บทที่ 3
การรักษาความปลอดภัยของการทำธุรกรรม (Transaction Security)

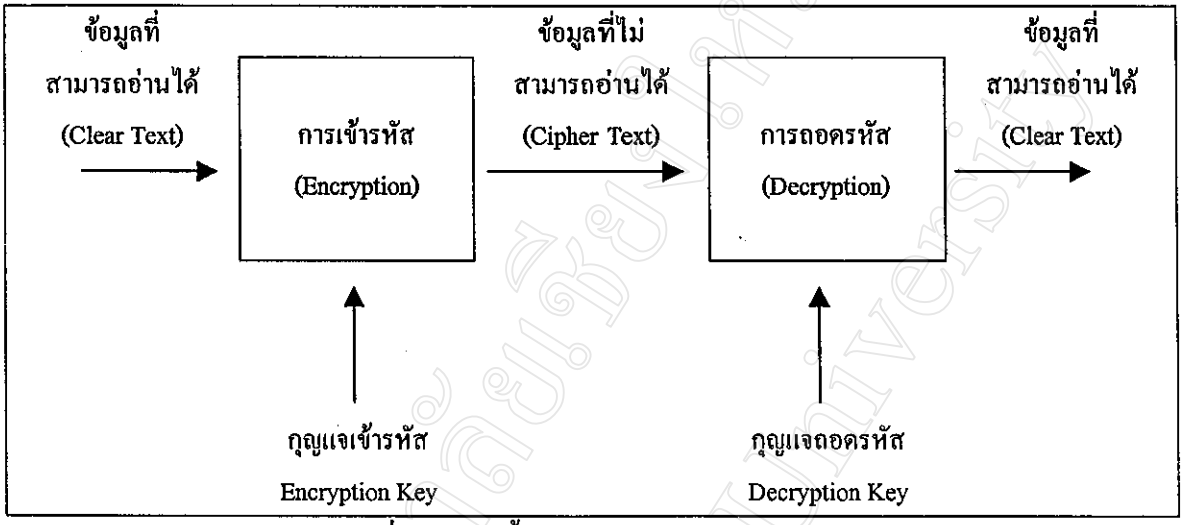
ในบทนี้จะอธิบายถึงการรักษาความปลอดภัยของข้อมูล โดยเฉพาะข้อมูลที่ส่งผ่านออกไปจากเครือข่าย โดยอาศัยเทคโนโลยีการเข้ารหัสและการถอดรหัสข้อมูล ในบทนี้ยังกล่าวถึงวิธีการของการเข้ารหัสแต่ละวิธี รวมทั้งข้อดีข้อเสียของแต่ละวิธีการ อีกทั้งยังกล่าวถึงระบบ SSL และ SET ที่นำเอาวิธีการเข้ารหัสและถอดรหัสมาประยุกต์ใช้ เพื่อรักษาความปลอดภัยของของระบบพาณิชย์อิเล็กทรอนิกส์

3.1 การเข้ารหัสและถอดรหัสข้อมูล (Encryption and Decryption)

ในการปกป้องข้อมูลนั้นมีอยู่หลายประการที่จะต้องคำนึงถึง วิธีการหนึ่งที่นำมาใช้กันอย่างกว้างขวางและมีประสิทธิภาพอย่างยิ่งก็คือการนำวิธีการเข้ารหัสข้อมูลมาใช้เพื่อสร้างความปลอดภัยให้กับข้อมูล หลักการสำคัญของวิธีการนี้ก็คือการที่ข้อความถูกส่งผ่านระบบเครือข่ายคอมพิวเตอร์สามารถใช้สื่อในการส่งที่ไม่ปลอดภัยที่เรียกว่า Insecure Channel นั้น จำเป็นจะต้องสร้างเกราะความปลอดภัยให้กับข้อมูลก่อนที่จะถูกส่งออกไป

3.1.1 พื้นฐานของการเข้ารหัสข้อมูล

จุดประสงค์ในการเข้ารหัสข้อมูลคือการรักษาความลับของข้อมูล โดยที่ข้อมูลนั้นจะถูกเปิดเผยต่อบุคคลที่ได้รับอนุญาตเท่านั้น ขั้นตอนในการเข้ารหัสมีดังนี้คือ



ภาพที่ 5 แสดงพื้นฐานการเข้ารหัสและถอดรหัสข้อมูล[15]

จากภาพที่ 5 ข้อความที่สามารถอ่านได้นั้นเรียกว่า Clear Text ซึ่งเป็นข้อความที่ต้องการส่งออกไปโดยผ่านระบบเครือข่ายคอมพิวเตอร์ แต่เนื่องจากในระบบเครือข่ายคอมพิวเตอร์นั้นไม่สามารถจะทำการรับรองความปลอดภัยของข้อมูลได้ เพราะหากมีการขโมยข้อมูลในระหว่างทำการส่ง จะทำให้เกิดความเสียหายเนื่องจากการเปิดเผยข้อมูลที่เป็นความลับ ดังนั้นวิธีการแก้คือทำให้ข้อมูลที่เป็นความลับและไม่สามารถจะอ่านออกได้ที่เรียกว่า Cipher Text เฉพาะในตอนที่ทำการส่งข้อความ กระบวนการเปลี่ยนข้อความที่อ่านได้ไปเป็นข้อความที่ไม่สามารถอ่านได้นี้เรียกว่าการทำ Encryption ซึ่งต้องอาศัย Encryption Key เมื่อเสร็จสิ้นการเข้ารหัสแล้ว ผลที่ได้ก็คือ Cipher Text ซึ่งจะถูกส่งออกไปยังระบบเครือข่ายเพื่อส่งต่อไปยังจุดหมายปลายทางต่อไป และหากในระหว่างการส่งนั้นข้อมูลถูกขโมยไปโดยผู้ไม่ประสงค์ดี ข้อมูลนั้นก็จะไม่เปิดเผยความลับแก่บุคคลนั้น เนื่องจากว่าไม่สามารถอ่านและเข้าใจข้อความนั้นได้เพราะในการอ่านข้อความ Cipher Text นั้นจะต้องใช้ขั้นตอนอีกขั้นตอนหนึ่งก็คือ การถอดรหัส (Decryption)

การถอดรหัสคือการเปลี่ยนข้อความที่ไม่สามารถอ่านออกได้ให้กลับไปเป็นข้อความที่สามารถอ่านออกได้ โดยการใช้กุญแจถอดรหัส และหากกุญแจถอดรหัสนี้เหมือนกันทั้งสองข้าง

---

[15] เรื่องเดียวกัน : 110

นั่นคือ Encryption Key = Decryption Key เรียกกระบวนการเข้ารหัสและถอดรหัสนี้ว่าการรหัสแบบสมมาตร แต่หากกุญแจถอดรหัสทั้งสองไม่จำเป็นต้องเหมือนกันแล้วนั้น เรียกว่าการรหัสแบบอสมมาตร

(1) การแทนค่าตัวอักษรโดยการใช้สัญลักษณ์อื่น

เนื่องจากว่ากระบวนการเข้ารหัส และถอดรหัสของข้อมูลนั้นเป็นวิธีการทางคณิตศาสตร์ หมายถึงก่อนที่จะทำการเข้ารหัสของข้อมูล จะต้องมีการแทนค่าตัวอักษรโดยตัวเลขก่อน หรือที่เรียกว่า Coding แสดงได้ดังภาพที่ 6

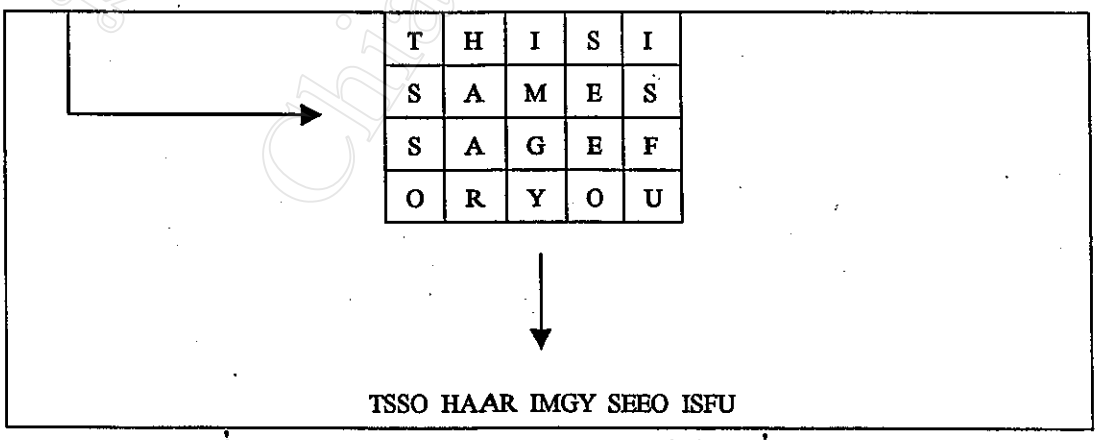
ตัวอักษร :	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
แทนค่า :	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

ตัวอักษร :	P	Q	R	S	T	U	V	W	X	Y	Z
แทนค่า :	15	16	17	18	19	20	21	22	23	24	25

ภาพที่ 6 แสดงการแทนค่าตัวอักษรโดยการใช้สัญลักษณ์อื่น[16]

(2) การแทนค่าตัวอักษรโดยการใช้วิธีการเลื่อนค่า

การแทนค่าตัวอักษรด้วยวิธีนี้มีจุดประสงค์คือการกระจายความซ้ำกันของตัวอักษร(Diffusion) ซึ่งแตกต่างจากวิธีที่แล้ว การแทนค่าเพื่อทำให้เกิดความสับสนซับซ้อนในข้อความ(Confusion) หลักการวิธีนี้สามารถอธิบายได้โดยภาพที่ 7



ภาพที่ 7 แสดงการแทนค่าตัวอักษรโดยการใช้วิธีการเลื่อนค่า[17]

---

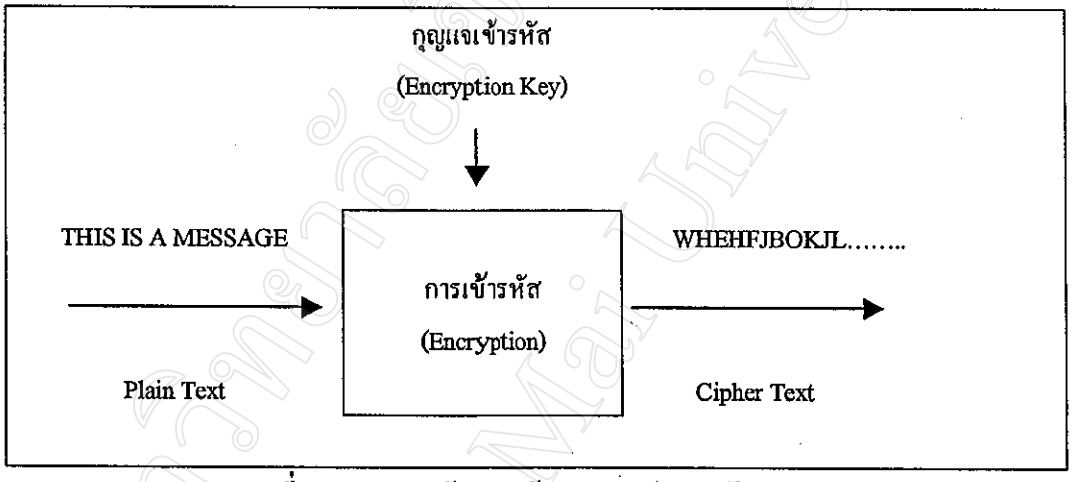
[16] เรื่องเดียวกัน : 111

[17] เรื่องเดียวกัน : 115

จากภาพที่ 7 จะเห็นได้ว่าข้อความที่สามารถอ่านได้นั้นคือ THIS IS A MESSAGE FOR YOU จะถูกนำมาจัดเรียงใหม่ในรูปเมตริกซ์ โดยเริ่มจากซ้ายไปขวา จากนั้นก็ทำการจัดเรียงตัวอักษรใหม่โดยใช้การเรียงตัวใหม่ในแนวตั้ง ผลที่ได้ก็คือตัวอักษรที่ไม่สามารถอ่านเข้าใจได้นั้นคือ TSSO HAAR IMGY SEEO ISFU

(3) การเข้ารหัสข้อมูลแบบทีละตัว (Stream Cipher)

การเข้ารหัสแบบนี้เป็นการเปลี่ยนตัวอักษรของข้อความไปเป็นสัญลักษณ์ Cipher ทีละตัว ขั้นตอนในการเข้ารหัสแบบนี้สามารถดูได้จากภาพที่ 8



ภาพที่ 8 แสดงการเข้ารหัสข้อมูลแบบทีละตัว[18]

จากภาพที่ 8 จะเห็นได้ว่าการเข้ารหัสแบบนี้จะทำการเข้ารหัสของข้อความทีละตัว โดยข้อความ THIS IS A MESSAGE. นั้น จะถูกทำการเข้ารหัสโดยมี E G A S S ..... ถูกเข้ารหัสทีละตัว และข้อความที่ได้คือข้อความที่เป็น Cipher Text ปรากฏออกมาทางด้านขวามือ วิธีการเข้ารหัสแบบนี้มีข้อดี และข้อเสีย ดังนี้

ข้อดีของการเข้ารหัสทีละตัว (Stream Cipher)

- ความเร็ว(Speed of Transformation) เนื่องจากการเข้ารหัสวิธีนี้ทำทีละตัว โดยที่ขั้นตอนในการเข้ารหัสนั้นไม่ต้องรอหรือเกี่ยวข้องกับตัวอักษรอื่น ๆ ในข้อความ ดังนั้นการเข้ารหัสแบบนี้จึงรวดเร็วเมื่อเปรียบเทียบกับวิธีการอื่น ๆ

[18] เรื่องเดียวกัน : 115

- ความผิดพลาดต่ำ(Low Error Propagation) การเข้ารหัสแบบนี้จะให้ความผิดพลาดต่ำเมื่อเปรียบเทียบกับวิธีอื่น ๆ เนื่องจากความผิดพลาดที่เกิดขึ้นกับตัวอักษรตัวใดตัวหนึ่งในระหว่างการทำการเข้ารหัสนั้นจะไม่มีผลต่อกระบวนการเข้ารหัสของตัวอักษรอื่น ๆ เลย

ข้อเสียของการเข้ารหัสทีละตัว(Stream Cipher)

- มีความสามารถต่ำในการกระจายความซ้ำกันของตัวอักษร(Low-Diffusion) เนื่องจากการเข้ารหัสแบบนี้ทำทีละตัว โดยไม่คำนึงถึงตัวอักษรอื่น ดังนั้นการกระจายความซ้ำกันจึงไม่อาจทำได้ และก่อให้เกิดสิ่งที่เรียกว่ารูปแบบ(Pattern) ของตัวอักษรขึ้น ซึ่งจะทำให้ง่ายต่อการวิเคราะห์ของนักเจาะรหัส
- ง่ายต่อการดัดแปลงแก้ไข (Susceptibility to malicious insertion and modifications) เพราะว่าการเข้ารหัสแบบนี้ไม่ต้องอาศัยความถูกต้องในการเข้ารหัสของตัวอักษรอื่น ๆ เลย ดังนั้นความเป็นไปได้ประการหนึ่งก็คือหากมีผู้เจาะรหัสที่สามารถล้วงความลับของข้อมูลได้แล้ว ก็อาจทำการเปลี่ยนแปลงแก้ไขข้อมูลนั้น ๆ หรือทำการใส่ข้อความเพิ่มเติมเข้าไปได้โดยที่ผู้ทำการถอดรหัสไม่อาจล่วงรู้ได้ว่ามีการทุจริตกับข้อความที่ได้รับมา เช่น การขโมยที่เกี่ยวกับจำนวนเงินในบัญชีธนาคารที่ถูกส่งผ่านระบบเครือข่าย แล้วนำเอาไปปลอมแปลงจำนวนเงินที่มีอยู่พร้อมทั้งโอนย้ายจำนวนเงินดังกล่าวไปสู่บัญชีของตน เป็นต้น

(4) การเข้าข้อมูลแบบเป็นกลุ่ม (Group Cipher of Block Cipher)

การเข้ารหัสข้อมูลแบบนี้จะทำเป็นกลุ่ม(Group) หรือเป็น Block ของข้อมูลแทนที่จะทำการเข้ารหัสทีละตัว การเข้ารหัสแบบนี้มีข้อดีหลายประการที่เหนือกว่าการเข้ารหัสแบบทีละตัวดังนี้

ข้อดีของการเข้ารหัสแบบเป็นกลุ่ม(Group Cipher)

- การกระจายความซ้ำกันของตัวอักษร(Diffusion) การทำการเข้ารหัสแบบนี้จะทำให้ตัวอักษรของข้อความที่อ่านได้แต่ละตัวนั้นถูกแทนค่าด้วยตัวอักษรหลายตัวในข้อความที่เข้ารหัสแล้ว(Cipher Text) ดังนั้นการวิเคราะห์หาข้อความเดิมจึงทำได้ยากกว่า
- สามารถต่อต้านการดัดแปลงต่อเติมข้อมูลได้(Insertion Resistant) เนื่องจากวิธีนี้ข้อมูลจะถูกเข้ารหัสทีละกลุ่ม ดังนั้นการขโมยข้อมูลนี้ไปต่อเติม จะไม่สามารถ

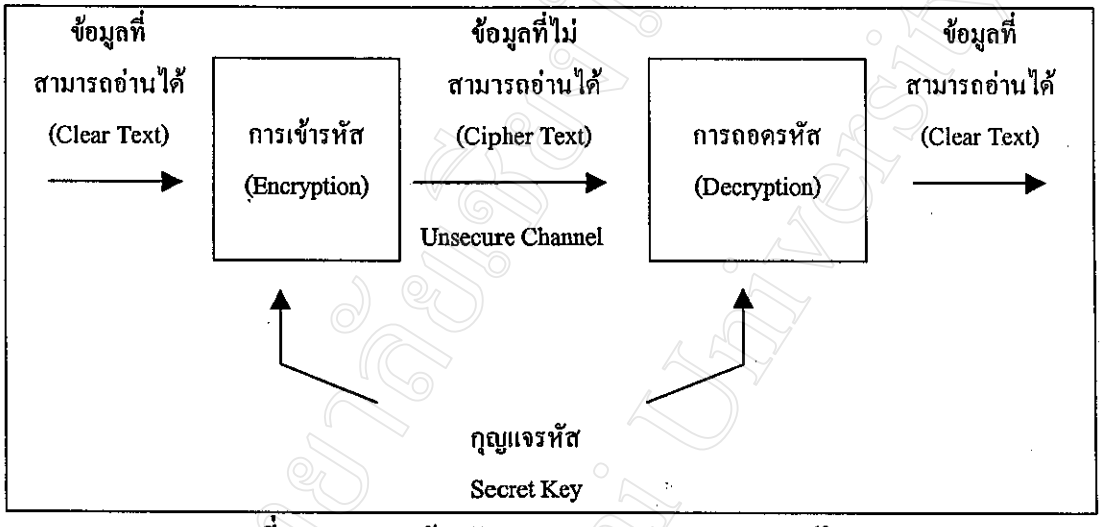
ทำได้ เนื่องจากว่าความยาวของข้อมูลใน Block จะเปลี่ยนไป ทำให้ไม่สามารถทำการถอดรหัสได้อย่างถูกต้อง

ข้อเสียของการเข้ารหัสแบบเป็นกลุ่ม(Group Cipher)

- ใช้เวลานาน(Slowness of Encryption) การเข้ารหัสแบบนี้ไม่สามารถที่จะทำได้หากข้อมูลที่จะทำการเข้ารหัสไม่ครบหรือไม่เต็ม Block ดังนั้นก่อนที่จะทำการเข้ารหัสจำเป็นต้องรอข้อมูลให้เต็มเสียก่อน และการรอนี้จะทำให้เกิดความล่าช้าและช้ากว่าเมื่อเทียบกับการเข้ารหัสทีละตัวเพราะในการเข้ารหัสทีละตัวสามารถจะทำได้เลยกับตัวอักษรแต่ละตัวที่มีอยู่
- มีความผิดพลาดต่อเนื่อง(Error Propagation) การเข้ารหัสแบบนี้ก่อให้เกิดความผิดพลาดของตัวอักษรที่สามารถส่งต่อความผิดพลาดไปยังตัวอักษรอื่น ๆ ได้ ดังนั้นหากเกิดความผิดพลาดตัวใดตัวหนึ่งขึ้นมาซึ่งอาจเกิดขึ้นได้ในระหว่างการส่งข้อความ ก็อาจทำให้ทั้ง Block ของข้อมูลเกิดความผิดพลาดได้ ซึ่งหากเปรียบเทียบกันกับการเข้ารหัสแบบทีละตัวแล้วนั้น หากเกิดความผิดพลาดขึ้นกับตัวอักษรตัวใดตัวหนึ่งก็จะไม่มีผลต่อเนื่องเกิดขึ้นกับตัวอักษรตัวอื่น ๆ เลย

3.1.2 การเข้ารหัสแบบ Secret Key Encryption

การเข้ารหัสแบบนี้อาศัยกุญแจเข้ารหัสและถอดรหัส ดังนั้นกุญแจรหัสนี้จะต้องเก็บไว้เป็นความลับ เพื่อว่าหากใครก็ตามขโมยข้อความ Cipher Text นี้ไปแล้วจะไม่สามารถทำการถอดรหัสข้อมูลได้เนื่องจากไม่มีกุญแจรหัส



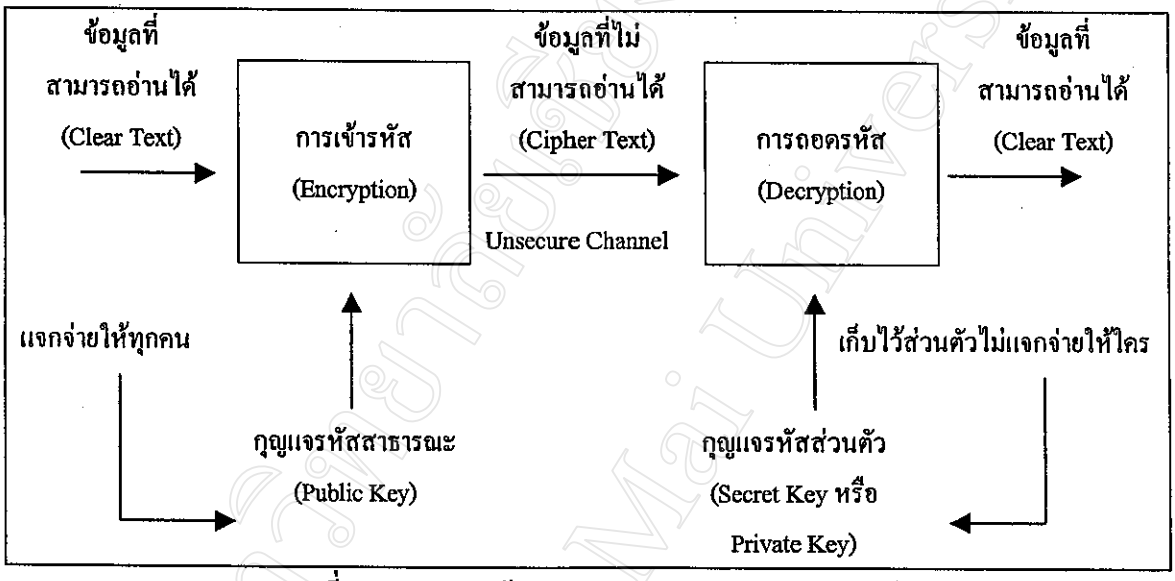
ภาพที่ 9 แสดงการเข้ารหัสแบบ Secret Key Encryption[19]

จากภาพที่ 9 จะเห็นว่ากุญแจรหัส Secret Key เพียงอันเดียวสามารถนำมาใช้ทั้งในการเข้ารหัส และถอดรหัส อย่างไรก็ตามในทางปฏิบัติแล้วการนำระบบนี้ไปใช้ก็มีปัญหาเรื่องความปลอดภัยในการแจกจ่ายกุญแจรหัส Secret Key เพราะในการถอดรหัสนั้นจำเป็นต้องใช้กุญแจรหัส และ การส่งกุญแจรหัสผ่านช่องสัญญาณที่ไม่ปลอดภัยนั้นมีความเสี่ยงสูงต่อการถูกจารกรรม

[19] เรื่องเดียวกัน : 118

3.1.3 การเข้ารหัสแบบ Public Key Encryption

การเข้ารหัสแบบนี้ได้ถูกคิดค้นขึ้นในปี ค.ศ. 1976 โดย Diffie Hellman ซึ่งการเข้ารหัสแบบนี้ไม่จำเป็นต้องเก็บกุญแจรหัสไว้เป็นความลับ แต่จะอาศัยกุญแจคู่หนึ่งคือกุญแจรหัสส่วนตัว(Secret Key) และกุญแจรหัสสาธารณะ(Public Key) ใช้ในการเข้ารหัสและถอดรหัส ซึ่งวิธีการนี้เรียกว่าการเข้ารหัสแบบ Asymmetric key Encryption แผนผังการเข้ารหัสมีดังนี้



ภาพที่ 10 แสดงการเข้ารหัสแบบ Public Key Encryption[20]

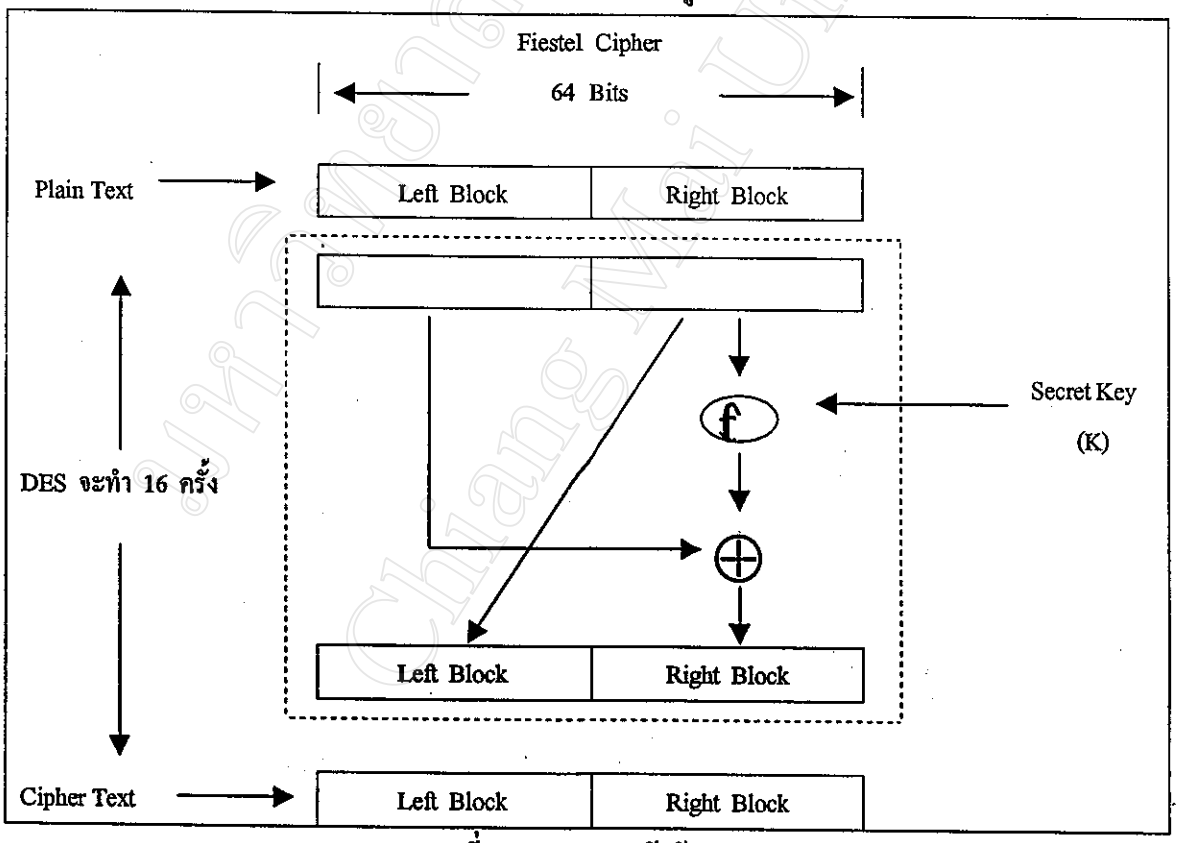
จากภาพที่ 10 เห็นได้ว่าการเข้ารหัสแบบนี้ ใช้กุญแจอย่างละอันในการเข้ารหัสและถอดรหัส โดยทั่วไปแล้วการเข้ารหัสแบบนี้ ผู้ใช้แต่ละคนจะมีกุญแจคนละหนึ่งคู่คือ Secret Key ส่วน Public Key นั้นสามารถจะแจกจ่ายไปให้ใครก็ได้ที่อยู่ในระบบและไม่ต้องทำการเก็บรักษาไว้เป็นความลับ ดังนั้นหากผู้ใช้ต้องการที่จะส่งข้อความไปถึงบุคคลอื่นที่อยู่ในระบบก็สามารถที่จะใช้ Public Key ของบุคคลนั้นมาทำการเข้ารหัสเสียก่อนแล้วจึงส่งออกไป และเมื่อผู้รับได้รับข้อความแล้วก็สามารถถอดรหัสได้แต่เพียงผู้เดียว เพราะกุญแจรหัสลับ Secret Key นั้นจะถูกเก็บไว้เป็นความลับเฉพาะบุคคลและจะไม่แจกจ่ายไปให้ใคร ดังนั้นถึงแม้คนอื่นในระบบจะได้รับข้อความก็ไม่อาจทำการถอดรหัสได้เนื่องจากว่าไม่มีกุญแจรหัส Secret Key ที่เป็นคู่กันกับกุญแจ Public Key ที่ใช้ในการเข้ารหัสข้อความนั้น

---

[20] เรื่องเดียวกัน : 119.

3.1.4 การเข้ารหัสข้อมูลแบบ DES (Data Encryption Standard)

การเข้ารหัสแบบนี้เป็นการเข้ารหัสแบบ Block Cipher อย่างหนึ่งซึ่งถูกพัฒนาขึ้นในประเทศสหรัฐอเมริกา ในปี ค.ศ. 1980 เป็นวิธีการเข้ารหัสแบบนี้มีความปลอดภัยที่สูงมาก และมักใช้ในธุรกิจการธนาคารที่ต้องการความปลอดภัยของข้อมูลสูงสุด วิธีการนี้ได้พัฒนามาจากการเข้ารหัสแบบ Feistel Ciphers ซึ่งใช้การเข้ารหัสแบบ Iterated Block Cipher แต่การเข้ารหัสแบบ DES นี้จะมีความปลอดภัยสูงมากเนื่องจากมีการทำการเข้ารหัสข้อมูลโดยวิธี Feisted Ciphers ถึง 16 ครั้ง และข้อมูลที่จะนำมาทำการเข้ารหัสนั้น จะมีความยาว 64 บิต ในแต่ละกลุ่ม ส่วนขนาดของกุญแจที่นำมาใช้ในการเข้ารหัสนั้นจะใช้ขนาด 56 บิต ซึ่งสามารถใช้ในการรักษาความปลอดภัยของข้อมูลได้อย่างดีมากในระดับหนึ่ง แต่อย่างไรก็ตาม เนื่องจากการพัฒนาทางด้านความเร็วของฮาร์ดแวร์คอมพิวเตอร์ที่สามารถนำมาใช้ช่วยในการวิเคราะห์ขโมยข้อมูล ทำให้คาดคะเนว่าขนาดของกุญแจรหัสลับนี้น่าจะเพิ่มขึ้นมากกว่า 56 บิต จึงจะสามารถช่วยรักษาความปลอดภัยของข้อมูลได้



ภาพที่ 11 แสดงการเข้าข้อมูลแบบ DES[21]

---

[21] Rhee, Man Young. **Cryptography and Secure Communication.** New York : McGraw-Hill, 1994 : 156.

จากภาพที่ 11 เป็นการนำ Fiestel Cipher มาทำเป็น DES โดยมีการทำซ้ำกันถึง 16 ครั้ง แต่การทำ DES นั้นก็มีข้อจำกัดอยู่แล้วคือ ขนาดของกุญแจรหัสลับนั้นอาจไม่เพียงพอในการรักษาความปลอดภัย ทางแก้วิธีหนึ่งก็คือใช้วิธีการที่เรียกว่า Triple DES ซึ่งเป็นการนำ DES มาทำการเข้ารหัสซ้ำกัน 3 ครั้งโดยใช้กุญแจเข้ารหัสคู่หนึ่ง ดังนั้นผลที่ได้ก็คือขนาดของกุญแจที่เพิ่มเป็น 2 เท่านั้นคือ 112 บิต (จากเดิม 56 บิต)

3.1.5 การเข้ารหัสข้อมูลแบบ RSA (Rivest – Shamir – Adelman Encrytption)

การเข้ารหัสข้อมูลแบบนี้ถูกประดิษฐ์ขึ้นในปี ค.ศ. 1978 และจนถึงทุกวันนี้ยังสามารถใช้รักษาความปลอดภัยของข้อมูลได้เป็นอย่างดี หลักการทำงานของการเข้ารหัสข้อมูลแบบนี้ก็คือความยากในการหาส่วนประกอบที่เป็นตัวเลขไพรม์(Prime Number) ของตัวเลขไพรม์ขนาดใหญ่ การประดิษฐ์วิธีการเข้ารหัสแบบ RSA นี้ทำให้การเข้ารหัสแบบ Public – Key Encryption สามารถนำมาใช้ได้จริงในทางปฏิบัติ การเข้ารหัสแบบ RSA นี้ให้ความปลอดภัยสูงมาก และมีการนำไปใช้อย่างแพร่หลายในปัจจุบัน

(1) ขั้นตอนการเข้ารหัสแบบ RSA[22]

- หาค่าตัวเลขไพรม์ขนาดใหญ่ P และ Q (ตัวอย่างเช่น ตัวเลขไพรม์ ที่มีขนาด 400 บิต) แล้วคำนวณหา n โดยที่ $n = pq$
- เลือกตัวหารร่วมมาก(ห.ร.ม.) และกำหนดให้ค่านี้เป็นกุญแจถอดรหัสที่เรียกว่า Decryption Exponent หรือ d ซึ่งตัวเลข d นั้นต้องไม่มีตัวหารร่วมใด ๆ กับค่า $(p-1)$ และ $(q-1)$ และตัวเลขนี้จะทำหน้าที่เป็นส่วนประกอบของ Private key โดยอาศัยสูตรดังต่อไปนี้เพื่อกำหนดความสัมพันธ์ระหว่างค่าต่างๆ ดังนี้คือ

  $\gcd (p-1)(q-1) = 1$
- คำนวณหาค่า Encryption Exponent หรือ ค่า e ซึ่งจะทำหน้าที่เป็นส่วนประกอบของ Public Key โดยกำหนดความสัมพันธ์ระหว่างค่าต่างๆ ดังนี้คือ

  $ed = 1 \bmod (p-1)(q-1)$

  (หมายเหตุ : $a = b \bmod n$ หมายความว่า เมื่อ b หารด้วย n แล้วเหลือเศษ a เช่น $2 = 11 \bmod 3$ เพราะ $11/3 = 3$ เหลือเศษ 2)

  ความสัมพันธ์นี้บอกว่า ed=1 เป็นค่าที่เกิดจากผลคูณของ (p-1)(q-1)

---

[22] Rhee, Man Young. **Cryptography and Secure Communication**. New York : McGraw-Hill, 1994 : 76.

- กำหนดค่า Public Key - (e,n) โดยค่า n = pq และค่า Public Key นี้สามารถที่จะแจกจ่ายออกไปได้
- ในการเข้ารหัสข้อมูลนั้นจะใช้ Public Key = (e,n) มาทำการเข้ารหัสข้อมูล m ได้ดังนี้ คือ $c = m^{e} \bmod n$

  โดยข้อมูลที่ได้หลังจากการเข้ารหัสคือ c = Cipher Text ซึ่งสามารถที่จะส่งออกไปสู่ระบบเครือข่ายภายนอกได้อย่างปลอดภัย เนื่องจากในการถอดรหัสนั้นจะต้องใช้กุญแจ d ที่ถูกเก็บไว้เป็น Private Key
- ในการถอดรหัสนั้นจะใช้ Private Key = d มาใช้ในการถอดรหัสเพื่อให้ได้ข้อความเดิม m กลับมา

  $m = cd \bmod n$

  นั่นคือการนำเอาข้อความที่เป็น Cipher Text, c มาทำการถอดรหัสเพื่อให้ได้ข้อความเดิม m กลับคืนมา โดยใช้กุญแจรหัส d ที่ถูกเก็บไว้เป็นความลับ และไม่แจกจ่ายให้ใคร
- สาเหตุที่การเข้ารหัส และถอดรหัสโดยวิธีการ RSA สามารถทำการเข้ารหัส และถอดรหัสข้อมูลได้นั้น สามารถดูได้จากขั้นตอนทางคณิตศาสตร์ ดังต่อไปนี้คือ

  n = pq ; โดยที่ q คือตัวเลข Prime

  ดังนั้น

  $x(p-1)(q-1)+1$ โดยที่ $n = pq$

  ซึ่งหมายความว่า ถ้า S เป็นตัวเลข Integer ตัวหนึ่งแล้ว

  $n = S*[(p-1)(q-1)] + 1$; โดยที่ $n = qp$

  $cd = (m^{e})d = ms(p-1)(q-1) = m^{e}d\ (m \pmod n)$

ตัวอย่างของการคำนวณ RSA

p = 7 q = 11

pq = 77

(p-1)(q-1) = (7-1)(11-1) = (6)(10) = 60

เลือก d = 13 ดังนั้น ตัว ห.ร.ม. ของ 13 กับ 60 คือ 1

ดังนั้น e = 37 เนื่องจากว่า

$37 * 13 = 481\ (1 \bmod 60)$

สมมติว่า ข้อความ m = 2 (โดยที่ $2 < n = 77$) ดังนั้น

$c = m^{e} \bmod n = 237 \bmod 7 = 51 \longrightarrow$ Cipher Text

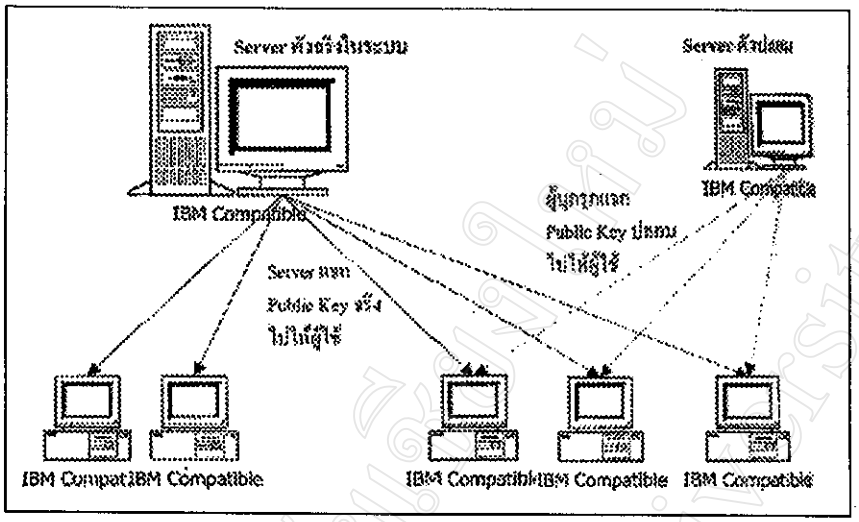
$m = cd \bmod n = 5113 \bmod 77 = 2 \longrightarrow$ Plain Text

ดังนั้นจะได้ m = 2 กลับมาเหมือนเดิม

(2) ความปลอดภัยของการเข้ารหัสแบบ RSA

ความปลอดภัยในการเข้ารหัสแบบ RSA ขึ้นกับความยากในการคำนวณหาค่า d จากค่า n และ e ที่มีอยู่ เพราะถ้าสามารถทำการถอดรากหาตัวประกอบของค่า n แล้ว ก็จะสามารถที่จะคำนวณหาค่า p และ q ได้ จากนั้นก็สามารถหาค่า d ซึ่งเป็น Private Key ได้ด้วย หากทำการถอดรากหาตัวประกอบของค่าตัวเลขนั้นๆ ไม่มีความยากแล้ว จะทำให้การเข้ารหัสแบบ RSA นั้นไม่มีความปลอดภัย คือผู้ไม่ประสงค์ดีสามารถทำการคำนวณหาค่า d ได้ และนำค่า d ไปใช้ในการคำนวณถอดรหัสหาข้อความเดิม m ซึ่งเป็น Plain Text จากข้อความ c ที่ขโมยที่เป็น Cipher Text โดยไม่ได้รับอนุญาต ด้วยเทคโนโลยีปัจจุบันสามารถทำการถอดรากหาตัวประกอบตัวเลขที่มีขนาดใหญ่มากที่สุดได้ถึง 400 บิต แต่ก็ได้มีการวิจัยอย่างกว้างขวางที่จะพยายามเพิ่มขนาดให้ถึง 512 บิต ซึ่งเป็นขนาดที่ใช้ในการเข้ารหัสแบบ RSA คำถามที่สำคัญ คือ ความปลอดภัยของการเข้ารหัสแบบ RSA ขึ้นอยู่กับความยากในการถอดหาตัวประกอบของตัวเลขไพรม์อย่างเดียวหรือไม่ เพราะอาจมีวิธีอื่น ๆ ที่สามารถนำมาใช้ในการคำนวณหา Plain Text จาก Cipher Text ได้

(3) ปัญหาในการแจกจ่ายกุญแจรหัสที่ใช้ในการเข้ารหัสโดยวิธี Public Key โดยใช้ RSA



ภาพที่ 12 แสดงการแจกกุญแจรหัสให้กับเครื่องต่าง ๆ ในระบบเครือข่าย[23]

ปัญหาประการหนึ่งในการแจกจ่าย Public Key ในระบบเครือข่ายไปยังผู้ใช้ในระบบคือ การพิสูจน์ว่าผู้ใช้นั้นได้รับกุญแจจริงหรือไม่ เพราะอาจเกิดการปลอมแปลงกุญแจจากผู้ไม่ประสงค์ดีที่บุกรุกเข้ามาในระบบได้ ดังนั้นจึงต้องมีวิธีที่สามารถบอกได้ว่ากุญแจนั้นเป็นกุญแจจริง(Genuine key) วิธีการที่นำมาใช้พิสูจน์ก็คือการใช้ลายเซ็นทางอิเล็กทรอนิกส์ (Digital Signature) ซึ่งตัวเซิร์ฟเวอร์จะทำการเซ็นลายเซ็นทางอิเล็กทรอนิกส์ และส่งไปพร้อมกับ Public Key และผู้ใช้ก็จะทำการพิสูจน์ว่าลายเซ็นอิเล็กทรอนิกส์นั้นเป็นลายเซ็นที่ออกมาจากตัว Server จริงหรือไม่ หากจริงแสดงว่ากุญแจ Public Key นั้นเป็นของจริงด้วย

(4) คุณสมบัติของการเข้ารหัสแบบ RSA

- การเข้ารหัสแบบ RSA นั้นเป็นการเข้ารหัสแบบ Block Cipher
- ปกติแล้วการเข้ารหัสแบบ RSA จะช้ากว่าการเข้ารหัสแบบอื่น ๆ มาก เนื่องจากว่าต้องใช้การคำนวณที่สลับซับซ้อน และขนาดกุญแจที่ใช้มีขนาดใหญ่มาก เมื่อเปรียบเทียบกับการเข้ารหัสแบบ DES แล้วนั้น การเข้ารหัสแบบ RSA จะช้ากว่าประมาณ 1,000 เท่า

---

[23] ณรงค์ชัย นมิตบุญอนันต์. **Computer Security for E-Commerce.** กรุงเทพ : บริษัทซีเอ็ดยูเคชั่น จำกัด (มหาชน), 1999 : 130.

- เนื่องจากความช้าในการเข้ารหัสข้อมูล จึงไม่นิยมเอา RSA ไปใช้ในการเข้ารหัสข้อความที่มีขนาดใหญ่ แต่จะนำเอาไปใช้ในการเข้ารหัสข้อมูลขนาดเล็กที่ต้องการความปลอดภัยสูงมาก ๆ เช่น ใช้ในการเข้ารหัส และแจกจ่าย Secret Key ที่ใช้เป็น Session Key ในการติดต่อสื่อสารกันระหว่างเครื่องคอมพิวเตอร์ในแต่ละครั้ง

3.1.6 หลักการเข้ารหัสข้อมูลที่ดี

(1) ระดับความปลอดภัยของข้อมูลที่ได้ ควรจะแปรผันตรงกับความยากของการเข้ารหัสข้อมูล นั่นคือหากวิธีการเข้ารหัสนั้นมีความสลับซับซ้อนมาก ก็ควรให้ระดับของความปลอดภัยของข้อมูลที่สูงด้วย

(2) ไม่ควรมีข้อจำกัดในการเลือกใช้กุญแจเข้ารหัสและในการเลือกใช้วิธีการ เพราะหากการเลือกใช้นั้นมีความยากและไม่สะดวกแล้วการเข้ารหัสนั้นไม่เป็นที่นิยมใช้

(3) กระบวนการนำวิธีการเข้ารหัสไปใช้จะต้องมีความสะดวกและง่าย เพราะหากการเข้ารหัสยากมากเกินไปแล้ว อาจทำให้เกิดความผิดพลาดในระหว่างกระบวนการพัฒนาและนำไปใช้งานได้

(4) ความผิดพลาดของการเข้ารหัส ณ จุดใดจุดหนึ่งของข้อมูลต้องไม่ขยายไปสู่ส่วนอื่นๆ

(5) เมื่อเสร็จจากการเข้ารหัสข้อมูลแล้ว ขนาดของข้อมูล Cipher Text ต้องมีขนาดไม่ใหญ่กว่าขนาดของ Clear Text

3.2 นโยบายการเข้ารหัส

เดิมทีเทคโนโลยีเข้ารหัสถือเป็นเทคโนโลยีที่ใช้เฉพาะในการทหาร อย่างไรก็ตามการประยุกต์ใช้เทคโนโลยีเข้ารหัสในด้านอื่น ๆ ในปัจจุบันทำให้เทคโนโลยีดังกล่าวพ้นสภาพจากการเป็นเทคโนโลยีด้านการทหารมาสู่เทคโนโลยีที่สามารถใช้งานทั้งด้านการทหารและด้านพลเรือน กล่าวคือในปัจจุบันธุรกิจอาจใช้เทคโนโลยีดังกล่าวในการประกอบการพาณิชย์อิเล็กทรอนิกส์ ทั้งการซื้อขายสินค้าผ่านเครือข่ายอินเทอร์เน็ตซึ่งถือเป็นการพาณิชย์อิเล็กทรอนิกส์ ทั้งการซื้อขายสินค้าผ่านเครือข่ายเอกชนเสมือน (Virtual Private Network,VPN) ในการพาณิชย์อิเล็กทรอนิกส์ระหว่างธุรกิจและธุรกิจ การเข้ารหัสสัญญาณภาพของเคเบิลทีวีเพื่อป้องกันผู้ที่ไม่ใช่สมาชิกสามารถรับชมรายการได้ ตลอดจนการที่ประชาชนทั่วไปใช้เทคโนโลยีดังกล่าวเพื่อป้องกันการถูกดักฟังในการติดต่อสื่อสารทางโทรศัพท์เป็นต้น

การที่เทคโนโลยีดังกล่าวกลายเป็นเทคโนโลยีที่ใช้ทั้งในด้านการทหารและด้านพลเรือนทำให้เกิดปัญหาว่าจะสามารถสร้างความสมดุลย์ระหว่างการสร้างความสามารถของรัฐในการคุ้มครองประชาชนจากภัยคุกคามต่างๆ กับการคุ้มครองความเป็นอยู่ส่วนตัว และเสรีภาพในการสื่อสารของประชาชนตลอดจนความมั่นใจในการดำเนินธุรกิจได้อย่างไร กล่าวคือหากรัฐมีนโยบายปล่อยให้ประชาชนและธุรกิจสามารถใช้เทคโนโลยีดังกล่าวอย่างเสรีโดยไม่มีข้อจำกัดแล้ว รัฐอาจประสบปัญหาในการบังคับใช้กฎหมายในการตรวจจับการสื่อสารของผู้ก่อการร้าย อาชญากร หรือรัฐบาลของประเทศศัตรู ในทางตรงกันข้าม หากรัฐมีนโยบายในการควบคุมการใช้เทคโนโลยีดังกล่าวอย่างเข้มงวดเกินไป ก็จะปิดโอกาสของธุรกิจและประชาชนในการใช้ประโยชน์จากเทคโนโลยีดังกล่าวและละเมิดความเป็นอยู่ส่วนตัว และเสรีภาพในการสื่อสารของประชาชน

ประเทศต่าง ๆ พยายามแก้ไขปัญหาดังกล่าวโดยอนุญาตให้ประชาชนมีเสรีภาพในการใช้เทคโนโลยีดังกล่าวได้ในสภาวะปรกติ แต่กำหนดให้รัฐสามารถเข้าถึงและถอดรหัสข้อมูลที่เข้ารหัสได้โดยชอบด้วยกฎหมายหรือที่เรียกกันว่า "การเข้าถึงข้อมูลโดยชอบด้วยกฎหมายโดยหน่วยงานรัฐ" (Lawful state access)

ในบางสถานการณ์ เช่น เมื่อสงสัยว่าจะมีการก่อการร้ายหรือการละเมิดกฎหมายต่างๆ เช่น การฟอกเงินการหลบเลี่ยงภาษี การฝ่าฝืนกฎหมายการแข่งขัน เป็นต้น สามารถเรียกนโยบายการควบคุมเทคโนโลยีเข้ารหัสในลักษณะดังกล่าวตลอดจนนโยบายอื่นที่เกี่ยวกับการควบคุมการผลิต การใช้ประโยชน์ การส่งออก และการนำเข้าเทคโนโลยีเข้ารหัสโดยรวมๆ ว่า "นโยบายเทคโนโลยีเข้ารหัส" (Encryption policy)[24]

---

[24] Rhee, Man Young. **Cryptography and Secure Communication.** New York : McGraw-Hill, 1994 : 244.

ประเทศอุตสาหกรรมในตะวันตกส่วนใหญ่มักไม่มีข้อจำกัดในนำเข้าเทคโนโลยีดังกล่าวจากประเทศอื่น แต่มักควบคุมการส่งออกผลิตภัณฑ์ที่มีเทคโนโลยีเข้ารหัสไปยังประเทศที่เคยปกครองในระบบสังคมนิยมหรือประเทศอื่นๆที่มีความสัมพันธ์ทางการเมืองที่ตึงเครียด เพื่อป้องกันการส่งออกเทคโนโลยีเข้ารหัสและผลิตภัณฑ์ที่มีความอ่อนไหวในด้านความมั่นคงไปยังประเทศเหล่านั้น ประเทศตะวันตกส่วนใหญ่ได้ทำความตกลงที่เรียกว่า "ความตกลงวัสเซนน่าร์ว่าด้วยการควบคุมการส่งออกอาวุธยุทโธปกรณ์และสินค้าและเทคโนโลยีที่ใช้ได้ทั้งในด้านการทหารและพลเรือน" (Wassenaar Arrangement on Export Controls for conventional Arms and Dual-use Goods and Technologies) ส่วนประเทศในค่ายสังคมนิยมเดิมเช่นจีนและรัสเซียหรือประเทศที่มีความเป็นห่วงด้านความมั่นคงสูงเช่นเกาหลีใต้มักมีข้อจำกัดในการนำเข้าเทคโนโลยีดังกล่าว[25]

นอกเหนือจากการควบคุมการส่งออกหรือการนำเข้าแล้ว วิธีการในการควบคุมเทคโนโลยีเข้ารหัสที่สำคัญอื่นๆ คือการจำกัดความยาวของคุญแจ(Key Length)ที่สามารถใช้ได้ และการกำหนดให้มีระบบการเก็บหรือกู้กุญแจ การจำกัดความยาวของกุญแจที่สามารถใช้ได้จะทำให้หน่วยงานรัฐสามารถใช้เครื่องคอมพิวเตอร์ที่มีขีดความสามารถสูงในการถอดรหัสของข้อมูลที่ต้องการตรวจสอบได้ อย่างไรก็ตามการควบคุมโดยวิธีนี้จะทำให้ระบบข้อมูลโดยรวมมีความปลอดภัยต่ำลงและเสี่ยงต่อการถูกผู้อื่นนอกจากหน่วยงานรัฐถอดรหัสด้วยวิธีการเดียวกัน การอนุญาตให้ใช้เทคโนโลยีเข้ารหัสที่มีขีดความสามารถสูง แต่กำหนดให้หน่วยงานรัฐที่เกี่ยวข้องสามารถเข้าถึงข้อมูลโดยชอบด้วยกฎหมายโดยใช้ระบบการเก็บกุญแจหรือการกู้กุญแจจึงเป็นวิธีที่ดีกว่า

การเข้าถึงข้อมูลโดยชอบด้วยกฎหมายของหน่วยงานรัฐโดยใช้ระบบเก็บกุญแจ(Key Archiving) หมายถึงการที่รัฐกำหนดให้ผู้ใช้เทคโนโลยีเข้ารหัสต้องทำกุญแจลับสำรองแล้วจัดเก็บไว้ที่ใดที่หนึ่ง ตัวอย่างที่รู้จักกันดีของระบบดังกล่าวคือระบบฝากกุญแจ(Key Escrow) ซึ่งกำหนดให้เจ้าหน้าที่หรือบุคคลที่รัฐแต่งตั้ง เช่นองค์กรออกใบรับรองของผู้ใช้เก็บกุญแจสำรองไว้เพื่อใช้ในการถอดรหัสในกรณีที่รัฐต้องการตรวจสอบ ในช่วงต้นปี 1996 รัฐบาลสหรัฐเคยจะนำระบบดังกล่าวมาใช้แต่ไม่สามารถดำเนินการได้เนื่องจากได้รับการต่อต้านอย่างรุนแรงจากองค์กรสิทธิมนุษยชนต่าง ๆ ในประเทศ ด้วยเหตุผลว่ามาตรการดังกล่าวเป็นการละเมิดสิทธิเสรีภาพในการแสดงออกและความเป็นส่วนตัวของประชาชน[26]

ส่วนการเข้าถึงข้อมูลโดยชอบด้วยกฎหมายของหน่วยงานรัฐโดยใช้ระบบกู้กุญแจ(Key Recovery) เป็นวิธีการที่ผู้ใช้เทคโนโลยีเข้ารหัสไม่ต้องฝากกุญแจลับของตนไว้กับผู้อื่น แต่จะใช้กุญแจสาธารณะของหน่วยงานกู้กุญแจเข้ารหัสกุญแจลับของตนแล้วผนวกลงไปในข้อมูลที่ต้องการเข้ารหัส

---

[25] ชัชวาล ชิดชัยมงคง. "ความปลอดภัยของระบบการค้าอินเทอร์เน็ต". BCM. (เมษายน 1998) : 139.

[26] เรื่องเดียวกัน : 140.

ด้วย เมื่อรัฐต้องการตรวจสอบก็จะสามารถใช้กุญแจลับของหน่วยงานกู้กุญแจถอดรหัสกุญแจลับของผู้ใช้มาถอดรหัสดูข้อมูลอีกทีหนึ่ง เมื่อปี 1997 หน่วยงานสอบสวนกลาง(FBI)ของสหรัฐเคยประกาศห้ามใช้เทคโนโลยีเข้ารหัสที่มีขีดความสามารถสูงที่ไม่มีระบบการกู้กุญแจ (Key Recovery) อย่างไรก็ตามการควบคุมดังกล่าวก็ถูกต่อต้านอย่างหนักเช่นเดียวกัน[27]

3.2.1 ตัวอย่างนโยบายเทคโนโลยีเข้ารหัส

ตามกฎหมายของสหรัฐในปัจจุบันเทคโนโลยีเข้ารหัสถือเป็นสินค้ายุทธภัณฑ์เช่นเดียวกับอาวุธยุทโธปกรณ์ทั้งหลาย การส่งออกเทคโนโลยีดังกล่าวถูกควบคุมด้วยกฎหมายว่าด้วยการค้าอาวุธ ซึ่งเดิมเรียกว่ากฎหมายการค้าอาวุธระหว่างประเทศ(International Traffic in Arms Regulation หรือ ITAR) กฎหมายดังกล่าวกำหนดให้การส่งออกเทคโนโลยีดังกล่าวจะกระทำได้ก็ต่อเมื่อได้รับใบอนุญาตจากกระทรวงพาณิชย์ของสหรัฐ (Ministry of Commerce) เท่านั้น อย่างไรก็ตามในระยะหลังรัฐบาลสหรัฐเริ่มตระหนักว่านโยบายดังกล่าวไม่เป็นผลดีต่ออุตสาหกรรมคอมพิวเตอร์ของสหรัฐเอง โดยจะผลักดันให้ผู้ประกอบการสหรัฐต้องย้ายฐานการผลิตไปต่างประเทศ จึงได้เริ่มผ่อนคลายข้อจำกัดดังกล่าวลงจนในที่สุดยินยอมให้ผู้ผลิตสามารถส่งออกเทคโนโลยีเข้ารหัสที่มีความยาวของกุญแจไม่เกิน 40 บิต และ 56 บิตในกรณีการส่งออกเพื่อใช้ในสถาบันการเงิน และต่อมาในเดือนกันยายน 1999 รัฐบาลได้ผ่อนคลายกฎระเบียบในการส่งออกอีกครั้ง โดยลดข้อจำกัดในการส่งออกผลิตภัณฑ์เทคโนโลยีเข้ารหัสที่มีความยาวของกุญแจไม่เกิน 64 บิต โดยให้ผู้ส่งออกขออนุญาตกระทรวงพาณิชย์ครั้งเดียวสำหรับผลิตภัณฑ์แต่ละรุ่น ส่วนผลิตภัณฑ์เทคโนโลยีเข้ารหัสที่มีความยาวของกุญแจเกิน 64 บิต ก็จะสามารถส่งออกได้เป็นการพิเศษหากเป็นเทคโนโลยีที่ออกแบบให้ใช้กับผู้ใช้ทั่วไปที่ไม่ต้องการการสนับสนุนทางเทคนิคมาก และประเทศที่ส่งออกไม่ใช่ประเทศในบัญชีรายชื่อต้องห้าม

แคนาดาไม่มีข้อจำกัดในการส่งออกเทคโนโลยีเข้ารหัสใด ๆ ไปยังสหรัฐ และสามารถส่งออกผลิตภัณฑ์ลายมือชื่อดิจิตอลได้โดยไม่มีข้อจำกัด นอกจากนี้แคนาดามีนโยบายการควบคุมการส่งออกเทคโนโลยีเข้ารหัสเช่นเดียวกับสหรัฐ ในอดีตแคนาดาเคยอนุญาตให้ส่งออกเทคโนโลยีเข้ารหัสที่มีความยาวของกุญแจไม่เกิน 40 บิตเท่านั้น ยกเว้นสถาบันการเงินต่าง ๆ ได้รับอนุญาตให้ส่งออกเทคโนโลยี DES ที่มีความยาวของกุญแจไม่

---

[27] ธีรา ทานตวณิช. "Web Security ขั้นตอนการสร้างความปลอดภัยสำหรับ E-Commerce". **Microcomputer**. (เมษายน 2000) : 126.

เกิน 56 บิตได้ ต่อมาในปี 1996 แคนนาดาได้ทดลองเปิดการส่งออกเทคโนโลยีเข้ารหัสที่มีความยาวของกุญแจไม่เกิน 56 บิตไปยังประเทศต่างเป็นการทั่วไป [28]

3.2.2 แนวคิดในการกำหนดนโยบายควบคุมเทคโนโลยีเข้ารหัส

ในการกำหนดนโยบายเทคโนโลยีเข้ารหัส ผู้กำหนดนโยบายควรมุ่งรักษาสมดุลระหว่างการส่งเสริมการพาณิชย์อีเล็กทรอนิกส์ การคุ้มครองเสรีภาพในการสื่อสารของประชาชนและการเข้าถึงข้อมูลโดยชอบด้วยกฎหมายโดยรัฐ ตลอดจนรักษาความสอดคล้องทางนโยบายกับประเทศต่างๆ ตัวอย่างการกำหนดนโยบายในลักษณะดังกล่าวที่ประเทศไทยสามารถอ้างอิงเป็นต้นแบบได้คือแนวทางการใช้เทคโนโลยีเข้ารหัสขององค์กรความร่วมมือด้านเศรษฐกิจและการพัฒนา(OECD) ซึ่งบางประเทศเช่นเกาหลีใต้ใช้เป็นแนวทางในการออกกฎหมายควบคุมเทคโนโลยีการเข้ารหัส (Cryptography law)

(1) แนวทางการใช้เทคโนโลยีเข้ารหัสขององค์กรความร่วมมือด้านเศรษฐกิจและการพัฒนา ประกอบด้วยหลักการ 8 ข้อดังนี้[29]

- วิธีการในการใช้เทคโนโลยีเข้ารหัสจะต้องน่าเชื่อถือ เพื่อสร้างความมั่นใจในการใช้ระบบสารสนเทศและระบบสื่อสาร
- ผู้ใช้ควรมีสิทธิในการเลือกใช้วิธีการเข้ารหัสใด ๆ ตามกรอบของกฎหมาย
- วิธีการเข้ารหัสควรได้รับการพัฒนาขึ้นเพื่อตอบสนองความจำเป็น ความต้องการและความรับผิดชอบของประชาชน ธุรกิจและหน่วยงานรัฐ
- มาตรฐานทางเทคนิค ข้อกำหนด และโปรโตคอล(protocol) ในการเข้ารหัสควรได้รับการพัฒนาขึ้นในระดับชาติ และระดับนานาชาติ
- สิทธิพื้นฐานของประชาชนในการรักษาความเป็นอยู่ส่วนตัว(Privacy) ตลอดจนการรักษาความลับในการติดต่อสื่อสารและการคุ้มครองข้อมูลส่วนตัว ควรได้รับการยอมรับในนโยบายของประเทศในการควบคุมเทคโนโลยีเข้ารหัส การออกแบบและการใช้เทคโนโลยีดังกล่าว
- นโยบายควบคุมเทคโนโลยีเข้ารหัสของประเทศอาจยินยอมให้รัฐเข้าถึงกุญแจลับที่ใช้ในการเข้ารหัส ข้อมูลที่ถอดรหัส(plaintext) หรือข้อมูลที่เข้ารหัสโดย

---

[28] กมลภัทร บุญค้ำ. "การเข้ารหัส 56 บิต ยังไม่เพียงพอ". BCM. (ธันวาคม 1999) : 39.

[29] ธีรา ทานตวณิช. "Web Security ขั้นตอนการสร้างความปลอดภัยสำหรับ E-Commerce". Microcomputer. (เมษายน 2000) : 127.

ชอบด้วยกฎหมาย อย่างไรก็ตามนโยบายเหล่านี้จะต้องสอดคล้องกับหลักการข้ออื่นๆ มากที่สุดเท่าที่จะเป็นไปได้

- หน้าที่และความรับผิดชอบซึ่งเกิดขึ้นตามสัญญาหรือผลของกฎหมายของประชาชน หรือหน่วยงานที่ให้บริการเข้ารหัส เก็บรักษาหรือเข้าถึงคุญแจที่ใช้ในการเข้ารหัส ควรได้รับการประกาศอย่างชัดแจ้ง
- รัฐบาลของประเทศต่าง ๆ ควรร่วมมือและประสานนโยบายเทคโนโลยีเข้ารหัสและควรระวังการอ้างนโยบายดังกล่าวในการกีดกันทางการค้า

ในฐานะที่ประเทศไทยไม่ใช่ประเทศผู้ผลิตเทคโนโลยีดังกล่าว การเปิดกว้างให้ประชาชนและธุรกิจสามารถเลือกใช้เทคโนโลยีได้ตามความต้องการของตนเองโดยไม่มีข้อจำกัดเรื่องการนำเข้าและการใช้น่าจะมีผลดีในการเอื้ออำนวยให้เกิดการรับนวัตกรรมทางเทคโนโลยีใหม่ ๆ จากต่างประเทศ และส่งเสริมการใช้เทคโนโลยีดังกล่าวในการพาณิชย์อิเล็กทรอนิกส์ อย่างไรก็ตามในอนาคตหน่วยงานด้านความมั่นคงและหน่วยงานที่บังคับใช้กฎหมายต่าง ๆ อาจเห็นความจำเป็นในการควบคุมเทคโนโลยีเข้ารหัส โดยเฉพาะการเข้าถึงข้อมูลโดยชอบด้วยกฎหมายโดยหน่วยงานรัฐเพื่อป้องกันการก่อการร้าย การก่ออาชญากรรม การฟอกเงิน การเผยแพร่สารสนเทศที่ขัดกับกฎหมาย เช่น ภาพลามกอนาจาร หรือการละเมิดกฎหมายอื่น

(2) นโยบายการเข้าถึงข้อมูลโดยชอบด้วยกฎหมายของรัฐ

- กำหนดขอบเขตการแทรกแซงของรัฐเฉพาะในกรณีการใช้เทคโนโลยีเข้ารหัสในการรักษาความลับของข้อมูลเท่านั้น โดยไม่ให้รัฐแทรกแซงการใช้เทคโนโลยีดังกล่าวในการระบุตัวบุคคล(Authentication) หรือรักษาความถูกต้องของข้อมูล (Integrity)
- กำหนดหลักเกณฑ์ที่ชัดเจนในการอนุญาตให้รัฐเข้าถึงข้อมูลโดยชอบด้วยกฎหมาย เช่น ให้ทำได้ต่อเมื่อได้รับคำสั่งหรือหมายศาลเท่านั้น
- กำหนดระยะเวลาที่แน่นอนในการอนุญาตให้รัฐเข้าถึงข้อมูลโดยชอบด้วยกฎหมาย และอนุญาตให้เข้าถึงเฉพาะข้อมูลที่เกี่ยวข้องกับเรื่องที่ตรวจสอบอยู่เท่านั้น
- กำหนดให้บุคคลซึ่งช่วยเหลือรัฐในการเข้าถึงข้อมูลโดยชอบด้วยกฎหมาย เช่น ผู้รักษากุญแจลับที่เกี่ยวข้องไม่มีความผิดจากการกระทำดังกล่าว

- วางระบบตรวจสอบที่มีความโปร่งใส เช่น กำหนดให้มีการเก็บบันทึกการเข้าถึงโดยชอบด้วยกฎหมาย เพื่อให้สามารถตรวจสอบจากภายนอกได้ ในทางปฏิบัติการกำหนดนโยบายดังกล่าวอาจทำได้โดยออกบทบัญญัติในกฎหมายคุ้มครองข้อมูล หรือกฎหมายอาชญากรรมทางคอมพิวเตอร์ ซึ่งศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติกำลังอยู่ในระหว่างเตรียมการยกร่าง การพิจารณาว่าเนื้อหาดังกล่าวควรถูกบัญญัติในกฎหมายฉบับใดนั้นอาจขึ้นอยู่กับแนวทางการปฏิบัติ เช่น หากต้องการกำหนดแนวทางของรัฐในการสืบค้นและยึดหลักฐานในการประกอบอาชญากรรมทางคอมพิวเตอร์ก็อาจกำหนดบทบัญญัติดังกล่าวในกฎหมายอาชญากรรมคอมพิวเตอร์[30]

3.3 ความปลอดภัยในการพาณิชย์อิเล็กทรอนิกส์และเทคโนโลยีที่เกี่ยวข้อง

ความปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์เป็นสิ่งสำคัญที่จะสร้างความเชื่อมั่นให้เกิดกับการพาณิชย์อิเล็กทรอนิกส์ ทั้งการพาณิชย์อิเล็กทรอนิกส์ระหว่างธุรกิจและผู้บริโภค และการพาณิชย์อิเล็กทรอนิกส์ระหว่างธุรกิจและธุรกิจ ธุรกรรมอิเล็กทรอนิกส์ที่มีความปลอดภัยอย่างแท้จริงจะต้องเกิดขึ้นในระบบที่มีความสามารถใน 4 ด้าน คือการระบุตัวบุคคล(Authenticity) การรักษาความลับ (Confidentiality) การรักษาความถูกต้อง(Integrity) และการป้องกันการปฏิเสธความรับผิดชอบ(Non-Repudiation) ดังตารางที่ 5

ตารางที่ 5 แสดงความหมายของรูปแบบของการรักษาความปลอดภัยแบบต่าง ๆ[31]

ความสามารถ	ความหมาย
การระบุตัวบุคคล (Authenticity)	สามารถระบุได้ว่าบุคคลที่ติดต่อด้วยนั้นเป็นบุคคลตามที่กล่าวอ้างหรือมีอำนาจหน้าที่ตามที่กล่าวอ้างจริง
การรักษาความลับ (Confidentiality)	สามารถรักษาความลับมิให้มีผู้อื่นแอบดูข้อมูลที่เก็บไว้หรือข้อมูลส่งผ่านไปทางเครือข่าย
การรักษาความถูกต้อง (Integrity)	สามารถรักษาความถูกต้องของข้อมูลมิให้มีการแก้ไขโดยไม่ปรากฏร่องรอย
การป้องกันการปฏิเสธความรับผิดชอบ (Non-Repudiation)	สามารถป้องกันการปฏิเสธความรับผิดชอบ จากฝ่ายต่างๆ ที่เกี่ยวข้องว่าไม่ได้มีการส่งหรือรับข้อมูล

---

[30] "พาณิชย์อิเล็กทรอนิกส์". [http://www.ecomerce.or.th]. 2002.

[31] ฉรงค์ชัย นมิตบุญอนันต์. **Computer Security for E-Commerce**. กรุงเทพ : บริษัทซีเอ็ดยูเคชั่น จำกัด (มหาชน), 1999 : 198.

ตัวอย่างของเทคโนโลยีที่ช่วยในการรักษาความปลอดภัยในการพาณิชย์อิเล็กทรอนิกส์ที่มีความสามารถครบทั้ง 4 ประการดังกล่าวมาข้างต้นคือเทคโนโลยีการเข้ารหัสที่ใช้กุญแจลับ(Secret Key) คู่กับกุญแจสาธารณะ (Public Key) หรือที่จะเรียกสั้น ๆ ว่าเทคโนโลยีการเข้ารหัสด้วยกุญแจสาธารณะ ซึ่งเป็นเทคโนโลยีที่ใช้กุญแจดอกหนึ่งในการเข้ารหัสและใช้อีกดอกหนึ่งในการถอดรหัส

นอกจากเทคโนโลยีการเข้ารหัสด้วยกุญแจสาธารณะแล้ว เทคโนโลยีอื่น ๆ ที่เกี่ยวข้องกับการรักษาความปลอดภัยในการพาณิชย์อิเล็กทรอนิกส์ได้แก่ เทคโนโลยีการเข้ารหัสด้วยกุญแจลับเพียงดอกเดียว ซึ่งมีความสามารถครบทั้ง 4 ประการแต่ไม่สะดวกที่จะใช้ในสภาพแวดล้อมแบบเปิดเช่นเครือข่ายอินเตอร์เน็ต ส่วนเทคโนโลยีอื่น ๆ เช่นการใช้รหัสผ่านและการใช้หมายเลขประจำตัวบุคคลจะมีความสามารถในการระบุตัวบุคคลแต่ไม่มีความสามารถอื่น ๆ ที่เหลือ ในขณะที่การใช้ลักษณะทางชีวภาพ(Biometrics) เช่นลายนิ้วมือ หรือเสียงจะสามารถระบุตัวบุคคลและการป้องกันการปฏิเสธความรับผิดชอบได้เท่านั้น แต่ไม่มีความสามารถอื่น ๆ

3.3.1 ลายมือชื่อและใบรับรองอิเล็กทรอนิกส์

ลายมือชื่ออิเล็กทรอนิกส์เป็นการประยุกต์ใช้เทคโนโลยีต่าง ๆ ดังกล่าวข้างต้นในการระบุตัวบุคคล ลายมือชื่ออิเล็กทรอนิกส์ที่สร้างจากเทคโนโลยีเข้ารหัสด้วยกุญแจสาธารณะเรียกว่าลายมือชื่อดิจิตอล(Digital signature) ในการลงลายมือชื่อดิจิตอลกำกับข้อความที่ต้องการส่งผ่านทางเครือข่าย ผู้ส่งข้อความจะใช้กุญแจลับของตนในการลงลายมือชื่อโดยผ่านกระบวนการคำนวณทางคณิตศาสตร์ ผู้รับจะสามารถตรวจสอบความถูกต้องของลายมือชื่อดังกล่าวได้โดยใช้กุญแจสาธารณะของผู้ส่งที่แสดงอยู่ในใบรับรองดิจิตอล(Digital certificate) ซึ่งมักจัดเก็บโดยบุคคลหรือองค์กรซึ่งเป็นผู้ออกใบรับรองนั้น นอกจากช่วยในการระบุตัวผู้ส่งข้อมูลแล้วการลงลายมือชื่อดิจิตอลยังป้องกันข้อมูลให้มีความถูกต้องไม่ถูกแก้ไขโดยไม่ทิ้งร่องรอยไว้ได้อีกด้วย[32] นอกเหนือไปจากกุญแจสาธารณะแล้ว ใบรับรองดิจิตอลยังแสดงข้อมูลอื่น ๆ อีกหลายอย่าง เช่น ใบรับรองดิจิตอลที่ออกตามมาตรฐาน X.509 v3 ซึ่งมาตรฐานที่แพร่หลายที่สุดจะต้องมีข้อมูลดังนี้ หมายเลขของใบรับรอง(Serial number)วิธีการที่ใช้ในการเข้ารหัสข้อมูล(Algorithm) หน่วยงานที่ออก(Issuer) เวลาที่ใบรับรองเริ่มใช้ได้(Starting time) กุญแจสาธารณะของผู้ได้รับการรับรอง(Subject's public key) ลายมือชื่อดิจิตอลของหน่วยงานที่ออกใบรับรอง(CA signature)

---

[32] สมเกียรติ ตั้งกิจวานิชย์. **ลายมือชื่ออิเล็กทรอนิกส์และองค์กรออกใบรับรอง**. งานวิจัยสถาบันเพื่อการพัฒนาประเทศไทย, 1999 : 23.

(1) การแบ่งใบรับรองดิจิตอลตามลักษณะการใช้งาน สามารถแบ่งออกเป็นกลุ่ม ๆ ได้ดังนี้คือ

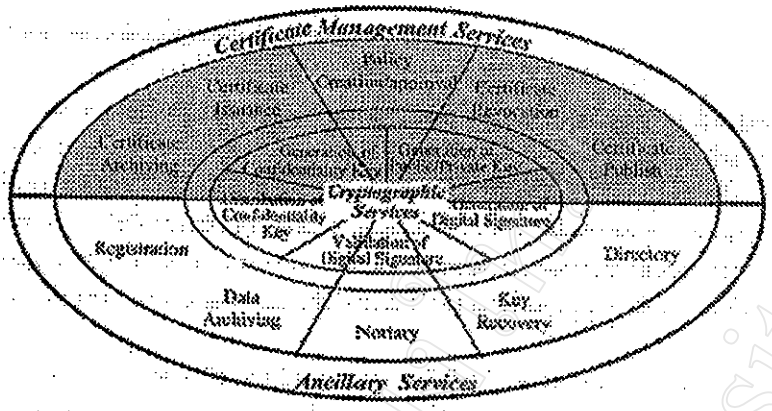
- ใบรับรองเครื่องเซิร์ฟเวอร์(Server certificate) เช่นใบรับรองเครื่องแม่ข่าย SSL ที่ใช้ทั่วไปในการพาณิชย์อิเล็กทรอนิกส์ ซึ่งจะมีชื่อของบริษัทที่เกี่ยวข้อง ชื่อโดเมนของเครื่องและกุญแจสาธารณะของเครื่อง เป็นต้น
- ใบรับรองบุคคล(Personal certificate) หรือใบรับรองเครื่องไคลเอ็นต์(Client certificate) ซึ่งจะระบุชื่อบุคคลนั้นและข้อมูลอื่น ๆ
- ใบรับรององค์กรออกใบรับรอง(Certification authority certificate) ซึ่งจะมีชื่อองค์กรออกใบรับรองที่ได้รับการรับรอง กุญแจสาธารณะขององค์กรนั้น และลายมือชื่อดิจิตอลขององค์กรออกใบรับรองที่ให้การรับรอง ซึ่งอาจเป็นการรับรองตนเอง (Self–certified)ก็ได้ในกรณีที่องค์กรออกใบรับรองทั้งสองเป็นหน่วยงานเดียวกัน

(2) องค์กรออกใบรับรอง

การระบุตัวบุคคลโดยใช้ใบรับรองดิจิตอลอาจทำได้โดยการออกใบรับรองให้แก่บุคคลอื่นซึ่งรู้จักกันในลักษณะการแนะนำกันต่อเป็นทอด ๆ ในลักษณะของสายใยแห่งความเชื่อถือ(Web of trust) อย่างไรก็ตามการตรวจสอบการระบุตัวบุคคลในลักษณะดังกล่าวเป็นสิ่งที่มีความยุ่งยากมากและมีความน่าเชื่อถือต่ำ เนื่องจากเป็นการรับรองกันเป็นทอด ๆ โดยผู้รับรองแต่ละคนมีมาตรฐานในการรับรองที่แตกต่างกัน

โครงสร้างพื้นฐานซึ่งจะช่วยให้สามารถระบุตัวบุคคลได้อย่างสะดวก และมีความน่าเชื่อถือสูงคือหน่วยงานที่เรียกว่าองค์กรออกใบรับรอง(Certification Authority หรือ CA) หรือที่เรียกกันว่าโครงสร้างพื้นฐานของระบบกุญแจสาธารณะ(Public Key Infrastructure หรือ PKI) ซึ่งจะเป็นตัวกลางในการตรวจสอบและออกใบรับรองให้แก่ผู้อื่น ตามแนวทางนี้จะมีบุคคลต่าง ๆ ที่เกี่ยวข้องกัน 3 ฝ่ายคือ ผู้ถือใบรับรอง(Certificate holder) เรียกว่าเป็นบุคคลที่หนึ่ง ผู้ใช้ใบรับรองในการระบุตัวผู้ถือใบรับรอง(Relying party) เรียกว่าเป็นบุคคลที่สอง และองค์กรออกใบรับรองซึ่งเรียกว่าเป็นบุคคลที่สาม

องค์กรออกใบรับรองโดยทั่วไปจะมีบทบาทในการให้บริการใน 3 ด้านใหญ่ๆ คือ การให้บริการเทคโนโลยีเข้ารหัส(Cryptographic service) บริการที่เกี่ยวข้องกับการออกใบรับรอง(Certification management service) และบริการเสริม(Ancillary service) ต่าง ๆ ดังมีรายละเอียดดังภาพที่ 13



ภาพที่ 13 แสดงองค์กรออกใบรับรองและการบริการด้านต่าง ๆ[33]

- บริการเทคโนโลยีเข้ารหัสซึ่งจะประกอบไปด้วยการสร้างกุญแจลับ การส่งมอบกุญแจลับ การสร้างกุญแจสาธารณะและกุญแจลับ การสร้างลายมือชื่อดิจิตอล และการรับรองลายมือชื่อดิจิตอล
- บริการที่เกี่ยวข้องกับการออกใบรับรองซึ่งประกอบไปด้วยการออกใบรับรอง (Certificate issuance) การยกเลิกใบรับรอง(Certificate revocation) การตีพิมพ์ใบรับรองเผยแพร่แก่บุคคลทั่วไป(Certificate publishing) การเก็บต้นฉบับใบรับรอง (Certificate archiving) และการกำหนดนโยบายการออกและอนุมัติใบรับรอง(Policy creation /approval) เช่น ขั้นตอนในการปฏิบัติงานในการออกใบรับรอง
- บริการเสริมซึ่งได้แก่การบันทึก(Registration) ข้อมูลต่าง ๆ ที่จำเป็นต้องใช้ในการออกหรือยกเลิกใบรับรอง การเก็บต้นฉบับข้อมูล(Data achiving)เพื่อการตรวจสอบในระยะยาว การตรวจสอบสัญญาต่าง ๆ (Notarial authentiation) การกู้กุญแจ(Key recovery)ในกรณีที่ผู้ใช้ทำกุญแจของตนหาย การทำทะเบียน(Directory) ข้อมูลต่าง ๆ ที่เกี่ยวข้องกับผู้ใช้บริการ เช่นที่อยู่ หมายเลขโทรศัพท์

---

[33] เรื่องเดียวกัน : 25..

3.3.2 สภาพแวดล้อมแบบเปิดและสภาพแวดล้อมแบบปิด

เราอาจแบ่งสภาพแวดล้อมในการออกใบรับรองออกเป็นออกเป็นสภาพแวดล้อมเปิด (Open PKI) และสภาพแวดล้อมแบบปิด(Closed PKI) ในสภาพแวดล้อมเปิดซึ่งพบมากในการค้าปลีกผ่านเครือข่ายอินเตอร์เน็ตและการพาณิชย์อิเล็กทรอนิกส์ระหว่างธุรกิจและผู้บริโภคอื่นๆ ฝ่ายต่างๆที่เกี่ยวข้องมักไม่รู้จักกันมาก่อน และไม่มีความสัมพันธ์ในเชิงสัญญา (Contractual relationship)กันล่วงหน้า ในสภาพแวดล้อมนี้บทบาทขององค์กรออกใบรับรองคือการออกใบรับรองตัวบุคคล(Identity certificate)เพื่อให้ทั้งสองฝ่ายสามารถระบุตัวบุคคลอีกฝ่ายหนึ่งได้[34]

ส่วนในสภาพแวดล้อมแบบปิด ฝ่ายต่าง ๆ ที่เกี่ยวข้องจะรู้จักกัน และมักมีความสัมพันธ์ในเชิงสัญญากันอยู่แล้ว จะพบได้บ่อยในการพาณิชย์อิเล็กทรอนิกส์ระหว่างธุรกิจ-ธุรกิจ เช่น การซื้อขายสินค้าผ่านเครือข่ายเอ็กซ์ทราเน็ต(Extranet) หรือเครือข่ายอีดีไอ(EDI) การติดต่อระหว่างบุคคลต่าง ๆ ในองค์กรเดียวกันผ่านเครือข่ายอินทราเน็ต(intranet) หรือแม้กระทั่งการพาณิชย์อิเล็กทรอนิกส์ระหว่างธุรกิจผู้บริโภคในบางรูปแบบ เช่น การทำธุรกรรมด้านการเงินระหว่างธนาคารและลูกค้าของธนาคาร เป็นต้น ในบางกรณีบุคคลที่สองและบุคคลที่สามอาจเป็นบุคคลเดียวกัน ทำให้เหลือเพียงฝ่ายต่าง ๆ ที่เกี่ยวข้องเพียงสองฝ่าย เช่น ธนาคารเป็นผู้ออกใบรับรองให้แก่ลูกค้า และใช้ใบรับรองการระบุตัวลูกค้าของตนในการทำธุรกรรมหรือบริษัทเป็นผู้ออกใบรับรองนั้นในการกำหนดสิทธิในการใช้เครื่องคอมพิวเตอร์ ในสภาพแวดล้อมนี้บทบาทขององค์กรออกใบรับรองอาจเปลี่ยนจากการออกใบรับรองตัวบุคคลไปสู่การออกใบรับรองสิทธิหรืออำนาจหน้าที่แทน(Authority certificate) เช่น การออกใบรับรองว่าผู้สั่งซื้อสินค้าเป็นเจ้าหน้าที่ซึ่งมีอำนาจในการสั่งซื้อจริง

---

[34] เรื่องเดียวกัน : 26.

3.3.3 ข้อจำกัดในการระบุตัวบุคคลด้วยใบรับรองดิจิตอล

แม้ว่าการใช้ใบรับรองดิจิตอลจะช่วยแก้ปัญหาความปลอดภัยในการทำธุรกรรมทางการพาณิชย์ทรอนิกส์ได้ในระดับหนึ่งจากการช่วยให้ฝ่ายต่าง ๆ สามารถระบุตัวบุคคลอื่นที่ติดต่อด้วยได้ก็ตาม

(1) วิธีการตรวจสอบและออกใบรับรอง ในปัจจุบันยังมีข้อจำกัดที่สำคัญหลายประการคือ[35]

- การระบุตัวบุคคลด้วยใบรับรองดิจิตอลยึดหลักในการระบุตัวบุคคลกุญแจลับซึ่งเป็นสิ่งที่บุคคลนั้นมีในครอบครอง ในทางปฏิบัติผู้ครอบครองกุญแจลับอาจไม่ใช่เจ้าของใบรับรองนั้นก็ได้ ซึ่งแตกต่างจากการระบุตัวบุคคลด้วยลักษณะทางชีวภาพ(Biometrics)
- ใบรับรองตามมาตรฐาน X.509v3 ซึ่งเป็นมาตรฐานหลัก ไม่มีข้อมูลที่เพียงพอในการระบุตัวบุคคลในบางสถานการณ์ เช่น ไม่ระบุอายุหรือเพศของผู้ถือใบรับรอง ซึ่งอาจจำเป็นต้องใช้ในเว็บไซต์บางแห่ง เช่น เว็บไซต์ที่ให้บริการ เฉพาะผู้ที่อายุเกิน 20 ปีขึ้นไป หรือเว็บไซต์ที่ให้บริการเฉพาะผู้หญิง
- ในการใช้ใบรับรองตามมาตรฐาน X.509v3 ผู้ถือใบรับรองไม่สามารถเลือกเปิดเผยข้อมูลบางส่วนในใบรับรองได้แต่ต้องเปิดเผยทั้งหมด ทั้งที่ในบางสถานการณ์ข้อมูลอื่นในใบรับรองอาจไม่เกี่ยวข้องในการใช้เลยก็ตาม เช่น ในการใช้เว็บไซต์ที่จำกัดเพียงอายุของผู้ใช้ ผู้ใช้อาจไม่ต้องการเปิดเผยชื่อที่อยู่
- การตรวจสอบหลักฐานว่าบุคคลนั้นเป็นบุคคลตามที่กล่าวอ้างหรือไม่นั้น มักใช้วิธีง่าย ๆ เพื่อประหยัดต้นทุนในการตรวจสอบ ทำให้ผู้ใช้ใบรับรองในการระบุตัวผู้อื่นไม่มีความมั่นใจอย่างเต็มที่
- การออกใบรับรองตัวบุคคลในการพาณิชย์อิเล็กทรอนิกส์ระหว่างธุรกิจกับผู้บริโภคส่วนใหญ่ยังเป็นการออกใบรับรองให้แก่เฉพาะธุรกิจ หรือรับรองเครื่องแม่ข่ายแบบ SSL ซึ่งทำให้ผู้บริโภคสามารถระบุตัวผู้ขายได้ แต่ผู้ขายยังไม่สามารถระบุตัวผู้ซื้อได้ ทั้งนี้เนื่องจากผู้ซื้อยังไม่มีแรงจูงใจในการขอใบรับรองดังกล่าว

---

[35] เรื่องเดียวกัน : 30.

ข้อจำกัดเหล่านี้บางข้อเป็นเพียงข้อจำกัดที่เกิดจากมาตรฐาน หรือวิธีการในการออกใบรับรองในปัจจุบัน ในขณะที่บางข้อเป็นข้อจำกัดที่แท้จริงของเทคโนโลยีใบรับรองดิจิตอล เทคโนโลยีและวิธีการในการระบุตัวบุคคลที่ใช้ในการพาณิชย์อิเล็กทรอนิกส์ในอนาคตจึงอาจแตกต่างจากเทคโนโลยีและวิธีการที่ใช้ในปัจจุบันเป็นอย่างมาก ซึ่งผู้กำหนดนโยบายหรือผู้ยกร่างกฎหมายที่เกี่ยวข้องจะต้องพิจารณาถึงพัฒนาการดังกล่าวด้วย

3.4 ระบบ SET (Secure Electronic Transaction)

ระบบ SET หรือ Secure Electronic Transaction นั้นเป็นระบบที่ใช้ในการจับจ่ายใช้สอยเงินโดยใช้บัตรเป็นสื่อผ่านระบบเครือข่ายคอมพิวเตอร์ และเป็นระบบที่ได้รับการพัฒนาขึ้นมาโดยความร่วมมือกันระหว่างบริษัท วีซ่าการ์ด(Visa Card) และบริษัทมาสเตอร์การ์ด(Master Card) การที่บริษัทยักษ์ใหญ่ทั้งสองบริษัทกำหนดมาตรฐานของระบบการจับจ่ายใช้สอยที่เรียกว่า SET ขึ้นมานั้นมีผลกระทบอย่างมากมายมหาศาลต่อวงการธุรกิจในระดับโลกที่เกี่ยวข้องกับการใช้บัตรต่าง ๆ เป็นสื่อในการจ่ายเงินแทนเงินสดไม่ว่าจะเป็นบัตรเครดิต บัตรเงินสด บัตรสมาร์ทการ์ด หรือบัตรชนิดอื่น ๆ ทั้งนี้เหตุผลประการสำคัญที่มาตรฐาน SET นี้จะมีผลกระทบสำคัญต่อวงการนี้คือบริษัททั้งสองครอบครองส่วนแบ่งในตลาดโลกไว้ทั้งสิ้นประมาณ 75% โดยที่บริษัทวีซ่าการ์ดมีส่วนแบ่ง 50% และบริษัทมาสเตอร์การ์ดมีส่วนแบ่ง 25% โดยประมาณ ดังนั้นธนาคารและสถาบันการเงินต่าง ๆ ที่ต้องการให้บริการทางการเงินแก่ลูกค้าของตนโดยใช้บัตรต่าง ๆ เป็นสื่อนั้นจะต้องหันมาพิจารณาอย่างจริงจัง และเตรียมพร้อมไว้อย่างดี สำหรับระบบ SET ที่จะเข้ามามีบทบาทสำคัญยิ่งต่อมาตรฐานของสื่ออิเล็กทรอนิกส์ในระบบการเงินของโลก[36]

ในการทำธุรกิจพาณิชย์อิเล็กทรอนิกส์นี้จะประสบความสำเร็จได้ก็ต่อเมื่อผู้ใช้สื่ออิเล็กทรอนิกส์มีความมั่นใจว่าระบบและมาตรฐานการจ่ายเงินนั้น ๆ จะสามารถรักษาความปลอดภัยของข้อมูลทางด้านการเงินได้เป็นอย่างดี เช่น หมายเลขบัตรเครดิตของผู้ซื้อจะต้องได้รับการปกป้องไม่ให้รั่วไหลได้เลย และอีกทั้งจำนวนเงินที่ร้านค้าจะสามารถถอนและโอนจากบัญชีของลูกค้านั้นจะต้องเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาตไม่ได้(Integrity) อีกประการหนึ่งที่สำคัญก็คือในระหว่างการทำธุรกิจพาณิชย์ในขณะนั้นๆ ระบบที่ใช้อยู่จะต้องสามารถบ่งบอกชี้ชัดได้ว่าใครคือลูกค้า และใครคือร้านค้าที่เกี่ยวข้องโดยไม่มีใครปลอมแปลงเข้ามาในระบบได้(Authenicity)

ระบบ SET นี้ถูกออกแบบมาเพื่อใช้กับลักษณะของกิจกรรมการทำพาณิชย์อิเล็กทรอนิกส์โดยระบบนี้จะสามารถรักษาความลับของข้อมูลข่าวสารที่ถูกส่งผ่านระบบเครือข่ายคอมพิวเตอร์ได้

---

[36] Baurn, Ford, Warwick, Michael S., **Secure Electronic Commerce**. Chicago : Prentice-Hall, 1997 : 34.

เป็นอย่างดี และยังสามารถรับประกันความถูกต้องโดยไม่มีการปลอมแปลงของข้อมูลที่เกี่ยวกับการเบิกจ่ายเงินได้เป็นอย่างดี และอีกประการหนึ่งที่สำคัญก็คือระบบ SET นี้สามารถที่จะบ่งบอกชี้ชัดได้ว่าใครเป็นผู้ซื้อและผู้ค้าได้อย่างถูกต้อง โดยไม่มีการปลอมแปลง

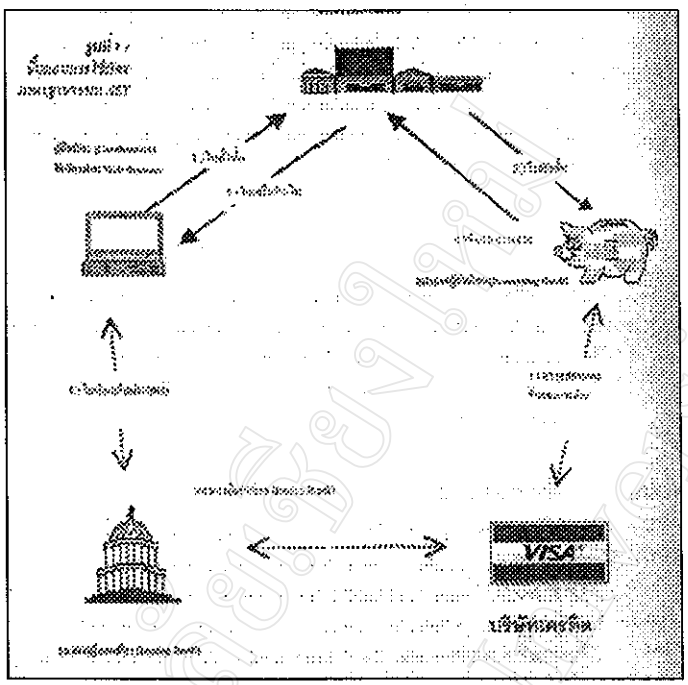
3.4.1 การทำงานของระบบ SET(Secure Electronic Transaction)

ก่อนที่ผู้ใช้จะสามารถเข้าร่วมกิจกรรมทางพาณิชย์อิเล็กทรอนิกส์ได้นั้น ก่อนอื่นจะต้องเข้าเป็นส่วนหนึ่งของระบบก่อนโดยการเป็นสมาชิกบัตรเครดิตต่าง ๆ ที่สามารถรับระบบ SET ได้ ขั้นตอนในการออกบัตรให้แก่ผู้ใช้บัตร(Cardholders) ของระบบ SET มีดังนี้คือ

(1) ลูกค้าเปิดบัญชีกับธนาคาร(Issuing Bank) ที่ให้บริการทางด้านบัตรเครดิต เช่น Visa Card หรือ Master Card และทางธนาคารได้ออกบัตรให้ลูกค้า ดังนั้นลูกค้าของธนาคารนั้นจะเป็นผู้ถือบัตร(Cardholders)

(2) ผู้ถือบัตรจะได้รับการรับรองทางอิเล็กทรอนิกส์(Digital Certificate) โดยในการรับรองนั้นผู้ใช้จะได้กุญแจเข้ารหัสสาธารณะ(Public Key) ซึ่งจะมีอายุการใช้งานในระยะเวลาหนึ่ง และกุญแจนี้ธนาคารจะเซ็นลายเซ็นทางอิเล็กทรอนิกส์(Digitally Signed)ไว้ด้วยเพื่อป้องกันการปลอมแปลงกุญแจนี้

(3) ร้านค้า(Merchants) ที่อยู่ในระบบนี้ ก็จะได้การรับรองทางอิเล็กทรอนิกส์(Digital Certificate) จากทางธนาคารด้วยเช่นกัน โดยจะได้รับกุญแจทั่วไป (Public Key) ของร้านค้าเองและของธนาคารด้วย



ภาพที่ 14 แสดงระบบการทำงานของ SET[37]

จากระบบการใช้กุญแจเข้ารหัสดังที่กล่าวมาแล้วนี้ SET ได้นำระบบใหม่ที่มีประโยชน์ในทางปฏิบัติอย่างยิ่งต่อการซื้อขายบนอินเตอร์เน็ต ระบบนี้เรียกว่าระบบสองลายเซ็น(Dual Signatures) เทคโนโลยีใหม่นี้จะสามารถทำให้ธนาคารที่ทำการจ่ายโอน(Processing Bank) สามารถทำการพิสูจน์ผู้ซื้อและผู้ขายได้ว่าถูกต้อง ก่อนที่จะอนุญาตให้ทำการเบิกโอนเงินผ่านระบบเครือข่ายคอมพิวเตอร์ โดยที่ทางธนาคารนั้นจะรู้ได้ว่าผู้ซื้อและร้านค้านั้นเป็นผู้ที่ได้รับอนุญาตจากทางธนาคารจริงหรือไม่ และได้ทำการติดต่อซื้อขายกันจริงหรือไม่ อีกทั้งระบบ SET นี้ยังสามารถเก็บความลับระหว่างทั้งสามฝ่ายที่เกี่ยวข้องกับการซื้อขายนี้ได้ด้วย โดยที่ผู้ค้าจะไม่มีทางรู้ข้อมูลเกี่ยวกับการเงินของลูกค้าได้เลย เช่น หมายเลขบัญชี หรือหมายเลขบัตรเครดิต มีเพียงแต่ธนาคารที่เกี่ยวข้องเท่านั้นที่จะสามารถเข้ามาอ่านข้อมูลนี้ได้ ในขณะเดียวกันทางธนาคารผู้เบิกจ่ายก็ไม่อาจรู้รายละเอียดเกี่ยวกับสินค้าหรือการซื้อขายได้ เพียงแต่จะทำหน้าที่พิสูจน์และเบิกโอนเงินเท่านั้น ซึ่งลักษณะเช่นนี้ไม่ค่อยจะปรากฏในระบบอื่น ๆ ที่ใช้อยู่ในปัจจุบัน และนับว่าเป็นจุดที่ดีมากของระบบ SET

---

[37] ณรงค์ชัย นมิตบุญอนันต์. **Computer Security for E-Commerce**. กรุงเทพ : บริษัทซีเอ็ดยูเคชั่น จำกัด (มหาชน), 1999 : 208.

จากภาพที่ 14 ขั้นตอนในการใช้บัตรมาตรฐานระบบ SET ในการใช้จ่ายอินเตอร์เน็ตมีดังนี้คือ

(1) ผู้ถือบัตรสั่งซื้อสินค้าผ่านทางอินเตอร์เน็ตโดยใช้ Web Browser ตัว Web Browser นี้จะรับข้อมูลเกี่ยวกับการรับรองทางอิเล็กทรอนิกส์(Digital Certificate) จากร้านค้าและทำการพิสูจน์ว่าเป็นร้านค้าที่ได้รับอนุญาตจริงหรือไม่ เมื่อทำการพิสูจน์เสร็จสิ้นแล้วก็จะส่งไปสั่งซื้อผ่านทางระบบอินเตอร์เน็ตโดยใช้วิธีการเข้ารหัสข้อมูล

(2) ร้านค้าจะได้รับคำสั่งซื้อ และจะทำการพิสูจน์การรับรองทางอิเล็กทรอนิกส์ว่าเป็นผู้ซื้อที่ได้รับอนุญาตอย่างถูกต้องในระบบหรือเปล่า จากนั้นก็จะส่งข้อมูลต่อไปยังธนาคารที่เบิกจ่าย(Processing Bank) การส่งข้อมูลไปยังธนาคารนี้ก็จะใช้วิธีการเข้ารหัสข้อมูลเช่นกันเพื่อความปลอดภัยของข้อมูล

(3) ธนาคารที่ทำการเบิกโอน(Processing Bank) จะทำการพิสูจน์การซื้อขายนั้น ๆ โดยการใช้วิธีสองลายเซ็น(Dual Signatures) ดังที่ได้กล่าวมาแล้วข้างต้น และจะทำการตรวจสอบบัญชีของผู้ถือบัตรผ่านทางบริษัทเครดิตและทางธนาคารผู้ออกบัตร(Issuing Bank) และจะทำการรับรองการซื้อขายนั้น ๆ หากผู้ถือบัตรยังมีสิทธิ์ที่จะใช้บัญชีของตนได้อยู่

(4) ธนาคารที่ทำการเบิกโอนจะทำการรับรองการจ่ายเงินและส่งไปยังร้านค้า โดยใช้วิธีการเข้ารหัสข้อมูลก่อนส่งข้อมูลออกไปเพื่อความปลอดภัย

(5) ร้านค้าจะส่งใบเสร็จรับเงินกลับไปยังผู้ถือบัตร

(6) ทางธนาคารผู้ออกบัตรจะเรียกเก็บเงินจากผู้ถือบัตรเองโดยตรง

3.4.2 ระบบรักษาความปลอดภัยของ SET

ระบบมาตรฐาน SET นั้น ใช้วิธีการเข้ารหัสข้อมูลแบบใช้กุญแจหลายตัว (Asymmetric Key Encryption Algorithms) เพื่อทำการเซ็นลายเซ็นทางอิเล็กทรอนิกส์ และใช้ในการเข้ารหัสปกป้องกุญแจความลับแบบ Digital Envelope ระบบการเข้ารหัสที่ใช้เป็นหลักในการปกป้องข้อมูลนี้คือระบบที่เรียกว่า TSA public-key algorithm ซึ่งขนาดของกุญแจที่ใช้ในการเข้ารหัสนั้นจะมีผลต่อระดับความปลอดภัยของข้อมูล คือขนาดของกุญแจยิ่งใหญ่ก็ยิ่งมีความปลอดภัยสูง ขนาดของกุญแจเข้ารหัสที่ใช้ในส่วนต่าง ๆ ในระบบ SET มีขนาดใหญ่ถึง 1024 บิต ซึ่งสามารถให้ความปลอดภัยได้อย่างสูงมาก แต่เพื่อความปลอดภัยสูงสุดระบบ SET ใช้ขนาดของกุญแจถึง 2048 บิต เพื่อใช้ในการรับรองทางอิเล็กทรอนิกส์ชั้นสูงสุด (Root Certificate-CA) จากการศึกษาของบรรดานักวิจัยพบว่าระบบ RSA public-key algorithm นี้สามารถให้ความปลอดภัยได้อย่างเพียงพอในการทำกิจกรรมทางด้านพาณิชย์

อิเล็กทรอนิกส์ แต่ในการนำไปใช้นั้นจะต้องมีการอุดรอยรั่วและจุดอ่อนของระบบให้ดีเสียก่อน[38]

ระบบการเข้ารหัสข้อมูลอีกชนิดหนึ่งที่เป็นแบบใช้กุญแจเข้ารหัสตัวเดียวหรือที่เรียกว่า Symmetric-Key Encryption Algorithm นั้น ตัวที่ใช้เป็นหลักในการปกป้องความลับของข้อมูลคือระบบ Data Encryption Standard (DES) และขนาดของกุญแจที่ใช้ในการเข้ารหัสและถอดรหัสนี้มีขนาดถึง 56 บิต ในความเป็นจริงแล้วมีผลงานวิจัยหลายชิ้นบ่งชี้ว่าขนาดของกุญแจน่าจะมีขนาดประมาณ 70-75 บิต จึงจะสามารถปกป้องข้อมูลได้อย่างมีความมั่นใจสูงสุด แต่อย่างไรก็ตามขนาดของกุญแจ 56 บิต นี้ก็สามารถให้ความปลอดภัยได้อย่างเพียงพอในระดับหนึ่ง อย่างไรก็ตามภาพรวมของระบบ SET นี้ ดูมีความสามารถอย่างเพียงพอในการรักษาความปลอดภัยของข้อมูลในระบบพาณิชย์อิเล็กทรอนิกส์ในปัจจุบันและอนาคตอันใกล้ แต่หากในระยะยาวแล้วนั้นยังจะต้องมีการเพิ่มขีดความสามารถในการรักษาความปลอดภัยของข้อมูลให้สูงขึ้นไปอีก เพื่อความปลอดภัยแและความมั่นใจสูงสุดของผู้ใช้ระบบ SET นี้

ข้อเท็จจริงที่สำคัญอีกประการหนึ่งของเทคโนโลยีที่ต่าง ๆ ใช้ในการรักษาความปลอดภัยของข้อมูลก็คือไม่มีเทคโนโลยีใดในโลกที่สามารถรับประกันความปลอดภัยได้เต็มที่ 100 เปอร์เซ็นต์ เนื่องจากว่าระดับความปลอดภัยของเทคโนโลยีแต่ละชนิดนั้นขึ้นอยู่กับความก้าวหน้าของเทคโนโลยีทางด้านอื่น ๆ ด้วยเช่นความเร็วของคอมพิวเตอร์ หรือความก้าวหน้าในการพัฒนาเทคนิคใหม่ ๆ ที่นำมาใช้ในการค้นหากุญแจความลับ(Cryptanalysis) และในทางทฤษฎีแล้วนั้น ถ้าหากมีเวลาและทรัพยากรที่ใช้ในการคำนวณมากพอที่จะสามารถค้นหากุญแจเข้ารหัสได้ ดังนั้นสิ่งที่สำคัญที่สุดสำหรับผู้บริหารในการเลือกใช้ระบบรักษาความปลอดภัยที่นำมาใช้รักษาความปลอดภัยบนระบบพาณิชย์อิเล็กทรอนิกส์นั้นอยู่ที่ว่าระดับความปลอดภัยขนาดไหนจึงจะเป็นจุดที่คุ้มค่าแก่การลงทุน

---

[38] ธีรา ทานตวณิช. "Web Security ขั้นตอนการสร้างความปลอดภัยสำหรับ E-Commerce". **Microcomputer.** (เมษายน 2000) : 83.

3.4.3 การนำระบบ SET มาใช้งานอย่างมีประสิทธิภาพ

เนื่องจากว่าระบบ SET นี้มีความปลอดภัยสูงกว่า แต่ต้องการความสามารถในการคำนวณมากกว่าด้วย ดังนั้นหากนำระบบ SET มาใช้โดยไม่มีการปรับปรุงระบบเลยก็อาจทำให้เกิดความล่าช้าในการบริการลูกค้าในระหว่างการทำกิจกรรมทางด้านพาณิชย์อิเล็กทรอนิกส์นี้ ซึ่งอาจเป็นผลร้ายอย่างยิ่งในเชิงพาณิชย์

จากการวิจัยของบริษัทที่ปรึกษาที่มีชื่อเสียงของโลก(Gartner Group) พบว่ามีเทคโนโลยีใหม่ที่อาจนำมาใช้ร่วมกับระบบ SET เพื่อที่จะทำให้ระบบมีขีดความสามารถในการบริการลูกค้าได้เร็วขึ้น นั่นก็คือ[39]

(1) Symmetric Multiprocessing(SMP) CPU scaling ซึ่งเป็นระบบที่ใช้ CPU แต่ละตัวในการทำหน้าที่ใดหน้าที่หนึ่งโดยเฉพาะ

(2) Clustering เป็นการกระจายการทำงาน(Transaction Loading) ไปสู่ระบบย่อย ๆ หลายระบบเพื่อเป็นการแบ่งเบาภาระ

(3) Cryptographic Accelerators เป็นการใช้ฮาร์ดแวร์เฉพาะทางในการทำการเข้ารหัสลับ

(4) Elliptical Curve Cryptography(ECC) เป็นวิธีการเข้ารหัสที่ใช้ขนาดของกุญแจเล็กลง แต่ก็ยังให้ความปลอดภัยในระดับที่สูงเท่าเดิม ส่งผลให้ลดปริมาณการทำงานของระบบลงได้

---

[39] ธีรา ทานตวณิช. "Web Security ขั้นตอนการสร้างความปลอดภัยสำหรับ E-Commerce". **Microcomputer.** (เมษายน 2000) : 126.

3.5 ระบบ SSL (Secure Socket Layer)

ในปัจจุบันนี้ระบบที่ใช้กันอยู่ทั่วไปมีอยู่สองระบบคือ ระบบ Secure Socket Layer (SSL) และระบบ Secure Electronic Transaction (SET) โดยทั่วไปแล้วระบบ SET จะให้ความปลอดภัยที่สูงกว่าแต่ในทางกลับกันระบบ SET จะช้ากว่าระบบ SSL พิจารณาข้อดีข้อเสียของระบบ SET และ SSL ตามตารางที่ 6-7

ตารางที่ 6 แสดงข้อดีข้อเสียของระบบ SET[40]

ข้อดี	ข้อเสีย
1.) ใช้วิธีการเข้ารหัสลับที่ดีกว่าจึงให้ความปลอดภัยที่สูงกว่า	1.) ระบบ SET ยังอยู่ในระหว่างการพัฒนาและใกล้จะเสร็จสมบูรณ์แล้ว
2.) ร้านค้าสามารถพิสูจน์ทราบลูกค้าได้ทันทีว่าเป็นผู้ที่ได้รับอนุญาตในระบบหรือไม่ และเป็นผู้ที่มีเครดิตเพียงพอในการซื้อหรือไม่	2.) ยังไม่มีการทดสอบ และทดลองใช้อย่างเพียงพอ
3.) สามารถปกปิดความลับ หรือข้อมูลการทำธุรกิจของลูกค้าจากร้านค้า และจากธนาคารผู้ออกบัตรได้	3.) ยังไม่มีการนำไปใช้เชิงธุรกิจในวงกว้างมากนัก

ตารางที่ 7 แสดงข้อดีข้อเสียของระบบ SSL[41]

ข้อดี	ข้อเสีย
1.) มีการลงทุนน้อย หรือแทบไม่มีเลย เนื่องจากปัจจุบันเป็นระบบที่ใช้ในวงกว้าง	1.) ใช้วิธีการเข้ารหัสที่ล้าสมัย และใช้กุญแจเข้ารหัสที่มีขนาดเล็ก ดังนั้นความปลอดภัยอาจไม่เพียงพอ
2.) สามารถควบคุมการเข้าถึงข้อมูลส่วนต่างๆ ภายในระบบของผู้ใช้ได้หลังจากที่ผู้ใช้ได้รับอนุญาตให้เข้ามาในระบบ	2.) ทำการสื่อสารอย่างปลอดภัยได้เพียงสองจุดในแต่ละครั้ง แต่ในระบบพาณิชย์อิเล็กทรอนิกส์ที่ใช้บัตรเป็นสื่อนั้นต้องใช้มากกว่าสองจุดในเวลาเดียวกัน
3.) สามารถใช้ข้อมูลร่วมกันได้ ระหว่างสองจุด (Share Information)	3.) มีความเสี่ยงสูงเนื่องจากไม่มีการรับรองทางอิเล็กทรอนิกส์ระหว่างทุกฝ่ายที่ทำการซื้อขายในขณะนั้น ดังนั้นจึงอาจมีการปลอมแปลงเข้ามาในระบบได้
4.) มีระบบในการปกป้อง และตรวจสอบความถูกต้องของข้อมูลได้	4.) มีความเสี่ยงในการรั่วไหล ของข้อมูลที่สำคัญของลูกค้า เช่น หมายเลขบัตรเครดิต เนื่องจากร้านค้าสามารถเห็นข้อมูลเหล่านี้ได้

---

[40] ณรงค์ชัย นมิตบุญอนันต์. **Computer Security for E-Commerce.** กรุงเทพ : บริษัทซีเอ็ดยูเคชั่น จำกัด (มหาชน), 1999 : 211.

[41] เรื่องเดียวกัน : 212.