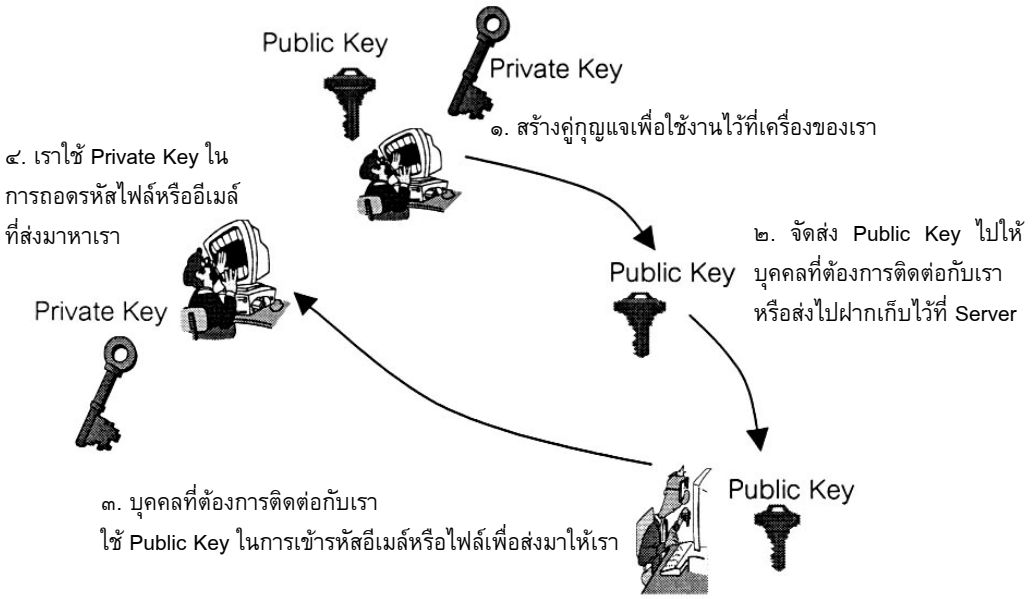
วันนี้คุณต้องการความเป็นส่วนตัวแค่ไหน

น.ต.ดร.ดนัย ปฏิยุทธ
กองวิชาวิศวกรรมศาสตร์

บทนำ

คอมพิวเตอร์มีความสำคัญกับโลกปัจจุบันอย่างยิ่งยวด เราใช้คอมพิวเตอร์ในการทำงานต่าง ๆ มากมาย ขณะที่ความสำคัญของมันเพิ่มมากขึ้นเรื่อย ๆ ความเป็นส่วนตัวของบุคคลกลับลดน้อยถอยลง เราจะเห็นได้ว่า อีเมล์ที่ส่งระหว่างบุคคลมีคนแอบอ่าน มีคนเข้ามาเปลี่ยนเนื้อหาหรือกระทั่งทำลายไฟล์ที่เราสร้างขึ้นมา ไดร์ฟที่ใช้ร่วมกันกับบุคคลอื่นมีคนถือวิสาสะเข้ามาดู ปัญหาต่าง ๆ เหล่านี้กำลังพยายามแก้ไขและทำให้ดีขึ้น วิธีหนึ่งในหลายๆวิธีคือการใช้ PGP(Pretty Good Privacy)ซึ่งเป็นโปรแกรมสำเร็จรูปที่ถูกสร้างขึ้นมาโดย Mr.Phillip R. Zimmermann ในปี พ.ศ.๒๕๓๔ จุดประสงค์หลักก็คือการใช้เข้าและถอดรหัส[๑] อีเมล์เพื่อให้การส่งข้อความตอบโต้ระหว่างบุคคลเป็นความลับมากขึ้น แต่ประโยชน์ของ PGP อย่างอื่น ๆ ก็มี อาทิเช่น การเข้าและถอดรหัสไฟล์ทุกชนิด การลบไฟล์ทิ้งอย่างถาวร การผลิตลายเซ็นอิเล็กทรอนิกส์รวมถึงการสร้างไดร์ฟลับ โดยที่โปรแกรม PGP นี้ ใช้ RSA (Rivest Shamir and Adleman) หรือ Diffie-Hellman/DSS เป็นอัลกอริทึมสำหรับการแลกเปลี่ยนกุญแจ[๒] และ IDEA (International Data Encryption Algorithm) เป็นอัลกอริทึมสำหรับการเข้ารหัสอีเมล์ และ PGP ใช้รูปแบบจำลองที่เรียกว่า Web of Trust ซึ่งหลักการทำงานต่าง ๆ ของ PGP มีอยู่ด้วยกัน ๓ ชนิดดังจะได้กล่าวต่อไปนี้

๑. หลักการทำงานของ PGP สำหรับการเข้า – ถอดรหัสอีเมล์และไฟล์ (Encryption-Decryption)



รูป ๑ ขั้นตอนการเข้า - ถอดรหัสอีเมล์และไฟล์

---

[๑] *การเข้ารหัส* (encryption) เป็นกรรมวิธีในการนำเอาข้อมูลมาแปลงจนไม่สามารถอ่านข้อมูลนั้นได้ จนกว่าจะได้มีการถอดรหัส (Decryption) เพื่อแปลงข้อมูลที่ถูกเข้ารหัสจนอ่านไม่ได้กลับมาอ่านได้เหมือนเดิม

[๒] *กุญแจ* (Key) คือโค้ดโปรแกรมที่ใช้การเข้าและถอดรหัส

การจะรับและส่งอีเมล์หรือไฟล์ให้ปลอดภัยนั้นมีขั้นตอนการเข้า – ถอดรหัสอีเมล์และไฟล์มีดังต่อไปนี้ (แสดงในรูป ๑)

๑. ขั้นตอนแรก คือ การสร้างคู่กุญแจสำหรับตัวเราเองโดยใช้โปรแกรม PGP โดยคู่กุญแจนั้นประกอบด้วยกุญแจส่วนตัว (Private Key) ซึ่งจะเก็บไว้ที่ตัวเราและใช้ในการถอดรหัสอีเมล์ที่ถูกเข้ารหัสและส่งมาถึงเรา และกุญแจสาธารณะ (Public Key) ที่ใช้สำหรับเข้ารหัสโดยจะอยู่ตามบุคคลที่เราต้องการติดต่อด้วย สำหรับคู่กุญแจนี้เราสามารถกำหนดไว้ว่าต้องการให้หมดอายุเมื่อไรหรือไม่หมดอายุเลยก็ได้ โดยคู่กุญแจที่เราสร้างนี้จะไปอยู่ที่ Keyring[๓] (คลังกุญแจ) ของเรา

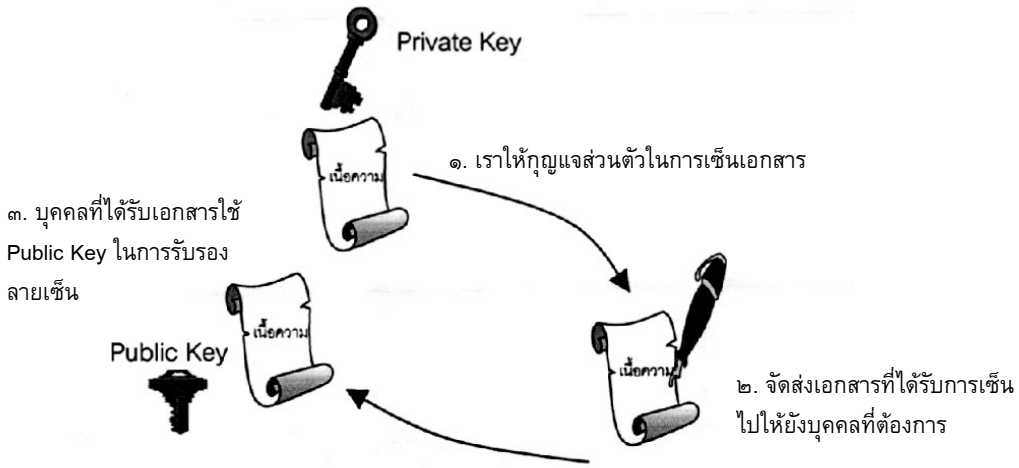
๒. ถ้าเราต้องการให้บุคคลที่เราติดต่อด้วยส่งอีเมล์หรือไฟล์ที่จะเข้ารหัสมาหาเรา เราก็ส่ง Public Key ไปให้บุคคลนั้น (ในทำนองกลับกัน ถ้าคนอื่นต้องการให้เราส่งอีเมล์และไฟล์ที่จะเข้ารหัสไปหาบุคคลนั้นก็ต้องส่ง Public Key ของตัวเองมาให้เรา) หรือบางครั้งเราก็สามารถส่ง Public Key ของเราไปฝากเก็บไว้ที่ Server เมื่อเพื่อนของเราต้องการใช้ ก็สามารถดึงไปใช้ได้เลยโดยไม่ต้องรอให้เราส่งไปให้

๓. เมื่อบุคคลที่เราต้องการติดต่อด้วยได้รับ Public Key บุคคลนั้นก็จะบอกโปรแกรม PGP ให้ใช้ Public Key ตัวนั้น ๆ เพราะจะมีแต่เราเท่านั้นที่สามารถเปิดอ่านอีเมล์หรือไฟล์ได้ เนื่องจากการเข้ารหัสโดยใช้ Public Key นั้น ต้องใช้ Private Key ในการถอดรหัสเท่านั้น (กระบวนการที่เข้ารหัสโดย Public Key และถอดรหัสโดย Private Key เรียกว่า Asymmetric Encryption ส่วนกระบวนการที่เข้ารหัสโดย Private Key และถอดรหัสโดย Private Key เรียกว่า Symmetric Encryption) หรือบางครั้งโปรแกรม PGP อาจสั่งให้ผลิตกุญแจชั่วคราว (Session Key) เพื่อใช้ในการเข้ารหัสในครั้งนั้น ๆ โดย Session Key จะถูกเข้ารหัสโดย Public Key อีกทอดหนึ่ง

๔. เมื่อเราต้องการเปิดอีเมล์หรือไฟล์ที่ถูกเข้ารหัส (จะต้องเข้ารหัสโดยใช้ Public Key ของเราเท่านั้น) ส่งมาให้เรา เราก็ถอดรหัสโดยใช้ Private Key ของเรา

๒. หลักการทำงานของ PGP สำหรับการผลิต (เซ็นต์) – รับรองลายเซ็นอิเล็กทรอนิกส์ (Signature – Verification)

[๓] *Keyring คือ* ไฟล์ที่ใช้เก็บคู่กุญแจที่เราสร้างขึ้นมา และ Public Key ของคนอื่นที่ส่งมาให้เราหรือที่เราไปดาวน์โหลดมาจาก Server



รูป ๒ ขั้นตอนการผลิตและรับรองลายเซ็นอิเล็กทรอนิกส์

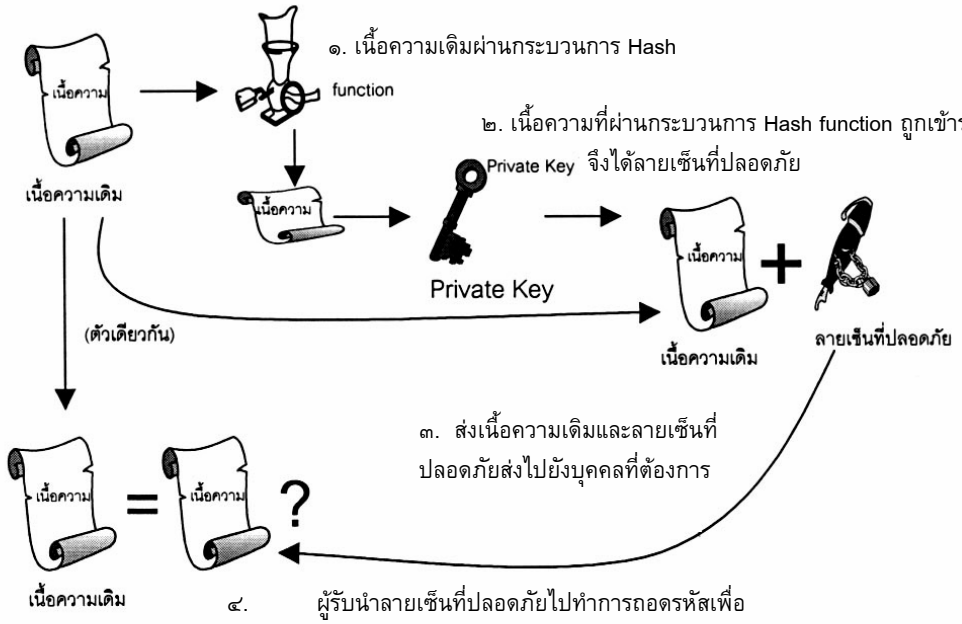
หากเราไม่ต้องการเข้ารหัสอีเมล์หรือไฟล์ที่เราส่งออกไป เพียงแต่ต้องการรับรองเฉย ๆ ว่าเป็นอีเมล์หรือไฟล์ที่ส่งออกจากเราจริง ๆ (คือมีคุณสมบัติ Authentication) เนื้อหาภายในยังคงไม่เปลี่ยนแปลง (คือมีคุณสมบัติ Integrity) และผู้ส่งไม่สามารถปฏิเสธได้ว่าไม่ได้ส่งไฟล์หรืออีเมล์นั้น ๆ มา (คือมีคุณสมบัติ Non-repudiation) ขั้นตอนการผลิตลายเซ็นอิเล็กทรอนิกส์มีดังต่อไปนี้ (แสดงในรูป ๒)

๑. ขั้นตอนแรก คือ การเซ็นรับรองเอกสารซึ่งอาจจะเป็นอีเมล์หรือไฟล์ด้วยกุญแจส่วนตัว (Private Key) ของคุณเอง (Private Key ที่ได้มาจากการสร้างคู่กุญแจนั่นเอง)

๒. ส่งไฟล์หรืออีเมล์ที่ได้รับการเซ็นไปยังบุคคลที่ต้องการได้เอกสารนั้น ๆ

๓. หลังจากที่ได้รับเอกสารที่ผ่านการเซ็นกำกับ บุคคลนั้น ๆ ก็จะใช้กุญแจสาธารณะ (Public Key) ในการรับรองลายเซ็นอิเล็กทรอนิกส์โดยตรวจสอบว่าเอกสารนั้น ๆ ส่งมาจากบุคคลที่ได้กล่าวอ้างจริง ๆ เนื้อหาภายในยังคงเหมือนเดิม และผู้ส่งไม่สามารถปฏิเสธได้ เพราะมีแต่ผู้ส่งเท่านั้นที่สามารถเข้ารหัสเอกสารด้วยกุญแจส่วนตัวของตนเอง

ส่วนการทำให้ลายเซ็นอิเล็กทรอนิกส์น่าเชื่อถือมากยิ่งขึ้นนั้นเราสามารถกระทำได้ดังกระบวนการต่อไปนี้ (แสดงในรูป ๓)



รูป ๓ ขั้นตอนการเข้าผลิตและรับรองลายเซ็นอิเล็กทรอนิกส์อย่างปลอดภัย

๑. นำเนื้อความที่ต้องการส่งไปผ่านกระบวนการ Hash Function

๒. จากนั้นจึงนำเนื้อความที่ผ่านกระบวนการ Hash Function (เนื้อความที่ผ่านกระบวนการ Hash Function เรียกว่า Message digest[๕])ไปเข้ารหัสด้วยกุญแจส่วนตัว(Private Key) เราก็จะได้ลายเซ็นที่ปลอดภัย

๓. ส่งเนื้อความเดิมและลายเซ็นที่ปลอดภัยส่งไปยังบุคคลที่ติดต่อกับเรา

๔. ผู้รับนำลายเซ็นที่ปลอดภัยไปทำการถอดรหัส (รายละเอียดของกระบวนการมีดังต่อไปนี้ กล่าวคือ ขั้นแรกสุด นำลายเซ็นที่ปลอดภัยไปถอดรหัสโดยใช้กุญแจสาธารณะของบุคคลที่ส่งลายเซ็นมาให้ซึ่งทำให้เราได้ Message digest หลังจากนั้นเราก็นำ Message digest ไปผ่านกระบวนการ Hash Function เพื่อให้ได้เนื้อความเดิม) เพื่อให้ได้เนื้อความเดิมแล้วนำไปเปรียบเทียบกับเนื้อความเดิมที่ไม่ได้ทำอะไรกับมัน ถ้าเนื้อความเหมือนกันจึงสามารถสรุปได้ว่าลายเซ็นนั้น ๆ เป็นลายเซ็นของจริง

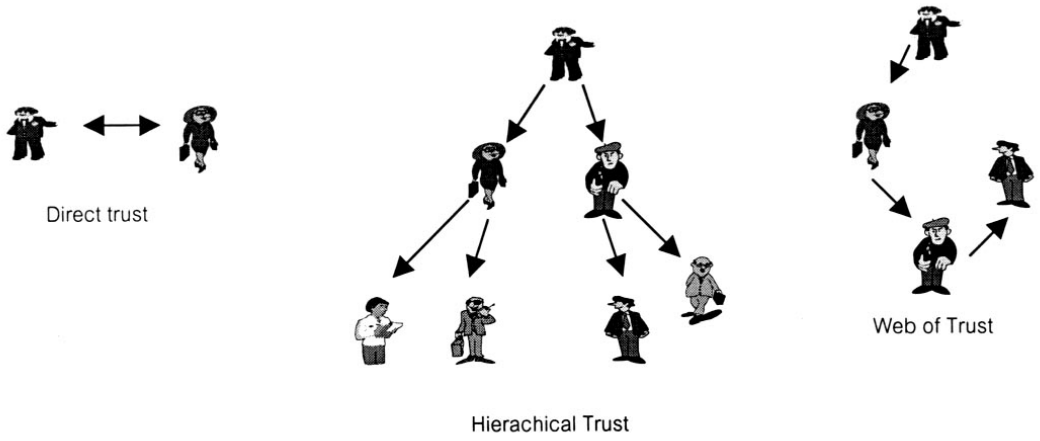
๓. ความเชื่อถือ

ถ้าเราต้องการทราบให้แน่ชัดว่า Certificate นั้น ๆ เป็นของคนนั้นจริงหรือไม่ มีวิธีการตรวจสอบหลายวิธีด้วยกัน ตัวอย่างเช่น การตรวจสอบ Public Key จากบุคคลนั้นโดยตรง การตรวจสอบว่า Certificate ไม่ได้ถูกถอดถอนการใช้งาน หรือการให้ความเชื่อถือ (Trust) ต่อบุคคลหรือองค์กรที่ออก Certificate

---

[๕] *Message digest คือ* เนื้อความที่ผ่านโปรแกรม Hash Function และจะมีความยาวน้อยลงเนื่องจากถูกบีบโดยโปรแกรม Hash Function

รูปแบบจำลองของการเชื่อถือมี ๓ แบบด้วยกันคือ Direct trust (คือความเชื่อถือโดยตรงระหว่างบุคคลกับบุคคลหรือองค์กรกับองค์กรที่รู้จักกัน), Hierachical trust (คือความเชื่อถือตั้งแต่ต้นของ CA จนถึงปลายทาง) และ Web of trust (คือการที่เราโยงความเชื่อถือระหว่างบุคคลตั้งแต่ต้นสายจนกระทั่งถึงปลายทางของการติดต่อ) ดังแสดงในรูปข้างล่าง



รูป ๔ รูปแบบจำลองต่าง ๆ ของความเชื่อถือ (Trust)

ซึ่งการเชื่อถือกันระหว่างบุคคลต่าง ๆ มีระดับของความน่าเชื่อถือไม่เท่ากันอันเนื่องมาจากความสนิทสนมที่ไม่เท่ากัน PGP ได้แบ่งระดับความเชื่อถือ (Trust) จากมากที่สุดคือ *Trusted* ไปจนถึงระดับที่ต่ำที่สุด คือ *Untrusted* เป็น ๓ ระดับคือ Complete trust, Marginal trust และ Notrust (Untrusted)

สรุป

ในขณะที่การรับ – ส่ง อีเมล์เป็นการสื่อสารยอดฮิตในยุคอินเตอร์เน็ตฟีเวอร์ เพื่อให้คุณแน่ใจว่าเมล์ของคุณเป็นความลับ มีความเป็นส่วนตัวไม่มีใครสามารถอ่านข้อความได้ เราก็สมควรต้องใช้โปรแกรมในการเข้าถอดรหัสอีเมล์นั้น ๆ โปรแกรมหนึ่งที่เป็นที่นิยมใช้ก็คือ PGP ข้อดีของโปรแกรม PGP คือเป็นโปรแกรมที่ใช้ได้กับทุกระบบปฏิบัติการ (โดยเมื่อคุณติดตั้ง PGP เรียบร้อยแล้ว โปรแกรมก็จะฝังตัวเองเข้าไปในโปรแกรมการรับ – ส่งอีเมล์ของเครื่องนั้น ๆ ที่ PGP สนับสนุนการใช้งาน (อาจจะเป็น Microsoft Outlook Express หรือ Eudora) โดยจะมีปุ่มคำสั่งเพิ่มขึ้นมาสำหรับการเรียกใช้ PGP) อีกทั้งยังเป็นฟรีแวร์ (โดยเราสามารถเข้าไปดาวน์โหลดโปรแกรมได้ที่ http://www.pgpi.org) ทำให้เป็นที่นิยมของผู้คน ข้อดีของ PGP อีกข้อหนึ่งก็คือความสามารถในการใช้กุญแจที่เปลี่ยนไปกับอีเมล์ต่าง ๆ (ใช้กุญแจที่ไม่ซ้ำกันกับอีเมล์ที่ต่างกัน) ทำให้ยากต่อการเดาหรือตรวจจับกุญแจ นอกจากนั้นการใช้โปรแกรม Message digest ใน PGP ก็ยังเป็นการรับประกันได้ว่าลายเซ็นอิเล็กทรอนิกส์นั้น ๆ ปลอดภัยจากการนำไปใช้โดยผู้อื่น หากไฟล์ที่เราสร้างขึ้นมา (อาจจะสร้างมาด้วยโปรแกรมสำเร็จรูปอะไรก็ได้ อาทิเช่น Word, Excel, Powerpoint, Access) เป็นเรื่องสำคัญ เราก็สามารถใช้ PGP ในการเข้ารหัสไฟล์เพื่อป้องกันการถูกอ่าน หากเครื่องของเรามีผู้ใช้งานร่วมกัน หากเราไม่ต้องการให้คนอื่นมาเปิดงานหรือ

ร่วมใช้งานที่เราทำได้ เราก็สามารถใช้ PGP เพื่อสร้างไดร์ฟลับป้องกันไม่ให้บุคคลอื่นเข้าไปดูไฟล์ใด ๆ ของเราได้ การป้องกันของ PGP กรณีที่เราไม่แน่ใจว่า Public Key ที่เราใช้นั้นเป็นของบุคคลที่เราติดต่อหรือไม่นั้นและหมดอายุการใช้งานหรือยัง โดยการใช้โปรแกรมที่เรียกว่า Digital certificates[๕] ซึ่งจะถูกส่งไปกับ Public Key อนึ่งในการเข้า – ถอดรหัสอีเมล์และไฟล์นั้น ทั้งทางผู้ส่งและผู้รับจะต้องติดตั้งโปรแกรม PGP ทั้งคู่

เอกสารอ้างอิง

๑. นิพนธ์ กิตติปภัสสร. ***เข้ารหัสถอดรหัสไฟล์และอีเมล์ด้วยโปรแกรม PGP 6.5.*** กรุงเทพมหานคร : ซีเอ็ดยูเคชั่น, ๒๕๔๔

[๕] *Digital certificate* คือ โปรแกรมที่ใช้แสดงว่า Public Key นั้น ๆ เป็นของผู้ส่งจริง ประกอบด้วย Public Key, ข้อมูลของผู้ส่ง, Digital signature ขององค์กรที่น่าเชื่อถือ