# ใบความรู้ที่ 4

# ความปลอดภัยของข้อมูล

**การเข้ารหัส (Cryptography)**

|  |
| --- |
| คือ การทำให้ข้อมูลที่จะส่งผ่านไปทางเครือข่ายอยู่ในรูปแบบที่ไม่สามารถอ่านออกได้ ด้วยการเข้ารหัส (Encryption) ทำให้ข้อมูลนั้นเป็นความลับ ซึ่งผู้ที่มีสิทธิ์จริงเท่านั้นจะสามารถอ่านข้อมูลนั้นได้ด้วยการถอดรหัส (Decryption)**ลายมือชื่อดิจิทัล  (Digital Signature****)**ลายมือชื่อดิจิตอล (Digital Signature) หรือเรียกอีกอย่างว่า ลายเซ็นดิจิตอล   ใช้ในการระบุตัวบุคคลเพื่อแสดงถึงเจตนาในการยอมรับเนื้อหาในสัญญานั้น ๆ   และป้องกันการปฏิเสธความรับผิดชอบ  เพิ่มความน่าเชื่อถือในการทำธุรกรรมร่วมกัน**กระบวนการสร้างและลงลายมือชื่อดิจิทัล**1.  นำเอาข้อมูลอิเล็กทรนอิกส์ต้นฉบับ (ในรูปแบบของ file)  ที่จะส่งไปนั้น    มาผ่านกระบวนการทางคณิตศาสตร์ที่เรียกว่า ฟังก์ชันย่อยข้อมูล (Hash Function) เพื่อให้ได้ข้อมูลที่สั้น  เช่นเดียวกับการเข้ารหัสข้อมูลอีกชั้นหนึ่ง   ซึ่งข้อมูลจะอ่านไม่รู้เรื่อง   จากนั้นก็นำข้อมูลดังกล่าวมาทำการเข้ารหัส (Encryption) อีกที2. จากนั้นทำการ  “ข้ารหัสด้วยกุญแจส่วนตัวของผู้ส่ง”   เรียกขั้นตอนนี้ว่า  “Digital Signature” 3. ส่ง  Digital Signature   ไปพร้อมกับข้อมูลต้นฉบับตามที่ระบุในข้อ 1   เมื่อผู้รับ  ๆ  ก็จะตรวจสอบว่าข้อมูลนั้นถูกแก้ไขระหว่างทางหรือไม่   โดยนำข้อมูลต้นฉบับที่ได้รับ   มาผ่านกระบวนการย่อยด้วย  ฟังก์ชันย่อยข้อมูล (Hash Function) จะได้ข้อมูลที่ย่อยแล้ว เช่นเดียวกับการคลายข้อมูลที่ถูกบีบอัดอยู่     และ4. นำ  Digital Signature มาทำการถอดรหัสด้วย “กุญแจสาธารณะของผู้ส่ง (Public Key)   ก็จะได้ข้อมูลที่ย่อยแล้วอีกอันหนึ่ง   จากนั้นเปรียบเทียบข้อมูลที่ย่อยแล้ว  ที่อยู่ในข้อ3  และข้อ  4  ถ้าข้อมูลเหมือนกันก็แสดงว่าข้อมูลไม่ได้ถูกแก้ไขระหว่างการส่ง**ใบรับรองดิจิทัล (Digital Certificate)**                การขออนุญาตใช้ใบรับรองดิจิทัล (Digital Certificate)  ก็เพื่อเพิ่มความน่าเชื่อถือในการทำธุรกรรมร่วมกันบนเครือข่าย Internet  ซึ่งหน่วยงานที่สามารถออกใบรับรองดิจิทัล (Digital Certificate) นี้ได้จะเป็น  “องค์กรกลาง”    ที่มีชื่อเสียงเป็นที่น่าเชื่อถือ  เรียกองค์กรกลางนี้ว่า  “Certification Authority: CA”**Digital Certificate** จะถูกนำมาใช้สำหรับยืนยันในการทำธุรกรรม   ว่าเป็นบุคคลนั้นจริงตามที่ได้อ้างไว้ ซึ่งสามารถจำแนกประเภทของใบรับรองดิจิตอล ได้ 3  ประเภท ได้แก่1. ใบรับรองเครื่องแม่ข่าย (Server)2. ใบรับรองตัวบุคคล3. ใบรับรองสำหรับองค์กรรับรองความถูกต้อง**Certification Authority (CA)**                CA   คือ   องค์กรรับรองความถูกต้อง   ในการออกใบรับรองดิจิตอล (Digital Certificate ) ซึ่งมีการรับรองความถูกต้องสำหรับบริการต่อไปนี้                1.  การให้บริการเทคโนโลยีการรหัส   ประกอบด้วย                          - การสร้างกุญแจสาธารณะ                          - กุญแจลับสำหรับผู้จดทะเบียน                          - การส่งมอบกุญแจลับ  การสร้างและการรับรองลายมือชื่อดิจิตอล                2.  การให้บริการเกี่ยวกับการออกใบรับรอง   ประกอบด้วย                           - การออก  การเก็บรักษา  การยกเลิก การตีพิมพ์เผยแพร่ ใบรับรองดิจิตอล                        - การกำหนดนโยบายการออกและอนุมัติใบรับรอง                3.  บริการเสริมอื่น  เช่น  การตรวจสอบสัญญาต่าง ๆ   การทำทะเบียน   การกู้กุญแจ สำหรับประเทศไทย  ยังไม่มีองค์กร  “CA”  ซึ่งปัจจุบันหน่วยงานที่ต้องการความน่าเชื่อถือในการทำธรรมบน Web  จำเป็นต้องใช้บริการเทคโนโลยีดังที่กล่าวมาจากต่างชาติ   แต่คงไม่นานคาดว่าหน่วยงานในภาครัฐอย่างเช่น NECTEC ([www.nectec.or.th](http://www.nectec.or.th/)) คงสามารถพัฒนาเทคโนโลยีต่าง ๆ ดังกล่าวเพื่อให้ใช้บริการภายในประเทศได้ |

**ประเภทของใบรับรองดิจิทัล แบ่งออกเป็น 3 ประเภท คือ**

|  |
| --- |
|                  1. ใบรับรองเครื่องแม่ข่าย                 2. ใบรับรองตัวบุคคล                  3. ใบรับรองสำหรับองค์รับรองความถูกต้องhttps://sites.google.com/site/mintandfha/_/rsrc/1472849424664/prapheth-khxng-birab-rxng-dicithal-baeng-xxk-pen-3-prapheth-khux/Nrca_info_15.jpg?height=200&width=190 |

**10 วิธีในการรักษาความปลอดภัยของข้อมูล PDF Print E-mail**

|  |
| --- |
|         คำว่าองค์กรมันผุดขึ้นมาใน ในทุกวันนี้เราใช้งาน  smartphones, tablets, laptops, and netbooks ในการทำธุรกรรมต่างๆไม่มากก็น้อย ดังนั้นหากเราไม่รู้วิธีการ รักษาความปลอดภัยให้กับข้อมูลส่วนตัวเหล่านั้นของเราแล้ว โอกาศที่จะเกิดความเสียหายเนี่ย ถือเป็นเรื่องใหญ่เลยล่ะครับ...        ในวันนี้ผมมีข้อแนะนำ 10 ข้อ มาให้ทุกๆท่านลองใช้งานดูเพื่อความปลอดภัยในข้อมูลของตัวท่านเองรายละเอียดมาดังนี้ครับ        1. เข้ารหัส USB Flash Drive  เพื่อให้มั่นใจว่าเราสามารถเปิดดูข้อมูลได้คนเดียว โดยในกรณีนี้ผมขอแนะนำให้ใช้โปรแกรม Truecryptในการเข้ารหัสข้อมูลต่างๆของเรา เพียงเท่านี้แหละครับเราก็จะสามารถเก็บข้อมูลต่างๆของเราที่เป็นความลับได้แล้วไม่ว่าจะเป็น รหัสเอทีเอ็ม รหัสบัตรวีซ่า รหัสเครดิตต่างๆของเราแม้กระทั่ง พาสเวิร์ด หรือข้อมูลส่วนตัวของเราที่มีเยอะแยะมากมายจนไม่สามารถจะจำได้...        2.เก็บข้อมูลใน Drive ที่มีการเข้ารหัส ในข้อ 1 เราสามารถเข้ารหัส USB Flash Drive เพื่อความปลอดภัยได้แล้ว แต่การใช้งานจำเป็นต้องใช้สิทธิ์ Admin ของระบบในการทำงาน ซึ่งในข้อนี้เราใช้โปรแกรม FreeOTFEในการเขียนไฟล์ลงใน Drive ที่เข้ารหัส โดยไม่ต้องใช้สิทธิ์ Admin        3.เข้ารหัสด้วย Text file ง่ายๆ ด้วยโปรแกรม LockNoteผู้ใช้งานสามารถเข้ารหัสง่ายๆด้วย LockNoteโดยโปรแกรมตัวนี้ไม่ต้องติดตั้งเพียง copy ลงเครื่องก็สามารถใช้งานได้เลยการเข้ารหัสใช้ กลไกการเข้ารหัสแบบ AES 256 ซึ่งเพียงพอในการป้องกัน Drive หรือ File ของท่านแล้ว        4.ซ่อนข้อมูลไว้ในไฟล์รูปภาพแล้วก็มีรหัสผ่านคอยป้องกันอีกชั้นหนึ่ง อันนี้บางคนอาจเคยทำเพราะมีรูปพิเศษ หรือหนังพิเศษที่ไม่อยากให้ใครมารู้ด้วยว่าเรามี ! ง่ายๆเลยครับวิธีนี้ก็คือการนำไฟล์เหล่านั้นไปซ่อนในรูปภาพซะเลยเวลาผู้ใช้งานเปิดเข้ามาดูก็จะไม่เจอ        5. เข้ารหัส Drive สำหรับ Linux เท่านั้น อ่านเพิ่ม        6.ส่งไฟล์โดยติดตั้ง โปรแกรม Drop box ซึ่งตัว Drop box จะทำหน้าที่เข้ารหัสการส่งข้อมูลของเราใครนึกไม่ออกให้ลองนึกถึง การส่งจดหมายระหว่างจุด Aไปจุด B โดยส่งผ่านท่อ PVC ซึ่งบุคคลภายนอกจะมองเห็นแต่ท่อ PVC แต่จะไม่รู้เลยว่าเราส่งอะไรผ่านท่อนั้น เหมาะอย่างยิ่งในการนำมาใช้ในการส่งข้อมูลที่เป็น Text file ในอีเมลล์ เพราะว่าในวันนี้ซอฟต์แวร์ในการดักข้อมูลที่เป็น Text file มีจำนวนมากเหลือเกิน        7.วิธีลบไฟล์ที่ปลอดภัย นอกจากการเข้ารหัสไฟล์แล้วในบางครั้งไฟล์ที่เราลบไปสามารถกู้คืนมาได้ ซึ่งเราอาจไม่ระมัดระวังตัว เช่น คืดว่าลบไฟล์ข้อมูลรหัสบัตร เอทีเอ็มที่เราเก็บไว้แล้ว ซึ่งน่าจะเพียงพอแล้วแต่จริงๆแล้วใครจะไปรู้ว่าอาจมีคนไปกู้ไฟล์ที่เราลบไปแล้วมาได้ \*0\* โดยในที่นี้ซอฟแวร์ที่ใช้ลบข้อมูลก็มีอยู่เยอะพอสมควรเลยครับ อ่านเพิ่มเติม        8.การเข้ารหัส Wifiที่เราใช้งาน        9.เก็บข้อมูลในการ log in ไว้ใน LastPassซึ่งเป็นบริการเพิ่มเติมจาก Amazon ประมาณว่าเก็บพาสเวิร์ดทุกอย่างของคุณไว้บนระบบ cloud  โดยมีการเข้ารหัสข้อมูลเป็นแบบ AES 256 bit อย่างดี และมีการเข้ารหัสไฟล์รหัสผ่านแบบ ssl pipeline โดยที่เราไม่ต้องเสียเวลาในการมานั่งเข้ารหัสเองแต่อย่าง แต่ทุกอย่างเก็บไว้ที่ ฐานข้อมูลของ Amazon นะครับถ้าเราไม่ซีเรียสก็ไม่เป็นไรครับ        10.ป้องกันข้อมูลแบบไม่ต้องออนไลน์ด้วยโปรแกรม KeePassโดยติดตั้งโปรแกรมนี้ไว้ที่เครื่องของเราเอง เหมือนเราสร้าง Master key ไว้เมื่อเปิดเข้าไปที่บัญชีของเราแล้วก็สามารถบันทึกข้อมูลรหัสผ่านเว็บไซต์อื่นๆ เช่น mail , server , messenger เหมือนไอ้เจ้า LastPassจาก Amazon นั่นแหละครับแต่ต่างกันที่เก็บไว้ที่เครื่องเราไม่ต้องไปฝากไว้ที่เครื่องคนอื่นเท่านั้นเองครับ |

**เทคโนโลยีในการรักษาความปลอดภัย**

|  |
| --- |
|              1. ความปลอดภัยของเครือข่าย (Networks Security)                     - เพื่อปกป้องความปลอดภัยของเครือข่ายภายในองค์กรจากเครือข่ายภายนอกที่ไม่น่าเชื่อถือ                     - การใช้ firewalls              2. การพิสูจน์ตัวตน (Authentication)                      - เพื่อให้มั่นใจได้ว่าฝ่ายที่กาลังติดต่อด้วยนั้นเป็นบุคคลที่ถูกต้อง ไม่ใช่ผู้แอบอ้าง                      - การใช้รหัสผ่าน, การใช้ digital certificates, การใช้ smart card ที่เข้ารหัส,         การใช้ biometrics (เช่น ลายนิ้วมือ, ม่านตา)                3. การเข้ารหัส (Encryption)                       - ใช้ในการปกป้องข้อมูลที่ส่งผ่านเส้นทางสาธารณะ                       - SSL Protocol, Public-key cryptography                4. นโยบายและการจัดการระบบความปลอดภัย (Security Policy and Management)                        - ครอบคลุมถึงระบบการบริหารบุคคล วิธีการเข้าถึงตัว server และอื่น ๆ                        - เป็นส่วนสำคัญในการทำให้ระบบพาณิชย์อิเล็กทรอนิกส์ปลอดภัยอย่างแท้จริง         **ความรู้เพิ่มเติม**                  1. ลายมือชื่อดิจิทัล (Digital Signature) คือข้อมูลอิเล็กทรอนิกส์ที่ได้จากการเข้ารหัสข้อมูลด้วยกุญแจส่วนตัวของผู้ส่งซึ่งเปรียบเสมือนเป็นลายมือชื่อของผู้ส่ง คุณสมบัติของลายมือชื่อดิจิทัล นอกจากจะสามารถ ระบุตัวบุคคล และเป็นกลไกการป้องกันการปฏิเสธความรับผิดชอบแล้ว ยังสามารถป้องกันข้อมูลที่ส่งไปไม่ให้ถูกแก้ไข หรือหากถูกแก้ไขไปจากเดิมก็สามารถล่วงรู้ได                  2. ใบรับรองดิจิทัล (Digital Certificate) จะถูกนำมาใช้สำหรับยืนยันในตอนทำธุรกรรมว่าเป็นบุคคลนั้นๆจริง ตามที่ได้อ้างไว้ ซึ่งออกโดยองค์กรกลางที่เป็นที่เชื่อถือ เรียกว่า องค์กรรับรองความถูกต้อง (Certification Authority) ซึ่งรายละเอียดในใบรับรองดิจิทัลทั่วไปมีดังต่อไปนี้                      - ข้อมูลระบุผู้ที่ได้รับการรับรอง ได้แก่ ชื่อ องค์กร ที่อยู่                      - ข้อมูลระบุผู้ออกใบรับรอง ได้แก่ ลายมือชื่อดิจิทัลขององค์กรที่ออกใบรับรอง หมายเลขประจำตัวของผู้ออกใบรับรอง                      - กุญแจสาธารณะของผู้ที่ได้รับการรับรอง                      - วันหมดอายุของใบรับรองดิจิทัล                      - ระดับชั้นของใบรับรองดิจิทัล ซึ่งมีทั้งหมด 4 ระดับ ในระดับ 4 จะมีกระบวนการตรวจสอบเข้มงวดที่สุด และต้องการข้อมูลมากที่สุด                      - หมายเลขประจำตัวของใบรับรองดิจิทัล |

**มาตรการการรักษาความปลอดภัยของข้อมูล**

|  |
| --- |
| ระบบรักษาความปลอดภัยของข้อมูลของพาณิชย์อิเล็กทรอนิกส์จึงต้องมีมาตรการดังต่อไปนี้                1. การระบุตัวบุคคล และ อำนาจหน้าที่ (Authentication & Authorization) คือ การระบุ ตัวบุคคลที่ติดต่อว่าเป็น บุคคลตามที่ได้กล่าวอ้างไว้จริง และมีอำนาจหน้าที่ตามที่ได้กล่าวอ้างไว้จริง (เปรียบเทียบได้กับการแสดงตัวด้วยบัตรประจำตัวซึ่งมีรูปติดอยู่ด้วย หรือ การใช้ระบบล็อกซึ่งผู้ที่จะเปิดได้จะต้องมีกุญแจอยู่เท่านั้น เป็นต้น)                2. การรักษาความลับของข้อมูล (Confidentiality) คือ การรักษาความลับของข้อมูลที่เก็บไว้ หรือส่งผ่านทางเครือข่ายโดยป้องกันไม่ให้ผู้อื่นที่ไม่มีสิทธิ์ลักลอบดูได้ (เปรียบเทียบได้กับ การปิดผนึกซองจดหมาย การใช้ชองจดหมายที่ทึบแสง การเขียนหมึกที่มองไม่เห็น เป็นต้น)              3. การรักษาความถูกต้องของข้อมูล (Integrity) คือ การป้องกันไม่ให้ข้อมูลถูกแก้ไข โดยตรวจสอบไม่ได้ (เปรียบเทียบได้กับ การเขียนด้วยหมึกซึ่งถ้าถูกลบแล้วจะก่อให้เกิดรอยลบขึ้น เป็นต้น)               4. การป้องกันการปฏิเสธ หรือ อ้าง ความรับผิดชอบ (Non-repudiation) คือ การป้องกันการปฏิเสธว่าไม่ได้มีการส่ง หรือ รับข้อมูล จากฝ่ายต่างๆที่เกี่ยวข้อง หรือ การป้องกันการอ้างที่เป็นเท็จว่าได้ รับหรือ ส่งข้อมูล (เปรียบเทียบได้กับการส่งจดหมายลงทะเบียน เป็นต้น) |