านแฮชฟังก์ชันแล้วเพื่อให้ได้ข้อความย่อยชั่วคราว จากนั้นนำข้อความย่อยชั่วคราวมาเปรียบเทียบกับข้อความย่อยที่ได้รับว่าตรงกันหรือไม่ หากตรงกันแสดงว่าข้อความมิได้ถูกแก้ไขระหว่างทาง แต่หากไม่ตรงกันก็ควรจะทิ้งข้อความนั้นเนื่องจากข้อความอาจถูกแก้ไขจากผู้ไม่หวังดี กุญแจสำคัญที่ทำให้การตรวจสอบบูรณภาพสำเร็จ คือ แฮชฟังก์ชัน หาก m แทนข้อความ $H()$ แทนแฮชฟังก์ชัน และ d แทนข้อความย่อยซึ่ง $d = H(m)$ แล้วแฮชฟังก์ชันที่ดีจะต้องมีคุณสมบัติ 3 ประการ คือ

1. หากผู้ประสงค์ร้ายรู้ d แล้วจะต้องไม่สามารถหา m' ซึ่ง $d = H(m')$
2. หากผู้ประสงค์ร้ายรู้ M และ d แล้วจะต้องไม่สามารถหา $m' \neq m$ ซึ่ง $H(m') = H(m)$
3. ผู้ประสงค์ร้ายต้องไม่สามารถหา $m' \neq m$ ซึ่ง $H(m') = H(m)$ ได้

วิธีการสร้างแฮชฟังก์ชันในอุดมคติ คือ การสุ่มบิตขนาดคงที่ (เช่น 16) เพื่อใช้เป็นข้อความย่อย พร้อมทั้งเก็บข้อความย่อยดังกล่าวกับข้อความนั้นไว้ในตาราง เมื่อต้องการสร้างข้อความย่อยของข้อความครั้งถัดไป ให้ตรวจสอบว่าเคยกับข้อความดังกล่าวไว้ในตารางหรือไม่ หากเคยเก็บข้อความดังกล่าวไว้ในตารางให้ตอบข้อความย่อยเดิมที่เคยเก็บไว้ แต่หากไม่พบในตารางให้สุ่มบิตเพื่อใช้เป็นข้อความย่อยใหม่

เนื่องจากขนาดของข้อความย่อยนั้นคงที่ ทำให้อาจมีสองข้อความซึ่งมีข้อความย่อยเดียวกัน คล้ายกับ ''หลักการของรังนกพิราบ'' ซึ่งกล่าวว่า หากมีรังนกพิราบ n รัง (ในที่นี้คือจำนวนข้อความย่อยที่เป็นไปได้) และมีนกพิราบ kn+1 ตัว (ในที่นี้คือจำนวนข้อความที่เป็นไปได้) แล้วจะมีอย่างน้อย 1 รัง ซึ่งมีนกพิราบอยู่ k+1 ตัว (ในกรณีนี้ คือ จะมีข้อความย่อยอย่างน้อย 1 ข้อความซึ่งถูกสร้างมาเหมือนกันจากข้อความ ต้นฉบับ k+1 ข้อความ)

6.1.2 การพิสูจน์ตัวจริงของสาร

การพิสูจน์ตัวจริงของสารสามารถทำด้วยการแฮชกุญแจกับข้อความเพื่อสร้างรหัส หาก m คือข้อความ k คือกุญแจ H() คือ แฮชฟังก์ชัน และ c คือรหัสแล้ว รหัสสามารถคำนวณได้จาก c=H(k|m) โดยที่ k|m หมายถึง การนำกุญแจมาต่อท้ายด้วยข้อความ ซึ่งผู้ประสงค์ร้ายจะไม่สามารถสร้างรหัสใหม่ได้เนื่องจากไม่รู้กุญแจ วิธีพิสูจน์ตัวจริงของสารนั้นคล้ายกับการตรวจสอบบูรณภาพกล่าวคือ ผู้ส่งข้อความต้องส่งข้อความพร้อมด้วยรหัส (c=H(k|m)) ของข้อความนั้น ผู้รับสามารถตรวจสอบตัวจริงของผู้ส่งข้อความดังกล่าว ด้วยการนำกุญแจกับข้อความ ที่ได้รับมาผ่านแฮชฟังก์ชันแล้วเพื่อสร้างรหัสชั่วคราว จากนั้นนำรหัสชั่วคราวมาเปรียบเทียบกับรหัสที่ได้รับว่าตรงกันหรือไม่ หากตรงกันแสดงว่าข้อความมาจากผู้ส่งตัวจริง แต่หากไม่ตรงกันก็ควรจะทิ้งข้อความนั้นเนื่องจากข้อความอาจถูกส่งมาจากผู้ไม่หวังดี การสร้างรหัสดังกล่าวอาจทำซ้ำหลายรอบกล่าวคือ c=H(k|H(k|m)) เป็นต้น นอกจากนั้นยังมีวิธีในการสร้างรหัสแบบอื่นอีก เช่น การเข้ารหัสโดยอาศัยหลักการแบบซีบีซี คือ การแบ่งข้อมูลเป็นบล็อก แล้วเอ็กออร์ข้อมูลบล็อกปัจจุบันกับข้อมูลที่เข้ารหัสแล้วของบล็อกก่อนหน้า โดยที่ n บิตซ้ายสุดของข้อมูลที่เข้ารหัสแล้วของบล็อกสุดท้ายจะถูกใช้เป็นรหัสสำหรับการพิสูจน์ตัวจริงของผู้ส่ง

6.2 แฮชฟังก์ชัน

เนื่องจากแฮชฟังก์ชั่นเป็นการสร้างข้อความย่อยขนาด(หรือความยาว)คงที่ จากข้อความต้นฉบับซึ่งขนาดใหญ่กว่า และมีขนาดไม่คงที่ ดังนั้นพื้นฐานการออกแบบแฮชฟังก์ชันส่วนใหญ่ คือ การวนซ้ำแฮชฟังก์ชันซึ่งรับข้อมูลนำเข้าขนาดคงที่ เช่น การแบ่งข้อความเป็นบล็อก $m_1, m_2, \ldots, m_k$ โดยที่ในแต่ละรอบจะสร้างข้อความย่อย $d_1, d_2, \ldots, d_k$ ผ่านฟังก์ชันย่อย F ซึ่ง $d_i = F(d_{i-1}, m_i)$ โดยที่ d_k คือผลลัพธ์สุดท้ายของแฮชฟังก์ชัน คุณสมบัติของแฮชฟังก์ชันจะขึ้นอยู่กับคุณสมบัติของฟังก์ชันย่อย F แฮชฟังก์ชันในปัจจุบันสามารถแบ่งเป็น 2 ประเภทตามการออกแบบฟังก์ชันย่อย F คือ กลุ่มแฮช

ฟังก์ชันที่ออกแบบฟังก์ชันย่อยใหม่เพื่อใช้สำหรับการแฮชฟังก์ชันโดยเฉพาะ และ กลุ่มที่อาศัยการเข้ารหัสที่มีอยู่แล้วเป็นฟังก์ชันย่อย

- กลุ่มแฮชฟังก์ชันที่ออกแบบฟังก์ชันย่อยใหม่โดยเฉพาะ ได้แก่ ตระกูลเอ็มดีซึ่งถูกประดิษฐ์โดยผู้คิดค้นอาร์เอสเอ ได้แก่ เอ็มดี2, เอ็มดี4 และ เอ็มดี5 ซึ่งเป็นเวอร์ชันล่าสุดของตระกูลนี้ โดยเอ็มดี5 จะอ่านข้อมูลบล็อกละ 512 บิตพร้อมกับสร้างข้อความย่อย ขนาด 128 บิต อีกตระกูลคือ ตระกูลเอสเอชเอ หรือ ชา ซึ่งถูกพัฒนาโดยนิสท์ ได้แก่ ชา-1, ชา-224, ชา-256, ชา-385 และ ชา-512 ซึ่งคุณลักษณะของแฮชฟังก์ชัน ตระกูลชาสามารถสรุปได้ดังตารางที่ 6.1 นอกจากนี้ยังมี

ตารางที่ 6.1: คุณลักษณะของแฮชฟังก์ชันตระกูลชา

คุณลักษณะ	ชา-1	ชา-224	ชา-256	ชา-384	ชา-512
ขนาดข้อความสูงสุด	$2^{64}-1$	$2^{64}-1$	$2^{64}-1$	$2^{128}-1$	$2^{128}-1$
ขนาดบล็อก	512	512	512	1024	1024
ขนาดข้อความย่อย	160	224	256	384	512
ขนาดเวิร์ด	32	32	32	64	64
จำนวนรอบ	80	64	64	80	80

แฮชฟังก์ชันตระกูลอื่นอีก ได้แก่ ตระกูลไรป์เอ็มดี (เช่น ไรป์เอ็มดี-160) ตระกูลไฮวอล เป็นต้น

- กลุ่มแฮชฟังก์ชันที่อาศัยการเข้ารหัสที่มีอยู่แล้ว เช่น ดีอีเอส เออีเอส กลุ่มแฮชฟังก์ชันกลุ่มนี้ได้แก่ เวิลด์พูล (ซึ่งจะกล่าวรายละเอียดในหัวข้อ 6.2.2)

6.2.1 แฮชฟังก์ชันชา-512

ชา-512 เป็นเวอร์ชันหนึ่งของชาซึ่งสร้างข้อความย่อยขนาด 512 บิต จากบล็อกของข้อมูล บล็อกละ 1024 บิต ซึ่งข้อมูลแต่ละบล็อกจะผสมกับผลลัพธ์ขนาด 512 บิตก่อนหน้าเพื่อสร้างผลลัพธ์ขนาด 512 บิต โดยที่ผลลัพธ์ของบล็อกสุดท้าย คือ ข้อความย่อยของชา-512

ก่อนที่จะเริ่มการแฮชด้วยชา-512 ข้อความต้นฉบับจะถูกทำให้เป็นบล็อก บล็อกละ 1024 บิต โดยเริ่มจากการนำข้อความต้นฉบับ นำมาต่อท้ายด้วยแพดดิ้ง และความยาวของข้อความซึ่งมีความยาว 128 บิตเสมอ นั่นหมายความว่าข้อความต้นฉบับจะมีความยาวได้ไม่เกิน $2^{128}-1$ หาก |M| คือความยาวของข้อความและ |P| คือความยาวแพดดิ้งแล้ว (|M|+|P|+128) mod 1024 ต้องมีค่าเป็น 0

การทำงานของชา-512 จะทำงานเป็นเวิร์ด โดยที่เวิร์ดคือ ข้อมูลขนาด 64 บิต หรือกล่าวอีกนัยหนึ่งว่า ข้อความต้นฉบับจะมีความยาวบล็อกละ 16 เวิร์ด โดยที่ข้อความย่อยและผลลัพธ์ในแต่ละขั้นจะถูกเก็บในที่พักข้อมูลจะมีความยาว 8 เวิร์ด ข้อความแต่ละบล็อกของต้นฉบับซึ่งมีความยาวบล็อกละ 16 เวิร์ดจะถูกขยายเป็น 80 เวิร์ด (เนื่องจากแต่ละบล็อกต้องเรียกฟังก์ชันย่อย 80 รอบ) เรียก $w_0, w_1, \ldots, w_{79}$ โดยที่เวิร์ด w_0 ถึงเวิร์ด w_{15} จะเหมือนกับ ข้อความต้นฉบับทั้ง 16 เวิร์ด เวิร์ดที่ w_{16}

ถึงเวิร์ดที่ w_{79} จะคำนวณจาก $w_i = w_{i-16} \oplus rs_{1-8-7}(w_{i-15}) \oplus w_{i-7} \oplus rs_{19-61-6}(w_{i-2})$ โดยที่ $rs_{a-b-c}(x)$ หมายถึง (การเลื่อนวนขวาของ x จำนวน a บิต) $\oplus$ (การเลื่อนวนขวาของ x จำนวน b บิต) $\oplus$ (การเลื่อนซ้ายของ x จำนวน c บิต) ยกตัวอย่างเช่น เวิร์ด w_{50} สามารถคำนวณได้จาก $w_{50} = w_{34} \oplus rs_{1-8-7}(w_{35}) \oplus w_{43} \oplus rs_{19-61-6}(w_{48})$

ค่าเริ่มต้นของข้อความย่อย เรียกว่า A_0 ถึง H_0 สามารถแสดงได้ในตารางที่ 6.2

ตารางที่ 6.2: ค่าเริ่มต้นของข้อความย่อยของชา-512

ชื่อค่าเริ่มต้น	ค่า(เลขฐาน 16)	ชื่อค่าเริ่มต้น	ค่า(เลขฐาน 16)
A_0	0x6A09E667F3BCC908	E_0	0x510E527FADE682D1
B_0	0xBB67AE8584CAA73B	F_0	0x9B05688C2B3E6C1F
C_0	0x3C6EF372EF94F828	G_0	0x1F83D9ABFB41BD6B
D_0	0xA54FE53A5F1D36F1	H_0	0x5BE0CD19137E2179

การแฮชข้อมูลแต่ละบล็อกจะวนซ้ำ 80 รอบโดยแต่ละรอบจะเป็นการผสมกันระหว่าง ข้อมูลในที่พักข้อมูลของรอบก่อนหน้า เวิร์ดที่ w_i ของข้อมูลต้นฉบับ และค่าคงที่สำหรับแต่ละรอบ k_i (ดังแสดงในตารางที่ 6.3) ซึ่งจะได้ผลลัพธ์เก็บอยู่ในที่พักข้อมูลขนาด 8 เวิร์ด ซึ่งหลังจากรอบสุดท้าย (รอบที่ 79) ผลลัพธ์ที่ได้ในแต่ละเวิร์ดจะถูกบวกกับค่าเริ่มต้น A_0 ถึง H_0

ในแต่ละรอบจะรับที่พักข้อมูลของรอบก่อนหน้า A_{i-1} ถึง H_{i-1} เพื่อสร้างที่พักข้อมูลใหม่ A_i ถึง H_i โดยที่เวิร์ดส่วนใหญ่จะเป็นการคัดลอกเวิร์ดทางซ้ายของรอบก่อนหน้า เช่น $B_i = A_{i-1}, C_i = B_{i-1}, D_i = C_{i-1}, F_i = E_{i-1}, G_i = F_{i-1}, H_i = G_{i-1}$ ยกเว้นเวิร์ด A_i และ E_i ซึ่งจะมีการคำนวณที่ซับซ้อนกว่า โดยที่ $A_i = (Maj(A_{i-1}, B_{i-1}, C_{i-1}) + Rot(A_{i-1})) + (H_{i-1} + Con(E_{i-1}, F_{i-1}, G_{i-1}$ $Rot(E_{i-1}) + w_i + k_i)$ และ $E_i = (H_{i-1} + Con(E_{i-1}, F_{i-1}, G_{i-1}) + Rot(E_{i-1}) + w_i + k_i) + D_{i-1}$ โดยที่

Maj(a,b,c) หมายถึง (a AND b) $\oplus$ (b AND c) $\oplus$ (c AND a)

Rot(a) หมายถึง a วนขวา 28 บิต $\oplus$ a วนขวา 34 บิต $\oplus$ a วนขวา 39 บิต

Con(a,b,c) หมายถึง (a AND b) $\oplus$ (NOT a AND c)

เครื่องหมาย + หมายถึง การบวกเลขแล้ว mod ด้วย 2^{64} เพื่อให้ผลลัพธ์มีขนาดไม่เกิน 64 บิต

6.2.2 แฮชฟังก์ชันเวิลด์พูล

แฮชฟังก์ชันเวิลด์พูลเป็นแฮชฟังก์ชันซึ่งใช้การเข้ารหัสแบบบล็อกด้วยกุญแจแบบสมมาตร โดยดัดแปลงมาจากเออีเอส แฮชฟังก์ชันเวิลด์พูลจะสร้างข้อความย่อยขนาด 512 บิต จากบล็อกของข้อมูลบล็อกละ 512 บิต ซึ่งข้อมูลแต่ละบล็อกจะผสมกับผลลัพธ์ขนาด 512 บิตก่อนหน้าเพื่อสร้างผลลัพธ์ขนาด 512 บิต โดยผลลัพธ์ดังกล่าวจะต้องถูกนำไปเอ็กซ์ออร์กับ บล็อกของข้อมูล และผลลัพธ์ของบล็อกก่อนหน้า

ตารางที่ 6.3: ค่าคงที่ประจำรอบของชา-512

ชื่อค่าคงที่	ค่า(เลขฐาน 16)	ชื่อค่าคงที่	ค่า(เลขฐาน 16)
k_0	0x428A2F98D728AE22	k_{40}	0xA2BFE8A14CF10364
k_1	0x7137449123EF65CD	k_{41}	0xA81A664BBC423001
k_2	0xB5C0FBCFEC4D3B2F	k_{42}	0xC24B8B70D0F89791
k_3	0xE9B5DBA58189DBBC	k_{43}	0xC76C51A30654BE30
k_4	0x3956C25BF348B538	k_{44}	0xD192E819D6EF5218
k_5	0x59F111F1B605D019	k_{45}	0xD69906245565A910
k_6	0x923F82A4AF194F9B	k_{46}	0xF40E35855771202A
k_7	0xAB1C5ED5DA6D8118	k_{47}	0x106AA07032BBD1B8
k_8	0xD807AA98A3030242	k_{48}	0x19A4C116B8D2D0C8
k_9	0x12835B0145706FBE	k_{49}	0x1E376C085141AB53
k_{10}	0x243185BE4EE4B28C	k_{50}	0x2748774CDF8EEB99
k_{11}	0x550C7DC3D5FFB4E2	k_{51}	0x34B0BCB5E19B48A8
k_{12}	0x72BE5D74F27B896F	k_{52}	0x391C0CB3C5C95A63
k_{13}	0x80DEB1FE3B1696B1	k_{53}	0x4ED8AA4AE3418ACB
k_{14}	0x9BDC06A725C71235	k_{54}	0x5B9CCA4F7763E373
k_{15}	0xC19BF174CF692694	k_{55}	0x682E6FF3D6B2B8A3
k_{16}	0xE49B69C19EF14AD2	k_{56}	0x748F82EE5DEFB2FC
k_{17}	0xEFBE4786384F25E3	k_{57}	0x78A5636F43172F60
k_{18}	0x0FC19DC68B8CD5B5	k_{58}	0x84C87814A1F0AB72
k_{19}	0x240CA1CC77AC9C65	k_{59}	0x8CC702081A6439EC
k_{20}	0x2DE92C6F592B0275	k_{60}	0x90BEFFFA23631E28
k_{21}	0x4A7484AA6EA6E483	k_{61}	0xA4506CEBDE82BDE9
k_{22}	0x5CB0A9DCBD41FBD4	k_{62}	0xBEF9A3F7B2C67915
k_{23}	0x76F988DA831153B5	k_{63}	0xC67178F2E372532B
k_{24}	0x983E5152EE66DFAB	k_{64}	0xCA273ECEEA26619C
k_{25}	0xA831C66D2DB43210	k_{65}	0xD186B8C721C0C207
k_{26}	0xB00327C898FB213F	k_{66}	0xEADA7DD6CDE0EB1E
k_{27}	0xBF597FC7BEEF0EE4	k_{67}	0xF57D4F7FEE6ED178
k_{28}	0xC6E00BF33DA88FC2	k_{68}	0x06F067AA72176FBA
k_{29}	0xD5A79147930AA725	k_{69}	0x0A637DC5A2C898A6
k_{30}	0x06CA6351E003826F	k_{70}	0x113F9804BEF90DAE
k_{31}	0x142929670A0E6E70	k_{71}	0x1B710B35131C471B
k_{32}	0x27B70A8546D22FFC	k_{72}	0x28DB77F523047D84
k_{33}	0x2E1B21385C26C926	k_{73}	0x32CAAB7B40C72493
k_{34}	0x4D2C6DFC5AC42AED	k_{74}	0x3C9EBE0A15C9BEBC
k_{35}	0x53380D139D95B3DF	k_{75}	0x431D67C49C100D4C
k_{36}	0x650A73548BAF63DE	k_{76}	0x4CC5D4BECB3E42B6
k_{37}	0x766A0ABB3C77B2A8	k_{77}	0x597F299CFC657E2A
k_{38}	0x81C2C92E47EDAEE6	k_{78}	0x5FCB6FAB3AD6FAEC
k_{39}	0x92722C851482353B	k_{79}	0x6C44198C4A475817

ก่อนที่จะถูกส่งไปยังการคำนวณบล็อกถัดไป โดยที่ผลลัพธ์ของบล็อกสุดท้าย คือ ข้อความย่อยของเวิลด์พูล

ก่อนที่จะเริ่มการแฮชด้วยเวิลด์พูล ข้อความต้นฉบับจะถูกทำให้เป็นบล็อก บล็อกละ 512 บิต โดยเริ่มจากการนำข้อความต้นฉบับ นำมาต่อด้วยแพดดิ้ง และความยาวของข้อความ ซึ่งมีความยาว 256 บิตเสมอ นั่นหมายความว่าข้อความต้นฉบับจะมีความยาวได้ไม่เกิน $2^{256} - 1$ หาก |M| คือความยาวของข้อความและ |P| คือความยาวแพดดิ้งแล้ว (|M|+|P|+256) mod 512 ต้องมีค่าเป็น 0

การเข้ารหัสของเวิลด์พูลเป็นการเข้ารหัส 10 รอบของข้อมูลบล็อกละ 512 บิต ด้วยกุญแจขนาด 512 บิต ซึ่งกุญแจดังกล่าวจะถูกนำไปสร้างกุญแจประจำรอบ 11 ดอก

รูปแบบข้อมูลของเวิลด์พูล

เวิลด์พูลมีรูปแบบข้อมูลคล้ายเออีเอส ยกเว้น บล็อกและสเตท ซึ่ง หนึ่งบล็อกมีขนาด 64 ไบต์ซึ่งถูกเขียนอยู่ในรูปของเมทริกซ์ 1×64 ในขณะที่ สเตท คือ สถานะของข้อมูลขนาด 64 ไบต์ซึ่งถูกเขียนอยู่ในรูปของเมทริกซ์ 8×8 โดยเขียนข้อมูลตามแถว เขียนทีละแถวจากแถวแรกจนถึงแถวสุดท้าย (ซึ่งต่างจากเออีเอสที่เขียนข้อมูลตามสดมภ์)

โครงสร้างในแต่ละรอบ

ในแต่ละรอบของเวิลด์พูลเป็นการแปลงจากสเตทหนึ่งไปยังอีกสเตทหนึ่งด้วยขั้นตอนย่อย ซึ่งประกอบด้วย 4 ขั้นตอนย่อย ได้แก่ การแทนที่ไบต์ การเลื่อนสดมภ์ การผสมแถว และ การผสมกุญแจ โดยปกติแล้วในแต่ละรอบของเออีเอสทำงานครบทั้ง 4 ขั้นตอนย่อย ยกเว้น ขั้นตอนก่อนรอบแรกจะประกอบด้วย การผสมกุญแจเพียงอย่างเดียว

- **การแทนที่ไบต์** การแทนที่ไบต์ของเวิลด์พูลจะเป็นการแทนที่ครั้งละ 1 ไบต์ ซึ่งทุกไบต์จะใช้ตารางเดียวกัน โดยที่ 4 บิตซ้ายสุดของไบต์นำเข้าจะชี้ที่แถว และ 4 บิตขวาสุดของไบต์นำเข้าจะชี้ที่สดมภ์ และค่าในตารางคือไบต์ส่งออกที่ใช้แทนที่ กล่องเอสที่ใช้ในการแทนที่ไบต์ ดังกล่าวแสดงในตารางที่ 6.4

- **การสลับที่ไบต์ (เลื่อนสดมภ์)** การสลับที่ไบต์ในเวิลด์พูลจะกระทำด้วยการเลื่อนไบต์ในแต่ละสดมภ์ โดยจำนวนไบต์ของการเลื่อนแต่ละครั้งคือตำแหน่งของสดมภ์ เช่น สดมภ์ที่ 0 จะไม่มีการเลื่อน สดมภ์ที่ 1 จะเป็นการเลื่อนไบต์ลง 1 ไบต์ สดมภ์ที่ 2 จะเป็นการเลื่อนไบต์ลง 2 ไบต์ จนถึง สดมภ์ที่ 7 จะเป็นการเลื่อนไบต์ลง 7 ไบต์

- **การผสมแถว** ขั้นตอนการแทนที่ไบต์และการเลื่อนไบต์ในแต่ละสดมภ์ที่กล่าวมานั้นเป็นการเปลี่ยนข้อมูลทั้งไบต์ ข้อมูลแต่ละบิตในไบต์ยังคงเหมือนเดิม ดังนั้นจึงจำเป็นต้องคละข้อมูลในแต่ละบิตใหม่ ด้วยวิธีการที่เรียกว่า ''การผสมแถว'' ด้วยการคูณแต่ละแถวด้วยเมตริกซ์ค่าคงที่ซึ่งจะได้

ตารางที่ 6.4: กล่องเอสเพื่อใช้ในการแทนที่ไบต์

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	18	23	C6	E8	87	B8	01	4F	36	A6	D2	F5	79	6F	91	52
1	60	BC	9B	8E	A3	0C	7B	35	1D	E0	D7	C2	2E	4B	FE	57
2	15	77	37	E5	9F	F0	4A	DA	58	C9	29	0A	B1	A0	6B	85
3	BD	5D	10	F4	CB	3E	05	67	E4	27	41	8B	A7	7D	95	D8
4	FB	EE	7C	66	DD	17	47	9E	CA	2D	BF	07	AD	5A	83	33
5	63	02	AA	71	C8	19	49	D9	F2	E3	5B	88	9A	26	32	B0
6	E9	0F	D5	80	BE	CD	34	48	FF	7A	90	5F	20	68	1A	AE
7	B4	54	93	22	64	F1	73	12	40	08	C3	EC	DB	A1	8D	3D
8	97	00	CF	2B	76	82	D6	1B	B5	AF	6A	50	45	F3	30	EF
9	3F	55	A2	EA	65	BA	2F	C0	DE	1C	FD	4D	92	75	06	8A
A	B2	E6	0E	1F	62	D4	A8	96	F9	C5	25	59	84	72	39	4C
B	5E	78	38	8C	D1	A5	E2	61	B3	21	9C	1E	43	C7	FC	04
C	51	99	6D	0D	FA	DF	7E	24	3B	AB	CE	11	8F	4E	B7	EB
D	3C	81	94	F7	B9	13	2C	D3	E7	6E	C4	03	56	44	7F	A9
E	2A	BB	C1	53	DC	0B	9D	6C	31	74	F6	46	AC	89	14	E1
F	16	3A	69	09	70	B6	D0	ED	CC	42	98	A4	28	5C	F8	86

แถวใหม่ โดยเมตริกซ์ค่าคงที่ดังกล่าวแสดงดังรูปที่ 6.1 การคูณเมทริกซ์ดังกล่าวคล้ายกับการ

$$M_{Constant} = \begin{bmatrix} 01 & 01 & 04 & 01 & 08 & 05 & 02 & 09 \\ 09 & 01 & 01 & 04 & 01 & 08 & 05 & 02 \\ 02 & 09 & 01 & 01 & 04 & 01 & 08 & 05 \\ 05 & 02 & 09 & 01 & 01 & 04 & 01 & 08 \\ 08 & 05 & 02 & 09 & 01 & 01 & 04 & 01 \\ 01 & 08 & 05 & 02 & 09 & 01 & 01 & 04 \\ 04 & 01 & 08 & 05 & 02 & 09 & 01 & 01 \\ 01 & 04 & 01 & 08 & 05 & 02 & 09 & 01 \end{bmatrix}$$

รูปที่ 6.1: เมตริกซ์ค่าคงที่

คูณเมทริกซ์ปกติแต่หากเป็นการคูณเมทริกซ์ซึ่งผลลัพธ์อยู่ใน จีเอฟ(2^8) ซึ่งสามารถคำนวณได้ดังรายละเอียดในหัวข้อที่ 4.1.2 โดยที่ค่าที่นำมาเอ็กซ์ออร์ในการคูณ คือ 00011101 (ต่างกับเออีเอสซึ่งเอ็กซ์ออร์กับ 00011011)

- **การผสมกุญแจ** กุญแจในแต่ละรอบของเวิลด์พูลมีความยาว 512 บิตเสมอซึ่งอยู่ในรูปของเมทริกซ์ 8×8 โดยที่การผสมกุญแจ คือ การเอ็กซ์ออร์ค่ากุญแจแต่ละไบต์เข้ากับแต่ละค่าของสเตท

การสร้างกุญแจประจำรอบ

วิธีการสร้างกุญแจของเวิลด์พูลจะแตกต่างจากเออีเอสโดยสิ้นเชิง โดยที่ เวิลด์พูลจะสร้างกุญแจ 11 ดอก โดยดอกแรกก็คือกุญแจนำเข้า ส่วนกุญแจดอกที่เหลือจะเป็นการเข้ารหัสเหมือนกับการเข้ารหัสแต่ละรอบ ยกเว้นกุญแจที่ใช้จะเป็นเมทริกซ์ค่าคงที่ขนาด 8×8 โดยที่แถวแรก จะใช้ค่าจากตารางที่ 6.4 โดยค่าของรอบ R สดมภ์ J จะเกิดจากค่าตำแหน่งที่ $8 \times (R-1) + J$ ของตารางดังกล่าว หรือกล่าวอีกนัยหนึ่งว่า แถวแรกของกุญแจรอบแรก คือ 8 ค่าแรกในตาราง แถวแรกของกุญแจรอบที่สอง คือ 8 ค่าถัดไปในตาราง เป็นต้น สำหรับแถวอื่นๆ ของเมทริกซ์ค่าคงที่จะมีค่าเป็น 0

6.3 ลายมือชื่อดิจิทัล

การลงลายมือชื่อกำกับเอกสาร เป็นการระบุว่าเอกสารนั้นถูกเขียนโดยบุคคลนั้นจริง ซึ่งเราสามารถตรวจสอบลายมือชื่อ เพื่อพิสูจน์ตัวจริงว่าเอกสารนั้นถูกเขียนโดยบุคคลนั้นจริง ในโลกดิจิทัล หากผู้ส่งต้องการส่งข้อมูลให้ผู้รับ ผู้รับสามารถพิสูจน์ว่าข้อมูลนั้นมาจากผู้ส่งตัวจริง โดยให้ผู้ส่งลงลายมือชื่อกำกับ ซึ่งลายมือชื่อดังกล่าวเรียกว่า ''ลายมือชื่อดิจิทัล'' ลายมือชื่อดิจิทัลนั้นอาจมีความแตกต่างกับลงลายมือชื่อในเอกสาร เช่น ลายมือชื่อปกติจะปรากฏอยู่ในเอกสาร ในขณะที่ลายมือชื่อดิจิทัลจะส่งแยกกับข้อมูล ผู้รับลายมือชื่อดิจิทัลสามารถพิสูจน์ตัวจริงโดยไม่ต้องมีลายมือชื่อตัวอย่างเก็บไว้เหมือน

การลงลายมือชื่อในเอกสาร ลายมือชื่อในเอกสารจะเหมือนกันทุกเอกสารในขณะที่ลายมือชื่อดิจิทัลจะแตกต่างกันในแต่ละข้อความ เป็นต้น

วิธีการลงลายมือชื่อดิจิทัลจะอาศัยการเข้ารหัสแบบอสมมาตรโดยใช้กุญแจส่วนตัวของผู้ส่งในการเข้ารหัส และกุญแจสาธารณะของผู้ส่งในการถอดรหัส ซึ่งผู้รับจะมั่นใจได้ว่าข้อความดังกล่าวมาจากผู้ส่ง เนื่องจากผู้ส่งเป็นบุคคลเดียวที่มีกุญแจส่วนตัวสำหรับการเข้ารหัส (ซึ่งจะต่างกับการเข้ารหัสแบบอสมมาตรเพื่อรักษาความลับซึ่งจะใช้กุญแจของผู้รับเพียงฝ่ายเดียว) แต่เนื่องจากการเข้ารหัสแบบอสมมาตรกับข้อความใหญ่จะค่อนข้างช้า ดังนั้นการการลงลายมือชื่อดิจิทัล จึงนิยมใช้กับไดเจสต์ของข้อความที่ผ่านแฮชฟังก์ชันแทน ซึ่งการใช้ลายมือชื่อดิจิทัลสามารถใช้เพื่อการพิสูจน์ตัวจริงของผู้ส่ง และบูรณภาพของข้อความ สำหรับการป้องกันการปฏิเสธความรับผิดชอบ จำเป็นต้องใช้คนกลางที่เชื่อถือได้ในการพิสูจน์ว่าผู้ส่งได้ส่งข้อความนั้นจริง ในทางปฏิบัติ การลงลายมือชื่อดิจิทัลนั้นสามารถทำได้หลายวิธี เช่น การเข้ารหัสด้วยวิธีอาร์เอสเอ เอลกามอล ชนอร์ ดีเอสเอส และ อีซีซี ซึ่งทุกวิธีจะใช้กุญแจส่วนตัวของผู้ส่งในการลงลายมือชื่อ และ กุญแจสาธารณะของผู้ส่งในการตรวจสอบ

6.4 สรุป

บทนี้ได้กล่าวถึง บูรณภาพและการพิสูจน์ตัวจริงของสาร แฮชฟังก์ชันกลุ่มต่างๆ ได้แก่ กลุ่มแฮชฟังก์ชันที่ออกแบบฟังก์ชันย่อยใหม่โดยเฉพาะ และ กลุ่มแฮชฟังก์ชันที่อาศัยการเข้ารหัสที่มีอยู่แล้ว นอกจากนั้นในบทนี้ยังได้กล่าวถึงเทคนิคที่เรียกว่า ลายมือชื่อดิจิทัล เพื่อการตรวจสอบบูรณภาพของสาร และการพิสูจน์ตัวจริงของสาร

6.5 แบบฝึกหัด

1. จงคำนวณหาจำนวนแพดดิ้งของ ชา-1 และ เวิลด์พูลในกรณีต่อไปนี้

   (a) ข้อความซึ่งมีความยาว 5120 บิต

   (b) ข้อความซึ่งมีความยาว 5121 บิต

   (c) ข้อความซึ่งมีความยาว 6143 บิต

2. จงเปรียบเทียบความแตกต่างของเออีเอส และ เวิลด์พูล ในประเด็น ขนาดบล็อก ขนาดกุญแจ วิธีการสร้างกุญแจ จำนวนรอบ วิธีการเปลี่ยนสเตท

3. จงเปรียบเทียบวิธีการใช้กุญแจของการเข้ารหัสแบบอสมมาตร เพื่อการรักษาความลับ และ ลายมือชื่อดิจิทัล

4. จงคำนวณหาค่า e ด้วยวิธีอาร์เอสเอ โดยที่ p=809, q=751, d=23 จากนั้นให้ใช้วิธีอาร์เอสเอเพื่อลงลายมือชื่อดิจิทัลของข้อความในกรณีต่อไปนี้

   (a) ลายมือชื่อ S_1 ข้อความ M_1 คือ 50

   (b) ลายมือชื่อ S_2 ข้อความ M_2 คือ 100

   (c) จงพิสูจน์ว่า หาก $M = M_1 \times M_2$ หรือ M=5000 แล้ว $S = S_1 \times S_2$

5. เหตุใดจึงไม่สามารถใช้กุญแจแบบสมมาตรในการลงลายมือชื่อดิจิทัลได้

6. หากค่า a,b และ c มีค่าเป็น 0x0123456789ABCDEF จงคำนวณหาค่าต่อไปนี้ใน ชา-512

   (a) ค่า Maj(a,b,c)

   (b) ค่า Rot(a)

   (c) ค่า Con(a,b,c)

บทที่ 7

การพิสูจน์ตัวจริงของเอนทิตีและการจัดการกุญแจ

- การพิสูจน์ตัวจริงของเอนทิตี
- การจัดการกุญแจ

บทที่ 7

การพิสูจน์ตัวจริงของเอนทิตีและการจัดการกุญแจ

ในบทนี้จะกล่าวถึงการพิสูจน์ตัวจริงของเอทิตีและการจัดการกุญแจ ซึ่งโพรโทคอลในการจัดการกุญแจส่วนใหญ่ จะใช้โพรโทคอลในการพิสูจน์ตัวจริงของเอนทิตี

7.1 การพิสูจน์ตัวจริงของเอนทิตี

การพิสูจน์ตัวจริงของเอนทิตี หมายถึง เทคนิคในการที่ฝ่ายหนึ่งพิสูจน์ตัวจริงของอีกฝ่ายหนึ่ง ซึ่งเอนทิตีในที่นี้อาจเป็นบุคคล กระบวนการ เครื่องบริการ เครื่องรับบริการ ซึ่งเอนทิตีที่ถูกพิสูจน์ จะเรียกว่า ''เคลมอน'' ในขณะที่เอนทิตีซึ่งเป็นผู้ตรวจสอบจะเรียกว่า ''เวอริฟายเออร์'' การพิสูจน์ตัวจริงของเอนทิตี จะต่างกับการพิสูจน์ตัวจริงของสาร (ดังแสดงรายละเอียดในหัวข้อ 6.1.2) การพิสูจน์ตัวจริงของเอนทิตี ต้องกระทำในทันทีทันใด (เช่น การพิสูจน์ตัวจริงของผู้ใช้บริการตู้เอทีเอ็ม) ในขณะที่การพิสูจน์ตัวจริงของสารนั้นจะกระทำเมื่อใดก็ได้ (เช่น การพิสูจน์ตัวจริงของผู้ส่งไปรษณีย์อิเล็กทรอนิกส์) การพิสูจน์ตัวจริงของสารนั้นต้องทำทุกข้อความ ในขณะที่การพิสูจน์ตัวจริงของเอนทิตีสามารถกระทำครั้งเดียว เป็นต้น

การพิสูจน์ตัวจริงของเอนทิตีสามารถกระทำได้ 3 วิธี คือ การพิสูจน์สิ่งที่รู้ การพิสูจน์สิ่งที่มี และการพิสูจน์สิ่งที่เป็น

- **การพิสูจน์สิ่งที่รู้** หมายถึง การที่เวอริฟายเออร์ตรวจสอบสิ่งที่เคลมอนรู้ เช่น รหัสผ่าน พินกุญแจลับ กุญแจส่วนตัว เป็นต้น
- **การพิสูจน์สิ่งที่มี** หมายถึง การที่เวอริฟายเออร์ตรวจสอบสิ่งที่เคลมอนเป็นเจ้าของ เช่น หนังสือเดินทาง ใบขับขี่ บัตรประชาชน บัตรเครดิต บัตรสมาร์ต เป็นต้น

- **การพิสูจน์สิ่งที่เป็น** หมายถึง การที่เวอริฟายเออร์ตรวจสอบสิ่งที่เคลมอนเป็นตามธรรมชาติ หรือลักษณะของเคลมอน เช่น การตรวจสอบลายเซ็น ลายนิ้วมือ เสียง รูปหน้า จอตา ลายมือ เป็นต้น

7.1.1 รหัสผ่าน

วิธีการใช้รหัสผ่านถือว่าเป็นวิธีที่เก่าที่สุดและง่ายที่สุดในการพิสูจน์ตัวจริง รหัสผ่านเป็นหนึ่งในวิธีการพิสูจน์สิ่งที่เคลมอนรู้ซึ่งสามารถแบ่งได้เป็นสองประเภท คือ รหัสผ่านคงที่ และ รหัสผ่านครั้งเดียว

รหัสผ่านคงที่

รหัสผ่านคงที่เป็นรหัสผ่านถูกใช้ซ้ำๆ ในการพิสูจน์ตัวจริง เช่น หากต้องการเข้าถึงเครื่องคอมพิวเตอร์ ผู้ใช้จะพิสูจน์ตัวจริงด้วยการกรอกรหัสผ่าน โดยใช้รหัสผ่านเดิมทุกครั้ง วิธีการใช้งานรหัสผ่านคงที่สามารถแบ่งได้เป็นหลายวิธี ได้แก่

- **ตารางเก็บรหัสผ่าน** เพื่อใช้ในการตรวจสอบบัญชีผู้ใช้และรหัสผ่านเมื่อมีผู้ใช้งาน แต่วิธีการดังกล่าวสามารถถูกโจมตีได้ เช่น การถูกดักจับรหัสผ่าน การขโมยรหัสผ่านจากผู้ใช้ (รหัสผ่านยาวเกินไปจะทำให้ผู้ใช้จำไม่ได้และต้องจดลงกระดาษซึ่งเสี่ยงต่อการถูกขโมย) การเข้าถึงตารางหรือแฟ้มข้อมูลที่เก็บรหัสผ่านซึ่งผู้โจมตีสามารถอ่านหรือแก้ไขรหัสผ่านที่ต้องการได้ การเดารหัสผ่าน (รหัสผ่านสั้นเกินไปจะทำให้เสี่ยงต่อการเดารหัสผ่านด้วยการลองทุกรหัสผ่านที่เป็นไปได้)
- **เก็บแฮชแทนรหัสผ่าน** เพื่อป้องกันเข้าถึงแฟ้มข้อมูลที่เก็บรหัสผ่าน โดยการเก็บแฮชของรหัสผ่านแทนรหัสผ่านจริงๆ ในแฟ้มข้อมูลดังกล่าว แต่อย่างไรก็ตามวิธีนี้ก็ยังคงเสี่ยงต่อการโจมตีด้วยวิธีการเดารหัสผ่าน เช่น การใช้พจนานุกรมเพื่อเดารหัสผ่านที่เป็นไปได้
- **เพิ่มความยาวรหัสผ่านก่อนแฮช** วิธีการนี้จะทำให้การเดารหัสผ่านทำได้ยากมากขึ้น ด้วยการเพิ่มความยาวของรหัสผ่าน ตัวอักขระที่เพิ่มต่อเข้าไปกับรหัสผ่านจะเรียกว่า ''ซอล์ท''
- **การใช้งานสองวิธีขึ้นไป** เช่น การพิสูจน์ตัวจริงด้วยสิ่งที่รู้และสิ่งที่มีด้วยการใช้บัตรเอทีเอ็ม เพื่อถอนเงินซึ่งจำเป็นต้องอาศัยสิ่งที่รู้ (รหัสผ่านหรือพิน) และสิ่งที่มี (บัตรเอทีเอ็ม) ในปัจจุบันธนาคารบางแห่งยังเพิ่มการพิสูจน์สิ่งที่เป็น เช่น มีการตรวจสอบลายนิ้วมือควบคู่กับการใช้บัตรเอทีเอ็มและการกดพิน

รหัสผ่านครั้งเดียว

รหัสผ่านครั้งเดียวหมายถึงการใช้งานรหัสผ่านแต่ละรหัสเพียงครั้งเดียวหลังจากนั้น รหัสดังกล่าวจะไม่ถูกนำกลับมาใช้ซ้ำ รหัสผ่านครั้งเดียวสามารถใช้งานได้หลายวิธี ได้แก่

- **การใช้รายการรหัสผ่าน** โดยทั้งเคลมอนและเวอริฟายเออร์จะต้องการรายการของรหัสผ่านทั้งหมดที่จะใช้ หากรหัสผ่านใดถูกใช้ไปแล้วรหัสผ่านนั้นจะไม่ถูกนำกลับมาใช้อีก
- **การใช้ห่วงโซ่รหัสผ่าน** โดยที่เริ่มต้นทั้งเคลมอนและเวอริฟายเออร์จะตกลงการใช้รหัสผ่านตัวแรก ในขณะที่เข้าใช้งานด้วยรหัสผ่านตัวแรกแล้วจะมีการสร้างรหัสผ่านตัวที่สอง เมื่อมีการเข้าใช้งานด้วยรหัสผ่านตัวที่สองจะมีการสร้างรหัสผ่านตัวที่สามอัตโนมัติไปเรื่อยๆ
- **การใช้ห่วงโซ่แฮช** โดยที่เริ่มต้นทั้งเคลมอนและเวอริฟายเออร์จะตกลงการใช้รหัสผ่านตัวแรก ในขณะที่เข้าใช้งานด้วยรหัสผ่านตัวแรกแล้วจะมีการสร้างรหัสผ่านตัวที่สอง ด้วยการแฮชรหัสผ่านตัวแรก เมื่อมีการเข้าใช้งานด้วยรหัสผ่านตัวที่สองจะมีการสร้างรหัสผ่านตัวที่สาม ด้วยการแฮชรหัสผ่านต่อก่อนหน้าแบบอัตโนมัติไปเรื่อยๆ

7.1.2 การท้าทายและตอบโต้

การพิสูจน์ตัวจริงด้วยรหัสผ่านนั้น เคลมอนต้องบอกรหัสผ่านให้เวอริฟายเออร์ซึ่งรหัสผ่านดังกล่าวอาจถูกดักจับระหว่างทางได้ วิธีการท้าทายและตอบโต้เป็นวิธีการพิสูจน์ตัวตนโดยที่เคลมอน ไม่ต้องส่งความลับใดๆ มาให้เวอริฟายเออร์ เวอริฟายเออร์จะเริ่มส่งคำท้าทายไปให้เคลมอน ซึ่งคำท้าทายดังกล่าวจะเป็นค่าที่ขึ้นกับเวลา เช่น เวลาขณะนั้น จากนั้นเมื่อเคลมอนได้รับคำท้าทาย เคลมอนจะนำคำท้าทายดังกล่าวคำนวณด้วยฟังก์ชันบางอย่างแล้วตอบโต้กลับมายังเวอริฟายเออร์ เวอริฟายเออร์จะตรวจสอบคำตอบโต้ดังกล่าวว่าถูกต้องหรือไม่ ถ้าถูกต้องแสดงว่าเคลมอนนั้นเป็นตัวจริง วิธีการท้าทายและตอบโต้สามารถกระทำได้หลายรูปแบบ ได้แก่ การใช้การเข้ารหัสด้วยกุญแจสมมาตร การใช้แฮชฟังก์ชันแบบมีกุญแจ การใช้การเข้ารหัสด้วยกุญแจอสมมาตร การใช้ลายมือชื่อดิจิทัล

การใช้การเข้ารหัสด้วยกุญแจสมมาตร

วิธีการท้าทายและตอบโต้โดยการใช้การเข้ารหัสด้วยกุญแจแบบสมมาตร สามารถกระทำโดย เวอริฟายเออร์ส่งคำท้าทายไปให้เคลมอน ซึ่งคำท้าทายดังกล่าวอาจเป็นตัวเลขสุ่มซึ่งแปรผันตามเวลา แล้วเคลมอนเข้ารหัสตัวเลขสุ่มดังกล่าวด้วยกุญแจแบบสมมาตรที่รู้กันระหว่างเคลมอนและเวอริฟายเออร์ จากนั้นเคลมอนจะส่งตัวเลขสุ่มที่เข้ารหัสแล้วกับมายังเวอริฟายเออร์เพื่อตรวจสอบ นอกจากนั้นหากนาฬิกาของเครื่องเคลมอนและเวอริฟายเออร์ตรงกันแล้ว เคลมอนอาจจะส่งเวลาซึ่ง เข้ารหัสด้วยกุญแจที่รู้กันระหว่างเคลมอนและเวอริฟายเออร์มาให้เวอริฟายเออร์เพื่อตรวจสอบ โดยไม่ต้องรอคำท้าทายจากเวอริฟายเออร์ก็ได้ ในบางครั้งทั้งเคลมอนและเวอริฟายเออร์จำเป็นต้อง พิสูจน์ตัวจริงทั้งสอบฝ่ายกล่าวคือ เวริฟายเออร์ส่งคำท้าทายมายังเคลมอนจากนั้นเคลมอนจะตอบโต้กลับ ด้วยคำท้าทายของเวอริฟายเออร์และคำท้าทายของตัวเองซึ่งถูกเข้ารหัสไว้ เมื่อเวอริฟายเออร์ตรวจสอบเคลมมอนเรียบร้อยแล้ว จะตอบ

กลับคำท้าทายของเคลมอนด้วยการเข้ารหัสคำท้าทายดังกล่าวกลับไปยังเคลมอน เพื่อให้เคลมอนพิสูจน์ตัวจริงของเวอริฟายเออร์

การใช้แฮชฟังก์ชันแบบมีกุญแจ

นอกจากการใช้การเข้ารหัสด้วยกุญแจแบบสมมาตรแล้ว แฮชฟังก์ชันแบบมีกุญแจก็ยังเป็นอีกวิธีหนึ่งซึ่งถูกนำมาใช้ในการท้าทายและตอบโต้ ด้วยการที่เคลมอนส่งข้อความพร้อมด้วยไดเจสท์ของข้อความนั้น ซึ่งถูกแฮชพร้อมกับกุญแจที่รู้กันระหว่างเคลมอนและเวอริฟายเออร์ เมื่อเวอริฟายเออร์ได้รับข้อความกับไดเจสท์จะตรวจสอบทั้งสองสิ่งด้วยการแฮชข้อความนั้น ด้วยกุญแจแล้วเปรียบเทียบกับไดเจสท์ที่ได้ หากไดเจสท์ตรงกันแสดงว่าเคลมอนนั้นเป็นตัวจริง

การใช้การเข้ารหัสด้วยกุญแจอสมมาตร

การเข้ารหัสด้วยกุญแจอสมมาตรสามารถนำมาใช้ในการท้าทายและตอบโต้ด้วยการที่เวอริฟายเออร์ สร้างตัวอักษรสุ่มแล้วเข้ารหัสด้วยกุญแจสาธารณะของเคลมอนเพื่อส่งไปให้เคลมอน เมื่อเคลมอนได้รับก็จะถอดรหัสด้วยกุญแจส่วนตัวของตัวเอง และส่งข้อความตอบโต้กลับไปหาเวอริฟายเออร์ด้วยข้อความสุ่มที่เวอริฟายเออร์ส่งมาตอนแรก นอกจากนั้นยังอาจมีการตรวจสอบกันทั้งสองฝ่ายกล่าวคือ เวอริฟายเออร์ตรวจสอบเคลมอนและเคลมอนตรวจสอบเวอริฟายเออร์ด้วยกุญแจของทั้งสองฝ่าย คล้ายกับการตรวจสอบด้วยกุญแจแบบสมมาตรที่ได้กล่าวไปแล้ว

การใช้ลายมือชื่อดิจิทัล

อีกวิธีหนึ่งที่ถูกนำมาใช้ในการท้าทายและตอบโต้คือการใช้ลายมือชื่อดิจิทัลด้วยการที่เวอริฟายเออร์ ส่งข้อความสุ่มไปให้เคลมอน จากนั้นเคลมอนจะลงลายมือชื่อดิจิทัลด้วยกุญแจส่วนตัวของตัวเอง เพื่อให้เวอริฟายเออร์ตรวจสอบด้วยกุญแจสาธารณะของเคลมอน

7.1.3 ความรู้เป็นศูนย์

อีกวิธีหนึ่งในการพิสูจน์ตัวจริงสำหรับเอนทิติ คือ ความรู้เป็นศูนย์ ซึ่งเป็นการที่เวอริฟายเออร์พิสูจน์เคลมอนโดยเคลมอนไม่จำเป็นต้องเปิดเผยข้อมูลใดๆ ทั้งสิ้นกับเวอริฟายเออร์ ปัจจุบันมีผู้คิดค้นวิธีการดังกล่าวหลายโพรโทคอล ได้แก่ โพรโทคอล เฟียท์-ชเมียร์ โพรโทคอล กุยลู-ควิสควอเตอร์ เป็นต้น

7.1.4 โพรโทคอล เฟียท์-ชเมียร์

การทำงานของโพรโทคอล เฟียท์-ชเมียร์ เริ่มต้นจากการที่เคลมอนคำนวณกุญแจสาธารณะ และ กุญแจส่วนตัวของตนเอง โดยกำหนดค่า n ซึ่งเกิดจากจำนวนเฉพาะ 2 ตัวคูณกัน แล้วเลือกค่า s ซึ่งอยู่ระหว่าง 1 กับ n-1 เพื่อใช้เป็นกุญแจส่วนตัวพร้อมกับคำนวณกุญแจสาธารณะ v จากสมการ $v = s^2 \bmod n$

เมื่อต้องการจะพิสูจน์ตัวจริง เคลมอนเลือกเลขสุ่ม r (ซึ่งมีค่าอยู่ระหว่าง 0 กับ n-1) พร้อมกับคำนวณหาค่า x จากสมการ $x = r^2 \bmod n$ และส่งค่า x ไปให้เวอริฟายเออร์ เมื่อเวอริฟายเออร์ได้รับค่า x ก็จะส่งคำท้าทาย c (มีค่าเป็น 0 หรือ 1) ไปยังเคลมอน เคลมอนจะโต้ตอบกับด้วยค่า y ซึ่งคำนวณจาก $y = rs^c \bmod n$ เมื่อเวอริฟายเออร์ได้รับค่า y ก็จะตรวจสอบค่าที่ได้รับว่า $y^2 \bmod n$ มีค่าเท่ากับ $xv^c \bmod n$ หรือไม่ หากค่าทั้งสองมีค่าไม่เท่ากับแสดงว่าเคลมอนเป็นตัวปลอม แต่หากเท่ากันก็จะเริ่มกระบวนวนซ้ำหลายๆ รอบ โดยเปลี่ยนค่า c ไปเรื่อยๆ ซึ่งเวอริฟายเออร์จะต้องตรวจสอบค่าที่ได้รับให้ถูกทุกรอบจึงจะถือว่าเคลมอนเป็นตัวจริง นอกจากนั้นยังมีผู้ปรับปรุงโพรโทคอลดังกล่าว เช่น โพรโทคอลของ พิซ-เฟียท์-ชเมียร์ ซึ่งจะใช้เวกเตอร์ของกุญแจส่วนตัว $(s_1, s_2, \ldots, s_k)$ เวกเตอร์ของกุญแจสาธารณะ $(v_1, v_2, \ldots, v_k)$ และเวกเตอร์ของคำท้าทาย $(c_1, c_2, \ldots, c_k)$ แทนค่าต่างๆ เพียงค่าเดียว(ไม่ใช่เวกเตอร์) โดยที่การเริ่มต้นคล้ายกับวิธีต้นฉบับ ยกเว้นหลังจากที่เวอริฟายเออร์ได้รับค่า x แล้วจะตอบกลับเป็นเวกเตอร์ของคำท้าทาย $(c_1, c_2, \ldots, c_k)$ เมื่อเคลมอนได้รับเวกเตอร์ดังกล่าวก็โต้ตอบกลับด้วยค่า y ซึ่งคำนวณจาก $y = (rs_1^{c_1} s_2^{c_2} \ldots s_k^{c_k}) \bmod n$ เมื่อเวอริฟายเออร์ได้รับค่า y แล้วจะพิสูจน์ตัวจริงของเคลมอนจากการเปรียบเทียบค่า x กับ $y^2 v_1^{c_1} v_2^{c_2} \ldots v_k^{c_k} \bmod n$ ว่าเป็นค่าเดียวกันหรือไม่ โดยทำแบบนี้หลายๆ รอบซึ่งจะต้องผ่านการตรวจสอบทุกรอบจึงจะถือได้ว่าเคลมอนเป็นเอนทิตีจริง

7.1.5 โพรโทคอล กุยลู-ควิสควอเตอร์

การทำงานของโพรโทคอล กุยลู-ควิสควอเตอร์ นั้นคล้ายกับโพรโทคอลเฟียท์-ชเมียร์ เริ่มต้นจากการที่เคลมอนคำนวณกุญแจสาธารณะ และ กุญแจส่วนตัวของตนเอง โดยกำหนดค่า n ซึ่งเกิดจากจำนวนเฉพาะ 2 ตัวคูณกัน (เรียก p และ q) จากนั้นกำหนดค่า e ซึ่งเป็นจำนวนเฉพาะสัมพัทธ์กับ ϕ โดยที่ $\phi = (p-1) \times (q-1)$ พร้อมทั้งเลือกค่า s และ v เพื่อเป็นกุญแจส่วนตัวและกุญแจสาธารณะตามลำดับ โดยที่ความสัมพันธ์ระหว่าง ค่า s และ v คือ $s^e \times v = 1 \bmod n$ หลังจากนั้นเคลมอนจะคำนวณหาค่า x จากสมการ $x = r^e \bmod n$ และส่งค่า x ไปให้เวอริฟายเออร์ เมื่อเวอริฟายเออร์ได้รับค่า x ก็จะส่งคำท้าทาย c (มีค่าอยู่ระหว่าง 1 กับ e) ไปยังเคลมอน เคลมอนจะโต้ตอบกับด้วยค่า y ซึ่งคำนวณจาก $y = rs^c \bmod n$ เมื่อเวอริฟายเออร์ได้รับค่า y ก็จะตรวจสอบค่าที่ได้รับว่า $y^e v^c$ มีค่าเท่ากับ x หรือไม่ หากค่าทั้งสองมีค่าไม่เท่ากับแสดงว่าเคลมอนเป็นตัวปลอม แต่หากเท่ากันก็จะเริ่มกระบวนวนซ้ำหลายๆ รอบ โดยเปลี่ยนค่า c ไปเรื่อยๆ ซึ่งเวอริฟายเออร์จะต้องตรวจสอบค่าที่ได้รับให้ถูกทุกรอบจึงจะถือว่าเคลมอนเป็นตัวจริง

7.1.6 ชีวมาตร

เทคนิคชีวมาตรเป็นการพิสูจน์ตัวจริงโดยใช้สิ่งที่เป็นของเอนทิตี ซึ่งสามารถเดาหรือขโมยได้ ซึ่งสามารถตรวจสอบได้ด้วยลักษณะทางกายภาพและพฤติกรรมของคนด้วยอุปกรณ์ตรวจสอบ เช่น เครื่องอ่าน

เครื่องรับรู้ อุปกรณ์ประมวลผลและจัดเก็บ ซึ่งถูกออกแบบสำหรับชีวมาตรโดยเฉพาะ โดยที่ก่อนใช้งานจำเป็นจะต้องมีการลงทะเบียนลักกษณะทางกายภาพ หรือ พฤติกรรมของบุคคลที่ต้องการจะตรวจสอบเอาไว้ล่วงหน้าก่อน

การใช้ลักษณะทางกายภาพ

การใช้ลักษณะทางกายภาพเพื่อการพิสูจน์ตัวจริงของบุคคล ควรจะใช้ลักษณะพิเศษซึ่งเป็นเอกลักษณ์ของแต่ละบุคคลและเปลี่ยนแปลงได้ยากเนื่องจาก อายุ การผ่าตัด ความเจ็บป่วย และ โรคต่างๆ ลักษณะดังกล่าว ได้แก่

- **ลายนิ้วมือ** การใช้ลายนิ้วมือเพื่อพิสูจน์ตัวบุคคลสามารถกระทำได้หลายวิธี เช่น การเก็บลักษณะของลายนิ้วมือว่าเริ่มตรงไหนสิ้นสุดที่ได้เกิดรอยแรกที่ใด การอ่านลายนิ้วมือเป็นรูปภาพ แล้วเปรียบเทียบรูปภาพลายนิ้วมือที่เก็บไว้ในฐานข้อมูล ถึงแม้ว่าลายนิ้วมือเป็นลักษณะพิเศษซึ่งใช้มากในปัจจุบัน แต่อย่างไรก็ตามลายนิ้วมือก็มีข้อเสียเนื่องจากสามารถเปลี่ยนแปลงได้ตามอายุ จากการได้รับบาดเจ็บ และ เป็นโรคบางชนิด
- **ม่านตา** ม่านตาเป็นลักษณะพิเศษซึ่งเป็นเอกลักษณ์ในแต่ละบุคคลซึ่งจะไม่เปลี่ยนตามอายุ ซึ่งการตรวจสอบดังกล่าวสามารถใช้ลำแสงอินฟราเรดเพื่อการอ่านม่านตา แต่อย่างไรก็ตาม ม่านตาก็สามารถเปลี่ยนแปลงได้เนื่องจากโรคตาบางชนิด เช่น ต้อกระจก
- **จอตา** วิธีนี้จะอาศัยการอ่านเส้นเลือดหลังตาเพื่อใช้ในการตรวจสอบตัวบุคคล แต่อย่างไรก็ตามวิธีการดังกล่าวยังไม่ค่อยได้รับความนิยมมากนักเนื่องจากอุปกรณ์ค่อนข้างมีราคาแพง
- **โครงหน้า** เทคนิคนี้จะอาศัยการวิเคราะห์ลักษณะของโครงหน้า โดยวัดระยะห่างระหว่างอวัยวะต่างๆ บนใบหน้า เช่น จมูก ปาก ตา เป็นต้น บางเทคนิคยังรวมการวิเคราะห์ผิวด้วย แต่อย่างไรก็ตามวิธีการดังกล่าว อาจมีข้อบกพร่องในเรื่องความถูกต้องได้
- **มือ** เทคนิคนี้จะอาศัยการวัดขนาดของมือ ความยาวของนิ้วมือ เพื่อการพิสูจน์ตัวบุคคล
- **เสียง** เทคนิคนี้จะวัดลักษณะเด่นของเสียง เช่น น้ำเสียง ระดับเสียง จังหวะการพูด ซึ่งอาจมีปัญหาในเรื่องความถูกต้องเนื่องจาก เสียงรบกวน อายุ และ ความเจ็บป่วย
- **ดีเอ็นเอ** ดีเอ็นเอถือว่าเป็นเทคนิคในการพิสูจน์ตัวจริงได้แม่นยำที่สุด ยกเว้น แฝดเหมือน ซึ่งจะมีดีเอ็นเอเหมือนกัน

การใช้ลักษณะทางพฤติกรรม

การใช้ลักษณะทางพฤติกรรมสามารถพิสูจน์ตัวจริงได้ เช่น การพิสูจน์ลายมือโดยการใช้อุปกรณ์ประเภทปากกาดิจิทัลซึ่งสามารถเปรียบเทียบลักษณะของลายเซ็น รวมถึงระยะเวลาของการเซ็นด้วย จังหวะการ

พิมพ์ดีดก็สามารถนำมาพิสูจน์ตัวจริงได้เช่นกัน เนื่องจากแต่ละคนใช้เวลาในการพิมพ์ น้ำหนักในการกดแป้นพิมพ์ อัตราการพิมพ์ผิดที่ไม่เท่ากัน แต่อย่างไรก็ตามวิธีนี้อาจไม่มีความถูกต้องมากนัก เนื่องจากความเร็วในการพิมพ์สามารถเปลี่ยนแปลงตามเวลาที่ฝึกฝนการพิมพ์ได้ และยังขึ้นกับตัวอักษรที่ต้องการพิมพ์อีกด้วย เป็นต้น

การวัดความถูกต้อง

การวัดความถูกต้องของเทคนิคทางชีวมาตรสามารถวัดได้ 2 วิธี คือ เอฟอาร์อาร์ และ เอฟเออาร์ indexอเฟอาร์อาร์@เอฟอาร์อาร์ indexอเฟเออาร์@เอฟเออาร์

- **เอฟอาร์อาร์** เป็นค่าที่ใช้วัดจำนวนครั้งของบุคคลซึ่งควรจะตรวจสอบได้แต่ตรวจสอบไม่ได้ ซึ่งนิยมแสดงผลเป็นร้อยละเทียบกับจำนวนครั้งทั้งหมด
- **เอฟเออาร์** เป็นค่าที่ใช้วัดจำนวนครั้งของบุคคลซึ่งควรจะตรวจสอบไม่ได้แต่ตรวจสอบได้ ซึ่งนิยมแสดงผลเป็นร้อยละเทียบกับจำนวนครั้งทั้งหมด

7.2 การจัดการกุญแจ

การเข้ารหัสด้วยกุญแจแบบสมมาตรนั้นจำเป็นต้องจัดการกุญแจ เช่น การจัดการกุญแจในกรณีที่ต้องการแลกเปลี่ยนข้อมูลกับหลายบุคคล การที่ทั้งผู้ส่งและผู้รับต้องหาวิธีในการตกลงกุญแจที่จะใช้ในการเข้ารหัส เป็นต้น ในขณะที่การเข้ารหัสด้วยกุญแจแบบอสมมาตรก็จำเป็นที่จะต้องหาวิธีให้ ผู้รับข้อความบอกกุญแจสาธารณะของตนเองให้กับผู้ที่ต้องการจะส่งข้อความลับมาให้ ซึ่งเรื่องราวดังกล่าวจะกล่าวถึงในหัวข้อต่อไปนี้

7.2.1 การแลกเปลี่ยนกุญแจในการเข้ารหัสแบบสมมาตร

ถึงแม้ว่าการเข้ารหัสด้วยกุญแจแบบสมมาตรจะสามารถเข้ารหัสได้รวดเร็วกว่าการเข้ารหัสแบบอสมมาตร แต่อย่างไรก็ตามการเข้ารหัสดังกล่าวจะเป็นจะต้องมีการจัดเก็บกุญแจที่ดีเนื่องจาก หากในระบบมีเครื่องที่ต้องการสื่อสารกัน n เครื่องจำเป็นต้องมีกุญแจ $\frac{(n-1)\times n}{2}$ ดอกเพื่อใช้ในการสื่อสารที่แต่ละคู่ใช้กุญแจดอกเดียวกัน โดยที่แต่ละเครื่องจะต้องเก็บรักษากุญแจ n-1 ดอก เพื่อติดต่อสื่อสารกับ n-1 เครื่องที่เหลือในระบบ การสื่อสารดังกล่าวสามารถใช้ศูนย์กลางการแลกเปลี่ยนกุญแจ (เคดีซี) เพื่อช่วยลดจำนวนกุญแจที่จัดเก็บในระบบทั้งหมด ซึ่งสามารถใช้งานได้ด้วยหลายโพรโทคอลซึ่งจะกล่าวในรายละเอียดถัดไป

ศูนย์กลางการแลกเปลี่ยนกุญแจ (เคดีซี)

ศูนย์กลางการแลกเปลี่ยนกุญแจ (เคดีซี) เป็นเครื่องที่เก็บรักษากุญแจ n ดอกซึ่งเป็นกุญแจที่ใช้สื่อสารระหว่าง แต่ละเครื่องกับศูนย์กลางดังกล่าว โดยที่แต่ละเครื่องไม่จำเป็นต้องเก็บรักษากุญแจของเครื่องอื่นที่เหลือ ยกเว้นเพียงกุญแจที่ใช้ในการติดต่อสื่อสารกับเคดีซีเท่านั้น หากที่เครื่องหนึ่งในระบบ ต้องการสื่อสารกับอีกเครื่องหนึ่ง เครื่องดังกล่าวจะติดต่อกับศูนย์กลางเพื่อขอกุญแจชั่วคราว ซึ่งกุญแจชั่วคราวดังกล่าวจะใช้ในการสื่อสารกับอีกเครื่องหนึ่งเพียงครั้งเดียวเท่านั้น โดยที่เครื่องทั้งสองจะใช้กุญแจชั่วคราวดอกเดียวกัน ในบางครั้งการใช้เคดีซีเพียงเครื่องเดียวอาจไม่เพียงพอในกรณีที่มีจำนวนผู้ใช้จำนวนมาก ดังนั้นในทางปฏิบัติแล้ว เคดีซีอาจมีมากกว่าหนึ่งเครื่องโดยการแบ่งเป็นโดเมน โดยที่เคดีซีแต่ละเครื่องจะรับผิดชอบเฉพาะผู้ใช้โดเมนของตนเอง เช่น เคดีซีหนึ่งเครื่องสำหรับผู้ใช้ทั้งหมดในโดเมนของมหาวิทยาลัยเทคโนโลยีสุรนารี เป็นต้น เครื่องเคดีซีทั้งหมดสามารถสื่อสารกันในกรณีที่มีการต้องการกุญแจข้ามโดเมน ซึ่งเครื่องเคดีซีทุกเครื่องสามารถจัดเรียงกันในรูปแบบของห่วงโซ่หรือรูปแบบของลำดับชั้นก็ได้

โพรโทคอลแบบง่าย

การใช้งานโพรโทคอลแบบง่ายโดยอาศัยเคดีซีซึ่งมีลำดับขั้นตอนดังนี้

1. เครื่องผู้ส่ง ส่งคำขอร้องการติดต่อกับเครื่องผู้รับ ไปให้เคดีซี (ไม่มีการเข้ารหัสใดๆ ทั้งสิ้น)
2. เครื่องเคดีซี ส่งกุญแจชั่วคราวและข้อความที่ถูกเข้ารหัสด้วยกุญแจของผู้รับ โดยที่ทั้งหมดเข้ารหัสด้วยกุญแจของผู้ส่ง ไปให้ผู้ส่ง
3. เครื่องผู้ส่งถอดรหัสด้วยกุญแจของตนเอง เก็บกุญแจชั่วคราวซึ่งเป็นกุญแจสำหรับใช้สื่อสารกับผู้รับ และส่งข้อความที่ถูกเข้ารหัสด้วยกุญแจของผู้รับไปให้ผู้รับ
4. เครื่องผู้รับจะถอดข้อความที่เข้ารหัสด้วยกุญแจของตนเอง ซึ่งจะพบกุญแจชั่วคราวสำหรับสื่อสารกับผู้ส่งอยู่ภายในนั้น

โพรโทคอลนีดแฮม-ชโรเดอร์

การใช้งานโพรโทคอลนีดแฮม-ชโรเดอร์ เป็นโพรโทคอลที่ใช้ตัวเลขสุ่มโดยอาศัยเคดีซีซึ่งมีลำดับขั้นตอนดังนี้

1. เครื่องผู้ส่ง ส่งคำร้องขอการติดต่อกับเครื่องผู้รับพร้อมข้อความสุ่ม ไปให้เคดีซี (โดยไม่มีการเข้ารหัสใดๆ ทั้งสิ้น)
2. เครื่องเคดีซี ส่งกุญแจชั่วคราว ข้อความที่ถูกเข้ารหัสด้วยกุญแจของผู้รับ และ ตัวเลขสุ่มที่ได้รับจากเครื่องผู้ส่ง โดยที่ทั้งหมดเข้ารหัสด้วยกุญแจของผู้ส่งไปให้ผู้ส่ง

3. เครื่องผู้ส่งถอดรหัสด้วยกุญแจของตนเอง เก็บกุญแจชั่วคราวซึ่งเป็นกุญแจสำหรับใช้สื่อสารกับผู้รับ และส่งข้อความที่ถูกเข้ารหัสด้วยกุญแจของผู้รับไปให้ผู้รับ
4. เครื่องผู้รับจะถอดข้อความที่เข้ารหัสด้วยกุญแจของตนเอง ซึ่งจะพบกุญแจชั่วคราวสำหรับสื่อสารกับผู้ส่งอยู่ภายในนั้น
5. เครื่องผู้รับทดลองส่งข้อความสุ่มซึ่งถูกเข้ารหัสด้วยกุญแจชั่วคราวกลับมาให้ผู้ส่ง
6. เครื่องผู้ส่งทดลองตอบกลับข้อความสุ่มโดยเข้ารหัสด้วยกุญแจชั่วคราวกลับมาให้ผู้รับ

โพรโทคอลของออทเวย์-รีส์

การใช้งานโพรโทคอลนีดแฮม-ชโรเดอร์ เป็นโพรโทคอลที่ใช้ตัวเลขสุ่มโดยอาศัยเคดีซีซึ่งมีลำดับขั้นตอนดังนี้

1. เครื่องผู้ส่ง ส่งตัวเลขสุ่มและข้อความที่เข้ารหัสด้วยกุญแจของตัวเองไปให้ผู้รับ
2. เครื่องผู้รับ ส่งข้อความที่เข้ารหัสด้วยผู้รับ และข้อความที่เข้ารหัสด้วยกุญแจของผู้ส่งที่ได้รับมาในขั้นตอนก่อนหน้านี้ไปยังเคดีซี
3. เคดีซี ถอดรหัสข้อความทั้งสองที่ได้รับจากผู้รับ เพื่อนำข้อความสุ่มที่อยู่ในแต่ละข้อความออกมา จากนั้นแบ่งข้อมูลเป็นสองชุด โดยชุดแรกประกอบด้วยตัวเลขสุ่มที่ได้รับจากผู้ส่งรวมกับกุญแจชั่วคราวแล้วเข้ารหัสด้วยกุญแจของผู้ส่ง อีกชุดประกอบด้วยตัวเลขสุ่มที่ได้รับจากผู้รับรวมกับกุญแจชั่วคราวแล้วเข้ารหัสด้วยกุญแจของผู้รับ โดยเคดีซีจะส่งข้อมูลทั้งสองชุดไปให้ผู้รับ
4. เครื่องผู้รับจะถอดข้อความที่เข้ารหัสด้วยกุญแจของตนเอง ซึ่งจะพบกุญแจชั่วคราวสำหรับสื่อสารกับผู้ส่งอยู่ภายในนั้น พร้อมทั้งส่งข้อมูลที่ถูกเข้ารหัสด้วยกุญแจของผู้ส่งไปให้ผู้ส่ง
5. เครื่องผู้ส่งจะถอดข้อความที่เข้ารหัสด้วยกุญแจของตนเอง ซึ่งจะพบกุญแจชั่วคราวสำหรับสื่อสารกับผู้รับอยู่ภายในนั้น
6. เครื่องผู้ส่งจะทดลองส่งข้อความสั้นๆ ซึ่งถูกเข้ารหัสด้วยกุญแจชั่วคราวไปให้ผู้รับ เพื่อแสดงให้ผู้รับเห็นว่าผู้ส่งมีกุญแจชั่วคราวดอกเดียวกับผู้รับ

7.2.2 เคอบีรอส

เคอบีรอสเป็นโพรโทคอลระบุตัวตนซึ่งสามารถเป็นเคดีซีได้ในตัวเอง โดยตั้งชื่อตามสุนัข 3 หัวซึ่งเฝ้าขุมนรกตามเทพนิยายกรีก โพรโทคอลเคบีรอสได้รับความนิยมมากและถูกใช้ในหลายระบบ เช่น วินโดวส์ 2000 ส่วนประกอบของเคอบีรอสประกอบด้วย เซิฟเวอร์ 3 ตัวได้แก่ เซิฟเวอร์สำหรับพิสูจน์ตัวตน

(เอเอส) เซิฟเวอร์สำหรับออกตั๋วชั่วคราว (ทีจีเอส) และเซิฟเวอร์ที่ผู้ใช้บริการต้องการใช้งานจริงๆ โดยเซิฟเวอร์สองตัวแรก (เอเอสและทีจีเอส) จะทำหน้าที่เป็นเคดีซี เอเอสจะทำหน้าที่พิสูจน์ตัวตนของผู้ใช้บริการ และแจกกุญแจชั่วคราวระหว่างผู้ใช้บริการกับทีจีเอส ทีจีเอสจะทำหน้าที่ออกตั๋วให้กับผู้ใช้บริการเพื่อใช้งานกับเซิฟเวอร์ที่ต้องการใช้บริการจริงๆ ซึ่งขั้นตอนการทำงานของเคอบีรอสทั้งหมดสามารถสรุปได้ดังนี้

1. ผู้ใช้บริการติดต่อไปยังเอเอส
2. เอเอสตอบกลับไปยังผู้ใช้บริการด้วยกุญแจชั่วคราวระหว่างผู้ใช้และทีจีเอส ข้อความที่ถูกเข้ารหัสด้วยกุญแจชั่วคราวระหว่างเอเอสกับทีจีเอส ซึ่งทั้งหมดจะถูกเข้ารหัสด้วยกุญแจระหว่างผู้ใช้บริการกับเอเอส
3. ผู้ใช้บริการจะส่งข้อความสุ่มที่เข้ารหัสด้วยกุญแจระหว่างผู้ส่งและทีจีเอส และ ข้อความที่ถูกเข้ารหัสด้วยกุญแจชั่วคราวระหว่างเอเอสกับทีจีเอส ไปให้ทีจีเอส
4. ทีจีเอสจะถอดรหัสด้วยกุญแจชั่วคราวระหว่างเอเอสกับทีจีเอส ซึ่งจะพบกุญแจกุญแจระหว่างผู้ใช้กับทีจีเอสอยู่ภายใน จากนั้นทีจีเอสจะส่งข้อความที่ถูกเข้ารหัสด้วยกุญแจระหว่างผู้ใช้กับทีจีเอสและข้อความที่ถูกเข้ารหัสด้วยทีจีเอสและเซิฟเวอร์ที่ให้บริการไปให้ผู้ใช้บริการ
5. ผู้ใช้บริการจะถอดรหัสข้อความที่ถูกเข้ารหัสด้วยกุญแจระหว่างผู้ใช้บริการกับทีจีเอส ซึ่งภายในจะพบกุญแจที่ใช้ระหว่างผู้ใช้บริการกับเซิฟเวอร์
6. ผู้ใช้บริการจะส่งข้อความที่ถูกเข้ารหัสด้วยทีจีเอสและเซิฟเวอร์ที่ให้บริการไปให้ผู้ให้บริการ พร้อมทั้งตัวเลขสุ่มซึ่งถูกเข้ารหัสด้วยกุญแจชั่วคราวกับเซิฟเวอร์ ไปให้เซิฟเวอร์ที่ให้บริการ
7. เซิฟเวอร์ที่ให้บริการจะถอดรหัสด้วยกุญแจระหว่างเซิฟเวอร์เองกับทีจีเอสซึ่งจะพบกุญแจชั่วคราวซึ่งสามารถใช้ระหว่างผู้ใช้บริการกับตัวเซิฟเวอร์เอง พร้อมทั้งตอบกลับตัวเลขสุ่มที่ได้รับโดยเข้ารหัสด้วยกุญแจชั่วคราวระหว่างผู้ใช้บริการกับเซิฟเวอร์

หากผู้ใช้ต้องการติดต่อกับเซิฟเวอร์หลายเครื่อง ผู้ใช้สามารถเริ่มต้นติดต่อกับทีจีเอสได้เลย โดยไม่ต้องเริ่มต้นติดต่อกับเอเอสอีก

7.2.3 การตกลงกุญแจในการเข้ารหัสแบบสมมาตร

การตกลงกุญแจในการเข้ารหัสแบบสมมาตรที่นิยมกันในปัจจุบันมีสองวิธี คือ การตกลงกุญแจด้วยวิธีเดฟฟี่-เฮลแมน และ การตกลงกุญแจด้วยวิธีจากเครื่องถึงเครื่อง ซึ่งวิธีการทั้งสองวิธีไม่จำเป็นต้องใช้เคดีซี

การตกลงกุญแจด้วยวิธีเดฟฟี่-เฮลแมน

การตกลงกุญแจด้วยวิธีเดฟฟี่-เฮลแมน เริ่มที่ทั้งสองฝ่ายเลือกเลขจำนวนเฉพาะขนาดใหญ่ p และเลขอีกจำนวนซึ่งเป็นรากปฐมฐานของ p เรียกว่า g โดยที่นิยามของรากปฐมฐาน g หมายถึงเลขซึ่งสามารถสร้างเลข 1 ถึง p-1 โดย สร้างจาก g mod p, g^2 mod p, ..., g^{p-1} mod p โดยที่ผลลัพธ์จะไม่ซ้ำกันและมีค่าตั้งแต่ 1 ถึง p ตัวอย่างเช่น หากค่า p คือ 7, เลข 3 จัดว่าเป็นรากปฐมฐานของ 7 เนื่องจาก $3^1 = 3 \equiv 3 \pmod 7$, $3^2 = 9 \equiv 2 \pmod 7$, $3^3 = 27 \equiv 6 \pmod 7$, $3^4 = 81 \equiv 4 \pmod 7$, $3^5 = 243 \equiv 5 \pmod 7$, $3^6 = 729 \equiv 1 \pmod 7$ ซึ่งจะได้เศษ คือ 3,2,6,4,5,1 ซึ่งมีค่าครบและไม่ซ้ำกันระหว่าง 1 ถึง (7-1) เป็นต้น โดยที่ค่า p และ g สามารถประกาศให้ทุกคนรู้ได้ จากนั้นผู้ส่งจะเลือกค่า x ($1 \leq x \leq p-1$) และ ผู้รับจะเลือกค่า y ($1 \leq y \leq p-1$) ซึ่งค่า x และ y จะถูกเก็บไว้ที่ตนเอง ผู้ส่งจะคำนวณหาค่า $R_1 = g^x$ mod p ส่งไปให้ผู้รับ ในขณะที่ผู้รับจะคำนวณหาค่า $R_2 = g^y$ mod p ส่งไปให้ผู้ส่ง ผู้ส่งจะคำนวณหาค่ากุญแจจาก $K = (R_2)^x$ mod p ในขณะที่ผู้รับจะคำนวณหาค่ากุญแจจาก $K = (R_1)^y$ mod p ซึ่งจริงๆ แล้วค่าของกุญแจที่ทั้งสองฝั่งตกลงกันก็คือ $K = g^{xy}$ mod p โพรโทคอลนี้อาจจะถูกโจมตีจากบุคคลตรงกลางหรือมือที่สาม กล่าวคือ ผู้โจมตีหลอกผู้ส่งว่าตัวเองเป็นผู้รับและหลอกผู้รับว่าตัวเองคือผู้ส่ง

การตกลงกุญแจด้วยวิธีจากเครื่องถึงเครื่อง

การตกลงกุญแจด้วยวิธีจากเครื่องถึงเครื่องนั้นอาศัยการทำงานของโพรโทคอลเดฟฟี่-เฮลแมน โดยเพิ่มการลงลายมือชื่อดิจิทัลเพื่อป้องกันการโจมตีจากบุคคลตรงกลาง ซึ่งข้อความที่แลกเปลี่ยนกันระหว่างผู้ส่งและผู้รับจะต้องถูกเซ็นด้วยกุญแจส่วนตัวของตนเองก่อนส่ง

7.2.4 การกระจายกุญแจสาธารณะ

วิธีการกระจายกุญแจสาธารณะมีหลายวิธี ได้แก่

- **การประกาศ** กุญแจสาธารณะสามารถประกาศตามสื่อต่างๆ เช่น บนเว็บไซต์หรือในหนังสือพิมพ์ แต่อย่างไรก็ตามวิธีการดังกล่าวอาจเสี่ยงอันตรายเนื่องจากไม่รู้ว่าจริงๆ แล้วให้เป็นคนประกาศกุญแจสาธารณะดังกล่าว
- **ศูนย์กลางที่เชื่อถือได้** กุญแจสาธารณะสามารถประกาศโดยอาศัยศูนย์กลางที่เชื่อถือได้ ซึ่งศูนย์กลางดังกล่าวจะจัดเก็บไว้ว่าใครเป็นเจ้าของกุญแจนั้นจริงๆ นอกจากนั้นวิธีการดังกล่าวยังสามารถเพิ่มความปลอดภัยด้วยการที่ศูนย์กลางดังกล่าว เซ็นตัวเลขสุ่มด้วยกุญแจส่วนตัวของศูนย์กลางเอง โดยตัวเลขสุ่มดังกล่าวจะถูกส่งมาจากผู้ที่ต้องการกุญแจสาธารณะของคนอื่น
- **ผู้มีอำนาจในการออกใบรับรอง** เพื่อป้องกันการที่ศูนย์กลางทำงานหนักเกินไปและการแก้ปัญหาการไม่เชื่อใจของกุญแจสาธารณะ เจ้าของสามารถไปขอใบรับรองจากผู้มีอำนาจในการออกใบรับรอง

เพื่อยืนยันว่ากุญแจสาธารณะดังกล่าวเป็นของตนจริงๆ โดยที่รูปแบบมาตรฐานของใบรับรองดังกล่าวจะเรียกว่า เอ็กซ์.509 ซึ่งประกอบไปด้วยฟิลด์หลายฟิลด์ ได้แก่ หมายเลขเวอร์ชัน หมายเลขซีเรียล รหัสของขั้นตอนวิธีที่ใช้ ผู้ที่ออกใบรับรอง เวลาที่ใบรับรองหมดอายุ เจ้าของใบรับรอง กุญแจสาธารณะของเจ้าของใบรับรอง หมายเลขประจำตัวผู้ออกใบรับรอง(ถ้ามี) หมายเลขประจำตัวของเจ้าของใบรับรอง(ถ้ามี) ส่วนขยาย(ถ้ามี) และ ลายเซ็น โดยที่ลายเซ็นดังกล่าวประกอบด้วยสามส่วน คือ ฟิลด์ที่ได้กล่าวไปแล้ว ไดเจสต์ของส่วนแรกซึ่งถูกเข้ารหัสด้วยกุญแจส่วนส่วนตัวของผู้ออกใบรับรอง และ ขั้นตอนวิธีที่ใช้ในส่วนที่สอง หากใบรับรองดังกล่าวใกล้หมดอายุ ผู้มีอำนาจในการออกใบรับรองจะออกประกาศใหม่ให้อัตโนมัติ (คล้ายกับบริษัทบัตรเครดิตที่จะออกบัตรเครดิตใหม่ให้เมื่อบัตรใกล้หมดอายุ) หากใบรับรองดังกล่าวถูกขโมยหรือกุญแจส่วนตัวที่เกี่ยวข้องกับใบรับรองถูกขโมย ใบรับรองดังกล่าวจะต้องถูกประกาศยกเลิก ในปัจจุบันเอ็กซ์.509 ได้เป็นพื้นฐานของใบรับรองสำหรับมาตรฐานการให้บริการที่เรียกว่า พีเคไอ ซึ่งทำหน้าที่ สร้าง กระจาย ยกเลิกใบรับรอง จัดเก็บกุญแจส่วนตัว ให้บริการกับโพรโทคอลอื่น รวมถึงวิธีการเข้าถึงข้อมูลที่ถูกจัดเก็บ ผู้ที่ออกใบรับรองสามารถมีได้มากกว่าหนึ่งแห่งโดยสามารถทำงานเป็นลำดับชั้นของความเชื่อใจกัน และสามารถตรวจสอบความเชื่อมโยงกันได้

7.3 สรุป

บทนี้ได้กล่าวถึง การพิสูจน์ตัวจริงของเอทิตีด้วยวิธีต่างๆ ได้แก่ รหัสผ่าน การท้าทายและตอบโต้ ความรู้เป็นศูนย์ โพรโทคอลเฟียท์-ชเมียร์ โพรโทคอลกุยลู-ควิสควอเตอร์ และชีวมาตร นอกจากนั้นบทนี้ยังได้กล่าวถึงการจัดการกุญแจ ซึ่งโพรโทคอลในการจัดการกุญแจส่วนใหญ่ จะใช้โพรโทคอลในการพิสูจน์ตัวจริงของเอนทิตี

7.4 แบบฝึกหัด

1. การใช้รหัสผ่านที่ยาวมากๆ มีข้อดีและข้อเสียอย่างไร
2. การเปลี่ยนรหัสผ่านบ่อยๆ มีข้อดีและข้อเสียอย่างไร
3. จงยกตัวอย่างวิธีการป้องกันการเดารหัสผ่าน
4. ข้อความสุ่มมีความสำคัญต่อการระบุตัวตนอย่างไร
5. หากการตกลงกุญแจด้วยวิธีเดฟฟี่-เฮลแมน มีค่า x=y จงพิสูจน์ว่า $R_1 = R_2$
6. หากการตกลงกุญแจด้วยวิธีเดฟฟี่-เฮลแมน มีค่า g=7, p=23, x=3, y=5 จงคำนวณหาค่า กุญแจ, ค่า R_1 และ R_2
7. หากการตกลงกุญแจด้วยวิธีเดฟฟี่-เฮลแมน มีค่า p=53 จงหาค่า g ที่เหมาะสม
8. หากการตกลงกุญแจด้วยวิธีเดฟฟี่-เฮลแมน มีค่า p=11 และค่า g=2
   (a) จงแสดงให้เห็นว่า 2 เป็นรากปฐมฐานของ 11
   (b) หากค่า R_1 มีค่าเท่ากับ 9 จงคำนวณหาค่า x
   (c) หากค่า R_2 มีค่าเท่ากับ 3 จงคำนวณหาค่าผลลัพธ์ของกุญแจที่ได้

บทที่ 8

ความมั่นคงในระบบเครือข่าย

- ความมั่นคงในระดับชั้นแอพพลิเคชัน
- ความมั่นคงในระดับชั้นทรานสปอร์ต
- ความมั่นคงในระดับชั้นเน็ตเวิร์ค

บทที่ 8

ความมั่นคงในระบบเครือข่าย

การใช้งานการเข้ารหัสทั้งหลายในปัจจุบันได้มุ่งเน้นไปที่ความมั่นคงในระบบเครือข่าย ระบบเครือข่ายที่ใช้กันในปัจจุบันอ้างอิงตาม แบบจำลองทีซีพี/ไอพี ซึ่งแบ่งเป็น 5 ลำดับชั้น เรียงจากบนลงล่างดังนี้

- **แอพพลิเคชัน** เป็นลำดับชั้นซึ่งให้บริการต่างๆ สำหรับซอฟต์แวร์หรือมนุษย์ที่ต้องการใช้งานเครือข่าย เช่น การให้บริการไปรษณีย์อิเล็กทรอนิคส์ การให้บริการถ่ายโอนแฟ้มข้อมูล เป็นต้น
- **ทรานสปอร์ต** เป็นลำดับชั้นที่รับผิดชอบในการส่งข้อมูลจะโปรเซสต้นทางไปยังโปรเซสปลายทาง ซึ่งโปรเซสในที่นี้หมายถึงโปรแกรมที่กำลังทำงานอยู่
- **เน็ตเวิร์ค** เป็นลำดับชั้นที่ทำหน้าที่ในการส่งข้อมูลจากเครื่องต้นทางไปยังเครื่องปลายทาง
- **เดต้าลิงค์** เป็นลำดับชั้นที่ทำหน้าที่ในการส่งกลุ่มของบิตระหว่างเครื่องที่อยู่ติดกัน
- **ฟิซิคอล** เป็นลำดับชั้นที่ทำหน้าที่ในการส่งบิตระหว่างเครื่องที่อยู่ติดกัน

การทำงานและคุณสัมบัติของลำดับชั้นฟิซิคอลและเดต้าลิงค์จะขึ้นกับอุปกรณ์เครือข่ายที่ใช้ สำหรับในเรื่องความมั่นคงปลอดภัยในระบบเครือข่ายจะสนใจเฉพาะลำดับชั้นที่ไม่ขึ้นอยู่กับอุปกรณ์เครือข่าย ได้แก่ ลำดับชั้นแอพพลิเคชัน ลำดับชั้นทรานสปอร์ต และ ลำดับชั้นเน็ตเวิร์ค

8.1 ความมั่นคงในระดับชั้นแอพพลิเคชัน

ในหัวข้อนี้จะกล่างถึงความมั่นคงในระดับชั้นแอพพลเคชันที่นิยมในบริการไปรษณีย์อิเล็กทรอนิกส์ 2 โพรโทคอล ได้แก่ พีจีพี ซึ่งเป็นโพรโทคอลที่ให้บริการด้านความมั่นคงที่นิยมใช้ในบริการไปรษณีย์อิเล็กทรอนิกส์ส่วนตัว ส่วนอีกโพรโทคอล คือ เอส/เอ็มไอเอ็มอี ซึ่งเป็นโพรโทคอลที่ให้บริการด้านความมั่นคงที่นิยมใช้ในระบบให้บริการไปรษณีย์อิเล็กทรอนิกส์ขององค์กร

การทำงานของบริการไปรษณีย์อิเล็กทรอนิกส์จะเริ่มจากผู้ส่งจะส่งข้อความไปยังเครื่องบริการไปรษณีย์อิเล็กทรอนิกส์ของเครือข่ายตนเอง จากนั้นเครื่องบริการไปรษณีย์อิเล็กทรอนิกส์ของผู้ส่ง จะส่งข้อความดังกล่าวไปให้เครื่องบริการไปรษณีย์อิเล็กทรอนิกส์ของผู้รับโดยจะถูกเก็บไว้ในตู้ไปรษณีย์ของผู้รับ และเมื่อผู้รับต้องการตรวจสอบไปรษณีย์อิเล็กทรอนิกส์ของตนเอง ผู้รับจะเข้าไปตรวจสอบตู้ไปรษณีย์ของตนเอง ซึ่งจะอยู่ในเครื่องบริการไปรษณีย์อิเล็กทรอนิกส์ของเครือข่ายผู้รับ เนื่องจากการทำงานของไปรษณีย์อิเล็กทรอนิกส์เป็นการทำงานแบบทางเดียว (ผู้รับไม่จำเป็นต้องตอบไปรษณีย์)และไม่มีการสร้างการเชื่อมต่อระหว่างผู้ส่งกับผู้รับ (ผู้ส่งและผู้รับไม่จำเป็นต้องทำงานพร้อมกัน) ดังนั้น โพรโทคอลที่ใช้ในการบริการไปรษณีย์อิเล็กทรอนิกส์จึงจำเป็นที่จะต้องคำนึงถึงลักษณะการทำงานดังกล่าวด้วย เช่น การตกลงว่าจะใช้การเข้ารหัสหรือแฮชฟังก์ชันรูปแบบใดจะต้องถูกส่งไปกับข้อความด้วย เนื่องจากไม่สามารถตกลงก่อนล่วงหน้าได้ การตกลงกุญแจระหว่างผู้ส่งกับผู้รับก็เป็นเรื่องที่สำคัญ บริการไปรษณีย์อิเล็กทรอนิกส์นิยมใช้การเข้ารหัสข้อความแบบสมมาตร เนื่องจากมีประสิทธิภาพดีกว่าแบบอสมมาตร แต่กุญแจที่ใช้จะต้องถูกเข้ารหัสด้วยกุญแจสาธารณะของผู้รับด้วยการเข้ารหัสแบบอสมมาตร

8.1.1 พีจีพี

พีจีพีเป็นโพรโทคอลซึ่งถูกคิดค้นโดย ฟิล ซิมเมอร์แมน ในการให้บริการด้านความมั่นคงปลอดภัยแก่บริการไปรษณีย์อิเล็กทรอนิกส์ เช่น บริการด้านความลับ บริการด้านบูรณภาพ บริการด้านการระบุตัวตนเพื่อตอบสนองความต้องการที่หลากหลายของผู้ใช้งาน ตั้งแต่การส่งไปรษณีย์แบบปกติไม่มีความมั่นคงปลอดภัย การส่งข้อความที่ต้องการความมั่นใจว่าข้อความดังกล่าวมิได้ถูกแก้ไขระหว่างทาง โดยที่ผู้ส่งต้องคำนวณหาไดเจสต์ของข้อความ พร้อมทั้งลงลายมือชื่อไดเจสต์ดังกล่าวด้วยกุญแจส่วนตัวของผู้ส่ง การส่งข้อความลับ ซึ่งพีจีพีจะอาศัยกุญแจชั่วคราวระหว่างผู้ส่งกับผู้รับโดยที่กุญแจดังกล่าว จะถูกเข้ารหัสด้วยกุญแจสาธารณะของผู้รับ กุญแจชั่วคราวดังกล่าว จะใช้ในการเข้ารหัสข้อความ (ซึ่งอาจจะถูกบีบอัด) กับได้เจสต์ของข้อความดังกล่าวซึ่งถูกลงลายมือชื่อด้วยกุญแจส่วนตัวของผู้ส่ง นอกจากนั้นพีจีพียังมีการให้บริการการบีบอัดข้อความ ซึ่งจริงๆ แล้วมิได้เกี่ยวอะไรกับความมั่นคงปลอดภัย แต่เป็นการลดปริมาณจราจรในช่องสัญญาณสื่อสาร บริการการแปลงรหัสตัวอักษรระหว่างแอสกีกับแรดิก-64 บริการการแบ่งขนาดของข้อความให้เหมาะสม เป็นต้น

พวงกุญแจของพีจีพี

พีจีพีได้ถูกออกแบบให้มีพวงกุญแจสองพวง คือ พวงกุญแจที่ไว้เก็บกุญแจส่วนตัว และ พวงกุญแจที่ไว้เก็บกุญแจสาธารณะ คนแต่ละคนสามารถมีคู่ของกุญแจส่วนตัวและกุญแจสาธาณะได้หลายคู่ เช่น คู่หนึ่งสำหรับติดต่อเรื่องงาน อีกคู่หนึ่งไว้สำหรับติดต่อเรื่องส่วนตัว เป็นต้น ซึ่งกุญแจแต่ละดอกก็จะถูกเก็บไว้ในพวงกุญแจที่เหมาะสม นอกจากนั้น กุญแจสาธารณะของคนอื่นที่เคยติดต่อก็จะถูกเก็บไว้ในพวงกุญแจสาธารณะของตนเองเช่นเดียวกัน

พวงกุญแจทั้งสองพวงดังกล่าวจะถูกเก็บในลักษณะของตาราง โดยที่ตารางของ พวงกุญแจส่วนตัว จะประกอบไปด้วย 5 ฟิลด์ได้แก่ ฟิลด์หมายเลขผู้ใช้ ซึ่งส่วนใหญ่นิยมเก็บหมายเลขที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ ฟิลด์หมายเลขกุญแจส่วนตัว ซึ่งจะใช้ 64 บิตแรกของกุญแจส่วนตัว ฟิลด์กุญแจสาธารณะ ซึ่งจะใช้เก็บกุญแจสาธารณะที่จะใช้คู่กับกุญแจส่วนตัวนี้ ฟิลด์กุญแจส่วนตัว กุญแจส่วนตัวดังกล่าวจะถูกเข้ารหัสไว้ ฟิลด์เวลาที่สร้างคู่กุญแจ ซึ่งจะไว้ช่วยในการตัดสินใจในการยกเลิกกุญแจเก่า

ตารางของพวงกุญแจสาธารณะจะประกอบไปด้วย 8 ฟิลด์ ได้แก่ ฟิลด์หมายเลขผู้ใช้ ซึ่งส่วนใหญ่นิยมเก็บหมายเลขที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ ฟิลด์หมายเลขกุญแจสาธารณะ ซึ่งจะใช้ 64 บิตแรกของกุญแจสาธารณะ ฟิลด์กุญแจสาธารณะ ซึ่งจะใช้เก็บกุญแจสาธารณะ ฟิลด์ระดับความน่าเชื่อถือของเจ้าของกุญแจสาธารณะ ซึ่งจะเก็บระดับความเชื่อใจ เช่น เชื่อใจมาก เชื่อใจปานกลาง ไม่น่าเชื่อใจ ฟิลด์ใบรับรอง ซึ่งจะเก็บใบรับรอง (อาจมีมากกว่า 1 ใบ) ฟิลด์ระดับความน่าเชื่อถือของใบรับรอง ซึ่งจะเก็บระดับความน่าเชื่อถือของใบรับรองแต่ละใบ ฟิลด์ระดับความน่าเชื่อถือของกุญแจ เป็นค่าซึ่งคำนวณจากความน่าเชื่อถือของใบรับรองแต่ละใบ ฟิลด์เวลาที่เก็บกุญแจ ซึ่งจะไว้ช่วยในการตัดสินใจในการยกเลิกกุญแจเก่า

ขั้นตอนวิธี

พีจีพีได้อาศัยขั้นตอนวิธีต่างๆ มากมายเพื่อใช้ในการเข้ารหัสแบบสมมาตร การเข้ารหัสแบบอสมมาตร แฮชฟังก์ชัน และ การบีบอัด ซึ่งขั้นตอนวิธีที่สามารถใช้งานได้ด้วยพีจีพี สามารถสรุปได้ดังตารางที่ 8.1

ใบรับรอง

ใบรับรองของพีจีพีมีลักษณะการทำงานต่างกับเอ็กซ์.509 ซึ่งกระบวนการออกใบรับรองของพีจีพีจะไม่มีผู้มีอำนาจในการออกใบรับรอง แต่ทุกคนสามารถออกใบรับรองให้ใครก็ได้ กล่าวคือ การรับรองของพีจีพีจะไม่มีลำดับชั้นซึ่งถ่ายทอดการรับรองแบบต้นไม้เหมือนกับเอ็กซ์.509 ดังนั้นจึงจำเป็นอย่างยิ่งที่จะต้องมีระดับความเชื่อใจของใบรับรอง เช่น เชื่อใจมาก เชื่อใจปานกลาง และ ไม่แน่ใจ โดยที่ระดับความเชื่อใจดังกล่าวจะถูกถ่ายทอดไปยังผู้ที่ถูกรับรอง ตัวอย่างเช่น A เชื่อใจ B มาก เมื่อ B ออกใบรับรองให้ C แล้ว A จะเชื่อใจ C มากด้วยเช่นกัน หาก A เชื่อใจ M ปานกลางใบรับรองทุกคนที่ออกโดย M ก็จะถูกเชื่อใจในระดับปานกลางด้วยเช่นเดียวกัน

8.1.2 เอส/เอ็มไอเอ็มอี

เอส/เอ็มไอเอ็มอี เป็นการให้บริการด้านความปลอดภัยซึ่งถูกออกแบบสำหรับใช้งานกับไปรษณีย์อิเล็กทรอนิกส์ ซึ่งเป็นโพรโทคอลที่เพิ่มความสามารถการทำงานด้านความมั่นคงปลอดภัยให้กับโพรโทคอลเอ็มไอเอ็มอี

ตารางที่ 8.1: ขั้นตอนวิธีที่สามารถใช้งานได้ในพีจีพี

ประเภทของขั้นตอนวิธี	หมายเลข	รายละเอียด
การเข้ารหัสแบบอสมมาตร	1	อาร์เอสเอ (เข้ารหัสและลงลายมือชื่อ)
	2	อาร์เอสเอ (เข้ารหัสเท่านั้น)
	3	อาร์เอสเอ (ลงลายมือชื่อเท่านั้น)
	16	เอลกามอล (เข้ารหัสเท่านั้น)
	17	ดีเอสเอส
	18	(จอง) เส้นโค้งอีลิปติก
	19	(จอง) อีซีดีเอสเอ
	20	เอลกามอล (เข้ารหัสและลงลายมือชื่อ)
	21	(จอง) เดฟฟี่-เฮลแมน
	100-110	ขั้นตอนวิธีส่วนตัว
การเข้ารหัสแบบสมมาตร	0	ไม่มีการเข้ารหัส
	1	ไอเดีย
	2	ดีอีเอสสามครั้ง
	3	แคส-128
	4	โบลว์ฟิช
	5	เซฟเฟอร์-เอสเค128
	6	(จอง) ดีอีเอส/เอสเค
	7	(จอง) เออีเอส-128
	8	(จอง) เออีเอส-192
	9	(จอง) เออีเอส-256
	100-110	ขั้นตอนวิธีส่วนตัว
แฮช	1	เอ็มดี5
	2	ชา-1
	3	ไรป์-เอ็มดี/160
	4	(จอง) ชาซึ่งมีความยาว 2 เท่า
	5	เอ็มดี2
	6	ไทเกอร์/192
	7	(จอง) ฮาวอล
	100-110	ขั้นตอนวิธีส่วนตัว
การบีบอัด	0	ไม่มีการบีบอัด
	1	ซิป
	2	ซีลิป
	100-110	ขั้นตอนวิธีส่วนตัว

เอ็มไอเอ็มอี

ในยุคเริ่มต้นการทำงานของไปรษณีย์อิเล็กทรอนิกส์ได้ถูกออกแบบให้ใช้งานง่ายซึ่งสามารถส่งได้เพียงข้อความ ความยาวของรหัสแอสกีไม่เกิน 7 บิตเท่านั้น ทำให้ไม่สามารถส่งข้อความที่ไม่สามารถแทนที่ได้ใน 7 บิต (เช่น ภาษาไทย ภาษาจีน ฯลฯ) ได้ นอกจากนั้นยังไม่สามารถส่งข้อมูลที่เป็นทวิภาค เช่น แฟ้มข้อมูลวีดีโอ แฟ้มข้อมูลเสียงได้ เอ็มไอเอ็มอีเป็นโพรโทคอลเสริมที่ทำให้บริการไปรษณีย์อิเล็กทรอนิกส์ สามารถส่งข้อมูลที่ไม่สามารถแทนที่ด้วยรหัสแอสกี 7 บิตได้ ด้วยการแปลงข้อมูลที่ต้องการส่งเป็นรหัสแอสกี 7 บิต

เอ็มไอเอ็มอีได้กำหนดรูปแบบส่วนหัวสำหรับระบุค่าการแปลงข้อมูลต่างๆ โดยส่วนหัวดังกล่าวจะถูกแทรกในส่วนหัวของจดหมายต้นฉบับ ดังนี้

- **เวอร์ชัน** ใช้ระบุเวอร์ชันที่ใช้ซึ่งปัจจุบันใช้เวอร์ชัน 1.1
- **ชนิดข้อมูล** ชนิดของรูปแบบข้อมูลซึ่งจะกำหนดในรูปของ <ชนิด/ชนิดย่อย;พารามิเตอร์> เช่น <ตัวอักษร/เฮชทีเอ็มแอล> <รูปภาพ/จีไอเอฟ> เป็นต้น ในปัจจุบันเอ็มไอเอ็มอีได้กำหนดชนิดไว้ 7 ชนิด ได้แก่ ตัวอักษร หลายชนิดประกอบกัน ส่วนข้อความ รูปภาพ วีดิโอ เสียง และ โปรแกรมประยุกต์
- **การเข้ารหัส** ใช้ระบุชนิดของการเข้ารหัสข้อมูล ได้แก่ รหัสแอสกี 7 บิต 8 บิต ทวิภาค แรดิก-64 และ ตัวอักษรที่อ่านได้เสมอ (สัญลักษณ์ที่มิใช่ตัวอักษรปกติจะถูกแปลงเป็นตัวอักษรที่อ่านได้โดยขึ้นต้นด้วยเครื่องหมายเท่ากับ แล้วตามด้วยตัวอักษรสองตัวซึ่งแทนค่าเลขฐาน 16 ของไบต์)
- **หมายเลข** ซึ่งจะใช้เรียกแทนข้อความนั้น
- **รายละเอียด** ซึ่งจะระบุรายละเอียดเพิ่มเติมของ รูป เสียง ภาพ

เอส/เอ็มไอเอ็มอี

เอส/เอ็มไอเอ็มอี เป็นส่วนที่เพิ่มความมั่นคงปลอดภัยให้กับเอ็มไอเอ็มอี โดยเพิ่มชนิดย่อยขึ้นมาใหม่ เช่น <แอพพลิเคชัน/พีเคซีเอส7-เอ็มไอเอ็มอี> พร้อมทั้งบอกชนิดการเข้ารหัสของข้อมูล ได้แก่ ข้อมูลธรรมดา ข้อมูลที่มีการลงลายมือชื่อโดยผู้ส่ง ข้อมูลที่เข้ารหัสแล้ว ข้อมูลพร้อมไดเจสท์ ข้อมูลที่ใช้ในการระบุตัวตน

ขั้นตอนวิธีที่สนับสนุนทั้งหมดใน เอส/เอ็มไอเอ็มอี สามารถสรุปได้ดังตารางที่ 8.2

ตารางที่ 8.2: ขั้นตอนวิธีที่สามารถใช้งานได้ในเอส/เอ็มไอเอ็มอี

ขั้นตอนวิธี	ผู้ส่งต้องสนับสนุน	ผู้รับต้องสนับสนุน	ผู้ส่งควรสนับสนุน	ผู้รับควรสนับสนุน
เข้ารหัสข้อมูล เข้ารหัสกุญแจ แฮช เข้ารหัสไดเจสท์ ระบุตัวตน	ทริปเปิ้ลดีอีเอส อาร์เอสเอ ชา-1 ดีเอสเอส	ทริปเปิ้ลดีอีเอส อาร์เอสเอ ชา-1 ดีเอสเอส เฮชแม็ค กับ ชา-1	เดฟฟี่-เฮลแมน อาร์เอสเอ	เออีเอส, อาร์ซี2/40 เดฟฟี่-เฮลแมน เอ็มดี5 อาร์เอสเอ

8.2 ความมั่นคงในระดับชั้นทรานสปอร์ต

ในหัวข้อนี้จะกล่าวถึงความมั่นคงในระดับชั้นทรานสปอร์ต 2 โพรโทคอลได้แก่ เอสเอสแอล และ ทีแอลเอส โพรโทคอลทั้งสองดังกล่าวจะช่วยสร้างความมั่นคงปลอดภัยให้กับโพรโทคอลในลำดับชั้นทรานสปอร์ต เช่น โพรโทคอลทีซีพี ซึ่งใช้กันอย่างกว้างขวางในอินเตอร์เน็ต เช่น การใช้งานธนาคารหรือการซื้อสินค้าผ่านอินเตอร์เน็ต โดยใช้โพรโทคอลเฮชทีทีพีเอส

8.2.1 เอสเอสแอล

โพรโทคอลเอสเอสแอลถูกออกแบบสำหรับการเข้ารหัส การลงลายมือชื่อ และการบีบอัดข้อมูลที่สร้างจากลำดับขั้นแอพพลิเคชัน ซึ่งโพรโทคอลดังกล่าวถูกออกแบบ สำหรับการให้บริการด้านการบีบอัดบูรณภาพ ความลับ

ขั้นตอนวิธีการแลกเปลี่ยนกุญแจ

เอสเอสแอลได้กำหนดวิธีการแลกเปลี่ยนกุญแจไว้ 6 วิธี ได้แก่ วิธีการซึ่งไม่มีการแลกเปลี่ยนกุญแจ วิธีการอาร์เอสเอ วิธีการเดฟฟี่-เฮลแมน วิธีการเดฟฟี่-เฮลแมนโดยเพิ่มการลงลายมือชื่อ วิธีการเดฟฟี่-เฮลแมนโดยเพิ่มใบรับรอง วิธีการฟอร์เทสซ่าซึ่งใช้ในกระทรวงกลาโหมสหรัฐอเมริกา

ขั้นตอนวิธีการเข้ารหัส

เอสเอสแอลได้กำหนดวิธีการเข้ารหัสไว้ 6 กลุ่ม ได้แก่ กลุ่มซึ่งไม่มีการเข้ารหัส กลุ่มการเข้ารหัสอาร์ซีแบบกระแส เช่น อาร์ซี4-40 อาร์ซี4-128 กลุ่มการเข้ารหัสอาร์ซีแบบบล็อก เช่น อาร์ซี2-ซีบีซี-40 กลุ่มการเข้ารหัสดีอีเอสแบบบล็อก เช่น ดีอีเอส-40-ซีบีซี ดีอีเอส-ซีบีซี ทริปเปิ้ลดีอีเอส-อีดีอี-ซีบีซี กลุ่มการเข้ารหัสไอเดียแบบบล็อก เช่น ไอเดีย-ซีบีซี กลุ่มการเข้ารหัสฟอร์เทสซ่าแบบบล็อก เช่น ฟอร์เทสซ่า-ซีบีซี

ขั้นตอนวิธีการแฮช

เอสเอสแอลได้กำหนดวิธีการแฮชไว้ 3 วิธี ได้แก่ วิธีการซึ่งไม่ใช้การแฮช วิธีแฮชเอ็มดี5 ชา-1

ชุดขั้นตอนวิธี

เอสเอสแอลได้จัดกลุ่มการขั้นตอนวิธีของการเข้ารหัสไว้เป็นชุดดังแสดงได้ในตารางที่ 8.3 โดยที่รูปแบบของชื่อขั้นตอนวิธีจะขึ้นต้นด้วยคำว่า ''SSL'' แล้วตามด้วยขั้นตอนการแลกเปลี่ยนกุญแจ ตามด้วยคำว่า ''WITH'' (หรือ ''EXPORT_WITH'' ซึ่งหมายถึงขั้นตอนวิธีที่อนุญาตให้ใช้นอกประเทศสหรัฐอเมริกาเนื่องจากในอดีต ประเทศสหรัฐอเมริกามีกฎหมายห้ามนำออกซึ่งการเข้ารหัสซึ่งยากต่อการถอดรหัสโดยรัฐบาลสหรัฐอเมริกา) แล้วตามด้วยชื่อขั้นตอนวิธีการเข้ารหัสและแฮชตามลำดับ

การทำงานของเอสเอสแอล

เอสเอสแอลประกอบด้วยโพรโทคอลย่อย 4 โพรโทคอล ได้แก่

- **โพรโทคอลเรคคอร์ด** เป็นโพรโทคอลย่อยที่ทำหน้าที่รวมการทำงานของโพรโทคอลย่อยอื่นในเอสเอสแอลแล้วส่งให้ลำดับชั้นทรานสปอร์ต
- **โพรโทคอลแฮนด์เช็ค** เป็นโพรโทคอลย่อยที่ทำหน้าที่ตกลงชุดชั้นตอนวิธีและแลกเปลี่ยนข้อมูลเริ่มต้น ซึ่งสามารถแบ่งเป็น 4 ขั้นตอนได้แก่ ขั้นตอนเริ่มต้นแลกเปลี่ยนข้อมูลพื้นฐาน ขั้นตอนการแลกเปลี่ยนกุญแจและบุตัวตนของเครื่องให้บริการ ขั้นตอนการแลกเปลี่ยนกุญแจและระบุตัวตนของเครื่องรับบริการ และขั้นตอนสิ้นสุดการแลกเปลี่ยนข้อมูลซึ่งหลังจากขั้นตอนนี้จะสามารถแลกเปลี่ยนข้อมูลได้
- **โพรโทคอลเชนจ์ไซเฟอร์สเปค** เป็นโพรโทคอลซึ่งทำหน้าที่เปลี่ยนสถานะการทำงานของเอสเอสแอล
- **โพรโทคอลอเลอท** เป็นโพรโทคอลที่ทำหน้าที่รายงานข้อผิดพลาดและสภาวะผิดปกติต่างๆ

8.2.2 ทีแอลเอส

ทีแอลเอสเป็นโพรโทคอลที่ทำหน้าที่และมีรูปแบบคล้ายเอสเอสแอล ซึ่งเอสเอสแอลถูกพัฒนาขึ้นโดยบริษัทเนสเคปในขณะที่ทีแอลเอสเป็นโพรโทคอลมาตรฐานที่ถูกกำหนดโดยหน่วยงานกำหนดมาตรฐานสำหรับอินเทอร์เน็ตที่เรียกว่า ไออีทีเอฟ ทีแอลเอสสนับสนุนการทำงานของชุดขั้นตอนวิธีคล้ายกับเอสเอสแอล ยกเว้น ไม่สนับสนุน ฟอร์เทสซ่า ซึ่งชื่อขั้นตอนวิธีเหล่านี้จะขึ้นต้นด้วย ''TLS'' เช่น TLS_RSA_WITH_RC4_128_MD5 เป็นต้น

ตารางที่ 8.3: ชุดขั้นตอนวิธีในเอสเอสแอล

ชุดขั้นตอนวิธี	การแลกกุญแจ	การเข้ารหัส	แฮช
SSL_NULL_WITH_NULL_NULL	ไม่มี	ไม่มี	ไม่มี
SSL_RSA_WITH_NULL_MD5	อาร์เอสเอ	ไม่มี	เอ็มดี5
SSL_RSA_WITH_NULL_SHA	อาร์เอสเอ	ไม่มี	ชา-1
SSL_RSA_EXPORT_WITH_RC4_40_MD5	อาร์เอสเอ	อาร์ซี4-40	เอ็มดี5
SSL_RSA_WITH_RC4_128_MD5	อาร์เอสเอ	อาร์ซี4-128	เอ็มดี5
SSL_RSA_WITH_RC4_128_SHA	อาร์เอสเอ	อาร์ซี4-128	ชา-1
SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5	อาร์เอสเอ	อาร์ซี2-ซีบีซี	เอ็มดี5
SSL_RSA_WITH_IDEA_CBC_SHA	อาร์เอสเอ	ไอเดีย	ชา-1
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	อาร์เอสเอ	ดีอีเอส40	ชา-1
SSL_RSA_WITH_DES_CBC_SHA	อาร์เอสเอ	ดีอีเอส	ชา-1
SSL_RSA_WITH_3DES_EDE_CBC_SHA	อาร์เอสเอ	ทริปเปิ้ลดีอีเอส	ชา-1
SSL_DH_DSS_EXPORT_WITH_DES40_CBC_SHA	ดีเฮช-ดีเอสเอส	ดีอีเอส40	ชา-1
SSL_DH_DSS_WITH_DES_CBC_SHA	ดีเฮช-ดีเอสเอส	ดีอีเอส	ชา-1
SSL_DH_DSS_WITH_3DES_EDE_CBC_SHA	ดีเฮช-ดีเอสเอส	ทริปเปิ้ลดีอีเอส	ชา-1
SSL_DH_RSA_EXPORT_WITH_DES40_CBC_SHA	ดีเฮช-อาร์เอสเอ	ดีอีเอส40	ชา-1
SSL_DH_RSA_WITH_DES_CBC_SHA	ดีเฮช-อาร์เอสเอ	ดีอีเอส	ชา-1
SSL_DH_RSA_WITH_3DES_EDE_CBC_SHA	ดีเฮช-อาร์เอสเอ	ทริปเปิ้ลดีอีเอส	ชา-1
SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	ดีเฮชอี-ดีเอสเอส	ดีอีเอส40	ชา-1
SSL_DHE_DSS_WITH_DES_CBC_SHA	ดีเฮชอี-ดีเอสเอส	ดีอีเอส	ชา-1
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA	ดีเฮชอี-ดีเอสเอส	ทริปเปิ้ลดีอีเอส	ชา-1
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	ดีเฮชอี-อาร์เอสเอ	ดีอีเอส40	ชา-1
SSL_DHE_RSA_WITH_DES_CBC_SHA	ดีเฮชอี-อาร์เอสเอ	ดีอีเอส	ชา-1
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA	ดีเฮชอี-อาร์เอสเอ	ทริปเปิ้ลดีอีเอส	ชา-1
SSL_DH_anon_EXPORT_WITH_RC4_40_MD5	ดีเฮช	อาร์ซี4-40	เอ็มดี5
SSL_DH_anon_WITH_RC4_128_MD5	ดีเฮช	อาร์ซี4-128	เอ็มดี5
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA	ดีเฮช	ดีอีเอส40	ชา-1
SSL_DH_anon_WITH_DES_CBC_SHA	ดีเฮช	ดีอีเอส	ชา-1
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA	ดีเฮช	ทริปเปิ้ลดีอีเอส	ชา-1
SSL_FORTEZZA_KEA_WITH_NULL_SHA	ฟอร์เทสซ่าเคอีเอ	ไม่มี	ชา-1
SSL_FORTEZZA_KEA_WITH_FORTEZZA_CBC_SHA	ฟอร์เทสซ่าเคอีเอ	ฟอร์เทสซ่า	ชา-1
SSL_FORTEZZA_KEA_WITH_RC4_128_SHA	ฟอร์เทสซ่าเคอีเอ	อาร์ซี4-128	ชา-1

8.3 ความมั่นคงในระดับชั้นเน็ตเวิร์ค

ในหัวข้อนี้จะกล่าวถึงความมั่นคงในระดับชั้นเน็ตเวิร์คซึ่งได้รับความนิยมที่มีชื่อว่า ''ไอพีเส็ก'' ซึ่งแบ่งการทำงานเป็น 2 รูปแบบ ได้แก่

- **ทรานสปอร์ต** เป็นรูปแบบซึ่งปกป้องข้อมูลจากลำดับชั้นทรานสปอร์ต แต่ไม่ปกป้องส่วนหัวของโพรโทคอลไอพี
- **ทันแนล** เป็นรูปแบบการปกป้องข้อมูลซึ่งรวมถึงโพรโทคอลไอพี

โพรโทคอลย่อยด้านความปลอดภัย แบ่งเป็น 2 รูปแบบ ได้แก่ เอเฮช และ อีเอสพี โดยที่เอเฮชให้บริการ การควบคุมการเข้าถึง ด้านบูรณภาพ การระบุตัวตน และ การป้องกันการโจมตีด้วยวิธีการส่งซ้ำ ในขณะที่อีเอสพีจะเพิ่มบริการด้านการรักษาความลับ

- **การควบคุมการเข้าถึง** จะอาศัยฐานข้อมูลความสัมพันธ์ด้านความมั่นคง (เอสเอ) หากได้รับข้อมูลจากเครื่องที่ไม่มีเอสเอ ข้อมูลดังกล่าวจะถูกเพิกเฉย
- **บูรณภาพ** จะอาศัยการสร้างไดเจสท์และส่งไปพร้อมกับข้อมูล
- **การระบุตัวตน** จะอาศัยเอสเอและการแฮชแบบมีกุญแจ
- **การป้องกันการโจมตีด้วยวิธีการส่งซ้ำ** จะอาศัยหมายเลขลำดับของข้อมูล
- **การรักษาความลับ** จะให้บริการเฉพาะอีเอสพีโดยอาศัยการเข้ารหัส

การส่งรับข้อมูลระหว่างเครื่องจะต้องมีการสร้างความสัมพันธ์ด้านความมั่นคง (เอสเอ) หากเครื่องใดยังไม่มีเอสเอจะสามารถสร้างด้วยโพรโทคอล อินเทอร์เน็ตคีย์เอ็กเชนจ์ (ไอเคอี) ซึ่งโพรโทคอลไอเคอีจะทำงานโดยอาศัยโพรโทคอลอื่นได้แก่ ไอเอสเอเคเอ็มพี (โพรโทคอลซึ่งเป็นขั้นตอนวิธีหลักของการทำงานของไอเคอี) โอคเลย์ (โพรโทคอลซึ่งช่วยสร้างกุญแจจากวิธีของเดฟฟี่-เฮลแมน) และ เอสเคอีเอ็มอี (โพรโทคอลที่ช่วยในการพิสูจน์เอนทิตีจากวิธีการเข้ารหัสด้วยกุญแจแบบอสมมาตร)

ก่อนที่จะรับส่งข้อมูลด้วยไอพีเส็กจะต้องมีการตรวจสอบข้อมูลดังกล่าวกับกฎความมั่นคง (เอสพี) จากฐานข้อมูลกฎความมั่นคง (เอสพีดี) ก่อนซึ่งจะมีผลลัพธ์ 3 รูปแบบได้แก่ การเพิกเฉยข้อมูลทิ้ง การใช้งานกฎ และ กรณีที่ไม่มีกฎที่ตรงกับข้อมูลดังกล่าวให้ส่งผ่านข้อมูลไปยังลำดับชั้นถัดไปได้เลย

8.4 สรุป

บทนี้ได้กล่าวถึง ความมั่นคงปลอดภัยในระบบเครือข่ายใน 3 ลำดับชั้นของแบบจำลองทีซีพี/ไอพี ได้แก่ ลำดับชั้นแอพพลิเคชัน ลำดับชั้นทรานสปอร์ต และ ลำดับชั้นเน็ตเวิร์ค

8.5 แบบฝึกหัด

1. จงเปรียบเทียบ พีจีพี กับ เอส/เอ็มไอเอ็มอี ในประเด็นต่อไปนี้

   (a) การเข้ารหัสแบบสมมาตร

   (b) การเข้ารหัสแบบอสมมาตร

   (c) แฮช

2. จงเปรียบเทียบใบรับรองของ เอ็กซ์.509 และ พีจีพี

3. จงหาความยาวของกุญแจสำหรับชุดความปลอดภัยต่อไปนี้

   (a) SSL_RSA_WITH_NULL_MD5

   (b) SSL_RSA_EXPORT_WITH_DES40_CBC_SHA

   (c) TLS_RSA_WITH_DES_CBC_SHA

   (d) TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA

4. ชุดกุญแจที่ประเทศสหรัฐอเมริกาอนุญาตให้ใช้นอกประเทศได้ ส่วนใหญ่แล้วจะมีกุญแจไม่เกิน 40 บิต ซึ่งมีความปลอดภัยต่ำ คุณคิดว่าเหตุใดจึงยังมีผู้ใช้ชุดกุญแจดังกล่าว

5. จงอธิบายความสัมพันธ์ของ ไอพีเส็ก และ ไอเคอี

6. หากต้องการส่งข้อมูลลับควรจะใช้การทำงานของไอพีเส็กแบบไหนเพราะเหตุใด

ภาคผนวก

ภาคผนวก ก

พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้า ฯ ให้ประกาศว่า โดยที่เป็นการสมควรมีกฎหมาย ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ จึงทรงพระกรุณาโปรดเกล้า ฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของสภานิติบัญญัติแห่งชาติ ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า ''พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐''

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดสามสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ในพระราชบัญญัตินี้

''ระบบคอมพิวเตอร์'' หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

''ข้อมูลคอมพิวเตอร์'' หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

''ข้อมูลจราจรทางคอมพิวเตอร์'' หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลาชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

''ผู้ให้บริการ'' หมายความว่า

(๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่นโดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

''ผู้ใช้บริการ'' หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

''พนักงานเจ้าหน้าที่'' หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

''รัฐมนตรี'' หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

มาตรา ๔ ให้รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจออกกฎกระทรวง เพื่อปฏิบัติการตามพระราชบัญญัตินี้ กฎกระทรวงนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้วให้ใช้บังคับได้

หมวด ๑ ความผิดเกี่ยวกับคอมพิวเตอร์

มาตรา ๕ ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้น มิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๖ ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบ ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๗ ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ

มาตรา ๘ ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๙ ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่ง

ข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๐ ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๑ ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

มาตรา ๑๒ ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐

(๑) ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันทีหรือในภายหลัง และไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่ ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

(๒) เป็นการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท ถ้าการกระทำความผิดตาม (๒) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่สิบปีถึงยี่สิบปี

มาตรา ๑๓ ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือมาตรา ๑๑ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(๕) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (๑)(๒) (๓) หรือ (๔)

มาตรา ๑๕ ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔

มาตรา ๑๖ ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือ ปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ ถ้าการกระทำตามวรรคหนึ่ง เป็นการนำเข้าข้อมูลคอมพิวเตอร์โดยสุจริต ผู้กระทำไม่มีความผิด ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้ ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือ บุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย

มาตรา ๑๗ ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและ

(๑) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้นหรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือ

(๒) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหายและผู้เสียหายได้ร้องขอให้ลงโทษ จะต้องรับโทษภายในราชอาณาจักร

หมวด ๒ พนักงานเจ้าหน้าที่

มาตรา ๑๘ ภายใต้บังคับมาตรา ๑๙ เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใดดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(๑) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(๒) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

(๓) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา ๒๖ หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่

(๔) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(๕) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(๖) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(๗) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(๘) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิดตามพระราชบัญญัตินี้

มาตรา ๑๙ การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิดตามพระราชบัญญัตินี้ เหตุที่ต้องใช้อำนาจ ลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิด เท่าที่สามารถจะระบุได้ ประกอบคำร้องด้วยในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็วเมื่อศาลมีคำสั่งอนุญาตแล้ว ก่อนดำเนินการตามคำสั่งของศาล ให้พนักงานเจ้าหน้าที่ส่งสำเนาบันทึกเหตุอันควรเชื่อที่ทำให้ต้องใช้อำนาจตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐาน แต่ถ้าไม่มีเจ้าของหรือผู้ครอบครองเครื่องคอมพิวเตอร์อยู่ ณ ที่นั้น ให้พนักงานเจ้าหน้าที่ส่งมอบสำเนาบันทึกนั้นให้แก่เจ้าของหรือ ผู้ครอบครองดังกล่าวในทันทีที่กระทำได้ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้า

มาตรา ๒๒ ห้ามมิให้พนักงานเจ้าหน้าที่เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา ๑๘ ให้แก่บุคคลใดความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้ หรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่ โดยมิชอบ หรือเป็นการกระทำตามคำสั่งหรือที่ได้รับอนุญาตจากศาลพนักงานเจ้าหน้าที่ผู้ใดฝ่าฝืนวรรคหนึ่งต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๓ พนักงานเจ้าหน้าที่ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา ๑๘ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๔ ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรือข้อมูลของผู้ใช้บริการ ที่พนักงานเจ้าหน้าที่ได้มาตามมาตรา ๑๘ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๕ ข้อมูล ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วยการสืบพยานได้ แต่ต้องเป็นชนิดที่มิได้เกิดขึ้นจากการจูงใจมีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น

มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวัน แต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้ ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท

มาตรา ๒๗ ผู้ใดไม่ปฏิบัติตามคำสั่งของศาลหรือพนักงานเจ้าหน้าที่ที่สั่งตามมาตรา ๑๘ หรือมาตรา ๒๐ หรือไม่ปฏิบัติตามคำสั่งของศาลตามมาตรา ๒๑ ต้องระวางโทษปรับไม่เกินสองแสนบาทและปรับเป็นรายวันอีกไม่เกินวันละห้าพันบาทจนกว่าจะปฏิบัติให้ถูกต้อง

มาตรา ๒๘ การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ ให้รัฐมนตรีแต่งตั้งจากผู้มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์ และมีคุณสมบัติตามที่รัฐมนตรีกำหนด

มาตรา ๒๙ ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่เป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตามประมวลกฎหมายวิธีพิจารณาความอาญามีอำนาจรับคำร้องทุกข์หรือรับคำกล่าวโทษและมีอำนาจในการสืบสวนสอบสวนเฉพาะความผิดตามพระราชบัญญัตินี้ ในการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีผู้กระทำความผิดตามพระราชบัญญัตินี้ บรรดาที่เป็นอำนาจของพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ หรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ให้พนักงานเจ้าหน้าที่ประสานงานกับพนักงานสอบสวนผู้รับผิดชอบเพื่อดำเนินการตามอำนาจหน้าที่ต่อไป ให้นายกรัฐมนตรีในฐานะผู้กำกับดูแลสำนักงานตำรวจแห่งชาติ และรัฐมนตรีมีอำนาจ ร่วมกันกำหนดระเบียบเกี่ยวกับแนวทางและวิธีปฏิบัติในการดำเนินการตามวรรคสอง

มาตรา ๓๐ ในการปฏิบัติหน้าที่ พนักงานเจ้าหน้าที่ต้องแสดงบัตรประจำตัวต่อบุคคลซึ่งเกี่ยวข้อง บัตรประจำตัวของพนักงานเจ้าหน้าที่ให้เป็นไปตามแบบที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้รับสนองพระบรมราชโองการ
พลเอก สุรยุทธ์ จุลานนท์
นายกรัฐมนตรี

หมายเหตุ

เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ เนื่องจากในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญ ของการประกอบกิจการ และการดำรงชีวิตของมนุษย์ หากมีผู้กระทำด้วยประการใด ๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้ หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่น ในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์ เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จ หรือมีลักษณะอันลามกอนาจาร ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน สมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว จึงจำเป็นต้องตราพระราชบัญญัตินี้

ภาคผนวก ข

โครงงานความมั่นคงปลอดภัยในเทคโนโลยีสารสนเทศ

วัตถุประสงค์

1. เพื่อให้นักศึกษามีความรู้ ความเข้าใจ ในเรื่องต่างๆ ที่เกี่ยวข้องกับ ความมั่นคงปลอดภัยในเทคโนโลยีสารสนเทศเพิ่มเติมจากเนื้อหาในชั้นเรียน
2. เพื่อให้นักศึกษาสามารถประยุกต์ใช้วิธีการและเครื่องมือที่เกี่ยวข้องกับ ความมั่นคงปลอดภัยในเทคโนโลยีสารสนเทศได้
3. เพื่อให้นักศึกษาสามารถ ค้นคว้า วิจัย และ วิเคราะห์ ด้วยตนเองได้

ตัวอย่างหัวข้อโครงงาน

- การโจมตี ตรวจจับ และ ป้องกัน เครือข่ายประเภทต่างๆ เช่น เครือข่ายไร้สาย เครือข่ายโทรศัพท์เคลื่อนที่ เครือข่ายบลูทูธ เครือข่ายกริดและกลุ่มเมฆ โพรโทคอลเครือข่าย และ อุปกรณ์ในเครือข่าย เป็นต้น
- การโจมตี ตรวจจับ และ ป้องกัน ระบบปฏิบัติการ ฐานข้อมูล ภาษาคอมพิวเตอร์
- การโจมตี ตรวจจับ และ ป้องกัน ระบบต่างๆ ในองค์กร เช่น พาณิชย์อิเล็กทรอนิกส์ ธนาคารผ่านอินเทอร์เน็ต เป็นต้น
- การโจมตี ตรวจจับ และ ป้องกัน อุปกรณ์ เช่น ไอโฟน แบล็กเบอร์รี่ เอ็กซ์บอกซ์ นินเทนโดวี บลูเรย์ ดีวีดี เป็นต้น

- เทคนิคที่เกี่ยวข้องด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ เช่น ชีวมาตร การโจมตีด้วยรูทคิต การโจมตีแบบกระจาย การเขียนโปรแกรมแบบปลอดภัย เป็นต้น
- หลักการและทฤษฎีทางคณิตศาสตร์ที่เกี่ยวข้อง เช่น เส้นโค้งอีลิปติก การออกแบบกล่องเอส การบีบอัด การสร้างตัวเลขสุ่ม เป็นต้น
- หัวข้ออื่นๆ ที่น่าสนใจ

รายงาน

รายงานจะต้องจัดให้อยู่ในรูปแบบของบทความวิจัยไม่ต่ำกว่า 10 หน้ากระดาษ โดยจะต้องมีองค์ประกอบคือ บทคัดย่อ บทนำ (และงานวิจัยที่เกี่ยวข้อง) รายละเอียดของเนื้อหา บทวิเคราะห์ บทสรุป(และงานวิจัยในอนาคต) เอกสารอ้างอิง

วิธีการให้คะแนน

การให้คะแนนจะเน้นคุณภาพเชิงวิจัย อาทิเช่น นักศึกษาที่มีการ ประดิษฐ์ คิดค้น ออกแบบ ทดลองด้วยตนเอง จะมีคะแนนมากกว่า นักศึกษาที่เปรียบเทียบหรือรายงานผลงานของคนอื่น เป็นต้น

ภาคผนวก ค

ประมวลการสอนรายวิชา

รายวิชา 204505 ความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ หน่วยกิต 3 (3-0-6)

ผู้รับผิดชอบรายวิชา อาจารย์ ดร. ธรา อั่งสกุล

เนื้อหาโดยสังเขป

วิชาบังคับก่อน : ไม่มี

แนวคิดเกี่ยวกับความมั่นคงปลอดภัยในระบบคอมพิวเตอร์ ความปลอดภัยในไปรษณีย์อิเลคโทรนิคส์และระบบยูนิกซ์ การตรวจสอบความถูกต้องของข้อความ การเข้ารหัสและการถอดรหัสชนิดต่างๆ คณิตศาสตร์ทางด้านความปลอดภัย กุญแจสาธารณะ เทคนิคการโจมตีและการป้องกันด้านความปลอดภัยของระบบเครือข่าย ความปลอดภัยของโปรแกรมประยุกต์ ประเด็นกฎหมายและจริยธรรมที่เกี่ยวข้อง แนวโน้ม และการประยุกต์งานด้านความมั่นคงปลอดภัย

คุณธรรมประจำวิชา จริยธรรมต้องนำหน้า เรียนศึกษาเพื่อป้องกัน

วัตถุประสงค์รายวิชา

1. เพื่อให้นักศึกษามีความรู้ความเข้าใจเกี่ยวกับความปลอดภัยของเทคโนโลยีสารสนเทศ ได้แก่

   (a) ภัยคุกคามทางคอมพิวเตอร์และระบบเครือข่ายในรูปแบบต่างๆ

   (b) ทฤษฎีทางคณิตศาสตร์พื้นฐานที่ใช้ในการป้องกันระบบคอมพิวเตอร์และระบบเครือข่าย

   (c) เทคโนโลยีและวิธีการที่ใช้ในการป้องกันและตรวจสอบผู้บุกรุกระบบคอมพิวเตอร์และเครือข่าย

   (d) คุณธรรมจริยธรรมและกฎหมายที่เกี่ยวข้องด้านความปลอดภัยของเทคโนโลยีสารสนเทศ

2. เพื่อให้นักศึกษามีทัศนคติที่ถูกต้องในการใช้ความรู้ความสามารถในด้านความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และระบบเครือข่าย

3. เพื่อให้นักศึกษาสามารถนำเครื่องมือและเทคโนโลยีด้านความปลอดภัยทางคอมพิวเตอร์ไปประยุกต์ใช้ เพื่อป้องกันและตรวจสอบระบบคอมพิวเตอร์และระบบเครือข่ายได้อย่างมีประสิทธิภาพ

4. เพื่อให้นักศึกษาสามารถศึกษา ค้นคว้า วิจัย และวิเคราะห์แนวโน้มทางด้านความปลอดภัยในระบบคอมพิวเตอร์และระบบเครือข่ายด้วยตนเอง

วิธีการสอน

ประกอบด้วยการบรรยายในชั้นเรียนเรียนสัปดาห์ละ 1 ครั้ง ครั้งละ 3 ชั่วโมง โดยการสอนจะเน้นการพัฒนาการเรียนรู้ของนักศึกษาใน 5 ด้าน ดังนี้

1. *วิธีการสอนที่จะใช้พัฒนาด้านคุณธรรมและจริยธรรม* สอดแทรกคุณธรรม จริยธรรมในระหว่างสอน และขณะที่ให้นักศึกษาทำงานที่มอบหมายในชั้นเรียน โดยการพูดคุยกับนักศึกษา และเน้นความรับผิดชอบต่องาน วินัย จรรยาบรรณ ความซื่อสัตย์ต่อหน้าที่ ความถ่อมตน และความมีน้ำใจต่อเพื่อนร่วมงาน ในเรื่องความรับผิดชอบและช่วยสร้างสรรค์ประโยชน์แก่สังคม การสอนจะทำโดยการยกตัวอย่างงานที่เกี่ยวข้องกับชุมชน แล้วโยงเข้าหาความรู้ทางด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ

2. *วิธีการสอนที่จะใช้พัฒนาด้านความรู้* บรรยายโดยเน้นทฤษฎีเป็นพื้นฐาน นำทฤษฎีไปใช้กับปัญหาจริง และตามด้วยแนวทางในการแก้ปัญหา แทรกประสบการณ์ของอาจารย์ในระหว่างสอนโดยผ่านการเล่าเรื่องต่างๆ อภิปรายโต้ตอบระหว่างอาจารย์และนักศึกษาในระหว่างการเรียนการสอน ให้คำปรึกษาหรือตอบปัญหาแก่นักศึกษา ผ่านระบบการเรียนรู้ทางอิเล็กทรอนิกส์อย่างน้อยสัปดาห์ละ 1 ครั้ง

3. *วิธีการสอนที่จะใช้พัฒนาทักษะทางปัญญา* ให้วิเคราะห์และวิจารณ์กลไกป้องกันของกรณีศึกษาและงานวิจัยที่เกี่ยวข้องกับความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ ในระหว่างการสอนจะมีการตั้งคำถามที่มาจากปัญหาจริงในองค์กร หรือบทความวิชาการ เพื่อให้นักศึกษาฝึกคิดหาวิธีการแก้ปัญหา

4. *วิธีการสอนที่จะใช้พัฒนาทักษะความสัมพันธ์ระหว่างบุคคลและความรับผิดชอบ* ให้ทำกิจกรรมร่วมกันเป็นกลุ่ม โดยเน้นการประยุกต์ความรู้ที่เรียนในวิชากับปัญหาที่กำหนด นักศึกษาแลกเปลี่ยนความรู้กันระหว่างการนำเสนอผลของกิจกรรมกลุ่มหน้าชั้นเรียน

5. *วิธีการสอนที่จะใช้พัฒนาทักษะทางการสื่อสาร และการใช้เทคโนโลยีสารสนเทศ* มอบหมายงานให้นักศึกษาค้นคว้าด้วยตนเอง จากเว็บไซต์ที่มีแหล่งข้อมูลที่น่าเชื่อถือ ส่งงานที่มอบหมายและ

ปรึกษาปัญหาผ่านทางระบบการเรียนรู้ทางอิเล็กทรอนิกส์ นำเสนอผลของการทำโครงงาน โดยใช้รูปแบบและเทคโนโลยีที่เหมาะสม

แผนการสอนรายสัปดาห์

สัปดาห์ที่	หัวข้อการสอน	บทที่	การวัดและประเมินผล
1	ความรู้พื้นฐานเกี่ยวกับความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ	1	แบบฝึกหัดท้ายบทที่ 1 การบ้านครั้งที่ 1
2	การเข้ารหัสด้วยกุญแจสมมาตรในอดีต	2	แบบฝึกหัดท้ายบทที่ 2
3	การเข้ารหัสด้วยกุญแจสมมาตรสมัยใหม่	3	แบบฝึกหัดท้ายบทที่ 3 การบ้านครั้งที่ 2
4	การเข้ารหัสด้วยกุญแจสมมาตรสมัยใหม่ขั้นสูง	4	แบบฝึกหัดบทที่ 4
5	การเข้ารหัสด้วยกุญแจแบบอสมมาตร	5	แบบฝึกหัดท้ายบทที่ 5 การบ้านครั้งที่ 3
6	บูรณภาพและการพิสูจน์ตัวจริงของสาร แฮช ฟังก์ชัน ลายมือชื่อดิจิทัล	6	แบบฝึกหัดท้ายบที่ 6
7	การพิสูจน์เอนทิตี และการจัดการกุญแจ	7	แบบฝึกหัดท้ายบทที่ 7 การบ้านครั้งที่ 4
8	ความมั่นคงปลอดภัยในระบบเครือข่าย	8	แบบฝึกหัดท้ายบทที่ 8
9	นำเสนอโครงงาน	-	วิเคราะห์ วิจารณ์
10	นำเสนอโครงงาน	-	วิเคราะห์ วิจารณ์
11	นำเสนอโครงงาน	-	วิเคราะห์ วิจารณ์
12	กฎหมาย จริยธรรม และ แนวโน้มด้านความมั่นคงปลอดภัย สรุปรายวิชา	ภาคผนวก ก	วิเคราะห์ วิจารณ์
13	สอบปลายภาค	1 - 8	ตรวจให้คะแนน

สื่อ ตำรา และเอกสารประกอบการเรียน

1. สื่อและอุปกรณ์

(a) เครื่องคอมพิวเตอร์และเครื่องฉาย

(b) สไลด์ประกอบการบรรยาย

(c) โปรแกรมประยุกต์ด้านความมั่นคงปลอดภัย

(d) ระบบการเรียนรู้ทางอิเล็กทรอนิกส์

2. ตำรา เอกสารประกอบการเรียนการสอน

(a) เอกสารหลัก

- ธรา อั่งสกุล. (2552). **ความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ**. นครราชสีมา: มหาวิทยาลัยเทคโนโลยีสุรนารี.

(b) เอกสารประกอบ

- บทความทางด้านความมั่นของปลอดภัยของเทคโนโลยีสารสนเทศ ที่ตีพิมพ์ในวารสารวิชาการที่ปรากฏในฐานข้อมูลสากล เช่น ISI และ Scopus
- Fourozan, B.A. (2008). **Cryptography and Network Security**. New York: Mcgraw-Hill.
- Stallings, W. (2005). **Cryptography and Network Security: Principles and Practices**. 4^{th} Edition. New Jersey: Pearson Education.

วิธีการวัดผล

การมีส่วนร่วมและพฤติกรรมในชั้นเรียน	5%
การบ้าน	35%
โครงงาน	30%
สอบปลายภาค	30%
รวม	100%

วิธีการประเมินผล

การประเมินผลจะเน้นการวัดผลด้านการพัฒนาการเรียนรู้ของนักศึกษาใน 5 ด้าน ได้แก่ ด้านคุณธรรมและจริยธรรม ด้านความรู้ ด้านทักษะทางปัญญา ด้านทักษะความสัมพันธ์ระหว่างบุคคลและความรับผิดชอบ และด้านทักษะทางการสื่อสารและการใช้เทคโนโลยีสารสนเทศ โดยแบ่งเป็น 4 ข้อ ซึ่งสอดคล้องกับวิธีการวัดผล ดังต่อไปนี้

1. การประเมินผลจากการมีส่วนร่วมและพฤติกรรมของนักศึกษาในชั้นเรียน
2. การประเมินผลจากการบ้านที่มอบหมายให้นักศึกษา
3. การประเมินผลจากการทำโครงงานของนักศึกษา
4. การประเมินผลจากผลการสอบปลายภาคของนักศึกษา

โดยการแจกแจงของคะแนนรวม และสังเกตการเกาะกลุ่มของจำนวนนักศึกษาเทียบกับคะแนนรวม แล้วให้ระดับคะแนนเป็นตัวอักษร A, B+, B, C+, C หรือ F

ระดับคะแนน	แต้มระดับคะแนน	คะแนนรวม
A	4.0	80 ขึ้นไป
B+	3.5	75 - 79
B	3.0	70 - 74
C+	2.5	65 - 69
C	2.0	60 - 64
F	0.0	ต่ำกว่า 60

หมายเหตุ : ช่วงคะแนนรวมในที่นี้ เป็นตัวอย่างเท่านั้น ในทางปฏิบัติช่วงคะแนนรวมดังกล่าว อาจแตกต่างไปจากตัวอย่างนี้ได้ ซึ่งจำเป็นต้องพิจารณาเป็นรายกรณีไป

บรรณานุกรม

Agrawal, M., Kayal, N. and Saxena, N. PRIMES is in P. (2004). **Annals of Mathematics** 160(2): 781-793.

Coppersmith, D. (1994). The Data Encryption Standard (DES) and Its Strenth Against Attacks. **IBM Journal of Research and Development.** 38(3): 243-250.

Cormen, T., Leiserson, C., Rivest, R. and Stein C. (2001). **Introduction to Algorithms.** MA: MIT Press

Daemen, J. and Rijmen, V. (2002). **The Design of Rijndael: AES - The Advanced Encryption Standard**. Berlin: Springer-Verlag.

Diffie, W. and Hellman, M. (1976). New Directions in Cryptograph. **IEEE Transactions on Information Theory.** 22(6): 644-654.

ElGamal, T. (1985). A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. **IEEE Transactions on Information Theory.** 31(4): 469-472.

Enge, A. (1999). **Elliptic Curves and Their Applications to Cryptography**MA: Kluwer Academic Publishers.

Fourozan, B.A. (2007). **Data Communication and Networking**. 4^{th} Edition. New Y-ork: Mcgraw-Hill.

Fourozan, B.A. (2008). **Cryptography and Network Security**. New York: Mcgraw-Hill.

Frankkel, S. (2001). **Demystifyint the IPSec Puzzle**. MA: Artech House.

Garrett, P. (2001). **Making, Breaking Codes: Introduction to Cryptology.** NJ: Prentice Hall.

Katzenbeisser, S. and Petitcolas F.A.P. (1999). **Information Hiding Techniques for Steganography and Digital Watermarking.** Boston: Artech House.

Rescorla, E. (2001). **SSL and TLS**. MA: Addison-Wesley.

Rivest, R.L., Shamir, A. and Adleman, L.M. (1978). A method for obtaining digital signatures and public-key cryptosystem. **Communications of the ACM.** 21(2): 120-126.

Stallings, W. (2005). **Cryptography and Network Security: Principles and Practices.** 4^{th} Edition. New Jersey: Pearson Education.

Stallings, W. (2006). The Whirlpool Secure Hash Function. **Cryptologia**. 30(1): 55-67.

Steiner, J. G., Neuman C., Schiller, J. I. (1988). Kerberos: An Authentication Service for Open Network Systems. **Proceedings of the Winter 1998 USENIX Conference.** (pp. 191-202) Texas: USENIX Association.

ดรรชนี