บทที่ 2
เอกสารและงานวิจัยที่เกี่ยวข้อง

2.1 แนวคิดและทฤษฎี

2.1.1 ความรู้ทั่วไปเกี่ยวกับบัตรเครดิต [1]

บัตรเครดิตเป็นที่รู้จักกันครั้งแรกในประเทศสหรัฐอเมริกา เมื่อราวปี พ.ศ. 2493 หรือ เมื่อ 48 ปีมาแล้ว ภายใต้ชื่อ Diners Club ตามมาด้วย American Express ในปี พ.ศ. 2501 Bank American Card ในปี พ.ศ. 2502 ซึ่งต่อมาได้พัฒนาเป็น Visa Card และธนาคารในแถบภาคตะวันออกของสหรัฐอเมริกาได้ร่วมกับธนาคารเวลล์ส ฟาโก (Wells Fargo) ออกบัตรเครดิตชื่อ Master Charge ในปี พ.ศ. 2509 ซึ่งก็คือ Master Card ในปัจจุบัน

สำหรับประเทศไทย ผู้ถือบัตรเครดิตชาวต่างประเทศ เริ่มนำบัตรเครดิตเข้ามาใช้กับร้านค้าในประเทศไทย เมื่อปี พ.ศ. 2503 ต่อมาบริษัท ไดเนอร์สคลับ (ประเทศไทย) จำกัด ได้ออกบัตรไดเนอร์ส ให้กับคนไทยได้ใช้เป็นครั้งแรกในปี พ.ศ. 2512 และถือเป็นบัตรเครดิตสากลใบแรกของไทย บัตรเครดิตได้รับความสนใจเพิ่มขึ้นในบรรดานักธุรกิจชั้นนำ ส่งผลให้ธนาคารพาณิชย์ไทยร่วมกับบริษัทในต่างประเทศออกบัตรเครดิตสากลเพื่อเพิ่มคุณสมบัติของการใช้บัตรเครดิตให้กว้างขึ้น

บัตรเครดิต (Credit Card) เกิดขึ้นจากผลพวงของการพัฒนาระบบการเงินและการธนาคาร เพื่อให้มีเครื่องมือทางการเงิน (Financial Instrument) มากชนิดขึ้น บัตรเครดิต หมายถึง การให้สินเชื่อของสถาบันผู้ออกบัตรแก่ผู้ถือบัตร ซึ่งผู้ถือบัตรสามารถซื้อสินค้าหรือบริการได้โดยไม่ต้องจ่ายเงินทันทีกับผู้ขายสินค้าและบริการ โดยสถาบันผู้ออกบัตรนั้นจะเรียกเก็บเงินจากผู้ถือบัตรในภายหลัง และประโยชน์อื่นที่ผู้ถือบัตรจะได้รับนั้นมีความแตกต่างกันไปตามเงื่อนไขของสถาบันผู้ออกบัตร นอกจากนี้การใช้จ่ายผ่านบัตรเครดิตสามารถสะท้อนสภาพคล่องหรือการถือเงินสดในมือของประชาชน รวมไปถึงพฤติกรรมการบริโภคและค่านิยมของการดำเนินชีวิตที่เกิดขึ้นในแต่ละช่วงเวลาได้อีกด้วย

บัตรเครดิตถือเป็นบริการสินเชื่ออย่างหนึ่งที่ต้องมีการทำตลาดเพื่อเพิ่มจำนวนผู้ถือบัตร กระตุ้นการใช้จ่ายผ่านบัตร และสร้างความภักดีในตัวสินค้าและบริการ ในปัจจุบันการแข่งขันในธุรกิจบัตรเครดิตได้มีการพัฒนาทั้งทางด้านการตลาด การส่งเสริมการขาย รวมทั้งการนำระบบเทคโนโลยีสารสนเทศ มาเป็นกลยุทธ์การตลาดเพื่อใช้เป็นจุดดึงดูดลูกค้า ในสภาวะเศรษฐกิจปัจจุบัน ผู้บริโภคส่วนใหญ่วางแผนการใช้จ่ายอย่างระมัดระวัง ดังนั้นผู้ออกบัตรจึงควรให้ความสน

ใจที่จะวางกลยุทธ์การตลาดในรูปแบบต่างๆ ให้มากขึ้น เพื่อรักษาอัตราการเติบโตของธุรกิจบัตรเครดิตไว้

รูปแบบของบัตรเครดิต

ในปัจจุบันสถาบันผู้ออกบัตรได้ให้บริการบัตรเครดิตประเภทต่างๆ หลากหลายรูปแบบ ซึ่งแตกต่างกันตามวัตถุประสงค์ของการใช้บัตร โดยบริษัท ศูนย์วิจัย ไทยพาณิชย์ จำกัด ได้จัดแบ่งประเภทของบัตรเครดิตออกได้เป็น 3 ประเภทหลักๆ ดังนี้

1. บัตรเครดิตภายในประเทศ (Local Credit Card) เป็นบัตรที่ผู้ถือบัตรสามารถใช้ได้เฉพาะภายในประเทศไทย โดยผู้ออกบัตรคือสถาบันการเงินไทย อย่างไรก็ดี เนื่องจากสถาบันการเงินไทยบางแห่งในปัจจุบันได้จัดตั้งสาขาในต่างประเทศขึ้น และมีบริการให้สมาชิกผู้ถือบัตรเครดิตนั้น สามารถใช้บริการบัตรเครดิตจากสาขาในต่างประเทศได้ด้วยเช่นกัน

2. บัตรเครดิตระหว่างประเทศ (International Credit Card) เป็นบัตรที่ผู้ถือบัตรสามารถใช้ได้ทั้งในและนอกประเทศทั่วโลก โดยผู้ออกบัตรคือ

2.1 ธนาคาร และ สาขาของธนาคารต่างประเทศที่อยู่ในประเทศไทย เช่น ซิตี้แบงก์ ธนาคารสแตนดาร์ดชาร์เตอร์ด และ ธนาคารฮ่องกงและเซี่ยงไฮ้ เป็นต้น

2.2 บริษัทบัตรเครดิต เช่น ไดเนอร์สคลับ และ อเมริกันเอ็กซ์เพรส (เอเม็กซ์) ซึ่งบัตรที่ออกโดย 2 บริษัทนี้ มุ่งเน้นให้บริการเพื่อการเดินทางท่องเที่ยว และการบันเทิง โดยมีชื่อเรียกอีกอย่างว่า T & E Card (Travel and Entertainment Card) บัตรประเภทนี้มีลักษณะเป็น Charge Card คือ ไม่จำกัดวงเงินใช้จ่าย แต่การชำระหนี้ต้องชำระเต็มทุกครั้งเมื่อถูกเรียกเก็บเงิน

2.3 ธนาคารและสาขาของธนาคารต่างประเทศ กับ บริษัทบัตรเครดิต คือ วีซ่าและมาสเตอร์การ์ด ทำการออกบัตรร่วมกัน เช่น บัตรสแตนดาร์ดชาร์เตอร์ด-วีซ่า บัตรซิตี้แบงก์-มาสเตอร์การ์ด และ บัตรธนาคารฮ่องกงและเซี่ยงไฮ้-วีซ่า เป็นต้น

2.4 ธนาคารพาณิชย์ไทยร่วมกับ วีซ่าหรือมาสเตอร์การ์ด เพื่อขยายการให้บริการแก่ลูกค้าให้ใช้บัตรเครดิตได้ทั้งในประเทศและต่างประเทศ เช่น บัตรไทยพาณิชย์-วีซ่า บัตรไทยพาณิชย์-มาสเตอร์การ์ด เป็นต้น

3. บัตรเครดิตร่วม (Affinity Card) เป็นบัตรที่ธนาคารพาณิชย์ไทย ธนาคารต่างประเทศหรือบริษัทบัตรเครดิต ออกบัตรร่วมกับองค์กรธุรกิจขนาดใหญ่ เช่น ห้างสรรพสินค้า โรงแรม ภัตตาคาร เป็นต้น เพื่อเพิ่มคุณค่าของการใช้บัตรให้มากขึ้น โดยผู้ถือบัตรสามารถใช้บัตรนี้ในฐานะ

เป็นบัตรเครดิตของสถาบันผู้ออกบัตร และเป็นบัตรลดเมื่อซื้อสินค้าหรือบริการต่างๆ จากองค์กรธุรกิจนั้นๆ

ความก้าวหน้าทางเทคโนโลยีกับบริการบัตรเครดิต

เนื่องจากสถาบันผู้ออกบัตรพยายามที่จะให้การบริการตรงตามความต้องการของลูกค้าแต่ละกลุ่มมากที่สุด เพื่อเป็นการรักษาจำนวนลูกค้าเดิมในปัจจุบันและเพิ่มลูกค้าใหม่ให้มากขึ้น การนำความก้าวหน้าทางเทคโนโลยีมาประยุกต์ใช้ให้บริการแก่ลูกค้าจึงเป็นความสำเร็จประการหนึ่งของสถาบันการเงินนั้น คือ การให้บริการ Electronic Banking แก่ลูกค้า เพื่อให้ได้รับบริการที่รวดเร็วและครบวงจร ซึ่งได้แก่

- การบริการโอนเงินทางอิเล็กทรอนิกส์ ณ จุดขาย (Electronic Fund Transfer at Point of Sale: EFT/POS) บริการนี้ลูกค้าสามารถชำระเงินค่าซื้อสินค้าและบริการตามจุดขาย (Point of Sale) ที่มีเครื่องอ่านบัตร (Electronic Data Capture: EDC) ได้ ซึ่งเครื่องจะทำการโอนเงินจากบัญชีลูกค้าไปเข้าบัญชีของร้านค้าในทันที ด้วยการส่งคำสั่งไปยังศูนย์คอมพิวเตอร์ของธนาคาร โดยที่ลูกค้าไม่จำเป็นต้องถอนเงินสดจากเครื่อง ATM

- การบริการเบิกถอนเงินอัตโนมัติ (Automatic Teller Machine: ATM) บัตรเครดิตมีคุณสมบัติเป็นบัตร ATM ในบัตรเดียวกัน ซึ่งอำนวยความสะดวกต่อลูกค้าในการเบิก/ถอนเงินสดจากบัญชีธนาคาร โดยเครื่อง ATM จะมีลักษณะการทำงานโดยเชื่อมต่อกับระบบคอมพิวเตอร์ของธนาคารพาณิชย์ในลักษณะ Online

- การบริการธนาคารทางโทรศัพท์ (Telephone Banking) การบริการนี้ช่วยให้ลูกค้าได้รับความสะดวกในการสอบถามข้อมูลบัตรเครดิตได้อย่างรวดเร็ว โดยไม่ต้องเดินทางไปยังที่ทำการของธนาคาร

- การบริการข้อมูลข่าวสารผ่านระบบเครือข่ายอินเตอร์เน็ต (Internet Web Site) เพื่อเพิ่มความสะดวกต่อลูกค้าให้ทราบข้อมูลข่าวสาร และกิจกรรมส่งเสริมการขาย (Promotion) ต่างๆ ของธนาคาร

- การบริการออกบัตรโดยมีรูปถ่ายสีของสมาชิกอยู่บนบัตร เพื่อป้องกันการสูญหายหรือถูกผู้อื่นนำบัตรไปใช้ และยังช่วยสร้างความเชื่อมั่นแก่ร้านค้าในการรับบัตร

บัตรเครดิตแต่ละใบจะมีรหัสประจำบัตรซึ่งเป็นรหัสเฉพาะบัตรนั้น ๆ อยู่ 16 หลัก [2]

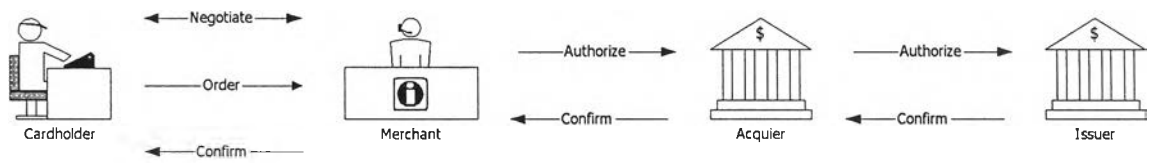
1. สำหรับบัตรภายในประเทศ 4 ตำแหน่งแรกจะใช้สำหรับรหัสของสถาบันการเงินภายในประเทศอ้างอิงตามรหัสของธนาคารไทย
2. สำหรับบัตรเครดิตต่างประเทศ จะใช้รหัสอ้างอิง 6 ตำแหน่งแรก เพื่อแสดงว่าเป็นบัตรของกลุ่มสถาบันการเงินใด เช่น บัตรในกลุ่ม MASTER CARD , บัตรในกลุ่ม VISA

กลุ่มผู้ที่เกี่ยวข้องกับการใช้บัตรเครดิต

กลุ่มผู้ที่เกี่ยวข้องกับการใช้บัตรเครดิตแบ่งได้เป็น 3 กลุ่ม คือ

1. ธนาคารพาณิชย์ที่ให้บริการบัตรเครดิตหรือบริษัทบัตรเครดิต (Issuer / Acquirer)
2. ผู้ถือบัตร (Card holder)
3. ร้านค้ารับบัตร (Merchant)

ซึ่งทั้ง 3 กลุ่มนี้สามารถแสดงความสัมพันธ์ที่มีต่อกันได้ ดังรูปที่ 2.1



รูปที่ 2.1 รูปแสดงความสัมพันธ์ของกลุ่มผู้ที่เกี่ยวข้องกับการใช้บัตรเครดิต

วิธีการชำระหนี้บัตรเครดิต

ผู้ใช้บริการบัตรเครดิต สามารถเลือกวิธีการชำระเงินได้หลายรูปแบบ เช่น

1. ตัดจากบัญชีออมทรัพย์หรือบัญชีเดินสะพัดที่ผู้ถือบัตรเครดิตมีบัญชีกับธนาคารโดยอัตโนมัติ ลูกค้าที่มีบัญชีกับธนาคาร เมื่อขออนุมัติใช้บริการบัตรเครดิตจะลงลายมือชื่อตัวอย่างไว้ และลายมือชื่อดังกล่าวจะถูกส่งไปตรวจสอบความถูกต้อง ณ ธนาคารที่ผู้ขอใช้บริการบัตรระบุบัญชีไว้
2. ชำระด้วยเงินสดหรือเช็คที่หน่วยบริการของธนาคารเจ้าของบัตร
3. ชำระผ่านเครื่องบริการเงินสดทันใจ (Automatic Teller Machine / ATM) ของธนาคารเจ้าของบัตร
4. ชำระผ่านบริการธนาคารทางโทรศัพท์ (Tele Banking)
5. ชำระผ่านเครื่องรับฝากเงินอัตโนมัติ (Cash Deposit Machine)

การใช้บริการบัตรเครดิต

ร้านค้าที่จะเปิดให้ลูกค้าใช้บริการผ่านบัตรเครดิตจะติดต่อกับหน่วยงานของธนาคารเจ้าของบัตร หรือบริษัทบัตรเครดิต เพื่อทำสัญญาการใช้บริการต่าง ๆ

การใช้บริการผ่านบัตรเครดิตในประเทศไทยสามารถใช้ได้ 2 รูปแบบ

1. เครื่องอ่านบัตรเครดิต ณ จุดให้บริการ ซึ่งมี 2 ประเภท

1.1 เครื่องรับบัตรเครดิตธรรมดา หรือทั่วไปเรียกว่า ZIP ZAP เป็นเครื่องใช้ทำสำเนาเลขที่บัตรเครดิตที่อยู่บนบัตรเครดิตลงบนใบเสร็จเพื่อให้ลูกค้าลงลายมือชื่อเมื่อใช้บริการ

เมื่อผู้ใช้บัตรตกลงซื้อสินค้าหรือบริการกับร้านค้าที่ให้บริการเครื่อง ZIP ZAP จะต้องดำเนินการดังนี้

1.1.1 ร้านค้าจะโทรศัพท์ไปยังศูนย์บริการบัตรเครดิตที่ติดต่อด้วย แจ้งเลขที่บัตรเครดิตเพื่อขอตรวจสอบสถานะบัตรและขอตรวจสอบวงเงิน

1.1.2 หากบัตรเครดิตดังกล่าวยังมีวงเงินให้ใช้จ่ายได้เพียงพอ เจ้าหน้าที่ศูนย์บริการบัตรเครดิตจะทำการตัดวงเงินตามที่ร้านค้าแจ้ง

1.1.3 ร้านค้าจะทำการรูดบัตรผ่านเครื่องอ่านเพื่อออกใบเสร็จให้ลูกค้าลงลายมือชื่อในใบเสร็จดังกล่าว เพื่อส่งเป็นหลักฐานการซื้อสินค้าหรือบริการ

1.1.4 เจ้าหน้าที่ร้านค้าตรวจสอบลายเซ็นของลูกค้าบนบัตรกับลายมือชื่อบนใบเสร็จ

1.1.5 ณ สิ้นวันทำการ ต้องรวบรวมใบเสร็จจากเครื่อง ZIP ZAP ที่มีลายเซ็น ส่งเอกสารดังกล่าวไปให้ศูนย์บริการบัตรเครดิตตรวจสอบอีกครั้ง

1.1.6 ศูนย์บริการตรวจสอบลายเซ็น ถ้าถูกต้องจะชำระเงินให้ร้านค้า และรายการเรียกเก็บเงินจากผู้ถือบัตร

1.2 เครื่องรับบัตรเครดิตอัตโนมัติ เป็นเครื่องที่เชื่อมต่อไปยังศูนย์บริการบัตรเครดิตโดยตรง ซึ่งเรียกแล้วแต่ว่าเป็นของธนาคารใด ทั่วไปเรียกว่า EDC (Electronic Data Capture) เพื่ออำนวยความสะดวกในการขออนุมัติวงเงินและพิมพ์ใบบันทึกรายการโดยอัตโนมัติ พร้อมส่งข้อมูลการขายเข้าระบบคอมพิวเตอร์ของธนาคารพาณิชย์ที่ให้บริการบัตรเครดิตหรือบริษัทบัตรเครดิตได้ทันที

เมื่อผู้ใช้บัตรตกลงซื้อสินค้าหรือบริการกับร้านค้าที่ให้บริการเครื่องอ่านบัตรเครดิตอัตโนมัติ จะต้องดำเนินการดังนี้

1.2.1 เจ้าหน้าที่ร้านค้าจะรูดบัตรผ่านเครื่องอ่าน ข้อมูลจากเครื่องอ่านจะถูกส่งผ่านระบบเครือข่ายที่วางไว้ในลักษณะของจุดต่อจุด (Point-to-Point) ส่งไปยังศูนย์ของธนาคารผู้ให้บริการหรือบริษัทเจ้าของบัตรเพื่อตรวจสอบสถานะบัตร และวงเงิน

1.2.2 หากบัตรมีสถานะการใช้งานถูกต้อง วงเงินเพียงพอ เครื่องจะทำการพิมพ์ใบเสร็จอัตโนมัติ เพื่อให้ลูกค้าลงลายมือชื่อ

1.2.3 เจ้าหน้าที่ร้านค้าตรวจสอบลายเซ็นของลูกค้าบนบัตรกับลายเซ็นบนใบเสร็จ

1.2.4 ณ สิ้นวันทำสรุปรายการรับลูกค้าทั้งหมดจากเครื่อง ส่งเอกสารสรุปรายการและใบเสร็จที่มีทั้งหมดส่งไปศูนย์บริการบัตรเครดิตตรวจสอบอีกครั้ง

1.2.5 ศูนย์บริการตรวจสอบลายเซ็น ถ้าถูกต้องทำรายการเรียกเก็บเงิน

1.2.6 กรณีของบัตรภายในประเทศที่ใช้บริการได้เฉพาะธนาคารนั้น ๆ จะไม่สามารถใช้บริการผ่านเครื่องรับบัตรเครดิตอัตโนมัติได้ ยกเว้นแต่ธนาคารนั้น ๆ ได้มีการตกลงร่วมให้มีการใช้บัตรข้ามธนาคารโดยมีการให้วงเงินข้ามธนาคารได้

1.2.7 ถ้าเครื่องรับบัตรเครดิตอัตโนมัติ เกิดการขัดข้องทางด้านการสื่อสารในช่วงระหว่างวันทำการ การขออนุมัติวงเงินยังคงสามารถทำได้ด้วยการขออนุมัติทางโทรศัพท์ เจ้าหน้าที่ของร้านค้ารับบัตร เมื่อขออนุมัติวงเงินทางโทรศัพท์จะได้รับรหัสเพื่อให้ป้อนข้อมูลประกอบรายการใช้บัตรเครดิตนั้น ๆ และรหัสดังกล่าวจะใช้ตรวจสอบอีกครั้งเมื่อมีการส่งเอกสารสรุปรายการ ณ สิ้นวัน

1.2.8 ถ้ารายการในเครื่องรับบัตรเครดิตอัตโนมัติกับรายการที่ผ่านระบบเครือข่ายมายังศูนย์ไม่ตรงกัน จะอ้างอิงตามรายการจากเครื่องรับบัตรเครดิตอัตโนมัติเทียบกับใบเสร็จที่ผู้ถือบัตรลงลายมือชื่อเป็นหลัก

2. การบันทึกข้อมูลลงใบสั่งซื้อสินค้าโดยผู้ซื้อเอง

เมื่อผู้ใช้บริการบัตรเครดิตตกลงซื้อสินค้ากับผู้ขายสินค้าซึ่งให้บริการผ่านทางใบสั่งซื้อ

2.1 ผู้ถือบัตรจะทำการกรอกข้อมูลการสั่งซื้อ , เลขที่บัตรเครดิตและลงลายมือชื่อลงบนใบสั่งซื้อ แล้วส่งใบสั่งซื้อไปยังผู้ขายสินค้า

2.2 ผู้ขายสินค้าจะส่งข้อมูลการสั่งซื้อไปยังธนาคารพาณิชย์ที่ให้บริการบัตรเครดิตหรือบริษัทบัตรเครดิตเพื่อตรวจสอบสถานะของบัตรเครดิตและขอตัดวงเงิน

2.3 เมื่อศูนย์บริการบัตรเครดิตได้รับเอกสารขากผู้ขายสินค้าจะทำการตรวจสอบสถานะบัตร , ตรวจสอบวงเงิน และตัวอย่างลายมือชื่อ

2.4 ถ้าสถานะของบัตรเครดิตไม่ถูกต้อง หรือวงเงินไม่เพียงพอ ธนาคารพาณิชย์ที่ให้บริการบัตรเครดิตหรือบริษัทบัตรเครดิตจะส่งรายการคืนผู้ขายสินค้า

2.5 ถ้าสถานะของบัตรเครดิตถูกต้อง หรือวงเงินไม่เพียงพอ ธนาคารพาณิชย์ที่ให้บริการบัตรเครดิตหรือบริษัทบัตรเครดิตจะรายการผ่านจะทำการตัดวงเงิน และแจ้งผลกลับยังผู้ขายว่ารายการที่ส่งมาสามารถทำรายการได้ในรายการใดบ้าง

หน่วยงานธุรกิจที่ต้องการจะเปิดช่องทางการค้าขายผ่านทางระบบอินเตอร์เน็ตในปัจจุบัน จะมีหลายทางใหม่เลือก ดังนี้

1. เปิดให้บริการบนพื้นที่ของตนเอง โดยขอหมายเลขประจำตัวบนระบบเครือข่ายของตนเอง (IP Address)
2. ขอใช้พื้นที่ของหน่วยงานธุรกิจที่ให้บริการพื้นที่ ซึ่งอาจมีการให้บริการหลายแบบ
    1. แบบฝากขาย คือไม่มีการสร้างพื้นที่หน้าร้านของตนเอง แต่ให้ข้อมูลสินค้าที่มีแล้วโฆษณาผ่านสื่อที่มี
    2. แบบเช่าพื้นที่ แล้วสร้างพื้นที่หน้าร้านเป็นของตนเอง
    3. แบบซื้อพื้นที่ หน่วยงานธุรกิจที่ให้บริการพื้นที่จะทำการขอหมายเลขประจำตัวบนระบบเครือข่ายให้ลูกค้า แล้วลูกค้าจะสามารถสร้างพื้นที่หน้าร้านเป็นของตนเองได้

โดยทั่วไปหน่วยงานธุรกิจที่ให้บริการพื้นที่เหล่านี้จะมีอัตราค่าบริการที่แตกต่างกันขึ้นกับประเภทของการขอใช้บริการ

ในส่วนของระบบรักษาความปลอดภัยที่หน่วยงานธุรกิจที่ให้บริการพื้นที่ ได้แก่

1. การขอใช้บริการจากหน่วยงานที่มีการให้บริการระบบรักษาความปลอดภัย เช่นการใช้บริการของบริษัท VERISIGN ซึ่งเป็นระบบรักษาความปลอดภัยที่ใช้ SOCKET SECURE LAYER (SSL) ซึ่งมีค่าบริการรายเดือน
2. สร้างระบบรักษาความปลอดภัยของตนเอง อาจทั้งทางด้านโปรแกรมระบบ และทางด้านอุปกรณ์ต่าง ๆ

2.1.2 ประเภทของพาณิชย์อิเล็กทรอนิกส์

พาณิชย์อิเล็กทรอนิกส์ถูกแบ่งไว้เป็นกลุ่มต่าง ๆ ในหลาย ๆ รูปแบบ เช่น

พาณิชย์อิเล็กทรอนิกส์จัดแบ่งตามความสัมพันธ์ระหว่างพาณิชย์อิเล็กทรอนิกส์กับกลุ่มผู้ใช้ เป็น 3 ประเภท ดังนี้

1. Consumer-to-Business คือ พาณิชย์อิเล็กทรอนิกส์ระหว่างผู้บริโภคกับธุรกิจ
2. Intra – Org E-commerce คือ พาณิชย์อิเล็กทรอนิกส์ภายในองค์กร เพื่อช่วยให้องค์กรใดองค์กรหนึ่งปรับปรุงการทำงานภายใน และให้บริการลูกค้าได้ดีขึ้น
3. Inter – Org E-commerce คือ พาณิชย์อิเล็กทรอนิกส์ระหว่างองค์กร เป็นแบบเดียวกับพาณิชย์อิเล็กทรอนิกส์ ระดับ B2B (Business to Business)

หรือพาณิชย์อิเล็กทรอนิกส์จัดแบ่งจัดแบ่งตามความสัมพันธ์ของกลุ่มผู้ใช้พาณิชย์อิเล็กทรอนิกส์ด้วยกัน เป็น 4 ประเภท ดังนี้

1. ระดับ B2B (Business to Business) คือ ประเภทที่ธุรกิจกับธุรกิจติดต่อซื้อขายกันผ่านอินเตอร์เน็ต
2. G2G (Government to Government) คือ ประเภทที่หน่วยงานรัฐบาลหน่วยงานหนึ่งติดต่อกับหน่วยงานรัฐบาลอีกหน่วยงานหนึ่งผ่านอินเตอร์เน็ต
3. B2G (Business to Government) คือ ประเภทที่ธุรกิจติดต่อกับหน่วยงานรัฐบาล
4. B2C (Business to Consumer) คือ ประเภทที่ผู้ซื้อปลีกใช้อินเตอร์เน็ตในการซื้อสินค้าจากธุรกิจที่โฆษณาอยู่บนอินเตอร์เน็ต

2.1.3 ความรู้ทั่วไปว่าด้วยการเข้ารหัส (Crytography) [3]

การเข้ารหัส (Cryptography) หมายถึง การเปลี่ยนแปลงข้อมูลให้อยู่ในรูปของรหัสอื่น ๆ เพื่อป้องกันมิให้ผู้ใดเข้าใจความหมายดังกล่าว รวมทั้งป้องกันมิให้ข้อมูลดังกล่าวถูกแก้ไขเปลี่ยนแปลงหรือถูกลบทิ้งหรือถูกนำไปใช้โดยไม่ได้รับอนุญาต โดยที่รหัสที่แปลงนั้นสามารถพิสูจน์ได้ว่าเป็นข้อมูลที่ถูกต้อง (Authenticity) ด้วยเหตุนี้เทคนิคการเข้ารหัสจึงมีความสำคัญเป็นอย่างยิ่งต่อการพัฒนาและการใช้ในเครือข่ายทางการสื่อสารทั้งในระดับระหว่างประเทศและในประเทศ และที่สำคัญอย่างยิ่งเทคโนโลยีการเข้ารหัสมีความสำคัญต่อการเกิดขึ้นและการพัฒนาของพาณิชย์อิเล็กทรอนิกส์ (Electronic Commerce)

เทคนิคในการเข้ารหัสนั้นมีสองประเภทคือ เทคนิคการเข้ารหัสแบบมีรูปลักษณะที่สมมาตร (Symmetric) และเทคนิคการเข้ารหัสแบบที่มีรูปลักษณะที่ไม่สมมาตร (Asymmetric)

เทคนิคการเข้ารหัสแบบมีรูปลักษณะที่สมมาตร (Symmetric) จะใช้มาตรฐาน DES (Data Encryption Standard) โดยที่การเข้ารหัสแบบดังกล่าวจะใช้กุญแจหรือรหัส (Key) เพียงดอกเดียวในการเข้ารหัสและถอดรหัสข้อมูล และจะมีบุคคลเพียงสองฝ่ายเท่านั้นที่ทราบรหัสหรือกุญแจดังกล่าว รหัสหรือกุญแจดังกล่าวจะต้องเก็บไว้เป็นความลับ (Secret)

ส่วนเทคนิคการเข้ารหัสแบบที่มีรูปลักษณะที่ไม่สมมาตร (Asymmetric) จะมีรหัสหรือกุญแจอยู่สองดอก โดยการเข้ารหัสดังกล่าวใช้มาตรฐานที่เรียกว่า RSA ซึ่งตั้งชื่อขึ้นตามผู้ที่ค้นพบคือ Rivest , Shamir และ Adleman มาตรฐาน RSA จะใช้ระบบกุญแจสาธารณะ (Public Key System) โดยจะมีกุญแจอยู่สองดอก ดอกหนึ่งเรียกว่ากุญแจลับ (Secret Key) และอีกดอกหนึ่งเรียกว่ากุญแจสาธารณะ (Public Key) ซึ่งกุญแจสาธารณะ (Public Key) นั้นจะถูกเก็บบันทึกไว้ในฐานข้อมูลที่ทุก ๆ คนสามารถเข้ามานำไปใช้เพื่อพิสูจน์ว่าลายเซ็นอิเล็กทรอนิกส์ดังกล่าวเป็นของบุคคลที่กล่าวอ้างหรือไม่ ส่วนกุญแจอีกดอกหนึ่งเรียกว่ากุญแจลับ (Secret Key) กล่าวคือเป็นกุญแจที่ถือเป็นความลับและจะใช้โดยผู้ที่มีอำนาจใช้ตามกฎหมายเท่านั้น

ในปัจจุบันการเข้ารหัสมักนิยมนำมาใช้เพื่อป้องกันการดักฟัง (Eavesdropping) การรบกวนสัญญาณ (Tampering) หรือการปลอมแปลงสัญญาณ (Forgery) และที่สำคัญอย่างยิ่งเทคโนโลยีการเข้ารหัสสามารถนำมาใช้เพื่อยืนยันความถูกต้อง (Authenticate) ว่าข้อมูลดังกล่าวมีความถูกต้องสมบูรณ์และเป็นของผู้ส่งจริง

2.1.4 ลายมือชื่อดิจิตอล (Digital signature) และลายมือชื่ออิเล็กทรอนิกส์อื่น ๆ [3]

ลายมือชื่อดิจิตอล (Digital signature) คือกลุ่ม (Set) ของตัวเลข (Alphanumeric Characters) ที่เกิดจากการเข้ารหัสทางคณิตศาสตร์ในข้อมูลอิเล็กทรอนิกส์โดยคอมพิวเตอร์

ในทางกฎหมาย ลายเซ็นดิจิตอลคือการทำเครื่องหมาย (Seal) บนข้อมูลดิจิตอลใช้รหัสลายเซ็นส่วนตัว (Private Signature Key) โดยที่การทำเครื่องหมายดังกล่าวจะมีความเกี่ยวเนื่องกับรหัสหรือกุญแจสาธารณะ โดยจะมีบุคคลภายนอกที่ทำหน้าที่รับรอง (Certification Authority) รับรองว่าลายเซ็นดิจิตอลดังกล่าวเป็นของผู้เซ็นจริง

ในทางเทคนิค ลายเซ็นดิจิตอลหมายถึง ค่าทางคณิตศาสตร์ (Numeric Value) ที่ประทับอยู่บนข้อมูลโดยใช้วิธีการทางคณิตศาสตร์สร้างความเชื่อมโยงทางคณิตศาสตร์ระหว่างกุญแจส่วนตัว (Private Key) และกุญแจสาธารณะ (Public Key) ซึ่งเป็นกุญแจที่สามารถใช้ยืนยันว่าลายเซ็นดังกล่าวเป็นของบุคคลที่กล่าวอ้างจริง และที่สำคัญผู้ที่ถือกุญแจหรือรหัสสาธารณะจะไม่สามารถสืบค้นในทางตรรกถึงกุญแจหรือรหัสส่วนตัวได้เลย

โดยวิธีการของลายเซ็นดิจิตอลนี้จะส่งผลให้ไม่มีผู้ใดสามารถเข้าไปแก้ไขข้อความในเอกสารที่ลงลายเซ็นไว้ได้เลย หากมีการแก้ไขแม้เพียงเล็กน้อย จะส่งผลให้กุญแจสาธารณะไม่สามารถยืนยันได้ว่าเอกสารและลายเซ็น ดังกล่าวเป็นของผู้กล่าวอ้างได้เลย

สรุปขั้นตอนในการใช้ลายเซ็นดิจิตอล

1. ผู้ใช้สร้างหรือได้รับกุญแจส่วนตัว (Private key) ที่เกี่ยวเนื่องทางตรรกะกับกุญแจสาธารณะ (Public Key)
2. ผู้ส่งตระเตรียมข้อมูลที่จะส่งทางคอมพิวเตอร์
3. ผู้ส่งทำการย่อยข้อมูล (Message Digest) โดยใช้สูตรทางคณิตศาสตร์ (Secure Hash Algorithm)
4. ผู้ส่งจะทำการเข้ารหัสข้อมูลที่ได้ทำการย่อย (digest) แล้วโดยใช้กุญแจส่วนตัว (Private Key) จะได้รับการผนวกเข้ากับข้อมูลที่ย่อยแล้วโดยใช้สูตรทางคณิตศาสตร์ (Mathmatical Algorithm) ดังนั้นลายเซ็นดิจิตอลจึงเป็นส่วนหนึ่งของข้อความที่จะส่ง หากข้อมูลถูกแก้ไขเพียงน้อยนิดย่อมส่งผลถึงความสมบูรณ์ของลายเซ็นดิจิตอลเสมอ
5. ผู้ส่งผนึกหรือแนบลายเซ็นดิจิตอลเข้ากับข้อความที่จะทำการส่ง
6. ผู้ส่งทำการส่งลายเซ็นดิจิตอลพร้อมกับข้อความ (ที่ได้รับการเข้ารหัสหรือไม่ก็ตาม) ไปยังผู้รับทางอิเล็กทรอนิกส์
7. ผู้รับใช้กุญแจหรือรหัสสาธารณะของผู้ส่งเพื่อตรวจสอบความถูกต้องในลายเซ็นดิจิตอลของผู้ส่ง การตรวจสอบความถูกต้องโดยใช้กุญแจสาธารณะ (Public Key) ของผู้ส่งจะพิสูจน์ว่าข้อมูลหรือข้อความดังกล่าวมาจากผู้ส่งจริง
8. ผู้รับยังสามารถ ย่อยข้อมูล (Message digest) ที่ส่งมา โดยใช้สูตรทางคณิตศาสตร์ (Secure Hash Algorithm) สูตรเดียวกับของผู้ส่ง
9. ผู้รับทำการเปรียบเทียบข้อมูลที่ได้รับการย่อยทั้งสอง หากเหมือนกันก็หมายความว่าข้อมูลดังกล่าวไม่ได้ถูกแก้ไขหลังจากการลงนาม ถ้าหากข้อความที่ส่งมาถูกแก้ไขเพียงแค่หนึ่งบิทข้อมูลที่ทดลองย่อยดูจะแตกต่างจากข้อมูลที่ผู้ส่งส่งมาอย่างเห็นได้ชัด

10. ผู้รับจะได้รับใบรับรอง (Certificate) จากหน่วยงานที่ทำหน้าที่รับรองความถูกต้อง (Certification Authority) ซึ่งจะยืนยันว่าลายเซ็นดังกล่าวมาจากผู้ส่งข้อความนั้นจริง โดยปกติแล้วผู้ที่ทำหน้าที่รับรองความถูกต้อง (Certification Authority) จะเป็นบุคคลที่สามที่ได้รับความไว้วางใจ (trusted Third Party) ซึ่งจะทำหน้าที่จัดการการออกใบรับรองในระบบลายเซ็นดิจิตอล โดยในใบรับรองดังกล่าวจะระบุรายละเอียดที่เกี่ยวกับกุญแจหรือแรหัสสาธารณะ (Public Key) และชื่อของผู้ส่ง (หรืออาจมีข้อมูลอื่น ๆ ถ้าจำเป็น) พร้อมทั้งลายเซ็นดิจิตอลของผู้ที่ทำหน้าที่รับรองความถูกต้อง (Certification Authority)

2.1.5 CyberCash Credit Card Protocol Version 0.8 [4]

Cybercash เป็นการพัฒนาระบบการชำระเงินทั่วไปบน Internet ซึ่งรุ่น 0.8 เป็นการอธิบายถึงการรับชำระด้วยบัตรเครดิต

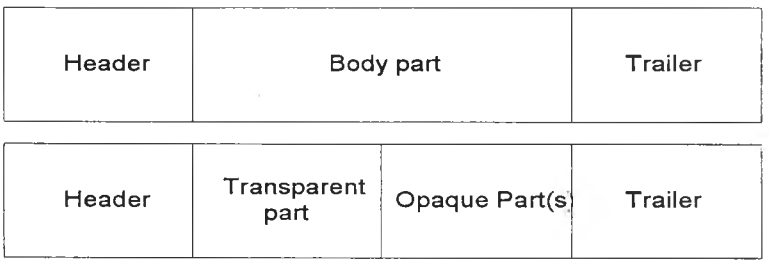
จุดประสงค์ของ CyberCash คือการสร้างการเชื่อมโยงที่เชื่อถือได้ระหว่างโลกของไซเบอร์สเปซกับระบบการธนาคารแบบดั้งเดิม โดยไซเบอร์สเปซจะบริการการรับชำระที่รวดเร็ว ง่าย และปลอดภัยระหว่างผู้ขาย ผู้ซื้อ และธนาคาร สิ่งที่สำคัญอีกอย่างคือผู้ซื้อและผู้ขายไม่จำเป็นต้องพบปะกันเลย

ระบบโดยรวม CyberCash จะให้บริการการรับชำระในหลายรูปแบบ เช่น บัตรเครดิต หรือเงินอิเล็กทรอนิกส์ เพื่อที่จะได้รับการบริการ สำหรับผู้บริโภคแค่มีเพียงเครื่องคอมพิวเตอร์ที่สามารถต่อเชื่อมเข้าระบบเครือข่ายได้ สำหรับผู้ค้าและธนาคารต้องมีกระบวนการทำงานสำหรับการนำรายการที่เกิดขึ้น (CyberCash Transactions) มาใช้งานร่วมกับเครือข่ายการเงินเดิมที่มีอยู่

ผู้ใช้สามารถขอ CyberCash ซอฟต์แวร์ได้จากระบบเครือข่ายอินเตอร์เน็ตซึ่ง ซอฟต์แวร์นี้จะทำการสร้าง (establishing) การเชื่อมโยงระหว่างผู้บริโภค , ผู้ขายและ ธนาคาร

รายการการซื้อสินค้าและ / หรือบริการที่เกิดขึ้นจะถูกส่งอัตโนมัติออกจากเครื่องของผู้บริโภคในรูปแบบที่เข้ารหัสแล้ว

การพิสูจน์ตัวจริง authentication ของข้อความใช้หลักการของ Public Key encrytion ซึ่งพัฒนาโดย RSA



รูปที่ 2.2 แบบข้อความที่ส่งของ CyberCash

แบบข้อความที่ส่งของ CyberCash ประกอบไปด้วยรูปแบบ ดังนี้

1. Header – บอกจุดเริ่มต้นของข้อความ CyberCash และข้อมูลของรุ่น
2. Body Parts

   Body Parts ประกอบไปด้วย 2 ส่วน คือ

   1.1 Transparent Part – เป็นส่วนข้อมูลสาธารณะ ไม่เป็นความลับ เช่น วันที่ขณะทำรายการ

   1.2 Opaque Part(s) – เป็นส่วนข้อมูลทางการเงิน ส่วนนี้จะเป็นข้อมูลลับที่จะถูกเข้ารหัส สามารถแสดงส่วนข้อมูลได้ 2 แบบ คือ

   1.2.1 "opaque" เมื่อเข้ารหัสด้วยลูกค้า

   1.2.2 "merchant-opaque" เมื่อเข้ารหัสด้วยพ่อค้า

   การเข้ารหัสใช้มาตรฐาน RSA ซึ่งใช้ระบบกุญแจสาธารณะ (Public Key System)
3. Trailer – บอกจุดสิ้นสุดของข้อความ CyberCash และประกอบไปด้วยค่าตรวจสอบ (check value) เพื่อผู้รับจะใช้สำหรับการตรวจสอบว่าข้อมูลที่ได้รับนั้นไม่ได้ถูกเปลี่ยนแปลงแก้ไขระหว่างการส่ง

2.1.6 Transaction Security Protocol

1. Secure Socket Layer (SSL)
2. Secure Electronic Transaction (SET)

Secure Socket Layer (SSL)

พัฒนาโดย Netscape ตั้งแต่ปี 2538 และได้รับการเสนอให้เป็นมาตรฐานโดย IETH ปัจจุบันเป็น Version 4 ออกแบบมาเพื่อรักษาความปลอดภัยบนระบบเครือข่าย TCP/IP โดยอาศัยการเข้ารหัสแบบกุญแจสาธารณะของ RSA Data Security,Inc ทำงานอยู่ระหว่างชั้น Network Layer ซึ่งในกรณีของอินเตอร์เน็ตคือ TCP/IP กับ Application Layer สามารถใช้ได้กับโปรแกรมประยุกต์ทุกตัวที่ทำงานบนโพรโตคอล TCP/IP เว็บเบราเซอร์ที่สนับสนุน SSL จะมีเครื่องหมายที่แสดงว่าเว็บเพจนั้นๆ ได้รับการรักษาความปลอดภัย เช่นกรณีของ Netscape Navigator จะแสดงด้วยรูปกุญแจที่มุมล่างด้านซ้าย SSL ถูกนำไปใช้อย่างแพร่หลายทั้งบนอินทราเน็ตและอินเทอร์เน็ตเซอร์ฟเวอร์ และ เบราเซอร์ (ไคลเอนต์) จากผู้ผลิตชั้นนำส่วนใหญ่ต่างก็ให้การสนับสนุน SSL

HTTP	Telnet	NNTP	FTP	SMTP	SHTTP	Etc ...
SSL						
TCP/IP						

รูปที่ 2.3 ภาพแสดงตำแหน่งของ SSL Protocol บนมาตรฐาน OSI

ขั้นตอนการทำงานของ SSL เมื่อไคลเอนต์ขอต่อเข้ามายังหน้าเว็บที่ได้รับการรักษาความปลอดภัยเอาไว้ด้วย SSL เซอร์ฟเวอร์จะขอเปิดการติดต่ออย่างปลอดภัยกลับไปยังไคลเอนต์ หากไคลเอนต์สนับสนุน SSL ก็จะตอบรับกลับมายังเซอร์ฟเวอร์ และถือเป็นการเริ่มติดต่อแบบ SSL (SSL Handshake) โดยเซอร์ฟเวอร์และไคลเอนต์จะแลกเปลี่ยนข้อมูลการรักษาความปลอดภัยซึ่งกันและกัน ในข้อมูลที่ไคลเอนต์ส่งกลับมายังเซอร์ฟเวอร์จะระบุหมายเลขประจำการติดต่อครั้งนั้น อัลกอริทึมของการเข้ารหัสที่จะใช้ และวิธีการบีบอัดข้อมูลที่ไคลเอนต์สนับสนุน จากนั้นเซอร์ฟเวอร์จะติดต่อกลับไปยังไคลเอนต์ด้วยวิธีที่ไคลเอนต์ขอ เซอร์ฟเวอร์กับไคลเอนต์จะส่งสำเนาใบรับรองดิจิตอลให้กันและกันเพื่อตรวจสอบ โดยเซอร์ฟเวอร์จะส่งกุญแจสาธารณะที่สร้างขึ้นเฉพาะสำหรับการติดต่อครั้งนั้น (Session Key) ไปยังไคลเอนต์ด้วย ไคลเอนต์จะใช้กุญแจที่ได้รับในการเข้ารหัสข้อมูลก่อนส่งไปยังเซอร์ฟเวอร์ และเซอร์ฟเวอร์จะสามารถถอดรหัสข้อมูลนั้นได้ด้วยกุญแจส่วนตัวที่คู่กัน ทำให้เวอร์ฟเวอร์และไคลเอนต์สามารถติดต่อกันได้อย่างปลอดภัยทั้งนี้ในการติดต่อกับแต่ละไคลเอนต์ จะใช้กุญแจที่ต่างกัน และกุญแจที่สร้างขึ้นเฉพาะนั้นจะหมดอายุหลังจาก 24 ชั่วโมง

โดยอัตโนมัติ โดยสรุป SSL ได้จัดเตรียมบริการด้านความปลอดภัยพื้นฐานเอาไว้ให้ 3 อย่างดังตาราง

ตารางที่ 2.1 ตารางแสดงบริการด้านความปลอดภัยพื้นฐานของระบบ SSL

บริการ	เทคโนโลยีที่ใช้	สิ่งที่ป้องกันได้
ความเป็นส่วนตัวของข้อความ ความถูกต้องของข้อความ การตรวจสอบซึ่งกันและกัน	การเข้ารหัส รหัสตรวจสอบข้อความ(ใช้ฟังก์ชั่นแฮชและการเข้ารหัส ใบรับรองดิจิตอลตามมาตรฐาน X.509	ผู้ลักลอบอ่านข้อความ ผู้ลักลอบแก้ไขข้อความ ผู้แอบอ้างเป็นบุคคลอื่น

ความเป็นส่วนตัวของข้อความ (Message Privacy) เกิดจากการใช้การเข้ารหัสทั้งแบบกุญแจสาธารณะ (Public Key Encryption) ร่วมกับแบบกุญแจสมมาตร (Symmetric Key Encryption) เพื่อให้สามารถทำการเข้ารหัสและถอดรหัสได้อย่างรวดเร็ว และในขณะเดียวกันก็ยังคงไว้ซึ่งความปลอดภัยในระดับสูง ข้อมูลทุกอย่างที่ส่งไปมาระหว่างเซอร์ฟเวอร์และไคลเอนต์จะถูกเข้ารหัสโดยใช้กุญแจและอัลกอริธึมการเข้ารหัสที่ตกลงกันตอนทำ SSL Handshake ทำให้แม้ผู้ลักลอบอ่านข้อความจะใช้อุปกรณ์ตรวจจับกลุ่มข้อมูลไอพี (IP packet Sniffer) มาอ่านข้อความก็จะมองเห็นแต่ข้อความที่ถูกรหัสเอาไว้

ความถูกต้องของข้อความ (Message Integrity) บริการนี้ช่วยให้สามารถมั่นใจได้ว่าข้อมูลจะไม่ถูกแก้ไขในระหว่างทางที่ส่งไปมาระหว่างเซอร์ฟเวอร์และไคลเอนต์ โดยอาศัยฟังก์ชันแฮช (Hash Function) ประกอบกัน

การตรวจสอบซึ่งกันและกัน (Mutual Authentication) ไคลเอนต์สามารถตรวจสอบใบรับรองกุญแจสาธารณะ (Digital Certificate) เซอร์ฟเวอร์ได้และบน SSL หากผู้ใช้ทางฝั่งไคลเอนต์มีใบรับรองดิจิตอลทางเซอร์ฟเวอร์ก็สามารถขอตรวจสอบตัวตนของผู้ใช้ได้ด้วยเช่นกัน โดยการแลกเปลี่ยนใบรับรองดิจิตอลจะเกิดขึ้นในขั้นตอน SSL Handshake เพื่อให้มั่นใจว่าฝ่ายที่แสดงใบรับรองดิจิตอลเป็นเจ้าของใบรับรองฯนั้นจริง ฝ่ายนั้นจะต้องเซ็นลายเซ็นดิจิตอล (Digital signature) กำกับข้อมูลทุกอย่างที่ส่งให้อีกฝ่ายหนึ่งในขั้นตอน SSL Handshake ซึ่งข้อมูลที่ถูกเซ็นกำกับจะมีตัวใบรับรองฯเองด้วย เพื่อป้องกันไม่ให้ผู้อื่นปลอมแปลงเป็นตัวคุณ โดยแสดงใบรับรองฯของคุณเพราะจะมีเพียงคุณ หรือ ผู้ซึ่งมีกุญแจส่วนตัวที่คู่กับกุญแจสาธารณะบนใบรับรองฯอยู่เท่านั้นที่สามารถเซ็นกำกับข้อมูลได้อย่างถูกต้อง

Secure Electronic Transaction (SET) [5] [6]

คิดค้นโดย VISA และ Master Card และพัฒนาต่อร่วมกับไมโครซอฟท์ ไซเบอร์แคช จีทีอี ไอบีเอ็ม และ เน็ตสเคป เริ่มใช้ในการซื้อขายจริงผ่านอินเตอร์เน็ตเมื่อวันที่ 18 ก.ค. 40 มีความแตกต่างจาก SSL อย่างมาก มีการรักษาความปลอดภัยสูงกว่า SSL โดยมีการตรวจสอบ 3 ฝ่าย คือ ลูกค้าหรือผู้ถือบัตรเครดิต ผู้ขายหรือร้านค้าผู้รับบัตร และธนาคารหรือบริษัทบัตรเครดิต (ธนาคารเป็นตัวกลางในการทำรายการชำระเงิน) และมีการคิดค่าธรรมเนียม ผู้ขายจะไม่ทราบหมายเลขบัตรเครดิตของผู้ซื้อ เนื่องจากข้อมูลเกี่ยวกับบัตรเครดิตจะถูกส่งไปยังธนาคารของผู้ขายโดยตรวจสอบความถูกต้องข้อมูลบัตรเดรดิต และวงเงินกับธนาคารเจ้าของบัตร เมื่อได้รับการอนุมัติวงเงินธนาคารผู้ขายก็จะนำเงินเข้าสู่บัญชีผู้ขาย การซื้อขายด้วยระบบ SET มีซอฟต์แวร์ที่เกี่ยวข้องดังนี้ คือ ทางผู้ซื้อต้องใช้กระเป๋าสตางค์อิเล็กทรอนิกส์ ด้านผู้ขายใช้เซิร์ฟเวอร์พ่อค้า ธนาคารใช้เซิร์ฟเวอร์ที่เป็นเกตเวย์จากระบบ SET ไปยังระบบการเงิน (Payment Gateway)

ตัวอย่างการทำงาน เมื่อผู้ถือบัตรเครดิตของธนาคารหนึ่งที่สนับสนุน SET และดาวน์โหลดกระเป๋าสตางค์อิเล็กทรอนิกส์ มาติดตั้งลงบนคอมพิวเตอร์ ก็จะสามารถขอใบรับรองดิจิตอลตามมาตรฐาน SET จาก CA ที่สนับสนุน SET ซึ่งมักจะเป็นธนาคารหรือบริษัทบัตรเครดิตที่ออกบัตรเครดิตนั้นให้ลูกค้าหรือผู้ถือบัตรมาติดตั้งเอาไว้บนเว็บเบราเซอร์ของลูกค้าหรือผู้ถือบัตร ลูกค้าหรือผู้ถือบัตรกรอกแบบฟอร์มลงทะเบียนบัตรเครดิตเข้าสู่ระบบ SET บนเว็บไซท์ของธนาคาร การทำให้มั่นใจได้ว่าเว็บไซท์ที่ลูกค้าหรือผู้ถือบัตรเข้าไปกรอกแบบฟอร์มนั้นเป็นของธนาคารผู้ออกบัตรจริง กระทำโดยการตรวจสอบใบรับรองของเว็บไซท์ธนาคารที่ส่งมายังเบเบราเซอร์ของลูกค้าหรือผู้ถือบัตรผ่าน SSL เมื่อระบบของทางธนาคารตรวจสอบข้อมูลที่ลูกค้าหรือผู้ถือบัตรกรอกกับฐานข้อมูลแล้วตรงกัน ลูกค้าหรือผู้ถือบัตรจะสามารถดาวน์โหลดใบรับรองมาติดตั้งบนกระเป๋าสตางค์อิเล็กทรอนิกส์ พร้อมที่จะชำระเงินด้วยบัตรเครดิตบนอินเตอร์เน็ต

ผู้ซื้อซึ่งถือใบรับรองของธนาคารและเข้าไปเลือกซื้อสินค้าหรือบริการบนเว็บไซท์ที่สนับสนุน SET หลังจากเลือกสินค้าหรือบริการใส่ลงในรถเข็นหรือตะกร้าอิเล็กทรอนิกส์ แล้วจึงคลิกปุ่มสั่งซื้อทางเซอร์ฟเวอร์ของผู้ขายหรือร้านค้ารับบัตร ผู้ขายหรือร้านค้ารับบัตรจะส่งใบสั่งซื้อที่ระบุรายการสินค้าหรือบริการพร้อมจำนวนและราคามาแสดงบนหน้าจอผู้ซื้อ ให้ผู้ซื้อกรอกที่อยู่สำหรับส่งสินค้าลงไป แล้วเลือกวิธีการชำระเงิน หากเลือกชำระเงินผ่านระบบ SET โปรแกรมกระเป๋าสตางค์อิเล็กทรอนิกส์จะถูกเรียกขึ้นมาโดยอัตโนมัติ ผู้ซื้อป้อนรหัสผ่านแล้วจึงเลือกบัตรเครดิตที่จะใช้ชำระเงิน จากนั้นเซ็นกำกับใบสั่งซื้อและข้อมูลการชำระเงินด้วยใบรับรองดิจิตอลตามมาตรฐาน SET ของผู้ซื้อส่งกลับคืนไปยังผู้ขาย ผู้ขายจะตรวจสอบลายเซ็นดิจิตอลของผู้ซื้อบนใบสั่งซื้อ และส่งต่อข้อมูลการชำระเงินไปยังธนาคารของผู้ขาย เพื่อขออนุมัติการชำระเงิน ธนาคารของผู้ขายจะตรวจสอบกับธนาคารผู้ออกบัตรฯ ว่าข้อมูลบัตรฯถูกต้องและมีวงเงินพอจ่ายหรือไม่

และส่งผลการตรวจสอบไปยังธนาคารผู้ขาย จากนั้นธนาคารของผู้ขายจะแจ้งผลไปยังผู้ขายอีกทอดหนึ่ง ซึ่งหากข้อมูลถูกต้องและมีวงเงินพอจ่าย ธนาคารผู้ออกบัตรฯจะบันทึกรายการชำระเงินของผู้ซื้อเพื่อเรียกเก็บเงินต่อไปส่วนธนาคารของผู้ขายจะโอนเงินเข้าสู่บัญชีของผู้ขาย และในขั้นตอนสุดท้ายผู้ขายจะส่งใบเสร็จให้ผู้ซื้อเก็บไว้ในกระเป๋าสตางค์อิเล็กทรอนิกส์ต่อไป ในทุกขั้นตอนจะมีการเข้ารหัสข้อมูลระหว่างการส่งทั้งหมด

ตารางที่ 2.2 ตารางสรุปข้อเปรียบเทียบระหว่าง SSL กับ SET

หัวข้อที่ทำการเปรียบเทียบ	ลักษณะที่แตกต่างของแต่ละโพรโตคอล	
	SSL	SET
จำนวนฝ่ายที่เกี่ยวข้อง	2 ฝ่าย (เซอร์ฟเวอร์ กับ เบราเซอร์)	3 ฝ่าย (ผู้ซื้อ ผู้ขาย และธนาคาร)
ใบรับรองดิจิตอล	มีเฉพาะฝั่งเซอร์ฟเวอร์	ทุกฝ่ายที่เกี่ยวข้องต้องมี
การตรวจสอบ	เซอร์ฟเวอร์ กับ เบราเซอร์ ต่างตรวจสอบซึ่งกันและกัน	ต้องมี CA ตรวจสอบทุกฝ่ายที่เกี่ยวข้อง
การป้อนข้อมูลบัตรเครดิต	ผู้ซื้อต้องป้อนทุกครั้ง	ข้อมูลบัตรฯ ถูกเก็บไว้ใน E-Wallet จึงป้อนเก็บไว้เพียงครั้งเดียว
การจำกัดการเข้าถึง	สามารถควบคุมการเข้าถึง เซอร์ฟเวอร์ ไดเรคทอรี แฟ้ม และบริการต่างๆ	-ธนาคารผู้ออกบัตรฯไม่ทราบรายละเอียดการซื้อ รักษาความเป็นส่วนตัวของลูกค้า -ผู้ขายไม่ทราบข้อมูลบัตรเครดิตลูกค้า รักษาความปลอดภัย
การใช้ข้อมูลร่วมกัน	เบราเซอร์ สามารถใช้ข้อมูลร่วมกับ เซอร์ฟเวอร์ และป้องกันบุคคลที่ 3 ไม่ให้เข้าถึงข้อมูลได้	คำสั่งซื้อที่เข้ารหัสแล้วถูกส่งให้ผู้ขาย ส่วนข้อมูลบัตรเครดิตที่เข้ารหัสแล้วถูกส่งให้ธนาคารผู้ออกบัตรเครดิต
การป้องกันข้อมูล	เซอร์ฟเวอร์สร้างกุญแจขึ้นสำหรับการสั่งซื้อครั้งนั้นโดยเฉพาะแล้วส่งให้กับเบราเซอร์เพื่อเข้ารหัสคำสั่งซื้อส่งกลับมา	ข้อมูลถูกเข้ารหัสด้วยกุญแจส่วนตัวของผู้ซื้อ
การพิสูจน์ตัวตนของลูกค้าและยอดเครดิตแบบทันที	ไม่สนับสนุน แต่สามารถทำได้โดยเขียนซอร์ฟแวร์จัดการเอง	สนับสนุน
การเข้ารหัสข้อมูลบัตรเครดิต	เข้ารหัสรายละเอียดคำสั่งซื้อกับข้อมูลบัตรรวมกัน จึงมีความแข็งแรงน้อยกว่า	เข้ารหัสคำสั่งซื้อกับข้อมูลบัตรฯ แยกจากกัน และเนื่องจากข้อมูลบัตรฯ มีขนาดตายตัว จึงสามารถเข้ารหัสได้แข็งแรงกว่า
การทำงาน	เบราเซอร์ตรวจสอบใบรับรองดิจิตอลของเซอร์ฟเวอร์ ซึ่งออกให้โดย CA เพื่อให้แน่ใจว่าเซอร์ฟเวอร์เป็นของผู้ขายหรือผู้ให้บริการจริง แล้วจึงใช้การเข้ารหัสแบบกุญแจสาธารณะในการเข้ารหัสข้อมูลโดยเซอร์ฟเวอร์จะสร้างกุญแจขึ้น 1 คู่ เพื่อใช้สำหรับการส่งข้อมูลครั้งนั้น โดยเฉพาะกุญแจส่วนตัวจะถูกเก็บไว้ที่เซอร์ฟเวอร์เอง ส่วนกุญแจสาธารณะจะถูกส่งไปให้เบราเซอร์ใช้ในการเข้ารหัสข้อมูลก่อนส่งมายังเซอร์ฟเวอร์ ข้อมูลที่เข้ารหัสแล้วจะถูกถอดรหัสได้โดยใช้กุญแจส่วนตัวซึ่งอยู่ที่เซอร์ฟเวอร์เท่านั้น	คำสั่งซื้อของลูกค้าจะถูกเข้ารหัสโดยใช้กุญแจส่วนตัวของผู้ซื้อก่อนส่งไปยังผู้ขาย ส่วนข้อมูลบัตรเครดิตจะถูกเข้ารหัสเช่นกันก่อนส่งไปยังธนาคารของผู้ขาย โดยมีการเซ็นลายเซ็นดิจิตอลกำกับข้อมูลที่เข้ารหัสแล้วทั้ง 2 ส่วน ผู้ขายและธนาคารผู้ออกบัตรฯจะถอดรหัสข้อมูลที่ได้รับจากผู้ซื้อ โดยใช้กุญแจสาธารณะของผู้ซื้อ ทำให้ทุกฝ่ายสามารถตรวจสอบตัวตนของอีกฝ่ายหนึ่งได้ก่อนที่ผู้ขายจะยอมรับคำสั่งซื้อ ธนาคารของผู้ขายจะตรวจสอบการอนุมัติวงเงินกับธนาคารผู้ออกบัตรฯ หากได้รับการอนุมัติธนาคารของผู้ขายจะจ่ายเงินเข้าบัญชีของผู้ขาย ส่วนธนาคารผู้ออกบัตรฯ จะบันทึกรายการบัตรฯ เพื่อเรียกเก็บเงินจากผู้ซื้อต่อไป

หัวข้อที่ทำการเปรียบเทียบ	ลักษณะที่แตกต่างของแต่ละโพรโตคอล	
	SSL	SET
ข้อเสีย	• เนื่องจากข้อกำหนดของกระทรวงการต่างประเทศของสหรัฐฯ ซึ่งกำหนดให้ใช้กุญแจที่มีความยาวเพียง 40 บิต ในการส่งข้อมูลระหว่างประเทศ และ 128 บิต สำหรับการส่งข้อมูลภายในประเทศ ทำให้เกิดความไม่แข็งแรงของการเข้ารหัส • สนับสนุนเพียงการส่งข้อมูลจากจุดหนึ่งไปยังอีกจุดหนึ่งเท่านั้น แต่การทำรายการบัตรเครดิตต้องเกี่ยวข้องกันอย่างน้อย 3 ฝ่าย ผู้ซื้อและผู้ขายมีความเสี่ยง โดยผู้ซื้อเสี่ยงต่อการที่ผู้ขายอาจนำข้อมูลบัตรเครดิตของผู้ซื้อไปใช้ในทางที่ไม่เหมาะสม หรือไม่ได้รับสินค้าจากผู้ขาย และผู้ขายเสี่ยงต่อการปลอมแปลงหมายเลขบัตรเครดิต การที่ธนาคารไม่อนุมัติวงเงินสำหรับการซื้อครั้งนั้น หรือการ ปฏิเสธการจ่ายเงินของเจ้าของบัตรฯ เนื่องจากถูกผู้อื่นนำหมายเลขบัตรไปใช้	• ยังมีปัญหาความเข้ากันได้ของระบบ SET จากผู้ผลิตที่ต่างกัน • ระบบสำหรับผู้ขายและธนาคารมีราคาสูงผู้ขายส่วนมากจึงยอมที่จะรับความเสี่ยงบน SSL ซึ่งมีสัดส่วนเพียงเล็กน้อย ผู้ซื้อจะต้องเสียค่าใช้จ่ายเพื่อให้ได้มาซึ่งใบรับรองดิจิตอลทำให้มีผู้ใช้น้อย

2.2 เอกสารและงานวิจัยที่เกี่ยวข้อง

2.2.1 การปกป้องข้อมูลบนอินเตอร์เน็ต [7]

ในระบบอินเตอร์เน็ตซึ่งมีลักษณะเป็น multi-user อาจมีผู้ไม่หวังดีก่อการกระทำอันก่อให้เกิดความเสียหายต่อระบบคอมพิวเตอร์ ซึ่งประกอบด้วย ข้อมูล ซอฟต์แวร์ และ ฮาร์ดแวร์ ซึ่งสามารถแบ่งได้เป็น 4 ลักษณะ คือ การดักจับข้อมูล การเปลี่ยนแปลงแก้ไขข้อมูล การปลอมแปลงข้อมูล และ การขัดจังหวะการทำงานของคอมพิวเตอร์ การป้องกันเหตุการณ์ดังกล่าวอาจทำโดยการเข้ารหัสลับข้อมูล หรือ การออเทนทิเคชันข้อมูลที่ส่งไปในระบบอินเตอร์เน็ต กระบวนการ Encryption (หมายถึง การแปลงรูปแบบข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถอ่านเข้าใจได้ มีวัตถุประสงค์เพื่อปกปิดหรือเก็บซ่อนข้อมูลจากผู้ที่ไม่ประสงค์จะให้ใช้หรือเห็นข้อมูลเหล่านั้น หรือแม้กระทั่งตัวข้อมูลที่ทำการแปลงรูปแล้ว) จัดทำขึ้นเพื่อป้องกันการติดต่อสื่อสารในช่องทางต่างๆที่ไม่ปลอดภัย เช่น A ต้องการส่งข้อมูลสำคัญไปให้ B ดังนั้นเพื่อรักษาความปลอดภัยข้อมูล นอกจาก B แล้ว บุคคลอื่นจะต้องไม่สามารถเห็นข้อมูลเหล่านั้นได้ A จะทำการเข้ารหัสข้อมูล ที่เรียกว่า Plaintext ด้วย Encrypt key ข้อมูลที่เข้ารหัสแล้ว เรียกว่า Ciphertext จะถูกส่งไปยัง B เมื่อ B ได้

รับ Ciphertext แล้ว ก็จะทำการถอดรหัสด้วย Decrypt key และอ่านข้อมูลเหล่านั้น สำหรับบุคคลอื่น ผู้ซึ่ง A ไม่ต้องการให้อ่านข้อมูลเหล่านั้น จะไม่สามารถอ่านข้อมูลดังกล่าวได้ แต่บุคคลเหล่านั้นอาจจะพยายามหา key มาถอดรหัสจนได้ถ้าระบบการเข้าและถอดรหัสที่ใช้ไม่มีประสิทธิภาพดีพอ ระบบการถอดรหัสที่มีอยู่ในปัจจุบันแบ่งได้เป็น 3 ลักษณะ คือ ระบบ Public key cryptosystem (Asymmetric cryptosystem) จะให้ key ที่เข้ารหัส และถอดรหัสที่แตกต่าง อีกระบบ คือ ระบบ Secret key cryptosystem (Symmetric cryptosystem) จะใช้ key เดียวทั้งการเข้ารหัสและถอดรหัส และ ระบบสุดท้าย คือ ระบบการเข้ารหัสลับแบบกุญแจผสม (Mixed Key Encryption)

2.2.2 คริปโตกราฟฟิกอัลกอริทึม

ปัญหาพื้นฐานของการเข้ารหัสข้อมูลคือการทำอย่างไรให้การแปลงเพลนเท็กซ์ (Plaintext) ไปเป็นไซเฟอร์เท็กซ์ (Ciphertext) โดยที่จะไม่ถูกแปลงกลับได้ง่ายโดยผู้ที่ไม่รู้คีย์ (Key) วิธีการแปลงวิธีหนึ่งคือ การใช้โค้ดซิสเท็ม (Code System) คือจะมีโค้ดบุ๊ค หรือคู่มือการแปลงข้อความอยู่ เพลนเท็กซ์ที่ถูกส่งเข้ามาทำการแปลงจะถูกแปลงโดยใช้โค้ดบุ๊คนี้ทำให้ได้ไซเฟอร์เท็กซ์ออกมาจะเห็นว่าคู่ข้อมูลของเพลนเท็กซ์และไซเฟอร์เท็กซ์จะถูกจำกัดโดยขนาดของโค้ดบุ๊คนี้อีกวิธีการหนึ่งเรียกว่า ไซเฟอร์ซิสเท็ม (Cipher System) วิธีการนี้การใช้งานจะต้องประกอบด้วยคริปโตกราฟฟิกอัลกอริทึม (Cryptographic Algorithm) และคริปโตกราฟฟิกคีย์ (Cryptographic Key) คริปโตกราฟฟิกอัลกอริทึม แบ่งได้เป็น 2 ประเภท คือ บล็อกไซเฟอร์อัลกอริทึม (Block Cipher Algorithm) คือ การที่ข้อมูลถูกเข้ารหัสและถอดรหัส เป็นบล็อกของข้อมูลซึ่งขนาดของบล็อกของข้อมูลถูกกำหนดไว้ล่วงหน้าแล้วโดยผู้สร้างอัลกอริทึมและอีกประการหนึ่งคือ สตรีมไซเฟอร์อัลกอริทึม (Stream Cipher Algorithm) คือ อัลกอริทึมที่ผู้ใช้สามารถกำหนดขนาดของข้อมูลที่ทำการเข้ารหัสและถอดรหัสได้เราสามารถจะใช้ทั้งบล็อกไซเฟอร์อัลกอริทึมและสตรีมไซเฟอร์อัลกอริทึมในการทำให้เกิดโหมดของการเข้ารหัสแบบต่าง ๆ ได้โดยอาศัยวิธีการฟีดแบ็ค (Feedback) หรือ เซนนิ่ง (Chaining) ซึ่งก็คือการเอาข้อมูลที่เกิดขึ้นในอดีตมาเป็นตัวกำหนดข้อมูลในปัจจุบันซึ่งนอกจากจะทำให้เกิดความปลอดภัยของข้อมูลเพิ่มมากขึ้นแล้วยังสามารถใช้ในการทำการออเทนธิเคชันได้ด้วย

ในกรณีของโค้ดบุ๊คจะเห็นว่าการแปลงเพลนเท็กซ์เป็นไซเฟอร์เท็กซ์จะถูกกำหนดและจำกัดโดยขนาดของโค้ดบุ๊คโดยถ้าโค๊ดบุ๊คมีขนาดเล็กความปลอดภัยของข้อมูลก็จะน้อยเราจะสามารถมองได้ว่าคริปโตกราฟฟิกอัลกอริทึม คือ โค้ดบุ๊คที่มีขนาดใหญ่มากและมีรูปแบบการแปลงเพลนเท็กซ์เป็นไซเฟอร์เท็กซ์ได้หลายรูปแบบมากโดยในแต่ละรูปแบบจะถูกกำหนดโดยคีย์ซึ่งรูปแบบของการแปลงจากเพลนเท็กซ์ไปเป็นไซเฟอร์เท็กซ์ก็จะมีน้อย การแปลงข้อมูลจากเพลน

เท็กซ์เป็นไซเฟอร์เท็กซ์นี้เรียกว่าการเข้ารหัส (Encryption) โดยในการแปลงแต่ละครั้งจะต้องสามารถทำการแปลงกลับจากไซเฟอร์เท็กซ์เป็นเพลนเท็กซ์ได้ด้วยคีย์เดียวกัน การทำเช่นนี้เรียกว่าการถอดรหัส (Decryption) นอกจากคริปโตกราฟฟิกอัลกอริทึมสามารถแบ่งออกเป็นบล็อกไซเฟอร์และสตรีมไซเฟอร์แล้วเรายังสามารถแบ่งตามลักษณะของการใช้คีย์ได้ด้วยคือการเป็นไพรเวทคีย์อัลกอริทึมและพับบลิคคีย์อัลกอริทึม โดยไพรเวทคีย์อัลกอริทึม คือ อัลกอริทึมที่ใช้คีย์ในการเข้ารหัสหรือถอดรหัสเป็นคีย์เดียวกัน ส่วนพับบลิคคีย์อัลกอริทึม คือ อัลกอริทึมที่อนุญาตให้ใครก็ได้ในข่ายสื่อสารนั้นสามารถทำการเข้ารหัสข้อมูลส่งมาให้เราผ่านทางข่ายสื่อสารสาธารณะโดยใช้พับลิคคีย์ ซึ่งเป็นคีย์ของเราซึ่งเปิดเผยต่อสาธารณชนดังนั้นทุกคนในข่ายสื่อสารนี้ก็สามารถจะรับไซเฟอร์เท็กซ์ชุดนี้ได้ แต่จะมีเพียงเราเท่านั้นที่สามารถจะถอดรหัสได้โดยใช้คีย์อีกตัวหนึ่ง ซึ่งเป็นซีเคร็ทคีย์ (Secret Key) หรือคีย์ที่เป็นความลับ

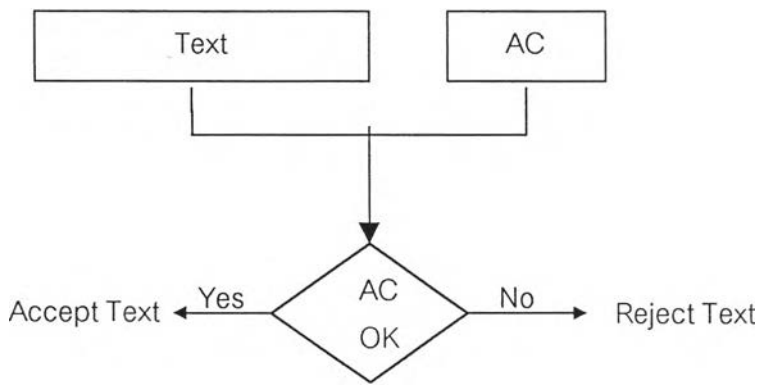
2.2.3 ออเทนทิเคชัน และ ลายเซ็นต์ดิจิตอล (Authentication & Digital Signature)

การออเทนทิเคชัน (Authentication) คือ กระบวนการที่ใช้สำหรับพิสูจน์ว่าข้อความหรือข้อมูลนั้นเป็นของจริงโดยสมบูรณ์ไม่ใช่ของที่ถูกทำเลียนแบบขึ้นมา หรือของจริงที่ถูกแก้ไขไปบางส่วนโดยปกติแล้วการทำออเทนทิเคชันจะมีหลักการคือ การสร้างรหัสรับรองข้อความขึ้นมาจากข้อความหรือข้อมูลนั้น เพื่อให้ได้เป็นข้อมูลอีกชุดหนึ่งสำหรับไว้ใช้เป็นตัวตรวจสอบ

Authentication Protocols สามารถใช้ได้ทั้งแบบ Secret key cryptosystem เช่น DES algorithm และแบบ Public key cryptosystem เช่น RSA ในการ Authentication แบบ Public key cryptosystem จะใช้ Digital signature การ Authentication โดยใช้ Digital signature คือการใช้ฟังก์ชันใดฟังก์ชันหนึ่งเพื่อประมวลผล Digital Document ซึ่งมีลักษณะคล้ายการเซ็นต์ชื่อรับรองเอกสารที่พิมพ์ออกมา signature หมายถึงส่วนข้อมูลที่ไม่สามารถปลอมแปลงได้ของบุคคลที่ทำการเซ็นต์กำกับเอกสารนั้น ส่วนผู้รับสามารถทำการตรวจสอบเอกสารว่า signature ที่ติดมาด้วยนั้นเป็นของผู้ส่งที่แท้จริงหรือไม่ ในระบบ Digital signature จะมีส่วนประกอบ 2 ส่วน ได้แก่ การ sign document เพื่อป้องกันการปลอมแปลง และ การตรวจสอบหรือยืนยัน signature ว่า sign มาจากผู้ส่งจริงหรือไม่ นอกจากนั้น ในระบบ Digital signature ไม่สามารถปฏิเสธ signature ที่ sign นั้นได้

การรับรองข้อความหรือเมสเสจออเทนทิเคชัน (Message Authentication)

เมสเสจออเทนทิเคชัน คือ การจัดการเกี่ยวกับข้อมูลเพื่อให้แน่ใจว่าข้อความที่ได้รับนั้นเป็นข้อความที่ผู้ส่งต้องการส่งให้เราจริง ถ้าหากว่ามีการแก้ไขเปลี่ยนแปลงหรือความผิดพลาดของข้อความเนื่องจากมีผู้ตั้งใจจะเปลี่ยนข้อความสัญญาณรบกวนในสายนำสัญญาณหรือด้วยสาเหตุใดก็ตาม "รหัสรับรองข้อความ" (Message Authentication Code) หรือ MAC หรือ AC ต่อท้ายมาด้วย ทางด้านผู้รับเมื่อได้รับข้อความข่าวสารก็จะสร้างรหัสรับรองข้อความนี้ขึ้นมาเปรียบเทียบกับรหัสรับรองข้อความที่ส่งมาถ้าหากว่ามีค่าเท่ากันก็จะถือได้ว่าข้อความข่าวสารนั้นเป็นข้อความที่มาจากแหล่งกำเนิดจริงถ้าหากว่าไม่เท่ากัน ก็แสดงว่าข่าวสารนั้นอาจจะถูกแก้ไขเปลี่ยนแปลงหรือถูกตัดตอนออกไป ดังรูปที่ 2.4



รูปที่ 2.4 แสดงวิธีตรวจสอบข้อความโดยใช้รหัสรับรองข้อความ

รหัสรับรองข้อความที่ดีซึ่งเป็นส่วนสำคัญของการทำการรับรองข้อความควรจะมีลักษณะดังนี้

1. ฝ่ายตรงข้ามไม่สามารถจะหาฟังก์ชันในการสร้างรหัสรับรองข้อความได้
2. ฝ่ายตรงข้ามไม่สามารถจะคำนวณหาข้อความใหม่ M' ในกรณีที่บังเอิญรหัสรับรองข้อความใหม่ AC' เหมือนกับรหัสรับรองข้อความเดิม AC ไม่เช่นนั้นแล้วฝ่ายตรงข้ามอาจจะแทนที่ข้อความเดิม M ด้วย M' ในขณะที่ยังคงทำให้ AC ไม่เปลี่ยนแปลง
3. รหัสรับรองข้อความ AC ควรจะมีค่าแตกต่างกันในกรณีที่ M = M' โดยความน่าจะเป็นของการแตกต่างกันของ AC คือ $1/2^{c}$ โดยที่ C จำนวนบิตใน AC

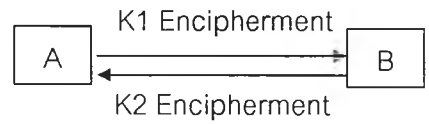
การรับรองข้อความ คือ วิธีการที่เมื่อมีการติดต่อส่งข้อมูลระหว่างฝ่ายรับและฝ่ายส่ง จะเป็นตัวแสดงว่าข้อมูลที่ฝ่ายรับได้รับเป็นข้อมูลที่แท้จริงที่ผู้ส่งต้องการส่งให้ หน้าที่ของการทำการรับรองข้อความ คือ การทำให้ผู้รับข้อมูลได้ทราบถึง สภาวะต่อไปนี้

1. ข้อมูลหรือข้อความนั้นถูกสร้างขึ้นมาและส่งโดยผู้ใด
2. เนื้อหาของข้อความนั้นไม่ถูกเปลี่ยนแปลงไปไม่ว่าจะด้วยความตั้งใจหรือบังเอิญ
3. ข้อความถูกส่งไปยังผู้รับที่ผู้ส่งตั้งใจจะส่งไปให้

การแสดงการรับรองการเป็นผู้สร้างข้อความ (Authentication of a Message's origin)

วิธีการที่จะแสดงว่าผู้ใดเป็นผู้สร้างข้อความ (ผู้ส่งข้อความ) 2 วิธี คือ

<u>วิธีที่ 1</u> ใช้คีย์ที่แตกต่างกันในการรับและส่งข้อความระหว่างผู้รับและผู้ส่ง ดังรูปที่ 2.5



รูปที่ 2.5 แสดงการเข้ารหัสโดยใช้คีย์ที่ต่างกัน

A และ B ใช้คีย์ K1 และ K2 โดยที่ K1 ใช้สำหรับส่งจาก A ไป B เท่านั้น และ K2 ใช้สำหรับส่งจาก B ไป A เท่านั้น B จะรู้ว่าข้อความถูกส่งมาจาก A ก็ต่อเมื่อใช้คีย์ K1 ในการถอดรหัสแล้วสามารถอ่านข้อความได้ ในทำนองเดียวกันจะสรุปได้ว่าข้อความถูกส่งมาจาก B ถ้าหากว่า A สามารถใช้คีย์ K2 ในการถอดรหัสและอ่านข้อความได้

<u>วิธีที่ 2</u> คือ A และ B ใช้คีย์เดียวกัน ในการรับและส่งข้อความในส่วนต้นของข้อความจะมีรหัสผ่าน (Password) อยู่โดยที่ A และ B จะรู้รหัสผ่านของกันและกันโดยสมมติว่า PW_a และ Pw_b เป็นรหัสผ่านของ A และ B ตามลำดับ A จะส่ง PW_a ไปกับข้อความที่จะส่งไป B ทุกครั้ง เมื่อ B ได้รับข้อมูลก็จะตรวจสอบว่ารหัสผ่านที่มากับข้อมูลนั้นตรงกับรหัสผ่านของ A ที่มีอยู่ในฐานข้อมูลหรือไม่ ถ้าตรงกันก็แสดงว่าข้อมูลนั้นถูกส่งมาจาก A

การแสดงการรับรองความถูกต้องของเนื้อหาของข้อวาม (Authentication of Message's content)

เนื้อหาของข้อความจะถูกพิสูจน์ว่าถูกต้องหรือไม่จากที่เราเรียกว่า **รหัสรับรองข้อความ** หรือ MAC ซึ่งถูกสร้างขึ้นมาจากผู้ส่งและต่อท้ายเข้าไปยังข้อความก่อนที่จะส่งมาให้ผู้รับ ซึ่งมี 2 วิธีคือ

1. รับรองความถูกต้องของเนื้อหาของข้อความโดยวิธีการเข้ารหัสที่มีคุณสมบัติของการแพร่กระจายความผิดพลาด

การรับรองความถูกต้องของเนื้อหาของข้อความจะไม่ยุ่งยากถ้าหากเราใช้วิธีการเข้ารหัสที่มีคุณสมบัติของการแพร่กระจายความผิดพลาดเช่นการใช้วิธีการเข้ารหัสที่เป็นแบบบล็อคเชนนิ่งเพลนเท็กซ์ ไซเฟอร์เท็กซ์ฟีดแบ็ค ตัวอย่างหนึ่งคือวิธีการการต่อท้ายข้อความที่จะส่งด้วยข้อความชุดหนึ่งที่รู้กันทั้งผู้ส่งและผู้รับ (เช่น เวกเตอร์เริ่มต้นหรือบล็อกแรกของข้อความนั้น X(i) ก่อนจะทำการเข้ารหัส หลังจากถอดรหัสแล้วเราจะตรวจสอบความถูกต้องของข้อความได้โดยการเปรียบเทียบส่วนที่ต่อท้ายเข้าไปนี้ระหว่าง ด้านรับและด้านส่งถ้าหากว่ามีค่าเท่ากันแสดงว่าข้อความถูกต้องแต่ถ้าไม่ตรงกันแสดงว่ามีข้อผิดพลาดขึ้นในข้อความนั้น สมมุติว่าข้อความที่นำมาต่อท้ายมีขนาด C บิต โอกาสในการที่จะพิสูจน์ได้ว่าข้อความนั้นถูกต้องหรือไม่มีถึง $(2^c-1)/2^c = 1-2^{c-1}$

2. การรับรองความถูกต้องของเนื้อหาของข้อความโดยวิธีการเข้ารหัสที่ไม่มีคุณสมบัติของการกระจายความผิดพลาด

ถ้าวิธีการเข้ารหัสที่เราใช้ไม่มีคุณสมบัติของการกระจายความผิดพลาด (ตัวอย่างเช่น ไซเฟอร์บล็อคเชนนิ่ง CBC) แล้ว การเปลี่ยนแปลงของไซเฟอร์เท็กซ์อาจจะไม่ทำให้บล็อคสุดท้ายของเพลนเท็กซ์ที่ถูกถอดรหัสกลับมาเปลี่ยนแปลงไปก็ได้ ในกรณีเช่นนี้การพิสูจน์ความถูกต้องของเนื้อหาของข้อความจะแตกต่างไปจากหัวข้อก่อนหน้านี้เล็กน้อย เนื่องจากความผิดพลาดในไซเฟอร์เท็กซ์บล็อคใด ๆ ไม่ทำให้เกิดการแพร่กระจายความผิดพลาดในเพลนเท็กซ์ที่ถูกรหัสกลับมาแต่จะเกิดความผิดพลาดเฉพาะบล็อคนั้นแทน ดังนั้นรูปแบบของของบิตที่จะนำไปต่อท้ายข้อความจะต้องขึ้นอยู่กับข้อความทั้งหมดหรือเป็นฟังก์ชัน ▲ ของข้อความทั้งหมด (ไม่ใช่เฉพาะส่วนใดส่วนหนึ่งของข้อความ) จะทำการแปลงข้อความ M ที่มีความยาว ขนาดเท่าไรก็แล้วแต่เป็นข้อความที่มีขนาดเล็กมีจำนวนบิตที่แน่นอนและโอกาสที่ข้อความ M และ M' ที่ต่างกันซึ่งมีบิตที่จะทำให้เกิดบิตที่จะต่อท้ายข้อความ ▲(M) และ ▲(M)' ที่ต่างกันมีความน่าจะเป็นสูงการเข้ารหัส ▲(M) นี้จะทำให้เกิดเป็นรหัสรับรองข้อความขึ้น

การแสดงการรับรองผู้รับข้อความ (Authentication of Message's Receiver)

การที่จะระบุว่าผู้รับรายใดคือผู้ที่ผู้ส่งตั้งใจจะส่งข้อความไปให้นั้นจะมีวิธีการคล้ายกับการรับรองว่าผู้ใดเป็นผู้สร้างข้อมูลดังได้กล่าวถึงแล้วในหัวข้อก่อนหน้านี้ ซึ่งจะกล่าวโดยสรุปเป็นข้อ ๆ ได้ดังนี้ สมมติว่า A และ B คือผู้ส่งและผู้รับข้อความตามลำดับ B จะสามารถรู้ว่าข้อความดังกล่าวถูกส่งมาให้ตัวเองจริงถ้าใช้วิธีการข้อใดข้อหนึ่งดังต่อไปนี้

1. A และ B ใช้คีย์ 2 คีย์โดยที่ทั้ง A และ B รู้คีย์ทั้งคู่โดยคีย์หนึ่งใช้สำหรับเข้ารหัสข้อมูลและส่งจาก A ไป B อีกคีย์หนึ่ง B ใช้เข้ารหัสข้อมูลแล้วส่งไปให้ A

2. A และ B ใช้คีย์เดียวกันในการเข้ารหัสและส่งข้อมูลระหว่างกัน แต่ส่งรหัสประจำตัว ของผู้รับลงไปในข้อความด้วย

วิธีการสำหรับการทำการรับรองข้อความ

จากการแสดงการรับรองของส่วนต่าง ๆ ของข้อความตามที่ได้กล่าวมาแล้วนั้นจะนำทั้งหมดมารวมเป็นวิธีหรือขั้นตอนที่ใช้ในการรับรองข้อความ มีคุณลักษณะดังนี้

1. ใช้วิธีการเข้ารหัสที่มีคุณสมบัติของการกระจายของความผิดพลาดในการรับรองเนื้อหาของข้อความ

2. ใช้รหัสผ่านเพื่อแสดงว่าผู้ใดเป็นผู้รับหรือผู้ส่ง

วิธีการรับรองข้อความที่มีคุณสมบัติครบทั้ง 3 ส่วน (ผู้ส่ง, เนื้อหา, ผู้รับ) จะให้ความปลอดภัยสูงสุด อย่างไรก็ตามในการประยุกต์ใช้งานบางงานเราไม่จำเป็นต้องสร้างวิธีรับรองข้อความให้มีคุณสมบัติครบทั้ง 3 ข้อ เพียงแต่ให้มีคุณสมบัติข้อใดข้อหนึ่งเหมาะสมกับงานนั้น ๆ ก็เพียงพอ

2.2.4 การเข้ารหัสลับ (Cryptography)

การแปลงข้อมูลให้อยู่ในรูปแบบอื่นที่แตกต่างไปจากเดิม เพื่อปกปิดเนื้อหาที่แท้จริง เรียกว่า การเข้ารหัสลับข้อมูล ในการเข้ารหัสลับนี้จะต้องมีอัลกอริทึมสำหรับเข้ารหัสลับ ซึ่งเป็นขั้นตอนการแปลง ข้อมูลให้มีรูปแบบที่เปลี่ยนไป และมีคีย์สำหรับเข้ารหัสลับ ซึ่งถูกเก็บเป็นความลับ และเมื่อต้องการเข้ารหัสลับข้อมูลก็จะนำข้อมูลและคีย์สำหรับการเข้ารหัสลับผ่านเข้าไปทำงานในอัลกอริทึม ก็จะได้ผลลัพธ์เป็นข้อมูลที่เข้ารหัสแล้ว มีเพียงเจ้าของและผู้มีสิทธิรู้ค่าคีย์สำหรับเข้ารหัสลับเท่านั้น ที่จะถอดรหัสข้อมูลให้อยู่ในรูปเดิมได้ โดยวิธีการเข้ารหัสลับนี้จะทำให้ข้อมูลมีความปลอดภัย เพราะถ้าข้อมูลนี้ตกไปอยู่ในมือของผู้อื่นที่ไม่มีสิทธิหรือฝ่าย

ตรงข้ามก็จะไม่มีประโยชน์เพราะข้อมูลอยู่ในรูปแบบที่ไม่อาจอ่านเข้าใจได้ ไม่ได้มีความหมายที่แท้จริงและไม่สามารถที่จะถอดรหัสข้อมูลได้ เนื่องจากไม่ทราบค่าคีย์สำหรับเข้ารหัสลับหรือไม่ทราบขั้นตอนการทำงานของอัลกอริทึมที่ใช้ในการถอดรหัส

สิ่งที่สำคัญสำหรับการเข้ารหัสลับ ก็คือ คีย์สำหรับการเข้ารหัสลับ ซึ่งจะต้องเก็บเป็นความลับไม่ให้ผู้ที่ไม่มีส่วนเกี่ยวข้องรู้ และอัลกอริทึมที่ใช้สำหรับการเข้ารหัส จะต้องมีการทำงานที่มีประสิทธิภาพ มีขั้นตอนการทำงานที่ซับซ้อน สามารถป้องกันข้อมูลให้มีความปลอดภัย ทำให้ผู้ที่สามารถดักจับข้อมูลได้จะไม่สามารถที่จะหาค่าคีย์หรือข้อมูลที่แท้จริงได้

การเข้ารหัสลับกระทำเพื่อปกปิดข้อมูลที่มีความสำคัญให้เป็นความลับ โดยการเปลี่ยนรูปแบบของข้อมูลให้อยู่ในรูปแบบอื่น ได้มีการใช้กันมาตั้งแต่สมัยอียิปต์โบราณกว่า 4000 ปีมาแล้ว และได้มีการพัฒนาวิธีการมาเป็นรูปแบบต่าง ๆ แบ่งได้กว้าง ๆ เป็น 2 ระบบ (Meyer and Matyas,1982) คือ ระบบการเข้ารหัสข้อมูลด้วยการใช้พจนานุกรม (Code System)(และระบบการเข้ารหัสลับ (Cryptographic System หรือ Cipher System) ในระบบการเข้ารหัสข้อมูลด้วยพจนานุกรม จะต้องมีพจนานุกรม (Code book หรือ Dictionary) เพื่อใช้ในการเข้ารหัสในระดับคำ วลี หรือประโยคของข้อมูลเนื้อแท้ (Plaintext) ให้ออกมาเป็นข้อมูลเข้ารหัส (Ciphertext) ส่วนระบบการเข้ารหัสลับ จะเป็นการเข้ารหัสในระดับที่เป็นตัวอักษรแต่ละตัวหรือในระดับบิตแต่ละบิตและจะต้องมีค่าคีย์ที่เป็นความลับ ข้อมูลเนื้อแท้และคีย์จะต้องผ่านการดำเนินการเพื่อให้ได้ผลลัพธ์ออกมาแตกต่างจากของเดิม เพื่อปกปิดข้อมูลที่แท้จริงไว้

วิธีการพื้นฐานของระบบการเข้ารหัสลับ เช่น วิธีการแทนที่ข้อมูล (Substitution Cipher) หรือวิธีการสลับตำแหน่งของข้อมูล (Transposition หรือ Permutation cipher) ซึ่งในสมัยก่อนวิธีการเหล่านี้ได้รับการยอมรับว่าทำให้ข้อมูลมีความปลอดภัย แต่เมื่อมาถึงยุคสมัยนี้ความเจริญทางด้านเทคโนโลยีได้ก้าวหน้าขึ้นมากและมีการนำคอมพิวเตอร์มาใช้ ทำให้การทำงานหรือการแก้ปัญหาต่าง ๆ ทำได้ในเวลาอันรวดเร็ว ทำให้วิธีการเหล่านี้ไม่มีความปลอดภัยเพียงพอสำหรับข้อมูลที่มีความสำคัญ จึงต้องหาวิธีการที่ทำให้มีความปลอดภัยสำหรับข้อมูลมากยิ่งขึ้น

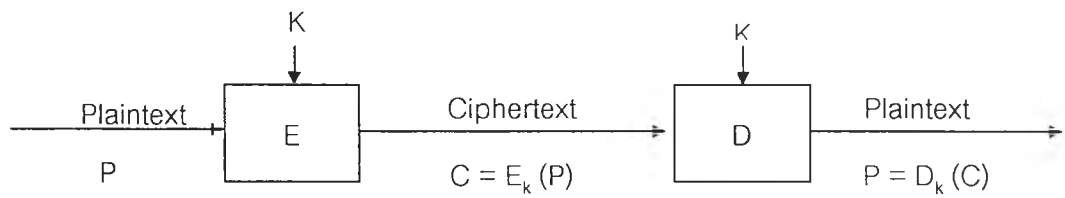
ส่วนประกอบที่สำคัญของระบบการเข้ารหัสลับประกอบด้วย 2 ส่วน คือ อัลกอริทึมสำหรับการเข้ารหัสลับ (Cryptiographic Algorithm) และคีย์สำหรับการเข้ารหัสลับ (Cryptographic Key)

อัลกอริทึมสำหรับการเข้ารหัสลับ (Cryptographic Algorithm) คือ ขั้นตอนหรือวิธีการในการเข้ารหัสลับข้อมูลให้เป็นความลับ มีการดำเนินการหลักอยู่ 2 ส่วน ส่วนแรก คือ การดำเนินการเข้ารหัส (Encryption หรือ Encipherment) เป็นการเปลี่ยนข้อมูลเนื้อแท้ให้เป็นข้อมูลเข้ารหัส โดยต้องมีคีย์สำหรับการเข้ารหัสลับส่งผ่านเข้าไปในส่วนการดำเนินการนี้ และส่วนที่สอง

คือ การดำเนินการถอดรหัส (Decryption หรือ Decipherment) เป็นการเปลี่ยนข้อมูลเข้ารหัสให้กลับเป็นข้อมูลเนื้อแท้เหมือนเดิม และจะต้องมีคีย์ที่ใช้สำหรับการถอดรหัสลับเช่นเดียวกัน

คีย์สำหรับการเข้ารหัสลับ (Cryptographic Key) คือข้อมูลที่ถูกเก็บเป็นความลับเพื่อใช้ในขณะที่ดำเนินการเข้าและถอดรหัสลับ คีย์นี้มีความสำคัญมากจะต้องเก็บเป็นความลับเนื่องจากถ้าหากว่ารู้ค่าของคีย์แล้วก็จะสามารถถอดรหัสข้อมูลได้ทันที

จากรูปที่ 2.6 E คือการดำเนินการเข้ารหัสลับข้อมูล และ D คือ การดำเนินการถอดรหัสลับข้อมูล P คือ ข้อมูลเนื้อแท้ ที่ต้องใส่เข้าในส่วนดำเนินการเข้ารหัส หรือได้จากการดำเนินการถอดรหัส C คือข้อมูลเข้ารหัส เป็นผลลัพธ์จากการดำเนินการเข้ารหัส และ K คือ คีย์สำหรับการเข้ารหัสลับ



รูปที่ 2.6 แสดงการดำเนินการเข้ารหัสลับและการดำเนินการถอดรหัสลับ

จะเห็นว่าระบบการเข้ารหัสลับที่จะสามารถป้องกันข้อมูลให้ปลอดภัยได้ จะขึ้นอยู่กับคีย์และ อัลกอริทึม โดยที่คีย์จะต้องถูกเก็บเป็นความลับและอัลกอริทึมสำหรับการเข้ารหัสลับจะต้องมีการออกแบบที่ดี มีขั้นตอนวิธีการทำงานที่ซับซ้อนและสามารถป้องกันข้อมูลได้อย่างมีประสิทธิภาพ แม้ว่าจะมีการลักลอบรู้ข้อมูลที่เข้ารหัสแล้ว แต่จะไม่สามารถถอดรหัสออกได้ว่าข้อมูลที่แท้จริงคืออะไร หรือถ้าจะสามารถถอดรหัสได้ ก็ต้องใช้ระยะเวลานานและใช้ทรัพยากรต่าง ๆ เป็นจำนวนมาก ทำให้ไม่สามารถที่จะหาข้อมูลนั้นได้ จึงทำให้ข้อมูลมีความปลอดภัย

National Bureau of Standards (NBS) ได้เสนอคุณสมบัติของอัลกอริทึม สำหรับการเข้ารหัสลับ (Meyer and Matyas,1982) ไว้ดังนี้

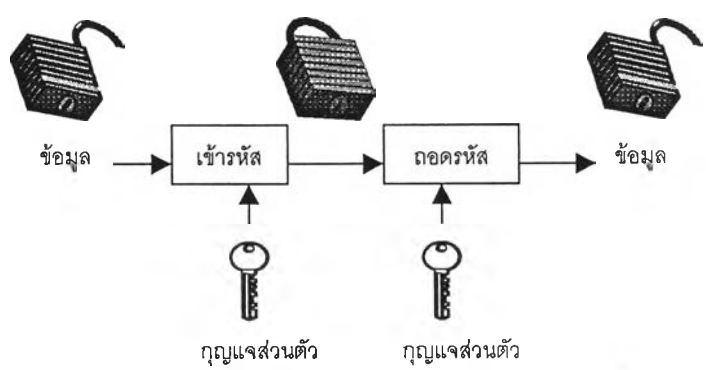
1. อัลกอริทึม ที่จะออกแบบจะต้องมีความสมบูรณ์ ชัดเจน และ ไม่คลุมเครือ
2. ต้องทราบว่าอัลกอริทึมนี้ มีความสามารถในการป้องกันข้อมูลได้แค่ไหน ต้องทราบระยะเวลาในการประมวลผล และจำนวนขั้นตอนการทำงานที่ใช้ในการค้นหาคีย์
3. ประสิทธิภาพในการป้องกันข้อมูลจะขึ้นอยู่กับคีย์ที่จะต้องเก็บเป็นความลับเท่านั้น ไม่ใช่เป็นเพราะอัลกอริทึมที่ถูกเก็บเป็นความลับ

4. ในการทำงานของอัลกอริทึมเพื่อเข้ารหัสลับ จะต้องไม่กระทบกระเทือนต่อการทำงานของผู้ใช้

ระบบเกี่ยวกับการเข้ารหัสลับ จำแนกตามลักษณะของคีย์สำหรับการเข้ารหัสที่ใช้ในอัลกอริทึมได้ 3 ประเภท คือ

1. ระบบการเข้ารหัสลับแบบสัญนิยม (Conventional Cryptographic System หรือ Symmetric System)

อัลกอริทึมของระบบการเข้ารหัสแบบสัญนิยมนี้ คีย์ที่ใช้สำหรับการดำเนินการเข้ารหัสลับ และการดำเนินการถอดรหัสลับข้อมูลจะต้องเหมือนกัน คือเป็นคีย์เดียวกัน หรือถ้าไม่เหมือนกัน คีย์หนึ่งจะสามารถถูกคำนวณจากอีกคีย์หนึ่งได้ และคีย์นี้จะต้องถูกเก็บเป็นความลับ ความเข้มแข็งของระบบการเข้ารหัสแบบสัญนิยม อยู่ที่ขั้นตอนการทำงานของอัลกอริทึมที่มีประสิทธิภาพ และค่าคีย์เป็นความลับ



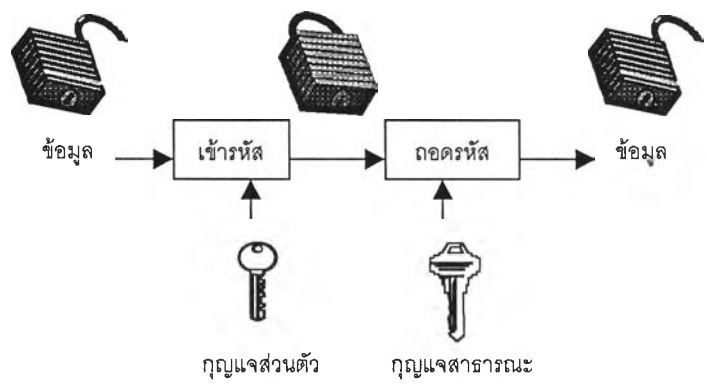
รูปที่ 2.7 การรหัสแบบกุญแจสมมาตร

ตัวอย่างของอัลกอริทึมของระบบการเข้ารหัสลับแบบสัญนิยมที่นิยมกัน และนำมาใช้เพื่อป้องกันข้อมูลที่มีความสำคัญอย่างกว้างขวาง คือ อัลกอริทึมเดส (Data Encryption Standard Algorithm (DES)

2. ระบบการเข้ารหัสลับแบบคีย์สาธารณะ (Public Key System หรือ Asymmetric System)

แนวความคิดเกี่ยวกับระบบการเข้ารหัสลับแบบคีย์สาธารณะได้ถูกเสนอขึ้นมาครั้งแรกโดย Diffie และ Hellman (Diffie and Hellman,1976) จากบทความ "New Directions in Cryptography" ในปี 1976 เป็นแนวความคิดใหม่สำหรับการเข้ารหัสลับ โดยที่ในระบบจะมีคีย์สำหรับการเข้ารหัสลับอยู่ 2 คีย์ที่ใช้คู่กัน ซึ่งคีย์ทั้งสองจะมีค่าแตกต่างกัน แต่จะมีความ

สัมพันธ์กัน คีย์หนึ่งใช้ในการดำเนินการเข้ารหัสลับเรียกว่าคีย์สาธารณะ (Public Key) เป็นคีย์ที่ไม่เป็นความลับเป็นที่รู้กันทั่วไป ส่วนอีกคีย์หนึ่งใช้สำหรับการดำเนินการถอดรหัสเรียกว่า คีย์ที่เป็นความลับ (Secret Key) เป็นคีย์ที่ถูกเก็บไว้เป็นความลับ หลักการสำคัญของระบบการเข้ารหัสลับแบบคีย์สาธารณะ คือ วิธีการคำนวณค่าคีย์สาธารณะ และคีย์ที่เป็นความลับ คีย์ทั้งสองมักจะคำนวณมาจากฟังก์ชันทางคณิตศาสตร์ที่ซับซ้อนและมีความสัมพันธ์กันและที่สำคัญ คือ การรู้ค่าคีย์สาธารณะจะต้องไม่สามารถที่จะคำนวณค่าคีย์ที่เป็นความลับได้ ดังนั้น ผู้ที่ทราบคีย์สาธารณะจะสามารถทำการเข้ารหัสลับข้อมูลได้ แต่จะมีเพียงเจ้าของหรือผู้ที่รู้ค่าคีย์เท่านั้นที่จะสามารถถอดรหัสข้อมูลออกได้

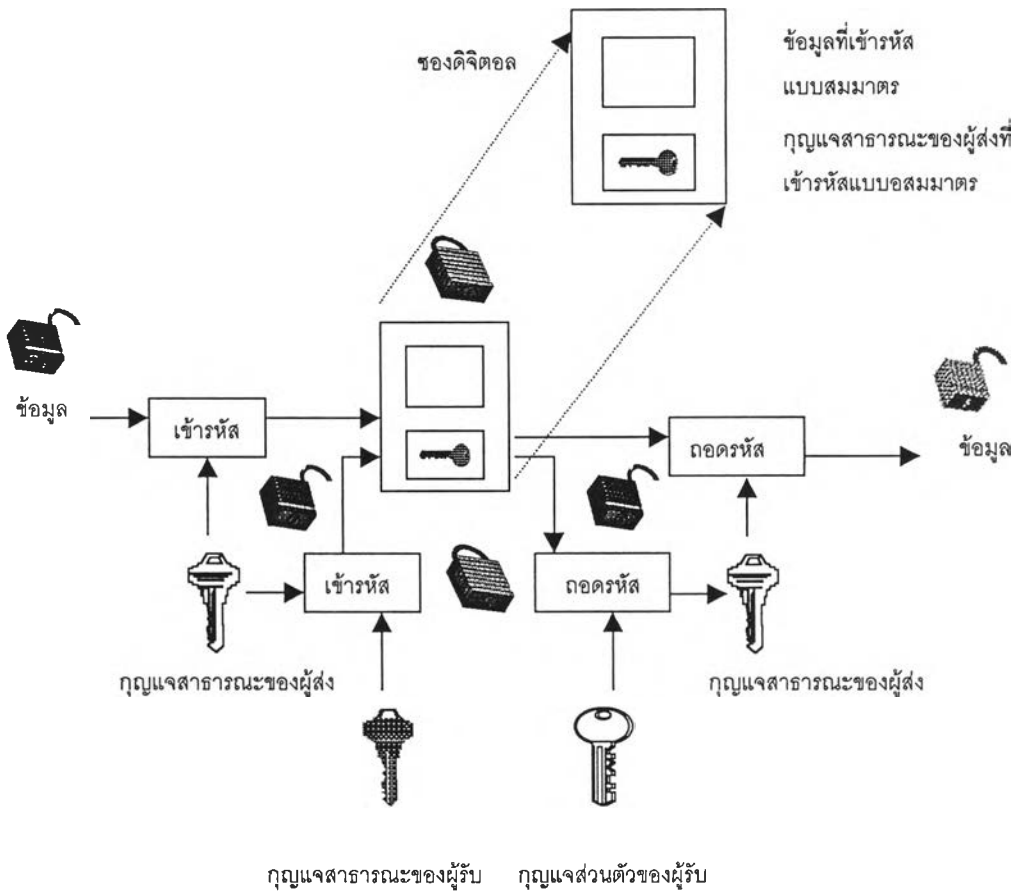


รูปที่ 2.8 การเข้ารหัสแบบกุญแจอสมมาตร

อัลกอริทึมต่าง ๆ ที่ใช้ระบบการเข้ารหัสแบบคีย์สาธารณะที่สำคัญ คือ อัลกอริทึมอาร์เอสเอ (Rivest-Shamir-Adleman Algorithm) และอัลกอริทึมแนฟแซ็ค (Knapsack Algorithm)

3. ระบบการเข้ารหัสลับแบบกุญแจผสม (Mixed Key Encryption)

การเข้ารหัสแบบกุญแจผสมเป็นการรวมเอาข้อดีของทั้ง 2 แบบแรกเข้าด้วยกัน เพื่อให้ได้ประสิทธิภาพที่ดีขึ้น เป็นการใช้การเข้ารหัสแบบกุญแจสมมาตรในการเข้ารหัสข้อมูล แล้วส่งไปพร้อมกับกุญแจสาธารณะที่ถูกเข้ารหัสด้วยการเข้ารหัสแบบกุญแจอสมมาตร ในซองดิจิตอล ดังรูปที่ 2.9 ซึ่งทำให้เกิดกลไกการรับรองที่เรียกว่า ใบรับรองดิจิตอลหรือบัตรประจำตัวดิจิตอล



รูปที่ 2.9 การเข้ารหัสแบบกุญแจผสม

แต่การเข้าใช้การเข้ารหัสแบบกุญแจผสม จำเป็นต้องอาศัยซอร์ฟแวร์ที่มีความสามารถเฉพาะ ตัวที่นิยมได้แก่ RSA แต่เนื่องจากเหตุผลทางด้านกฎหมายของประเทศสหรัฐอเมริกาที่ห้ามการส่งออกเทคโนโลยีการเข้ารหัสที่ใช้กุญแจขนาดใหญ่กว่า 40 บิต ออกนอกประเทศ ทำให้ทาง RSA Data Security Inc. ได้กำหนดวิธีที่เรียกว่า RC2 และ RC4 (RC ย่อมาจาก Ron 's Code) ที่ใช้กุญแจขนาด 40 บิตสำหรับใช้นอกประเทศ ซึ่งเทคโนโลยีดังกล่าวถูกบรรจุไว้ในโปรแกรม Web Browser ใน Microsoft และ Netscape รุ่นที่ 4 เป็นต้นไป เป็นต้น ชนิด RC2 เหมาะใช้แทน DES RC4 เหมาะสำหรับการประยุกต์ใช้งานที่เข้ารหัสแบบเวลาจริง (Real Time Encryption Application)

บัตรประจำตัวดิจิตอล (หนังสือเดินทางดิจิตอล ,ใบรับรองดิจิตอล) เป็นชุดข้อมูลการรับรองตัวบุคคลหรือองค์กรว่าเป็นผู้ส่งเอกสารนั้นจริง โดยมีผู้ที่ได้รับความไว้วางใจซึ่งเรียกว่าผู้รับรอง (Certificate Authority / Certifying Authority (CA)) เป็นผู้ออกบัตรประจำตัวดิจิตอลและตรวจ

สอบบัตรประจำตัวดิจิตอล ในการสร้างบัตรประจำตัวดิจิตอล ขั้นแรก เครื่องคอมพิวเตอร์ของผู้ขอบัตรฯจะสร้างกุญแจขึ้นมา 1 คู่ โดยเก็บกุญแจส่วนตัวไว้กับตัวเอง แล้วส่งกุญแจสาธารณะให้ผู้รับรอง พร้อมกับข้อมูลส่วนตัวที่ต้องการให้ปรากฏบนบัตรฯ จากนั้นผู้รับรองจะสร้างบัตรประจำตัวดิจิตอลขึ้น โดยในบัตรฯจะเก็บข้อมูลส่วนตัว ดังกล่าวข้างต้น กุญแจสาธารณะของเจ้าของบัตรฯ หมายเลขบนบัตรฯ (Serial Number) และระบุช่วงเวลาที่บัตรฯใช้งานได้ ชื่อผู้รับรองพร้อมทั้งลายเซ็นดิจิตอลของผู้รับรอง ดังรูปที่ 2.10 แล้วทำการเข้ารหัสบัตรฯ ด้วยกุญแจสาธารณะของผู้ขอบัตรฯแล้วส่งกลับไปให้ผู้ขอบัตรฯ ในขั้นตอนสุดท้าย ผู้ขอบัตรฯจะต้องใช้เครื่องคอมพิวเตอร์เครื่องเดิมซึ่งมีกุญแจส่วนตัวเก็บอยู่ในการขอรับบัตรฯ เพื่อให้สามารถถอดรหัสบัตรฯได้

ข้อมูลส่วนตัวของเจ้าของบัตรฯ เช่น ชื่อและที่อยู่อีเมลล์
กุญแจสาธารณะของเจ้าของบัตรฯ
หมายเลขบัตรฯ
ช่วงเวลาที่บัตรฯใช้งานได้
ชื่อผู้รับรอง
ลายเซ็นดิจิตอลของผู้รับรอง

รูปที่ 2.10 แสดงข้อมูลบนบัตรประจำตัวดิจิตอล

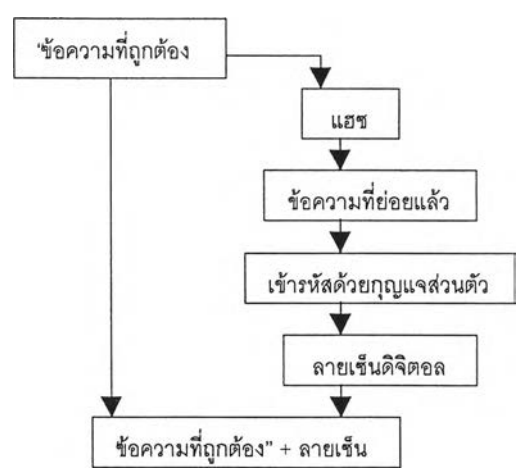
โดยสรุป บัตรประจำตัวดิจิตอล คือ ชุดข้อมูลการรับรองกุญแจสาธารณะของตัวบุคคลหรือองค์กร ซึ่งลงนาม (signed) โดยผู้รับรอง บัตรประจำตัวดิจิตอลจะถูกใช้ในการแลกเปลี่ยนข้อมูลบนอินเตอร์เน็ตใดๆที่ต้องการรับรองตัวผู้ส่งข้อมูลนั้น โดยผู้ส่งมาสามารถทำสำเนาบัตรประจำตัวดิจิตอลของตนเองแนบไปกับข้อมูลได้ หากปราศจากบัตรประจำตัวดิจิตอล เราย่อมไม่สามารถทราบได้เลยว่ากุญแจสาธารณะนั้นเป็นของบุคคลหรือองค์กรที่อ้างความเป็นเจ้าของจริงหรือไม่ จึงเห็นได้ว่า บัตรประจำตัวดิจิตอลมีประโยชน์หลักอยู่ 2 ประการ คือ ช่วยให้ผู้รับข้อมูลมั่นใจได้ว่าข้อมูลนั้นมาจากผู้ส่งจริง และผู้ส่งไม่สามารถบอกปัดความรับผิดชอบต่อการเป็นผู้ส่งข้อมูลนั้นได้

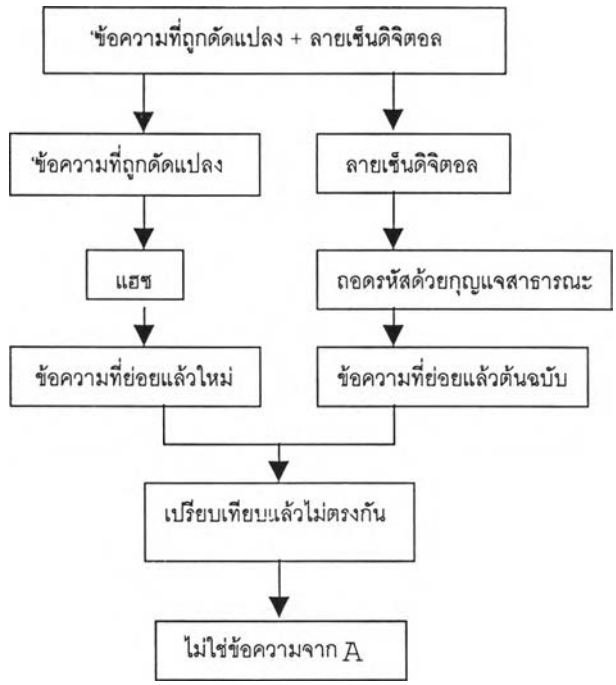
มาตรฐานของบัตรประจำตัวดิจิตอลที่ได้รับการยอมรับอย่างกว้างขวางที่สุด คือ มาตรฐานอุตสาหกรรม X.509 ของคณะกรรมการที่ปรึกษาการโทรศัพท์และโทรเลขระหว่างประเทศ (Consultative Committee on International Telephone and Telegraph หรือ (CCITT) ซึ่งปัจจุบันก็คือแผนกมาตรฐานโทรคมนาคมของสมาคมโทรคมนาคมระหว่างประเทศ (Telecommunication Standardization Sector of the International Telecommunications Union หรือ ITU-T) ดังนั้นบัตรประจำตัวดิจิตอลที่ตรงตามมาตรฐานจะสามารถเขียนหรืออ่านด้วยโปรแกรมประยุกต์ใดๆก็ตามที่ใช้มาตรฐานเดียวกันนี้ ด้วยเหตุนี้บางครั้งจึงถูกเรียกว่า ใบรับรอง

X.509 หรือใบรับรองกุญแจสาธารณะ นอกจากนี้ยังมีมาตรฐานอื่นๆที่พัฒนาต่อจาก X.509 เช่น Privacy-Enhanced Mail (PEM) ที่ออกแบบมาเพื่อให้รองรับการเข้ารหัสขอความได้ทั้ง DES และ RSA บนมาตรฐาน X.509 ซึ่ง PEM นี้ยังเป็นฉบับร่างอยู่ และ Public-key Cryptography Standards (PKCS) ซึ่งเป็นการขยาย PEM ที่รองรับการเข้ารหัสข้อความเพียงอย่างเดียว ให้รองรับการเข้ารหัสข้อมูลทั่วๆไปได้ด้วย

ลายเซ็นดิจิตอล คือ ข้อความย่อยที่เกิดจากการย่อยข้อความต้นฉบับด้วยฟังก์ชั่นแฮช แล้วเข้ารหัสด้วยกุญแจส่วนตัวของเจ้าของข้อความ เพื่อเป็นการยืนยันว่าข้อความนั้นเป็นของเจ้าของกุญแจส่วนตัวจริง โดยหลักการของลายเซ็นดิจิตอล ข้อมูลใดๆที่เข้ารหัสโดยใช้กุญแจส่วนตัวของผู้ส่งก็จะรับรองผู้ส่ง และข้อมูลใดๆที่เข้ารหัสโดยใช้กุญแจส่วนตัวของผู้รับก็จะรับรองผู้รับเช่นเดียวกัน เนื่องจากกุญแจส่วนตัวจะถูกใช้ได้โดยเจ้าของกุญแจเท่านั้น ข้อมูลใดๆที่เข้ารหัสโดยใช้กุญแจส่วนตัวย่อมเป็นการยืนยันว่ามาจากเจ้าของกุญแจนั้นจริง ผู้เสนอลายเซ็นดิจิตอลเป็นคนแรก ได้แก่ Whitfield Diffie ในปี พ.ศ. 2519 ในขณะที่อยู่มหาวิทยาลัยสแตนฟอร์ด

ในการใช้งานจริง เราจะส่งสำเนาบัตรประจำตัวดิจิตอลไปพร้อมกับลายเซ็นดิจิตอลด้วย เพื่อเป็นการรับรองกุญแจสาธารณะของผู้ส่ง ซึ่งถ้าทำครบทุกขั้นตอนอย่างสมบูรณ์ ก็จะไม่สามารถปลอมแปลงอีเมลล์นั้นได้เลย





รูปที่ 2.10 การส่งข้อความไปพร้อมกับลายเซ็นดิจิตอล และ การตรวจสอบข้อความด้วยลายเซ็นดิจิตอล

โดยหลักการผู้ออกบัตรประจำตัวดิจิตอลหรือผู้รับรองจะเป็นบุคคลหรือองค์กรใดก็ได้ ที่ได้รับความไว้วางใจในกลุ่มคนที่ใช้บัตรประจำตัวดิจิตอลนั้น ในกลุ่มคนที่ใช้บัตรประจำตัวดิจิตอลทุกคนจำเป็นต้องมีกุญแจสาธารณะของผู้รับรอง เพื่อที่จะสามารถอ่านข้อมูลในบัตรฯที่ออกโดยผู้รับรองได้ ผู้อื่นจะไม่สามารถปลอมแปลงบัตรได้เนื่องจากมีเพียงผู้รับรองเท่านั้นที่มีกุญแจส่วนตัวสามารถใช้เซ็นกำกับบัตรฯได้ มีเพียงกรณีเดียวที่การปลอมแปลงอาจจะเกิดขึ้นได้ ก็คือ มีผู้แอบอ้างว่าเป็นผู้รับรองเท่านั้น ซึ่งเป็นไปได้ยากมากในระบบการรับรองที่ใช้งานจริงบนอินเทอร์เน็ตในปัจจุบัน เนื่องจากผู้รับรองจะต้องเผยแพร่กุญแจสาธารณะของตนสู่สาธารณะ และ Web Browser ทั้งของ Netscape และ Microsoft ต่างบรรจุกุญแจสาธารณะของผู้รับรองที่เชื่อถือได้เหล่านี้ไว้ในโปรแกรมแล้ว เราเพียงเลือกว่าจะเชื่อถือผู้รับรองใดบ้างเท่านั้นเอง

การที่บัตรประจำตัวดิจิตอลจะเป็นที่เชื่อถืออย่างกว้างขวาง และสามารถใช้ได้ทั่วโลก จำเป็นต้องมีระบบโครงสร้างการรับรองพื้นฐานที่ใช้ร่วมกันทั่วทั้งโลก จึงทำให้เกิดลำดับชั้นของการรับรอง (Certification Hierarchies) ขึ้น โดยผู้ถือบัตรต้องได้รับการรับรองจากผู้รับรอง และผู้รับรองนั้นต้องได้รับการรับรองจากผู้รับรองที่อยู่เหนือขึ้นไปตามลำดับชั้นด้วย ในปัจจุบันมีหน่วยงานที่ได้รับความเชื่อถือให้เป็นผู้รับรองระดับนานาชาติอยู่มากมาย เช่น GTE , BelSign , CertiSign , IPS

, SSB และ VeriSign ที่มีชื่อเสียงในด้านกระบวนการอันเฉียบขาดในการตรวจสอบการระบุตัวอยู่ก่อนแล้ว เป็นหน่วยงานที่ได้รับความนิยมสูงสุด เนื่องจากเป็นผู้รับรองเชิงพาณิชย์รายแรก ซึ่งบริษัทยักษ์ใหญ่ในวงการ Web Browser ทั้ง Netscape และ Microsoft ต่างก็แนะนำให้ใช้ VeriSign จากมาตรฐานกลางของบัตรประจำตัวดิจิตอล เช่น X.509 ทำให้บัตรประจำตัวดิจิตอลที่ออกโดยผู้รับรองต่างรายการกันสามารถใช้งานร่วมกันได้ เนื่องจาก VeriSign เป็นผู้รับรองที่ได้รับความนิยมสูงสุด และมีบัตรฯหลายประเภทให้เลือกทดลองใช้งานดังนี้ บัตรประจำตัวดิจิตอลของ VeriSign แบ่งเป็น 3 ประเภท คือ บัตรส่วนบุคคล (Personal ID) บัตรสำหรับองค์กร (Server ID) และบัตรสำหรับผู้ผลิตซอร์ฟแวร์จำหน่ายบนอินเตอร์เน็ต (Developer ID) โครงงานนี้จึงขอบัตรประจำตัวดิจิตอลจาก VeriSign มาใช้ในโครงการ

ข้อสังเกต

การศึกษาระบบการเข้ารหัสลับสองวิธีแรกพบว่า ระบบการเข้ารหัสแบบคีย์สาธารณะจะทำงานช้ากว่า และต้องการขนาดของหน่วยความจำมากกว่าระบบการเข้ารหัสแบบสัญนิยม ตัวอย่างเช่น ชิป (chip) 1 ตัวที่ใช้เพื่อทำงานของอัลกอริทึมอาร์เอสเอ จะทำงานได้ในช่วง 100 ถึง 1000 บิตต่อวินาที ด้วยเทคโนโลยีในปี 1979 ในขณะที่อัลกอริทึมเดส สามารถทำงานได้ 1 เมกกะบิตต่อวินาที หรือในกรณีของอัลกอริทึมแนพแซค จะต้องใช้หน่วยความจำประมาณ 50 กิโลบิต ในขณะที่อัลกอริทึมเดส ต้องการเพียง 2 กิโลบิตเท่านั้น (Hellman,1979) อย่างไรก็ตาม การเข้ารหัสลับแบบระบบคีย์สาธารณะมีข้อดี คือสามารถแก้ปัญหาเกี่ยวกับเรื่องการจัดการคีย์ เนื่องจากการรักษาคีย์ให้เป็นความลับจะเป็นปัญหาใหญ่สำหรับระบบการเข้าระหัสแบบสัญนิยม เพราะมีความเสี่ยงสูงในการที่คีย์จะถูกขโมยไปได้ ต้องเสียทั้งเวลาและค่าใช้จ่าย ในธุรกิจบางประเภทต้องการความรวดเร็ว สามารถใช้ระบบคีย์สาธารณะเพื่อแก้ปัญหานี้ คือทำการเข้ารหัสข้อมูลเนื้อแท้ด้วยคีย์สำหรับเข้ารหัสลับ และทำการเข้ารหัสคีย์นี้ด้วยคีย์สาธารณะของผู้รับข้อมูล แล้วจึงนำคีย์นี้มาถอดรหัสข้อมูลจะได้ข้อมูลเนื้อแท้ที่ส่งมา จะเห็นว่าเป็นการส่งข้อมูลไปพร้อมกับคีย์ในคราวเดียวกัน ทำให้ไม่ต้องเสียเวลาที่จะต้องส่งคีย์ไปก่อน และทำให้คีย์มีความปลอดภัยมากขึ้น

ระบบการเข้ารหัสแบบคีย์สาธารณะ จะเป็นส่วนประกอบที่เพิ่มขึ้นมากเพื่อช่วยแก้ปัญหาการจัดการคีย์มากกว่าจะเป็นการแทนที่ระบบการเข้ารหัสแบบสัญนิยม

2.2.5 หลักการเข้ารหัสข้อมูลบนอินเทอร์เน็ตแบบอาร์ เอส เอ (RSA)

การเข้ารหัสข้อมูลบนอินเทอร์เน็ตแบบอาร์ เอส เอ (RSA) เป็นวิธีการเข้ารหัสที่น่าสนใจวิธีหนึ่งเพราะสามารถเปิดเผยกุญแจการเข้ารหัสได้ซึ่งต่างไปจากการเข้ารหัสแบบอื่นๆทั่วไป ความยากในการถอดรหัสวิธีนี้ ขึ้นกับหลักการทางคณิตศาสตร์ของจำนวนเฉพาะ (prime number) และการแยกตัวประกอบของจำนวนเต็มที่มีขนาดใหญ่ ปัจจุบันวิธีการนี้ได้มีการนำไปใช้ในโปรแกรม Netscape Web Browser

หลังจากที่มีการพัฒนาระบบ WWW อย่างแพร่หลายไปยังแวดวงธุรกิจการค้า เริ่มมีการโฆษณาขายสินค้าผ่าน WWW เมื่อมีการขายของก็ต้องมีการชำระค่าสินค้า วิธีการชำระค่าสินค้าที่นิยมคือการหักบัญชีจากเลขที่บัตรเครดิต แต่มีข้อควรระวังก็คือทราบได้อย่างไรว่าจะไม่ถูกหักเกินโดยที่มีคนอื่นแอบเอาเลขที่บัตรเครดิตของเราไปใช้ การทำงานของตัว WWW จะทำงานแบบ Client-Server โดยมีโพรโตคอลที่ใช้ในการส่งข้อมูลคือ HTTP (HyperText Transfer Protocol) เมื่อการใช้งานมีลักษณะของธุรกิจเข้ามาเกี่ยวข้อง จึงต้องมีวิธีการเข้ารหัสข้อมูลใน Web Browser เช่น Netscape จะใช้โพรโตคอลชื่อ S-HTTP (Secure HyperText Transfer Protocol) ซึ่งเพิ่มในส่วนการรักษาความปลอดภัยของข้อมูลเข้าไป โพรโตคอลหรือกติกาในการรับ-ส่งข้อมูลนี้ ได้รวมวิธีการเข้ารหัสแบบ RSA ไว้เพื่อให้การส่งข้อมูลผ่าน WWW มีความปลอดภัย ผู้อื่นไม่สามารถเปิดดูระหว่างทางได้ ข้อมูลที่วิ่งกันไปมาภายในเครือข่ายอินเทอร์เน็ตกว่าจะถึงมือผู้รับจริงๆก็ต้องผ่านไปหลายที่ จึงต้องมีการทำการเข้ารหัสข้อมูลโดยจะใส่วิธีการเข้ารหัสไว้ในส่วนของ Key Exchange Algorithms , SHTTP Signature Algorithms และ SHTTP Message Digest Algorithm ซึ่งวิธีการที่ใช้อยู่จะมีทั้ง RSA-MD2 และ RSA-MD5 นอกจากนี้การเข้ารหัสแบบเปิดเผยกุญแจ กุญแจในการเข้ารหัสและถอดรหัสจะเป็นคนละตัวกัน และที่สำคัญ กุญแจเข้ารหัสไม่สามารถนำมาใช้ในการถอดรหัสได้

ในปี 1978 R. Rivest, A Shamir , และ L. Adleman ได้คิดวิธีการเข้ารหัสแบบ อาร์ เอส เอ ซึ่งเป็นการเข้ารหัสที่เปิดเผยกุญแจได้ Public-Key Cryptosystems ซึ่งใช้การคำนวณทางคณิตศาสตร์ของเลขจำนวนเต็มที่มีขนาดใหญ่

ลักษณะที่สำคัญของการเข้ารหัสแบบนี้คือ

1. ขั้นตอนการเข้ารหัส E_k และขั้นตอนการถอดรหัสแบบ D_k จะเป็นการแปลงกลับได้ของตัวอักษร M ที่ต้องการเข้ารหัส และตัวอักษร C ที่เข้ารหัสแล้วที่กำหนดโดยกุญแจ K สำหรับแต่ละ K และ M ถ้า $C = E_k(K)$ จะได้ $M = D_k(C) = D_k(E_k(M))$
2. สำหรับแต่ละ K , E_k และ D_k สามารถคำนวณได้ง่าย
3. สำหรับแต่ละ K การคำนวณหาค่า D_k จาก E_k ทำได้ยากหรือไม่สามารถทำได้

ขั้นตอนในการเข้ารหัสหรือถอดรหัสเหมือนวิธีการเข้ารหัสทั่วๆไป คือ ต้องมีกุญแจการเข้ารหัสและข้อความ M เมื่อเข้ารหัสแล้วจะได้ข้อความเข้ารหัส C ซึ่งทุกๆคนสามารถใช้วิธีการเดียวกันได้ ความปลอดภัยของระบบนี้จะขึ้นกับการที่กุญแจสำหรับเข้ารหัสสามารถเปิดเผยได้ แต่จะไม่สามารถคำนวณ $D_k(C)$ ได้ และการลองหาค่า $E_k(M) = C$ ที่เป็นไปได้ทุกๆค่า ไม่สามารถทำได้ในทางปฏิบัติ ฟังก์ชันที่มีคุณสมบัติดังกล่าวจะเป็นฟังก์ชันประตูกลทางเดียว โดยกำหนดให้ One-way Function เป็นฟังก์ชันที่ง่ายต่อการคำนวณ แต่การคำนวณค่าฟังก์ชันย้อนกลับทำได้ยาก เช่น การที่กำหนดค่า X มาให้หาค่า f (x) นั้นทำได้ง่าย แต่ถ้ากำหนด f (x) มาให้หา x จะทำได้ยากซึ่งมีลักษณะเหมือนประตูกล (Trapdoor) คุณสมบัติในข้อที่ 1. เป็นคุณสมบัติขั้นพื้นฐานของการเข้ารหัส ส่วนข้อ 2. และข้อ 3. เป็นคุณสมบัติที่ทำให้สามารถนำระบบไปใช้ได้ ฟังก์ชันทางเดียวหมายความว่า การเข้ารหัส E สามารถทำได้ทางเดียว เช่น การคำนวณข้อความที่เข้ารหัส (Cryptogram) C โดยที่ทราบค่า (K,M) จะง่ายต่อการคำนวณ แต่การคำนวณข้อความ M โดยกำหนด (K,C) จะยากจนไม่สามารถทำได้

(K,M) → C ง่าย

(K,C) → M ยาก

ในการเข้ารหัสแบบ อาร์ เอส เอ ข้อความจะถูกแทนด้วยตัวเลขจำนวนเต็มที่อยู่ในช่วง [0, n -1] ผู้ใช้แต่ละคนจะเลือกค่า n ของตนเอง และเลขจำนวนเต็มอีกคู่ คือค่า e และค่า d ในลักษณะที่จะอธิบายต่อไปนี้ ผู้ใช้สามารถแสดงกุญแจเข้ารหัส (n,e) ไว้ในที่เปิดเผย เช่น สมุดโทรศัพท์ ส่วนกุญแจการถอดรหัสประกอบด้วยค่า (n,d) โดยที่ค่า d เก็บไว้เป็นความลับ การเข้ารหัสข้อความ C และข้อความที่ถูกถอดรหัส M กำหนดได้ดังนี้

การเข้ารหัส $M = E(M) = M^e \bmod n$

การถอดรหัส $M = D(C) = C^p \bmod n$

เมื่อ e และ n เป็นกุญแจในการเข้ารหัส

M จะถูกหากลับมาโดยวิธีเดียวกัน แต่โดยใช้ตัวเลขยกกำลัง d ที่ต่างกัน ค่า n ได้จากการเลือกจำนวนเฉพาะ 2 จำนวน p และ q ที่มีค่ามากๆ ค่า n จะเป็นผลคูณของ p และ q ดังนี้

$$n = pq$$

การเข้ารหัสและถอดรหัสสามารถทำได้โดยการคำนวณเลขยกกำลังแบบเร็ว (Fast Exponential Algorithm) ซึ่งผลลัพธ์จะได้เป็นจำนวนเต็มที่อยู่ในช่วง [0, n -1]

C = FastExp (M,e,n)

M = FastExp (C,d,n)

ในการเขารหัสและการถอดรหัสขึ้นกับ Euler 's Generalization of Format 's Theorem ซึ่งกล่าวว่าสำหรับแต่ละ M ที่สัมพันธ์เฉพาะกับจำนวน n

$$M\ W(n) \bmod n = 1$$

เมื่อ W(n) = (p-1)(q-1) เรียกว่า Euler Totient Function คุณสมบัตินี้หมายความว่าถ้า e และ d ที่สอดคล้องกับสมการ e d mod W(n) = 1 จะได้ว่า การเข้ารหัสและการถอดรหัสเป็นอินเวิร์สฟังก์ชันกัน ซึ่งแสดงได้ดังนี้

$$M\ W(n) \bmod n = 1$$

และให้ข้อความ M เป็นจำนวนเต็มที่อยู่ในช่วง [0, n -1] ที่ซึ่ง GCD(M,n) = 1 (GCD : Greatest Common Division) หรือตัวหารร่วมมาก จะได้

$$M = D(C) = D(E(M)) = M^{e} \bmod n)^{d} \bmod n = M^{e\,d} \bmod n$$

จาก e d mod W (n) = 1 หมายความว่า e d = t W (n) +1 สำหรับจำนวนเต็ม t ดังนั้นจะได้ว่า

$$M^{e\,d} \bmod n = M^{t\,W(n)+1} \bmod n$$

$$= M\,M^{t\,W(n)} \bmod n$$

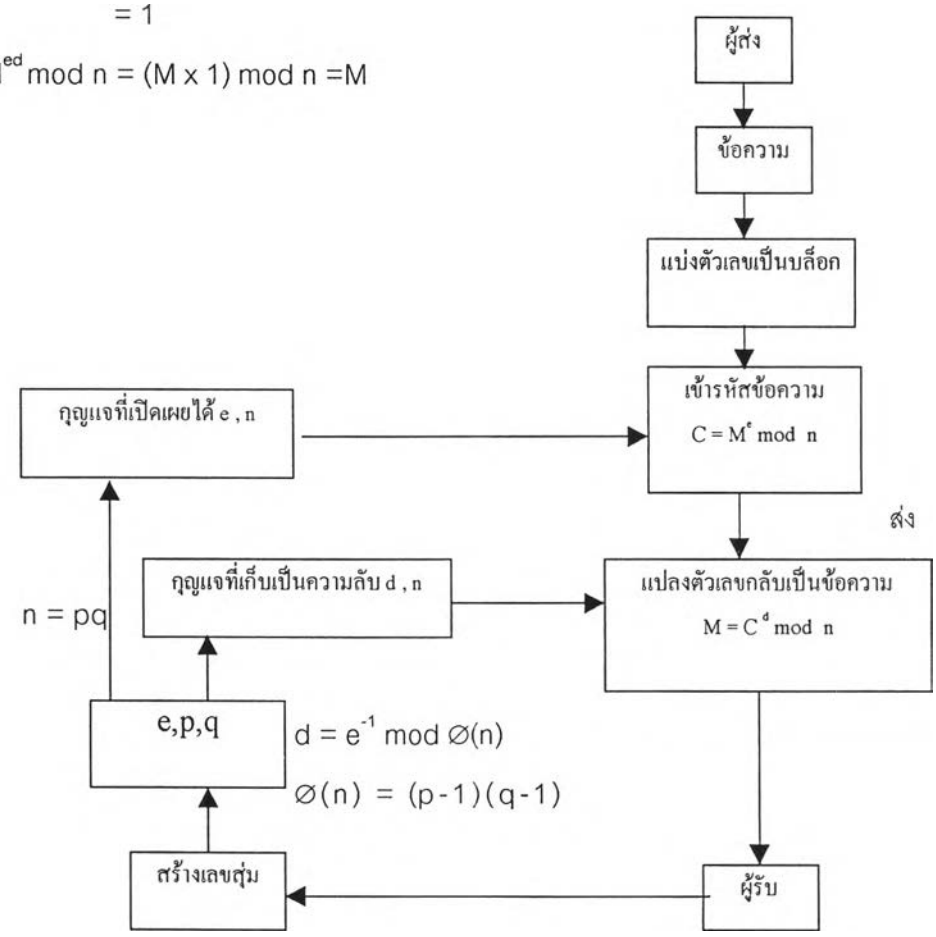
$$= M\,(M^{t\,W(n)} \bmod n) \bmod n$$

เมื่อ $M^{t\,W(n)} \bmod n = (M^{t\,W(n)} \bmod n)^{t} \bmod n$

$$= 1^{t} \bmod n$$

$$= 1$$

ดังนั้น $M^{ed} \bmod n = (M \times 1) \bmod n = M$



รูปที่ 2.10 แสดงขั้นตอนการเข้ารหัสแบบ RSA

การหาจำนวนเฉพาะ

ในขั้นตอนการเข้ารหัสต้องมีการหาจำนวนเฉพาะ p และ q ที่มีค่าใหญ่ โดยการสร้างเลขสุ่มขึ้นมา แล้วทดสอบว่าเป็นจำนวนเฉพาะหรือไม่ โดยไม่ต้องหาจากนิยามที่ว่าจำนวนเฉพาะคือจำนวนที่หารด้วย 1 กับตัวมันเองเท่านั้นลงตัว เนื่องจากการหาจำนวนเฉพาะจากนิยามจะติดข้อจำกัดที่ขนาดของจำนวนเต็มที่ใช้ เนื่องจากจำนวนเต็มขนาด N บิต จะมีค่าระหว่าง -2^N กับ 2^N-1 จึงต้องแก้ปัญหาด้วยการสร้างเลขสุ่มขึ้นมาแล้วใช้ความน่าจะเป็นทดสอบหาจำนวนเฉพาะ คุณสมบัติที่สำคัญของจำนวนเฉพาะคือ ผลคูณของจำนวนเฉพาะ 2 ตัวที่คูณกัน จะได้ตัวเลขใหม่ที่มีแต่เลขจำนวนเฉพาะ 2 ตัวที่ใช้คูณกันเท่านั้นที่สามารถหารเลขจำนวนดังกล่าวได้ลงตัว ดังนั้นหากเรามีเลขจำนวนเฉพาะที่มีจำนวนหลักมากๆ 2 ตัวคูณกัน การหาตัวประกอบของเลขจำนวนเฉพาะตัวนั้นจะใช้เวลานานมากเป็นทวีคูณ

ขั้นตอนการเข้ารหัสRSA

ต้องหาวิธีการจัดการกับเลขจำนวนเต็มที่มีขนาดใหญ่พร้อมกับวิธีการหาโมดูโลและวิธีการทดสอบจำนวนเฉพาะที่เลือกขึ้นมา โดยเลือกตัวเลขจำนวนหนึ่งที่มีจำนวนหลักตรงกับความต้องการ แล้วทดสอบว่าเป็นจำนวนเฉพาะหรือไม่ ถ้าไม่ใช่ให้เพิ่มค่าทีละหนึ่งแล้วทดสอบ ทำเช่นนี้ต่อไปเรื่อยๆ จนได้จำนวนเฉพาะ หลังจากเลือกจำนวนเฉพาะขึ้นมาได้ 2 ค่า เราก็จะได้ $n = pq$ โดยที่ n เป็นผลคูณของจำนวนเฉพาะที่เลือกขึ้นมาจากนั้นแปลงข้อความที่ต้องการเข้ารหัสให้เป็นตัวเลข เช่น A=01,B=02 แต่ในทางปฏิบัติเรานิยมใช้รหัสแอสกีซึ่งเป็นโค้ดมาตรฐาน 8 บิต ที่แทนตัวอักษร และตัวเลข ตลอดจนสัญลักษณ์พิเศษทั้งหมด เมื่อได้ข้อความที่แปลงเป็นตัวเลข จะทำการแบ่งข้อความออกเป็นบล็อกๆ โดยขนาดของแต่ละบล็อกต้องน้อยกว่าหรือเท่ากับจำนวนหลักของค่า n เพราะว่าเซ็ตทั้งหมดของเลขที่เกิดจากการหารเอาเศษจะได้ค่าที่อยู่ในช่วง [0,n-1] เช่น โมดูโลของ 10 เท่ากับ { 0,1,2,3,4,5,6,7,8,9 } โดย 0 หมายถึงหารลงตัว และ 1 หมายถึง หารแล้วเหลือเศษ 1 เป็นต้น ขนาดของบล็อกมีค่ามากกว่าขนาดของ n ค่าที่ได้จากการ mod จะทำให้ได้ค่าอินเวอร์สที่ผิด เมื่อแบ่งออกเป็นบล็อกเรียบร้อยแล้วจึงเข้ารหัสด้วยวิธีการ Fast Exponential ซึ่งเราต้องการหาโมดูโลของค่าเลขยกกำลังของแต่ละบล็อก

ถ้าจะทำวิธีตรงๆ คือ หาค่าเลขยกกำลังก่อนแล้วจึงนำไปหาโมดูโล ซึ่งวิธีนี้จะใช้เวลาในการทำขั้นตอนดังกล่าวมาก และเราไม่จำเป็นต้องทำเช่นนั้นเพราะค่าที่ได้จากการโมดูโลจะมีค่าจำกัดอยู่ที่ขนาดของ n ไม่มากเท่าขนาดของเลขยกกำลัง เมื่อเข้ารหัสเรียบร้อยแล้ว จะได้ข้อความที่เป็นตัวเลขจากนั้นก็สามารถส่งข้อความได้

ตัวอย่างการเข้ารหัสแบบ RSA

ถ้าต้องการเข้ารหัสข้อความว่า " COMPUTER SCIENCE " โดยแทนตัวอักษรด้วยตัวเลขต่อไปนี้ A=01,B=02,C=03,...,Y=25,Z=26,BLANK=00 จะถูกแปลงข้อความเป็นโค้ดตัวเลขได้ดังนี้ " 03151316212005180019030905140305 " เลือกบล็อก p=73 , q=151 จะคำนวณค่า n ได้จาก n = pq = 11023 โดยใช้กุญแจเข้ารหัส (e) เป็น 11 ขั้นตอนการเข้ารหัสจะแบ่งข้อความที่เข้ารหัสเป็นบล็อกๆ บล็อกละ 4 หลัก จากนั้นหาโมดูโล n โดยใช้กุญแจเข้ารหัส (e) เป็น 11 ทำการเข้ารหัสได้ดังนี้

$C_i = M_i^e \bmod n$

$C_1 = 0315^{11} \bmod 11023 = 4989$

$C_2 = 1316^{11} \bmod 11023 = 9567$

$C_3 = 2120^{11} \bmod 11023 = 1436$

$C_4 = 0518^{11} \bmod 11023 = 2023$

$C_5 = 0019^{11} \bmod 11023 = 7116$

$C_6 = 0309^{11} \bmod 11023 = 7111$

$C_7 = 0514^{11} \bmod 11023 = 5378$

$C_8 = 0305^{11} \bmod 11023 = 6064$

จะสังเกตได้ว่าขนาดของการแบ่งบล็อกของข้อความจะต้องน้อยกว่าค่า n เพราะเซ็ตทั้งหมดของโมดูโล n จะอยู่ในช่วง [0,n-1] การถอดรหัสจะทำได้โดยวิธีเดียวกันโดยใช้กุญแจถอดรหัสอีกตัวหนึ่ง (d) คือ 5891 ที่หามาจากคุณสมบัติ ed = 1 mod (p-1)(q-1) เพราะ 1 = 11* 5891 mod 10800 นั่นคือ 5891 เป็น inverse ของ 11 mod 10800

$M_1 = 4989^{5891} \bmod 11023 = 0315$

$M_2 = 9567^{5891} \bmod 11023 = 1316$

$M_3 = 1436^{5891} \bmod 11023 = 2120$

$M_4 = 2023^{5891} \bmod 11023 = 0518$

$M_5 = 7116^{5891} \bmod 11023 = 0019$

$M_6 = 7111^{5891} \bmod 11023 = 0309$

$M_7 = 5378^{5891} \bmod 11023 = 0514$

$M_8 = 6064^{5891} \bmod 11023 = 0305$

จากตัวอย่างที่แสดงไปแล้วนั้น ถ้าเลือก p และ q ที่มีจำนวนหลักมากๆ จะลดจำนวนครั้งในการเข้ารหัส ส่งผลให้การเข้ารหัสเร็วขึ้น

ตารางที่ 2.3 ตารางแสดงเวลาที่ใช้สำหรับแยกตัวประกอบของระบบ RSA

จำนวนหลัก	จำนวนครั้งของการกระทำ	เวลา
50	1.4×10^{10}	3.9 (ชั่วโมง)
75	9.0×10^{12}	104 (วัน)
100	2.3×10^{15}	74 (ปี)
200	1.2×10^{23}	3.8×10^{9} (ปี)
300	1.5×10^{29}	4.9×10^{15} (ปี)
500	1.3×10^{39}	4.2×10^{25} (ปี)

สรุปได้ว่าในการเข้ารหัสแบบ RSA อาศัยความยากในการแยกตัวประกอบซึ่งจะนำไปสู่กุญแจในการถอดรหัสเป็นตัวรักษาความปลอดภัย ตราบใดที่ยังไม่สามารถหาวิธีการที่มีประสิทธิภาพในการแยกตัวประกอบ การเข้ารหัสแบบ RSA ยังคงสามารถใช้ได้