ศัพท์ต่าง ๆ ที่เกี่ยวข้องกับการเข้าและถอดรหัส

1. **Plain Text** หมายถึง ข้อความหรือข้อมูลต่าง ๆ ที่ยังไม่ผ่านกรรมวิธีการเข้ารหัส

2. **Cipher Text** หมายถึง ข้อความ หรือข้อมูลต่าง ๆที่ผ่านการเข้ารหัสแล้ว และทำให้รูปแบบของข้อมูลเปลี่ยนแปลงไป

3. **Algorithm** หมายถึง แนวความคิดหรือลำดับความคิดที่มี รูปแบบที่สามารถนำไปประมวลผลทางคอมพิวเตอร์ได้โดยง่าย

4. **Encryption** หมายถึง กระบวนการหรือขั้นตอนในการเข้ารหัสข้อมูล ที่เปลี่ยนแปลงไปจากเดิม

5. **Decryption** หมายถึง กระบวนการหรือขั้นตอนในการถอดรหัสข้อมูล เพื่อให้ข้อมูลที่เข้ารหัสไว้คืนสู่สภาพเดิมก่อนเข้ารหัส

6. **Cryptography** หมายถึง ระบบการรักษาความปลอดภัยที่ประกอบด้วย **Encryption** และ **Decryption**

ระบบคีย์ (Keys System)

คีย์ (Keys) คือข้อมูลอีกชุดหนึ่ง นอกเหนือจากข้อมูลต้นฉบับ (Plain Text) ซึ่งผู้ทำการเข้ารหัสหรือถอดรหัสเป็นผู้สร้างขึ้นและนำมาใช้ร่วมกับ Algorithm เพื่อรักษาความปลอดภัยให้กับระบบ คีย์เป็นสิ่งที่เป็นความลับอย่างที่สุดของแต่ละบุคคลเพราะ Algorithm ถูกออกแบบมาเพื่อใช้คีย์ในการเข้าหรือถอดรหัสข้อมูล

1. Prime Number

เทคโนโลยีการเข้ารหัสโดยใช้ฟังก์ชันทางคณิตศาสตร์ โดยนำตัวเลข Prime Number (จำนวนเฉพาะ) ได้แก่ 2, 3, 5, 7 และ 11 เป็นต้น เมื่อนำ Primeสองจำนวนมาคูณกัน จะได้เลขที่ถูกหารด้วย ตัวใดตัวหนึ่ง เช่น 5 x 7 = 35 เราสามารถหาค่าของPrime Number ได้คือ 5 และ 7 เป็นต้น

การเข้ารหัสที่ใช้ผลคูณของ **Prime Number** ที่เป็นเลขจำนวนมาก ๆ นั้นคอมพิวเตอร์สามารถสร้างเลขได้ง่ายและรวดเร็วโดยสร้างคีย์คู่หนึ่งที่เป็นเลขไม่ซ้ำกัน คีย์เข้ารหัสจะเป็นการสร้างแบบสาธารณะ **(Public, Public Key)** โดยไม่ความเสี่ยงใด ๆ เนื่องจากการถอดรหัสทำได้ยากมากยกเว้นแต่จะมีรหัสในการถอดเท่านั้น

2. RSA

(R = Rivest, S = Shamir และ A = Adelman เป็นรหัสที่ตั้งตามนามสกุลของทุกคน)

ในปี ค.ศ. 1993 นักวิชาการกว่า 600 สถาบัน และนักวิชาการสมัครเล่นทั่วโลกพยายามที่จะถอดรหัสจาก RSA 129 ร่วมกัน ซึ่งสามารถทำได้สำเร็จในเวลาไม่ถึงหนึ่งปี โดยถอดรหัสเป็นเลข Prime Number สองตัวสำเร็จ ตัวหนึ่งมี 64 หลักและอีกตัวหนึ่งมี 65 หลัก นั่นคือ คีย์สาธารณะระบบ 129 หลัก ไม่เพียงพอที่จะเข้ารหัสข้อมูลที่สำคัญ ๆ ได้

3. คีย์ส่วนบุคคลหรือคีย์เดี่ยว (Private Keys หรือ Symmetric Keys)

ผู้ส่งจะทำการเข้ารหัสข้อมูลด้วยคีย์ตัวใดตัวหนึ่งที่กำหนดขึ้นเมื่อผู้รับได้รับข้อมูลก็จะต้องถอดรหัสข้อมูล โดยใช้คีย์ที่ส่งมาจากผู้ส่งที่ต้นทาง ซึ่งเป็นคีย์เดียวกันกับที่ใช้ในการเข้ารหัส ดังนั้นถ้ามีการดักจับคีย์ที่ผู้ส่งต้องส่งให้กับในผู้รับ ก็จะให้ข้อมูลไม่เป็นความลับอีกต่อไป

4. คีย์สาธารณะ (Public Keys หรือ Asymmetric Key)

ระบบนี้ออกแบบมาเพื่อแก้ปัญหาของคีย์ส่วนบุคคล เพราะจะไม่มีการส่งคีย์กับใครทั้งสิ้น ระบบคีบ์นี้ได้ออกแบบให้แต่ละคนมีคีย์ 1 คู่ ประกอบด้วย Public Keys และ Private Keys โดย Public Keys นั้นใครจะรู้ก็ได้ แต่ Private Keys จะต้องรักษาเป็นความลับ ผู้ส่งจะเข้ารหัสข้อมูลต้นฉบับด้วยคีย์สาธารณะ (Public Keys) จากนั้นผู้รับจะใช้คีย์ของตนเอง (Private Keys) ในการถอดรหัสให้ได้ข้อมูลต้นฉบับเดิมอีกครั้งหนึ่ง

SSL หมายถึง Protocol ที่ได้รับการพัฒนาให้เป็น Secure Protocol คือมีความสามารถทั้ง Encryption และ Decryption

Protocol ที่คล้ายกับ SSL มากที่สุด คือ SHTTP (Secure Hyper Text Transfer Protocol) ซึ่งนำเอาระบบคีย์สาธารณะมาใช้

การประยุกต์การเข้ารหัสกับการพัฒนาโปรแกรม ประยุกต์ SSLและ HTTPS

การนำ SSL มาใช้รักษาความปลอดภัยของข้อมูลในการค้าอิเล็กทรอนิกส์ ซึ่งติดต่อสื่อสารกันระหว่าง Web Browser กับ Web Server นั้น ทาง Server จะต้องทำการติดตั้งและให้บริการ SSL ก่อนส่วน Browser ของผู้ซื้อจะใช้โปรโตคอล HTTPS เช่น https://bucc3.buu.ac.th/

การทำงานของ SSL

การทำงานของ SSL นั้น เป็นโปรโตคอลที่ให้ความปลอดภัยในการสื่อสารที่เป็นการเชื่อมโยงระดับ TCP/IP จะใช้โดย IIS ในการจัดตั้ง Secure Connection ระหว่าง Client กับ Server ในเรื่องนี้เราเรียกว่า Server Certificate

Secure Sockets Layer (SSL)

SSL คิดค้นขึ้นมาโดยบริษัท Netscape

จุดประสงค์การทำงานของ SSL

- **เพื่อรักษาความลับของข้อมูล**
- **สามารถระบุผู้ส่งและผู้รับข้อมูลได้**

Secure Sockets Layer (SSL)

SSL ประกอบด้วย Protocol 2 ระดับ

SSL Handshake Protocol

สร้างกระบวนการรับส่งข้อมูล แลกเปลี่ยน Algorithm ในการเข้ารหัส

SSL Record Protocol

ทำหน้าที่จัดแบ่งบล็อกของข้อมูลที่ได้จาก Protocol ที่อยู่ใน ระดับเหนือขึ้นไปให้เป็น record ทำการบีบอัดข้อมูล กำหนด รหัสของข้อมูล หรือดำเนินการเข้ารหัสข้อมูล

คุณสมบัติของ SSL

การรักษาความลับของข้อมูล
การระบุตัวตนทางฝั่งเซิร์ฟเวอร์ (Server Authentication)
การระบุตัวตนทางฝั่งไคลเอนต์ (Client Authentication)
คงความแน่นอนของข้อมูล

SET (Secure Electronics Transaction)

เป็นโครงสร้างที่พัฒนาร่วมกัน โดยบริษัทเจ้าของบัตรเครดิต VISA และ Master Card เพื่อสนับสนุนการค้าแบบ Online ให้สามารถชำระเงินได้ด้วยบัตรเครดิตผ่านอินเตอร์เน็ตด้วยความปลอดภัยและมั่นใจกับการบริการ

โครงสร้างของระบบ SET

1. ผู้ออกบัตร
2. ผู้ถือบัตร
3. ผู้ประกอบการ
4. สถาบันผู้ประมวลผล
5. Payment Gateway
6. Certificate Authority

การเข้ารหัสโดยใช้กุญแจสาธารณะสามารถดำเนินการในขั้นตอนต่าง ๆ ได้ดังนี้

1. มีการเข้ารหัสในคำสั่งชำระเงิน เพื่อให้มั่นใจว่าไม่มีการเปลี่ยนแปลงระหว่างการส่งคำสั่งไป

2. ตรวจสอบความถูกต้องของผู้ถือบัตร เพื่อป้องกันการแอบอ้างและขโมยบัตรผู้อื่นมาใช้โดยมิชอบ

3. ตรวจสอบความถูกต้องของผู้ประกอบการ กันการทุจริตหลอกลวง

4. ตรวจสอบผู้ประมวลผล โดยผู้ประกอบการและผู้ถือบัตร เพื่อป้องกันการถอดรหัสสั่งซื้อจากผู้ที่ปลอมเป็นผู้ประมวลผล

5. เพื่อป้องกันผู้บุกรุกเข้ามาดักรับข้อมูลระหว่างทางในการส่งคำสั่งซื้อ

การรักษาความปลอดภัยให้กับธุรกิจอิเล็กทรอนิกส์

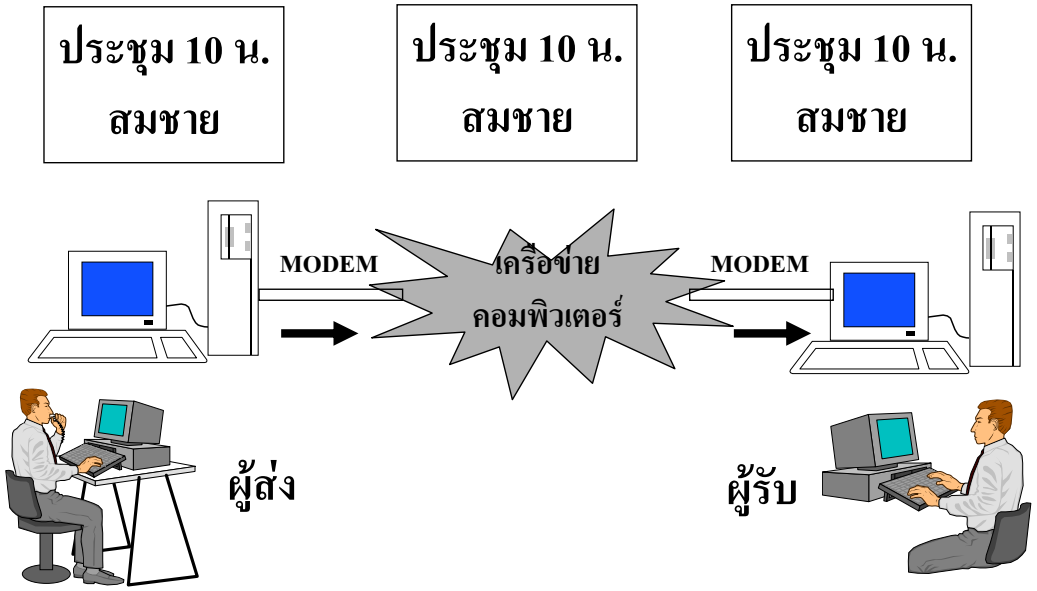
1. หลักการรักษาความปลอดภัย อาศัยหลักการของ 3A คือ

Account เป็นการสร้างและระบุตัวบุคคลในเครือข่าย

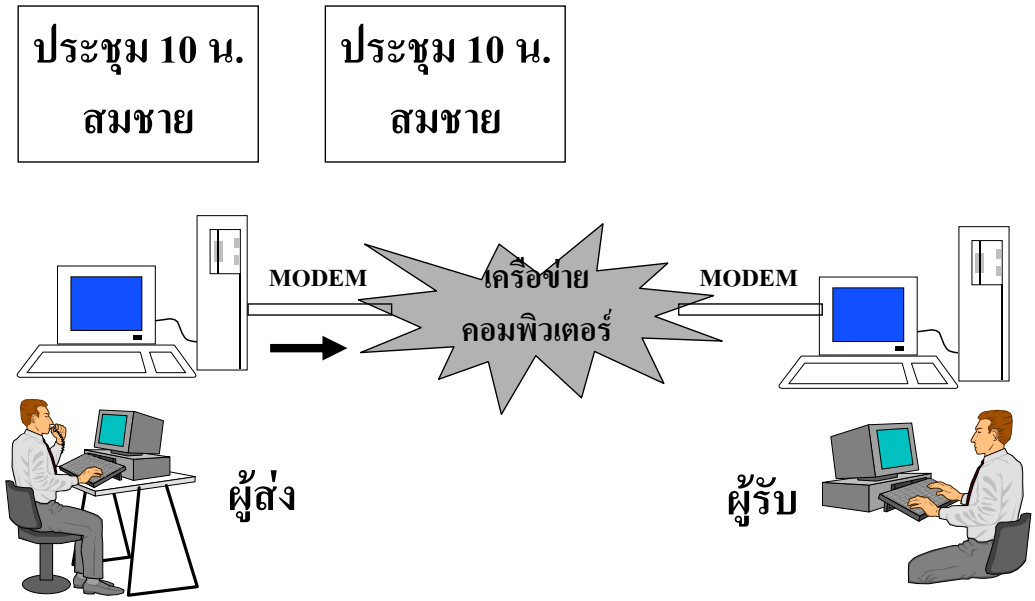
Authorization เป็นการสร้างและกำหนดสิทธิให้กับบุคคลนั้น ๆ กระทำการใด ๆ ตามสิทธิที่ได้รับ

Authenticity เป็นการพิสูจน์และยืนยันทั้งบุคคลและสิทธิที่ได้รับของบุคคลนั้น ๆ ข้อมูลจะต้องไม่ถูกแก้ไข

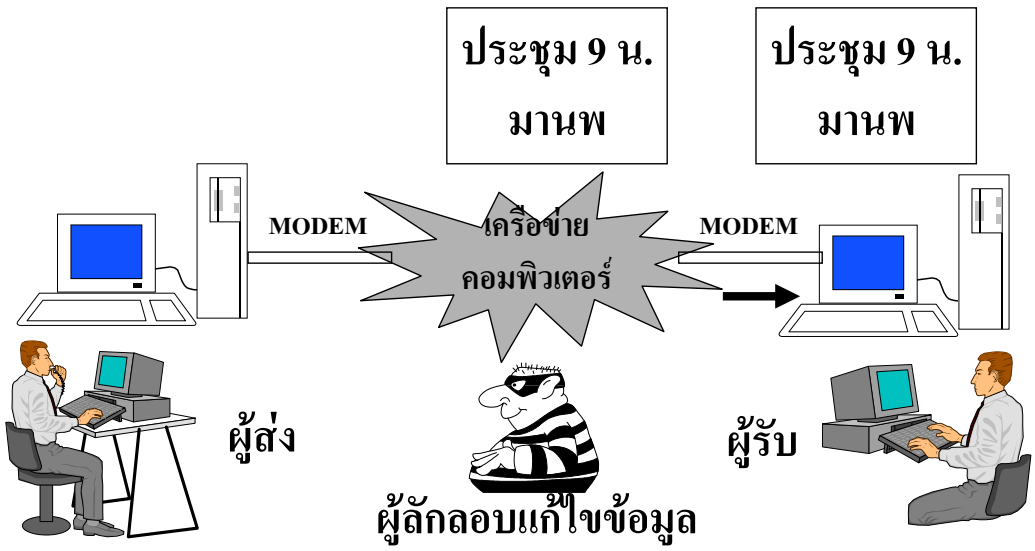
ตัวอย่างรูปแบบการสื่อสารผ่านเครือข่ายคอมพิวเตอร์



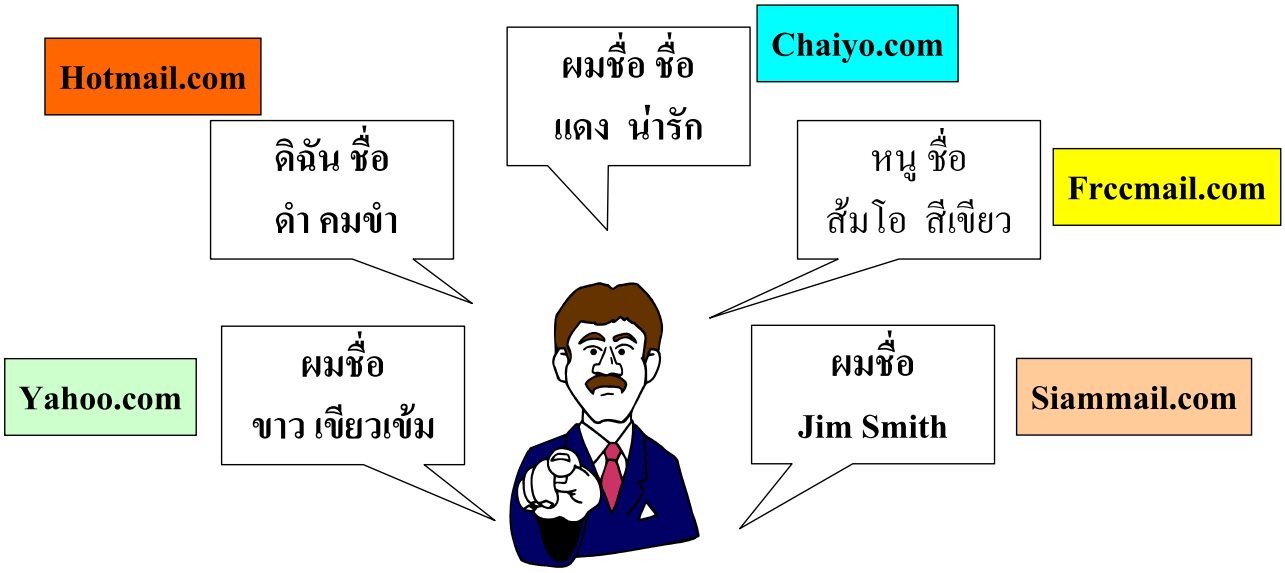
ตัวอย่างการแอบอ้างชื่อและลอบแก้ไขข้อมูล(1)



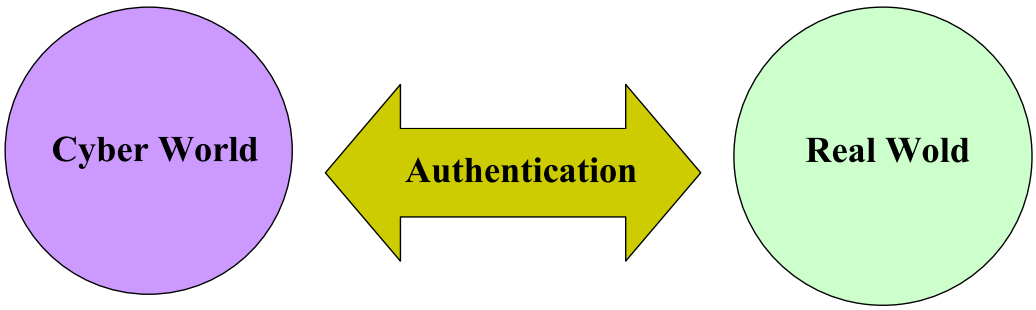
ตัวอย่างการแอบอ้างชื่อและลอกแก้ไขข้อมูล (2)



E-mail address

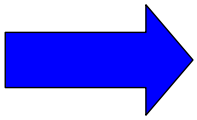


Who am I ?



ประเด็นเรื่องความปลอดภัยของข้อมูล (1)

หากท่านต้องการส่งข้อความที่ปกปิดหรือเป็นความลับผ่านเครือข่าย ท่านจะมั่นใจได้อย่างไรว่า บุคคลที่ท่านประสงค์จะส่งถึงหรือที่ได้รับอนุญาตเท่านั้น ที่อ่านข้อความได้

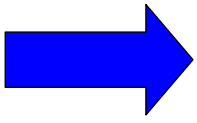


การรักษาความลับ

(Confidentiality)

ประเด็นเรื่องความปลอดภัยของข้อมูล (2)

- หากท่านได้รับข้อความที่ส่งมาถึงท่านฝ่านทางเครือข่าย ท่านจะแน่ใจได้อย่างไรว่า เป็นข้อความที่ส่งมาจากบุคคลที่อ้างว่าเป็นผู้ส่งนั้นจริง

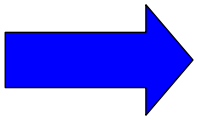


การระบุตัวบุคคล

(Authentication)

ประเด็นเรื่องความปลอดภัยของข้อมูล (3)

หากท่านได้รับข้อความที่ส่งมาถึงท่านผ่านทางเครือข่าย ท่านจะแน่ใจได้อย่างไรว่า ข้อความที่ท่านได้รับเป็นข้อความที่ถูกต้องแท้จริง ไม่ได้ถูกเปลี่ยนแปลงแก้ไขระหว่างทาง

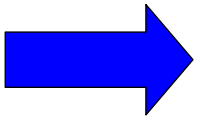


ความแท้จริงของข้อมูล

(Integrity)

ประเด็นเรื่องความปลอดภัยของข้อมูล (4)

หากท่านได้รับข้อความทางเครือข่าย เกี่ยวกับการดำเนินการอย่างใดอย่างหนึ่ง หรือเป็นข้อผูกพันทางสัญญา แต่ต่อมาผู้ส่งปฏิเสธว่าไม่ได้ส่งข้อความนั้น ท่านจะใช้อะไรอ้างอิงเพื่อไม่ให้ปฏิเสธ



การห้ามปฏิเสธความรับผิด

(Non-repudiation)

ความมั่นใจในการทำธุรกิจอิเล็กทรอนิกส์

การรักษาความลับ

(Confidentiality)

การระบุตัวบุคคล

(Authentication)

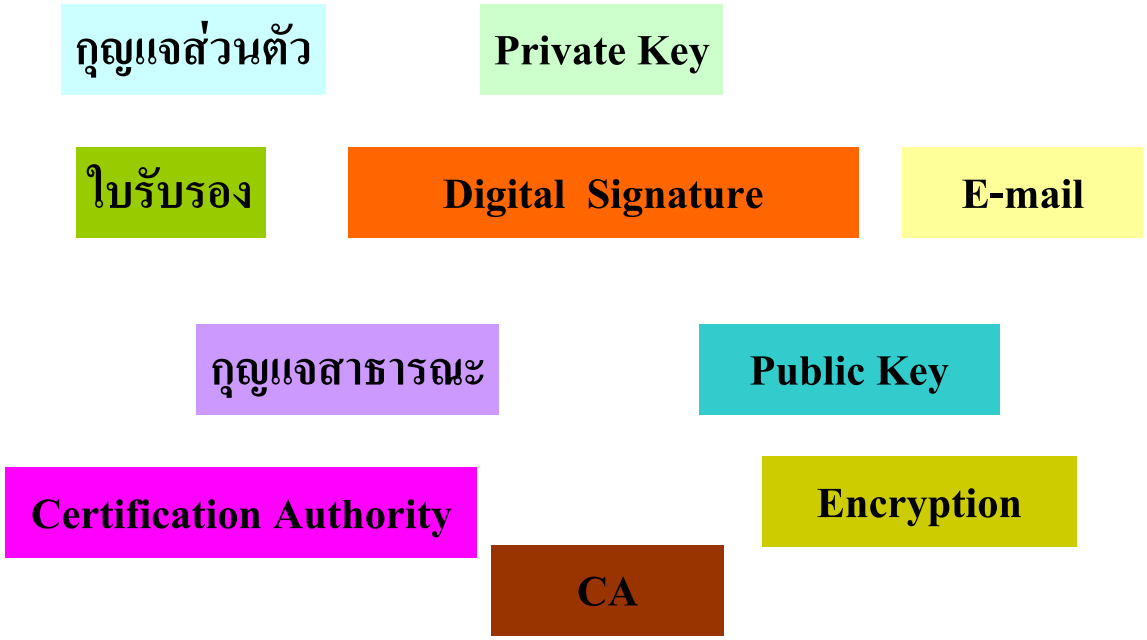
ความแท้จริง

(Integrity)

การห้ามปฏิเสธความรับผิด

(Non-repudiation)

โครงสร้างรองรับการประยุกต์ใช้งาน
ด้านการรักษาความปลอดภัยของข้อมูล



การสร้างลายมือชื่อดิจิทัล

ก.การสร้างกุญแจคู่ (Key Pairs)

- ก่อนการสร้างลายมือชื่อดิจิทัลนั้น ต้องมีการสร้างกุญแจคู่ขึ้นมาเสียก่อนด้วยกระบวนการทางคณิตศาสตร์
- เจ้าของกุญแจจะต้องเก็บกุญแจแรกที่เรียกว่า “กุญแจส่วนตัว” ไว้เป็นความลับเพื่อให้ตนเองเท่านั้นสามารถใช้กุญแจส่วนตัวได้แต่ผู้เดียว
- การเก็บรักษา “กุญแจส่วนตัว” จะบันทึกและเก็บไว้ในสมาร์ทการ์ด
- ส่วนกุญแจสาธารณะ ก็จะเปิดเผยไว้ในระบบฐานข้อมูลของผู้ประกอบการรับรอง (Certification Authority) เพื่อให้สามารถตรวจสอบตัวบุคคลได้โดยง่าย

ข.ขั้นตอนการแฮช หรือย่อย (hash function)

- เป็นขั้นตอนสำคัญในการนำข้อมูลอิเล็กทรอนิกส์ที่ผู้ส่งข้อมูลประสงค์จะส่งให้แก่ผู้รับข้อมูลนำมาคำนวณด้วยกระบวนการทางคณิตศาสตร์ (Algorithm) ที่เรียกว่า “ขั้นตอนการแฮช (Hash Function)” หรือ one-way cryptography หรือ one-way hash function
- เพื่อทำการย่อยหรือทำให้ข้อมูลอิเล็กทรอนิกส์นั้นมีขนาดเล็กลงอันจะทำให้ง่ายต่อการคำนวณทางคณิตศาสตร์และการจัดส่งให้ผู้รับข้อมูลในขั้นตอนต่อไป
- ผลลัพธ์ที่ได้จากขั้นตอนการแฮช จะทำให้ได้ข้อมูลที่ย่อย (Message Digest) ซึ่งมีขนาดเล็กลงและคงที่ (Fixed Length)

ขั้นตอนการแฮช

ข้อความก่อนการแฮช / ย่อย	ย่อย เป็น	“123234sglggkhk,vd” (ผลของการแฮชหรือย่อย)
“เรียน คุณสมหญิง ขอสั่งซื้อผลไม้ 20 กก. จาก นายสมชาย”	→	

ค.การสร้างลายมือชื่อดิจิทัล

- หลังจากนั้นก็นำกุญแจส่วนตัวมาทำการเข้ารหัสกับข้อมูลที่แฮช หรือ ย่อย (Message Disgest) ซอฟต์แวร์ก็จะทำการแปลข้อมูลอิเล็กทรอนิกส์เหล่านั้น ให้เป็นลายมือชื่อดิจิทัล (Digital Signature) และลายมือชื่อดิจิทัลนั้นก็จะมีลักษณะเฉพาะที่สัมพันธ์กับข้อมูลแฮช และกุญแจส่วนตัว กล่าวคือ ทุกครั้งที่ข้อมูลแฮชหรือกุญแจส่วนตัวเปลี่ยนแปลงไปจากเดิม ลายมือชื่อดิจิทัลที่ได้ก็จะเปลี่ยนแปลงตามไปด้วย ลายมือชื่อดิจิทัลจึงไม่มีโอกาสซ้ำกันเลย

เทคโนโลยีระบบรหัสแบบอสมมาตร (เทคโนโลยี Public Key)

- คำว่า อสมมาตร แสดงถึงความไม่เหมือนกันสองข้างซึ่งในที่นี้ คือ การใช้กุญแจต่างกัน เรียกว่ากุญแจคู่ประกอบด้วยกุญแจส่วนตัว (Private Key) และกุญแจสาธารณะ (Public Key) ในข้างผู้ส่ง และข้างผู้รับ

กุญแจเป็นข้อมูลในรูปอิเล็กทรอนิกส์ ซึ่งใช้ในการเข้ารหัสและถอดรหัส

ตัวอย่าง

00:bc:73:d4:ce:01:1b:b9:0c:00:15:c7:56

เทคโนโลยี Public Key

- กุญแจส่วนตัวต้องอยู่กับผู้เป็นเจ้าของเพียงที่เดียวและผู้เป็นเจ้าของต้องไม่ให้ผู้อื่นล่วงรู้ถึงกุญแจส่วนตัวนี้
- กุญแจสาธารณะควรจะอยู่ในที่ซึ่งบุคคลทั่วไปค้นหาได้โดยสะดวกและไม่จำเป็นต้องเก็บเป็นความลับแต่อย่างใด

ระบบรหัสแบบอสมมาตร
(เทคโนโลยี Public Key)

การรักษาความลับ

(Confidentiality)

การเข้ารหัส

(Encryption)

ลายมือชื่อดิจิทัล

(Digital Signatrue)

การระบุตัวบุคคล

(Authentication)

ความแท้จริง

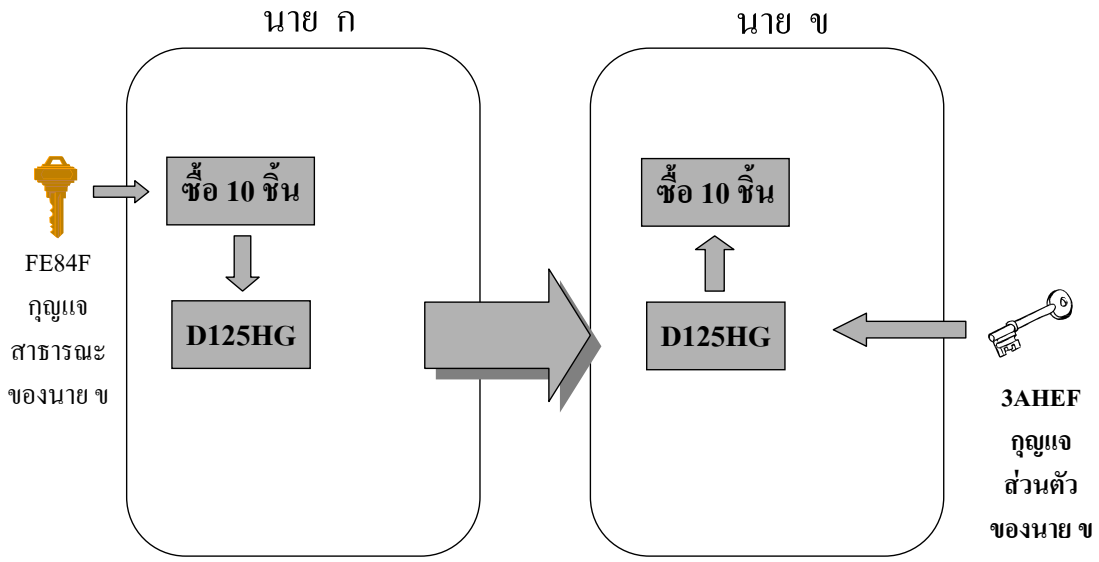
(Integrity)

การห้ามปฏิเสธ

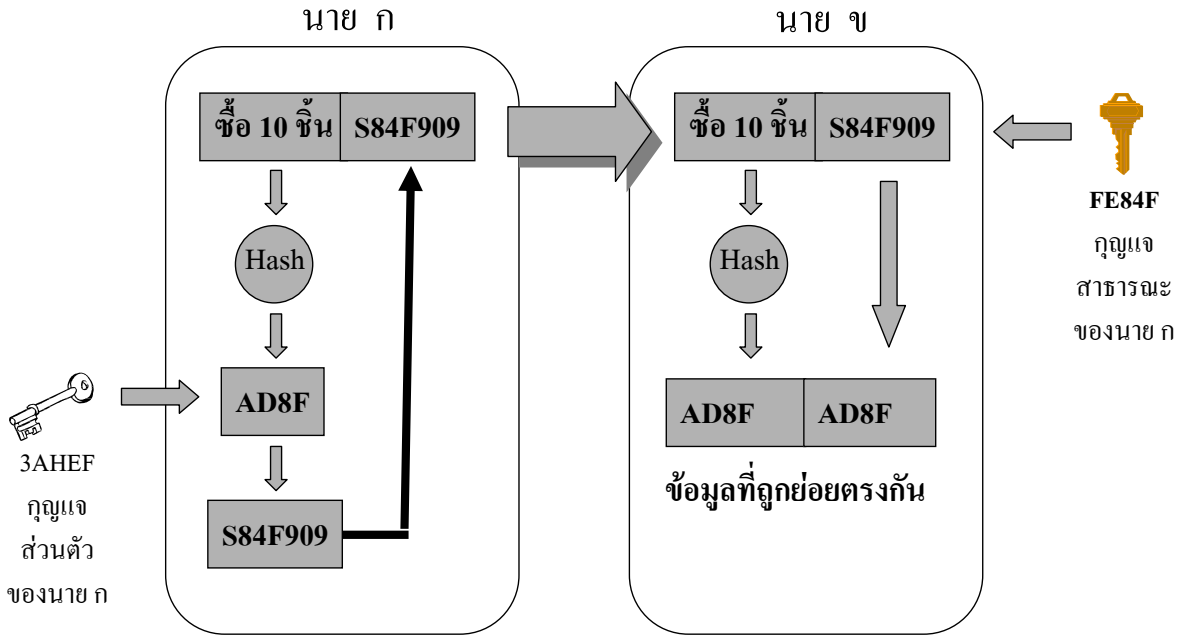
ความรับผิดชอบ

(Non-repudiation)

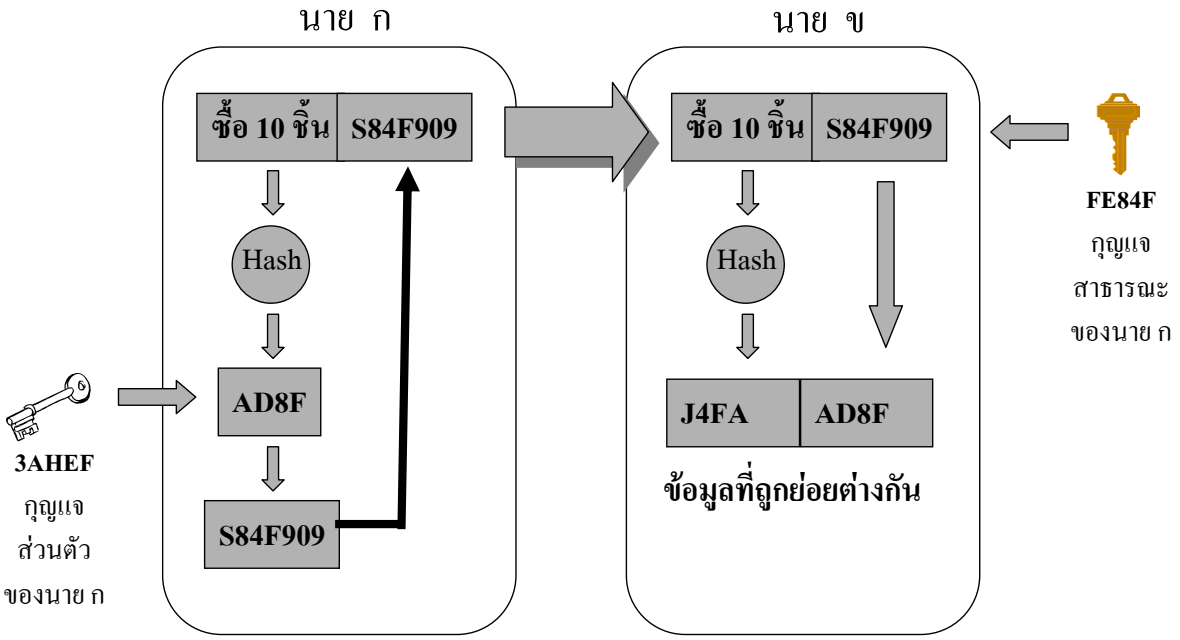
ตัวอย่างการเข้า/ถอดรหัส เพื่อรักษาความลับ



ตัวอย่างวิธีการสร้างและตรวจสอบลายมือชื่อดิจิทัล



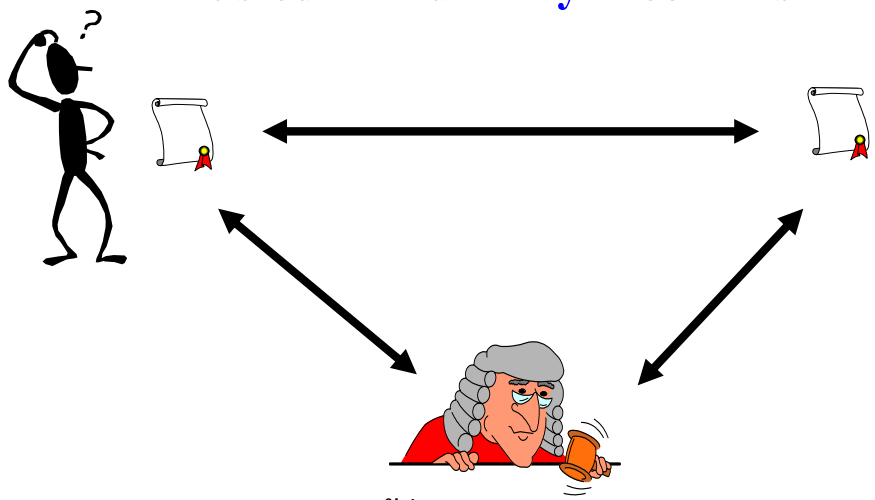
ตัวอย่างลายมือชื่อดิจิทัล (ข้อความถูกเปลี่ยนแปลง)



การบริหารจัดการกุญแจ (Key Management)

- ผู้ใช้กุญแจสาธารณะ (Public Key) ในการตรวจสอบลายมือชื่อดิจิทัล (Digital Signature) หรือใช้ในการเข้ารหัสข้อมูล (Encryption) จะมั่นใจได้อย่างไรว่ากุญแจสาธารณะนั้นเป็นของบุคคลที่อ้างถึงจริง
- ถ้าจำนวนผู้ใช้มีมาก จะจัดการกับกุญแจจำนวนมากๆ ได้ อย่างไร (Key Management)

Trusted Third Party Mechanism



ผู้ประกอบการรับรอง

Certification Authority (CA)

- ยืนยันและรับรองตัวบุคคล ซึ่งเป็นเจ้าของกุญแจสาธารณะ
- บริหารจัดการกุญแจสาธารณะ

ผู้ประกอบการรับรอง (Certification Authority)

- เป็นบุคคลฝ่ายที่สามทำหน้าที่สร้างกุญแจคู่ตามคำขอของผู้ขอใช้บริการ
- ออกใบรับรองยืนยันตัวบุคคลผู้ขอใช้บริหาร
- จัดเก็บกุญแจสาธารณะในฐานข้อมูล
- เปิดเผยกุญแจสาธารณะต่อสาธารณะชนที่ติดต่อทางเครือข่าย
- ยืนยันตัวบุคคลที่เป็นเจ้าของกุยแจสาธารณะตามคำขอของบุคคลทั่ว ๆ ไป
- ให้บริการอื่น ๆ ที่เกี่ยวข้อง

ใบรับรอง (Certificates)

- ลายมือชื่ออิเล็กทรอนิกส์ที่สร้างจากเทคโนโลยีการเข้ารหัสแบบอสมมาตรโดยอาศัยโครงสร้างพื้นฐานของกุญแจสาธารณะที่เรียกว่าลายมือชื่อดิจิทัลนั้น เมื่อส่งข้อความที่อยู่ในรูปข้อมูลอิเล็กทรอนิกส์พร้อมลายมือชื่อดิจิทัลไปยังผู้รับ จะสามารถตรวจสอบความถูกต้องของข้อมูลความดังกล่าวโดยใช้กุญแจสาธารณะของผู้ส่งซึ่งแสดงอยู่ในในรับรอง (Certificate) ซึ่งส่วนใหญ่จะเก็บไว้ในฐานข้อมูลของผู้ประกอบการรับรอง (Repository) และเปิดเผยเพื่อให้ประชาชนทั่วไปสามารถนำกุญแจสาธารณะนั้นไปตรวจสอบได้

มาตรฐานใบรับรอง

- รูปแบบใบรับรองที่กำหนดมาตรฐานโดย ITU (International Telecommunication Union) คือมาตรฐาน x.509
- เนื่องจากกำหนดรายละเอียดต่าง ๆจึงนิยมใช้กันอย่างแพร่หลาย และสามารถประยุกต์ใช้กับโปรแกรม หรือสามารถนำมาประยุกต์ใช้ในการแลกเปลี่ยนใบรับรอง
- ปัจจุบันมาตรฐานที่ได้รับความนิยมอย่างแพร่หลายคือ มาตรฐาน x.509 Version 3 ซึ่งมีรายละเอียดต่าง ๆ อาทิ หมายเลขของใบรับรอง ชื่อและนามสกุลของผู้ถือใบรับรอง กุญแจสาธารณะของผู้ถือใบรับรอง อายุของใบรับรอง วิธีการตรวจสอบลายมือชื่อดิจิทัล ชื่อผู้ประกอบการรับรอง ลายมือชื่อดิจิทัลของผู้ประกอบการรับรอง

ภาพแสดงรายการ ต่าง ๆ ที่กำหนดไว้มาตรฐาน x.509 Version 3 ของ ITU

- versionl mumber
- certificate serial mumber
- signature algorihm identifer
- issuer's name and uniqure identifer
- validity (or operational) period
- subject' s nam4e and unique identifier
- subject public key information
- standard extensions
  - certificate appropriate use definition
  - key usage limitation definition
  - certificate policy information
- other extensions
  - Application – specific
  - CA – specific

รายการหลักในใบรับรอง

- ชื่อของผู้ถือใบรับรอง
- ชื่อของผู้ประกอบการรับรอง
- วิธีการใช้ในการสร้างลายมือชื่อดิจิทัล
- กุญแจสาธารณะของผู้ถือใบรับรอง
- วันเวลาที่เริ่มและสิ้นสุดของการใช้ใบรับรอง
- ลายมือชื่อดิจิทัลของผู้ประกอบการรับรอง

ตัวอย่างใบรับรองอิเล็กทรอนิกส์ (1/2)

Extensions:

Identifier: Certificate Type

Critical: no

Certified Usage:

SSL Client

Secure E-mail

Object Signing

Identifier: Authority Key Identifier

Critical: no

Key Identifier:

75:b0:6d:14:d2:7f:9f:f6:d7:18:00:91:22:fe:f3:43:33:ff:18:1a

ตัวอย่างใบรับรองอิเล็กทรอนิกส์ (2/2)

Signature:

Algorithm: PKCS #1 SHA-1 With RSA Encrypiton

Signature:

82:03:9f:35:5a:f6:d5:d6:70:04:74:55:22:f5:d2:42:6f:7e:87:b9:3b:
59:33:68:19:21:85:ab:cb:a2:77:8e:97:f0:2e:52:28:8a:ed:fe:30:91:
52:11:9f:4b:1e:10:d5:96:2e:9f:17:48:3b:62:6b:b6:53:31:3b:a1:e6:
f5:a3:fa:80:bf:01:5c:42:4a:de:bf:b3:12:2f:8b:c0:63:80:13:89:54:
ae:52:b8:0b:f4:86:5d:09:43:bd:39:35:63:60:35:7e:c3:83:20:26:1e:
ac:af:6c:da:98:69:13:31:ba:7b:01:f9:59:57:71:27:1b:59:8aL16:1c:
09:24

ประเภทของบริการใบรับรองอิเล็กทรอนิกส์

- การแบ่งประเภทหรือระดับของใบรับรองนั้น โดยทั่วไปเป็นกรณีที่ผู้ประกอบการรับรอง (CA) แต่ละรายจะเป็นผู้กำหนดเอง

ก. บริการใบรับรองอิเล็กทรอนิกส์ส่วนตัว เหมาะสำหรับบุคคลทั่วไปที่ต้องการติดต่อสื่อสารผ่านเครือข่ายคอมพิวเตอร์แบบปลอดภัย โดยแบ่งระดับความปลอดภัยออกเป็น 2 ระดับ คือแบบธรรมดา และแบบพิเศษ

- แบบธรรมดา กุญแจส่วนตัวถูกเก็บในระบบคอมพิวเตอร์ของผู้ใช้
- แบบพิเศษ กุญแจส่วนตัวถูกเก็บบนสมาร์ทการ์ด

ประเภทของบริการใบรับรองอิเล็กทรอนิกส์

ข.บริการใบรับรองอิเล็กทรอนิกส์สำหรับเว็บไซต์

- เหมาะสำหรับหน่วยงานที่ต้องการสร้างความเชื่อมั่นในการเผยแพร่ข้อมูลแก่บุคคลทั่วไปผ่านเครือข่ายคอมพิวเตอร์ ว่าข้อมูลดังกล่าวมาจากเว็บไซต์ของหน่วยงานนั้นจริง
- นอกจากนี้ยังสามารถใช้ในการสร้างช่องทางสื่อสารแบบปลอดภัยระหว่างเว็บไซต์กับบุคคลทั่วไปได้อีกด้วย

ประเภทของบริการใบรับรองอิเล็กทรอนิกส์

ค. บริการบริหารจัดการใบรับอรองอิเล็กทรอนิกส์ส่วนตัวสำหรับองค์กร

– เหมาะสำหรับองค์กรที่ต้องการใช้เทคโนโลยีกุญแจสาธารณะในการรักษาความปลอดภัยของข้อมูลที่สื่อสารผ่านเครือข่ายคอมพิวเตอร์ เช่น อินเทอร์เน็ต (Internet) อินทราเน็ต (Intranet) หรือ เอ็กซ์ทราเน็ต (Extranet) โดยที่องค์กรสามารถออกใบรับรองอิเล็กทรอนิกส์ส่วนตัวเองโดยใช้ระบบของผู้ประกอบการรับรอง

ขั้นตอนที่เกี่ยวข้องกับการขอ/ออกใบรับรอง