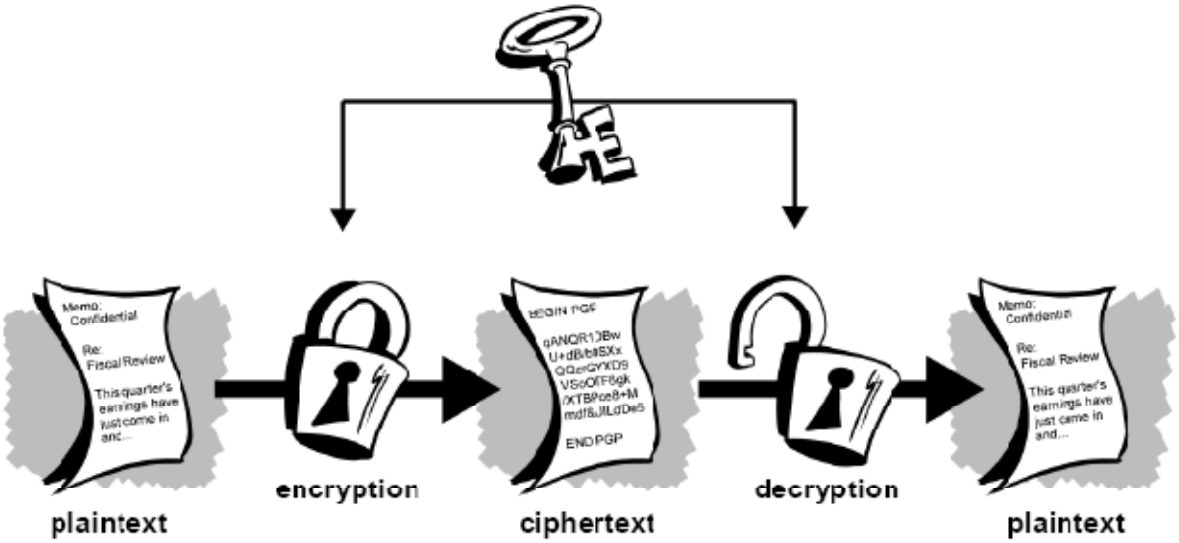
บทที่ 3. Confidentiality

ในกระบวนการสร้าง Confidentiality ในระบบคอมพิวเตอร์ จะใช้การเข้ารหัสลับเป็นกระบวนการหลัก การเข้ารหัสลับหรือ Encryption เป็นกระบวนการที่ต้องการให้ข้อมูลข่าวสารที่รับส่งนั้นเป็นความลับในขณะที่ยังไม่ถึงมือผู้รับ โดยการเข้ารหัสลับในโลกของคอมพิวเตอร์จะเป็นการเปลี่ยนรูปแบบข้อมูลออกไปเป็นข้อมูลที่ไม่สามารถแปลความหมายตามต้นฉบับได้ ซึ่งกระบวนการที่ใช้ในการเข้ารหัสลับนั้น จะมีวิธีการที่แตกต่างกันออกไปตามวัตถุประสงค์ มีความซับซ้อนในการเข้ารหัสลับต่างกัน ทำให้ระดับของการรักษาความปลอดภัยต่างกันด้วย

ในการเข้ารหัสลับเราจะเรียกข้อมูลต้นฉบับที่สามารถอ่านได้ว่า plain text หรือ clear text และจะเรียกกระบวนการที่ทำให้ข้อมูล Plaintext กลายเป็นข้อมูลที่ไม่อยู่ในรูปแบบที่สามารถอ่านได้ว่า Encryption ซึ่งข้อมูลที่ไม่อยู่ในรูปแบบที่สามารถอ่านได้นี้จะเรียกว่า ciphertext โดยในการส่งข้อมูลจะทำการส่งข้อมูล ciphertext ไปยังผู้รับแล้วจึงเข้าสู่กระบวนการ Decryption เพื่อถอดความ ciphertext สำหรับการเข้ารหัสลับจะใช้ศาสตร์ในการเข้ารหัสหรือเรียกว่า cryptography โดยทฤษฎีการเข้ารหัสลับจะแบ่งออกเป็น 2 กลุ่ม คือการเข้ารหัสลับแบบใช้คีย์ในการเข้ารหัสลับและถอดรหัสลับเหมือนกัน (Symmetric Cryptography) และการเข้ารหัสลับแบบที่ใช้คีย์ในการเข้ารหัสลับและถอดรหัสลับต่างกัน(Asymmetric Cryptography)

Symmetric Cryptography

Symmetric Cryptography เป็นกระบวนการเข้ารหัสลับและถอดรหัสลับที่มีการใช้คีย์ในการเข้ารหัสลับและถอดรหัสลับคือข้อมูลชุดเดียวกัน ตัวอย่างอัลกอริทึมในกลุ่มของ Symmetric Cryptography คือ DES (Data Encryption Standard)



รูปที่ 19 รูปการเข้ารหัสลับแบบ Symmetric Key

Data Encryption Standard (DES)

Data Encryption Standard (DES) เป็นอัลกอริทึมที่ใช้ในการเข้ารหัสที่มีการใช้งานอย่างแพร่หลาย คิดค้นขึ้นในปี 1976 โดยใช้คีย์ในการเข้ารหัสและถอดรหัสคือคีย์เดียวกัน (Symmetric Cryptography) เนื่องจาก DES มีการใช้งานคีย์ที่มีขนาด 56 บิต การถอดรหัสโดยไม่ทราบคีย์จึงต้องมีการสุ่มคีย์ทั้งหมด 72,000 ล้านล้านคีย์ ซึ่งถือว่าอัลกอริทึมดังกล่าวมีความปลอดภัยสูง ในกระบวนการเข้ารหัส DES จะทำการแบ่งข้อมูลออกเป็นบล๊อค บล๊อคละ 64 บิต แล้วทำการเข้ารหัสแต่ละบล๊อคโดยใช้คีย์ 56 บิต กระบวนการดังกล่าวจะทำการเข้ารหัสทั้งหมด 16 รอบตามกระบวนการของ DES ถึงแม้ว่า DES จะถือว่ามีความปลอดภัยสูง แต่ก็ยังมีการปรับปรุง DES ให้มีความปลอดภัยสูงขึ้นโดยการปรับเปลี่ยนเป็น "Triple DES" ซึ่งสามารถใช้คีย์ทั้งหมด 3 ชุด

ถึงแม้ว่า DES จะมีความปลอดภัยสูงแต่ก็ยังสามารถถอดรหัสได้ โดยในปี 1997 มีนักคณิตศาสตร์ Rivest - Sharmir - Adleman (ซึ่งภายหลังทั้งสามคนคิดค้นอัลกอริทึม RSA) โดยทำการถอดรหัสข้อมูลโดยได้รับความร่วมมือจากผู้ใช้คอมพิวเตอร์ประมาณ 14,000 เครื่องในอินเตอร์เน็ต ร่วมกันถอดรหัสข้อมูลเพื่อหาคีย์

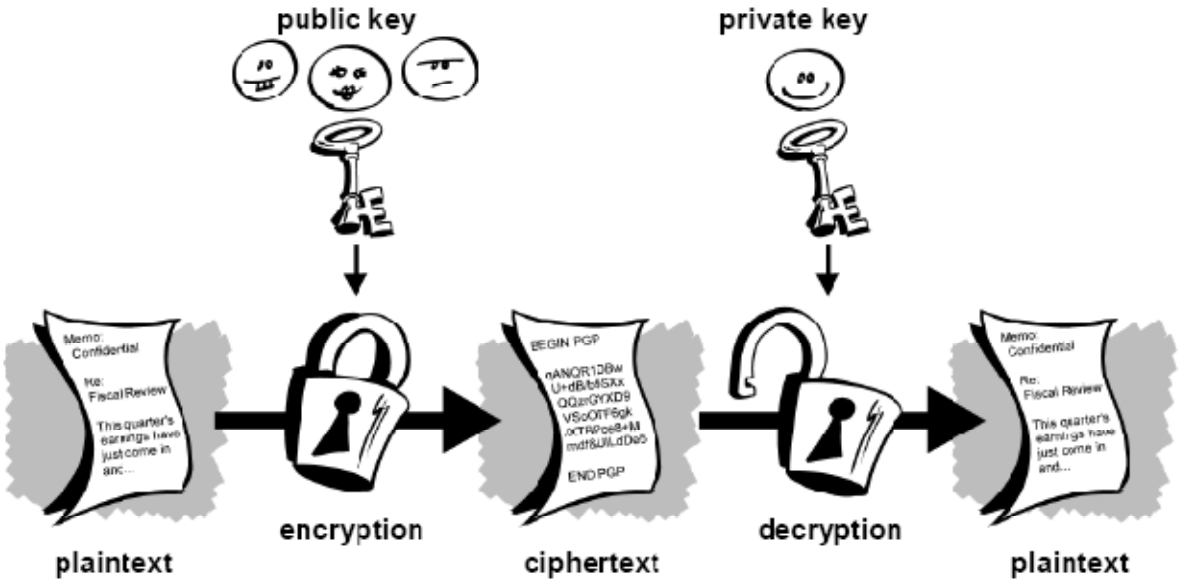
ในการถอดรหัส ซึ่งภายหลังสามารถถอดรหัสได้โดยการสุ่มตรวจคีย์ทั้งสิ้น 18,000 ล้านล้านคีย์ จนได้รับรางวัล 10,000 เหรียญสหรัฐ

ภายหลังมีการคิดค้นการถอดรหัส DES ด้วยวิธีการต่างๆ ได้แก่ ในปี 1998 มีการถอดรหัส DES โดยใช้เวลา 56 ชั่วโมงโดยใช้อุปกรณ์ EEF DES Cracker ในปี 1999 มีการคิดค้นกระบวนการในการถอดรหัส DES ได้ในเวลา 22 ชั่วโมง 15 นาที และล่าสุดในวันที่ 15 มีนาคม 2007 มีการออกแบบอุปกรณ์โดยเชื่อมต่อ FPGA แบบขนานขึ้นชื่อ COPACOBANA โดย University of Bochum and Kiel , Germany ซึ่งราคารวมประมาณ 10,000 เหรียญสหรัฐและทำการถอดรหัส DES โดยใช้เวลา 6.4 วัน

หลังจากที่มีการถอดรหัสข้อมูล DES ได้มากขึ้นจึงมีการคิดค้นกระบวนการในการเข้ารหัสใหม่ คือ Advanced Encryption Standard (AES) ซึ่งอัลกอริทึมนี้ได้พัฒนาโดย Joan Daemen และ Vincent Rijmen ในปี 2000 อัลกอริทึมนี้เป็นที่ยอมรับโดยหน่วยงานมาตรฐานและเทคโนโลยีของสหรัฐ หรือ National Institute of Standard and Technology (NIST) ให้เป็นมาตรฐานในการเข้ารหัสชั้นสูงของประเทศ อัลกอริทึมมีความเร็วสูงและมีขนาดกะทัดรัดโดยสามารถใช้กุญแจที่มีความยาวขนาด 128, 192 และ 256 บิตเพื่อเพิ่มความปลอดภัยให้สูงขึ้น นอกจากนี้ยังมีอัลกอริทึมอื่นๆ ที่ได้รับการสนับสนุนให้นำไปใช้ให้แพร่หลายอีกเช่น RC6, Serpent, MARS และ Twofish

<u>Asymmetric Cryptography</u>

Asymmetric Cryptography คือกระบวนการเข้ารหัสลับที่มีการใช้คีย์ในการเข้ารหัสกับคีย์ในการถอดรหัสต่างกัน ในการใช้งาน หากใช้คีย์ใดในการเข้ารหัสลับจะใช้คีย์อีกคีย์หนึ่งในการถอดรหัส สำหรับคีย์ที่ใช้ทั้งสองคีย์จะมีชื่อเรียกว่า Private Key และ Public Key โดย Private Key จะเป็นคีย์ประจำตัวของผู้ใช้งานจะถูกเก็บรักษาไว้เป็นความลับ ส่วน Public Key จะเป็นคีย์ในการเข้ารหัสข้อมูลเพื่อส่งให้กับเจ้าของคีย์ สามารถแจกจ่ายให้กับบุคคลทั่วไปได้ Asymmetric Cryptography จึงมีการใช้งานในอีกชื่อหนึ่งคือ Public Key Cryptography



รูปที่ 20 รูปแบบการเข้ารหัสแบบ Asymmetric Key

ในการใช้งาน ผู้ใช้งานจะสามารถดำเนินการได้ใน 2 รูปแบบคือ

1. การ Sign ข้อมูลที่จะส่งด้วย Private Key ของผู้ส่ง ทำให้ผู้รับสามารถมั่นใจได้ว่าข้อมูลที่ได้รับจะเป็นข้อมูลที่ถูกต้องโดยการตรวจสอบความถูกต้องโดยใช้ Public Key ของผู้ส่ง
2. ทำการเข้ารหัสลับข้อมูลที่จะส่งโดยใช้ Public Key ของผู้รับ ทำให้ผู้ที่สามารถถอดรหัสข้อมูลและใช้งานข้อมูลนั้นๆ ได้คือผู้รับเท่านั้น โดยผู้รับจะทำการถอดรหัสและนำข้อมูลไปใช้งานโดยใช้ Private Key ของตนเอง

ในการใช้งานในระบบจริง การใช้งาน Asymmetric Cryptography นั้นประสบความสำเร็จได้เนื่องจากมีระบบการบริหารจัดการคีย์ (Key Management System) ซึ่งเป็นระบบเกี่ยวกับการสร้าง การเก็บและการแจกจ่าย

Public Key ของผู้ใช้งานระบบได้โดยง่ายและน่าเชื่อถือ โดยระบบบริหารจัดการคีย์ที่ใช้กันอย่างแพร่หลายในปัจจุบันคือ Public Key Infrastructure หรือ PKI ซึ่งจะกล่าวถึงต่อไป ตัวอย่างของอัลกอริทึมในการเข้ารหัสแบบ Asymmetric Cryptography คือ RSA

RSA

RSA เป็นอัลกอริทึมในการเข้ารหัสข้อมูลโดยการใช้คีย์ในการเข้ารหัสกับถอดรหัสคนละคีย์กัน ซึ่งจากการทำงานดังกล่าวทำให้อัลกอริทึมนี้มีการใช้งานอย่างแพร่หลายโดยเฉพาะในการสร้าง Digital Signature ของข้อมูลต่างๆ RSA ถูกคิดค้นขึ้นโดย Ron Rives, Adi Shamir และ Len Adleman สำหรับชื่อ RSA นั้นมาจากการนำเอาตัวอักษรตัวแรกของผู้คิดค้นมาเรียงต่อกันตามลำดับ สำหรับแนวคิดของ RSA คือการคิดว่าการแยกตัวประกอบของตัวเลขจำนวนเฉพาะ 2 จำนวนใดๆ เป็นสิ่งที่สามารถทำได้ยาก

<u>การบริหารจัดการคีย์</u>

Public Key Infrastructure : PKI

ระบบโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure) PKI คือ ระบบป้องกันข้อมูลที่รับส่งกันผ่านเครือข่ายอินเตอร์เนต ในการทำงานของ PKI ทำได้โดยการใช้หลักการของ Asymmetric Encryption โดยการสร้าง Public Key และ Private Key ในการเข้ารหัสและถอดรหัสข้อมูล โดยกุญแจทั้งสองนี้จะได้มาพร้อมกับใบรับรองที่ Certificate Authority (CA) เป็นผู้ออกให้ โดย Private Key จะถูกเก็บไว้ที่เจ้าของใบรับรองเท่านั้น ส่วน Public Key จะถูกแจกจ่ายโดย CA เพื่อนำไปใช้ในการติดต่อกับเจ้าของใบรับรอง ทำให้การรับส่งข้อมูลใดๆ มีความน่าเชื่อถือมากขึ้น

Certificate Authority

ในชีวิตจริง เราจะเห็นได้ว่าความน่าเชื่อถือในตัวบุคคลต่างๆ มีต่ำมาก หลายๆ หน่วยงานจะเชื่อถือในหน่วยงานของรัฐหรือหน่วยงานต้นสังกัดของคนๆ นั้นเป็นหลัก ทำให้ในการทำธุรกรรมต่างๆ ไม่ว่าจะเป็นสมัครงาน สมัครเพื่อเรียนต่อ ซื้อทรัพย์สิน กู้เงิน เปิดบัญชีธนาคาร ฯลฯ จำเป็นต้องใช้บัตรประชาชนซึ่งออกให้โดยกรมการปกครอง กระทรวงมหาดไทย หรือบัตรอื่นๆ ที่ออกโดยหน่วยงานนั้นๆ จึงจะสามารถทำธุรกรรม หากหน่วยงานต่างๆ เชื่อถือในตัวประชาชนคนนั้นๆ จริงๆ จะต้องสามารถดำเนินการธุรกรรมต่างๆ ได้โดยไม่จำเป็นต้องใช้บัตรประชาชนเลย

นั่นหมายความว่าการทำธุรกรรมต่างๆ จะมีความเชื่อถือกรมการปกครอง กระทรวงมหาดไทย มากกว่าตัวบุคคลนั้นๆ ซึ่งเมื่อมองในความเป็นจริงก็เป็นสิ่งที่ปฏิเสธไม่ได้ เนื่องจากรูปลักษณ์ภายนอกของแต่ละคนสามารถปลอมแปลงกันได้ไม่ยาก

ในการทำธุรกรรมอิเลกทรอนิกส์ให้มีความปลอดภัยสูง การไว้ใจให้ผู้ใช้บริการสามารถทำธุรกรรมได้ด้วยตนเอง โดยการสร้างคู่กุญแจในการเข้ารหัสและถอดรหัสด้วยตนเองนั้น เป็นสิ่งที่มีความเสี่ยงสูงมาก ปัจจุบันจึงมีการตั้งหน่วยงานกลางในการสร้าง การรับรองและการแจกจ่ายคู่กุญแจเหล่านั้นแทนที่จะให้ผู้ใช้งานสร้างขึ้นเอง ด้วยเหตุผลหลักเพียงข้อเดียวคือไม่เชื่อถือในผู้ใช้งานแต่เชื่อถือในผู้ประกอบการรับรอง (Certificate Authority: CA) เท่านั้น

ผู้ประกอบการรับรอง (Certification Authority) หรือผู้ให้บริการรับรอง (Certification Service Provider) ซึ่งจะทำหน้าที่เป็นตัวกลางในการให้บริการ โครงสร้างพื้นฐานกุญแจสาธารณะ (PKI) เพื่อตอบสนองความต้องการพื้นฐานด้านความปลอดภัยของการทำธุรกรรมอิเล็กทรอนิกส์ CA คือผู้ประกอบกิจการรับรองการใช้ Key pairs ในรูปแบบของใบรับรอง อีกนัยก็คือผู้ที่รับรองความปลอดภัยของข้อมูลอิเลกทรอนิก และยืนยันความมีตัวตนของเจ้าของใบรับรองในการทำธุรกรรมได้ โดยหน้าที่ของผู้ออกใบรับรองฯ มีดังนี้

- สร้างคู่กุญแจ (Key pairs) ของผู้ใช้บริการ
- ออกใบรับรองฯ เพื่อยืนยันตัวผู้ใช้บริการ
- จัดเก็บและเผยแพร่กุญแจสาธารณะ

- หากมีการร้องขอให้ยืนยันตัวบุคคลเจ้าของกุญแจ จะดำเนินการยืนยันหรือปฏิเสธความเป็นเจ้าของกุญแจสาธารณะตามคำขอของบุคคลทั่วไป
- เปิดเผยรายชื่อใบรับรองฯ ที่ถูกยกเลิกแล้ว (Certificate Revocation List หรือ CRL) เพื่อเป็นการบอกแก่สาธารณชนว่าใบรับรองฯ นั้น ไม่สามารถนำมาใช้ได้อีกต่อไป

Digital Certificate

เพื่อให้ระบบมีความปลอดภัยและความน่าเชื่อถือมากขึ้น การดำเนินการต่างๆ จะมีการใช้ใบรับรองดิจิตอล (Digital Certificate) ซึ่งออกโดย CA เพื่อยืนยันในการทำธุรกรรมเพื่อรับรองว่าบุคคลที่ทำธุรกรรมนั้นเป็นบุคคลนั้นจริงตามที่ได้อ้างไว้ สำหรับรายละเอียดในใบรับรองดิจิตอลทั่วไปมีดังต่อไปนี้

- ข้อมูลของผู้ที่ได้รับการรับรอง
- ข้อมูลระบุผู้ออกใบรับรอง ได้แก่ ลายมือชื่อดิจิตอลขององค์กรที่ออกใบรับรอง หมายเลขประจำตัวของผู้ออกใบรับรอง
- กุญแจสาธารณะของผู้ที่ได้รับการรับรอง
- วันหมดอายุของใบรับรอง
- ระดับชั้นของใบรับรองดิจิตอล
- หมายเลขประจำตัวของใบรับรองดิจิตอล
- ประเภทของใบรับรองดิจิตอลซึ่งแบ่งออกเป็น 3 ประเภท คือ ใบรับรองเครื่องแม่ข่าย ใบรับรองตัวบุคคล ใบรับรองสำหรับองค์รับรองความถูกต้อง

ในส่วนของการทำ Encryption จึงแยกกระบวนการออกเป็น 2 กระบวนการหลักคือการเข้ารหัสลับ (Encryption) และการบริหารจัดการคีย์ (Key Management) ซึ่งกระบวนการทั้งสองมีส่วนเกี่ยวข้องกันคือ ระบบการเข้ารหัสจำเป็นต้องใช้คีย์ แต่ในการแจกจ่ายคีย์นั้นจำเป็นต้องมีกระบวนการในการแจกจ่าย รวมถึงการใช้งานคีย์ใดๆ ควรมีผู้รับรองว่าคีย์นั้นเป็นของบุคคลที่ต้องการติดต่อด้วยจริงๆ ไม่ใช่ แฮกเกอร์

ตัวอย่างการใช้งาน Encryption เพื่อป้องกันการโจมตีแบบต่างๆ

1. การใช้งาน IP Security ในเครือข่ายไอพี โดย IP Security จะเพิ่มความปลอดภัยในด้านการเข้ารหัสลับข้อมูล ก่อนการส่ง ซึ่งเป็นส่วนการทำงานเพิ่มเติมจาก IP Protocol
2. การใช้งาน SSL เพื่อเพิ่มความปลอดภัยในการใช้งานโพรโตคอล HTTP
3. การใช้โปรแกรมเพื่อเข้ารหัสไฟล์ข้อมูลต่างๆ ในเครื่องเพื่อป้องกันการนำข้อมูลนั้นๆ ไปใช้งาน โดยเจ้าของไฟล์ข้อมูลจะเป็นเพียงคนเดียวที่ทราบรหัสผ่านที่ใช้ในการถอดรหัสไฟล์ ก่อนนำไปใช้งาน
4. การใช้งาน WEP ในเครือข่ายไร้สาย เพื่อเข้ารหัสข้อมูลที่รับส่งในเครือข่ายไร้สาย (IEEE 802.11)
5. การใช้งาน Secure Shell แทนการเชื่อมต่อ Remote Terminal แทน Telnet เพื่อเข้ารหัสข้อมูลก่อนทำการส่ง