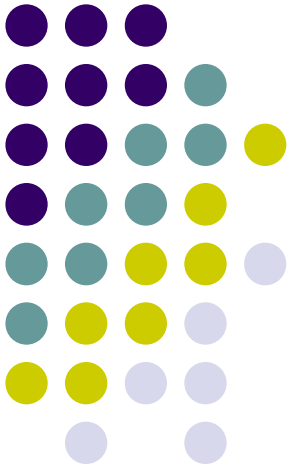
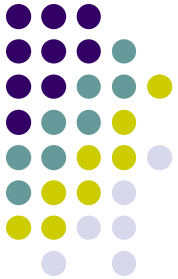
ภัยคุกคาม ระบบเครือข่าย



ตัวอย่างภัยคุกคามและการโจมตีเครือข่ายระบบคอมพิวเตอร์



- การจารกรรมข้อมูลความลับของทางการสหรัฐโดยพวกสายลับ KGB

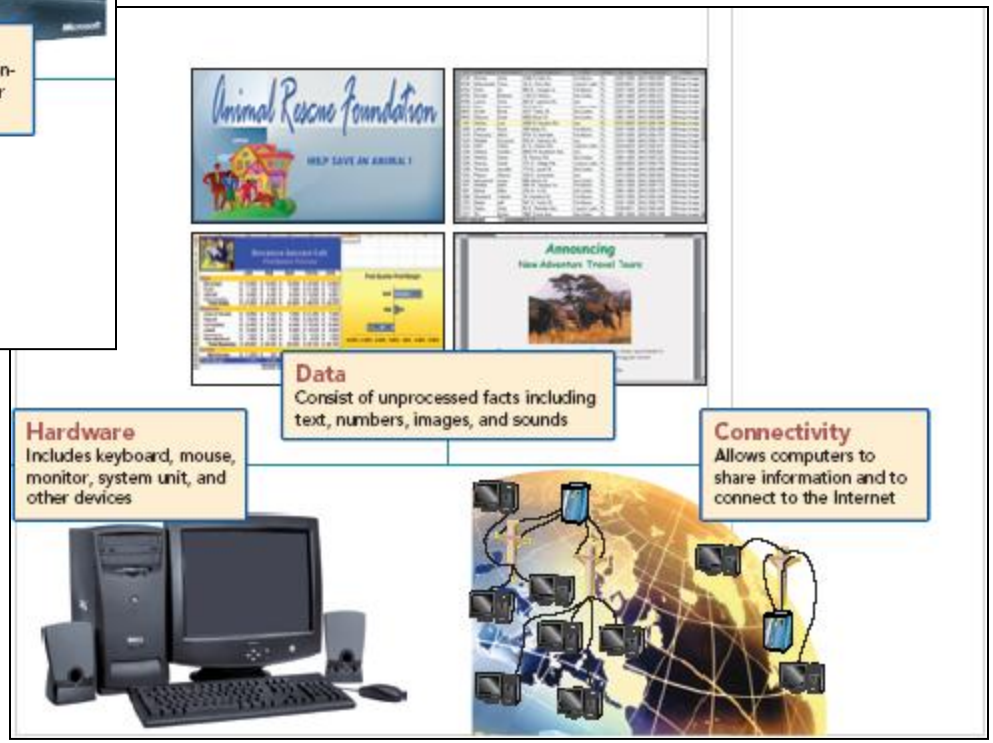
- การขโมยเงินจำนวน $25 ล้านเหรียญสหรัฐฯ ผ่านระบบเครือข่ายคอมพิวเตอร์

- การโจมตีระบบคอมพิวเตอร์ขององค์การอวกาศ NASA

ฯลฯ

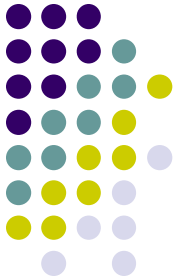
ระบบคอมพิวเตอร์

ฮาร์ดแวร์
ข้อมูล
ภาวะเชื่อมต่อ



บุคลากร
ระเบียบปฏิบัติการ
ซอฟต์แวร์

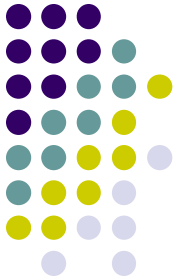
จุดประสงค์ของระบบการรักษาความปลอดภัย



1. เพื่อรักษาความลับของข้อมูล (Confidentiality) หมายถึง การปกป้องข้อมูลไม่ให้ถูกเปิดเผยต่อบุคคลที่ไม่ได้รับอนุญาตอย่างถูกต้อง และถ้ามีการขโมยข้อมูลไปแล้วก็ไม่สามารถอ่านหรือทำความเข้าใจได้

2. เพื่อป้องกันการปลอมแปลงข้อมูล (Integrity) คือ การรักษาความถูกต้องของข้อมูลและป้องกันไม่ให้มีการเปลี่ยนแปลงแก้ไขข้อมูลโดยมิได้รับอนุญาต ซึ่งการที่จะสามารถทำเช่นนี้ได้ ต้องมีระบบควบคุมว่าผู้ใดจะสามารถเข้าถึงข้อมูลได้และเข้าถึงแล้วทำอะไรได้บ้าง

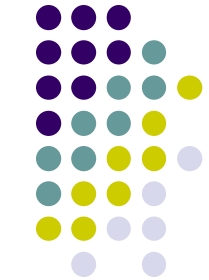
จุดประสงค์ของระบบการรักษาความปลอดภัย



3. เพื่อทำให้ระบบนั้นสามารถที่จะทำงานได้ตามปกติและเต็มประสิทธิภาพ (Availability) ระบบจะต้องสามารถทำงานได้อย่างดีตามจุดมุ่งหมายในการใช้และมีขีดความสามารถปฏิบัติงานได้ในปริมาณตามที่ต้องการได้ภายในเวลาที่กำหนดด้วย

ระบบการรักษาความปลอดภัยที่มีขีดความสามารถสูงอาจทำให้ขีดความสามารถและความสะดวกในการทำงานของระบบทั้งในด้านปริมาณงานและประสิทธิภาพลดลง ดังนั้น ต้องพิจารณาว่าระดับความปลอดภัยใดจึงจะเหมาะสมกับความสะดวก ปริมาณงาน และประสิทธิภาพของงานที่ต้องการ

ภัยคุกคามที่มีต่อระบบต่าง ๆ



- ภัยต่อระบบฮาร์ดแวร์

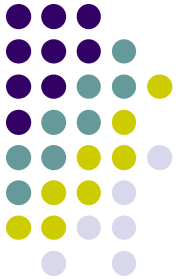
- ภัยต่อระบบการจ่ายไฟฟ้าแก่คอมพิวเตอร์
- ภัยที่เกิดจากการทำลายทางกายภาพ
- ภัยจากการลักขโมยโดยตรง

- ภัยที่มีต่อระบบซอฟต์แวร์

- การลบซอฟต์แวร์
- การขโมยซอฟต์แวร์
- การเปลี่ยนแปลงแก้ไขซอฟต์แวร์

- ภัยที่มีต่อระบบเครือข่าย

ผู้เจาะระบบรักษาความปลอดภัย



แบ่งเป็น 2 ประเภทหลัก ๆ ได้แก่

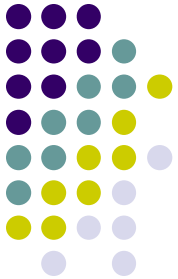
- **Hacker**

  มีวัตถุประสงค์เพื่อทดสอบขีดความสามารถของระบบ

- **Cracker**

  มีวัตถุประสงค์เพื่อบุกรุกระบบเพื่อขโมยข้อมูลหรือทำลายข้อมูลผู้อื่นโดยผิดกฎหมาย

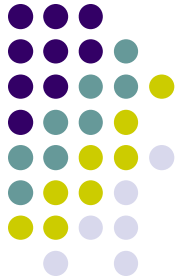
ภัยคุกคามด้านความปลอดภัย



1. **ภัยคุกคามบนระบบเครือข่าย (Denial of service)** โดยจะส่งผลให้เครื่องคอมพิวเตอร์หรือระบบหยุดทำงานโดยไม่ทราบสาเหตุ สามารถแบ่งได้เป็น 2 ประเภท

   - Spamming or E-mail Bombing
   - Viruses , Worms, Trojan Horses

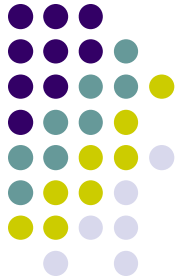
ภัยคุกคามด้านความปลอดภัย



Spam คืออะไร

- Spam เมล์คือเมล์ที่เราไม่ต้องการ โดยมีจุดประสงค์คือผู้ส่งส่วนใหญ่ต้องการโฆษณาบริการต่างๆที่ตัวเองมี เป็นประเภทหนึ่งของ Junk เมล์หรือเมล์ขยะ

ภัยคุกคามด้านความปลอดภัย

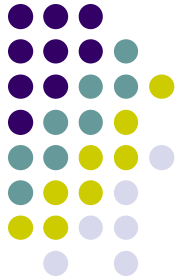


- **Viruses** เป็นโปรแกรมคอมพิวเตอร์ประเภทหนึ่งที่มีหน้าที่คอยทำลายซอฟต์แวร์หรือโปรแกรมต่าง ๆ ในเครื่องโดยถูกออกแบบมาให้แพร่กระจายตัวเองจากไฟล์หนึ่งไปยังไฟล์อื่นๆ ภายในเครื่องคอมพิวเตอร์ ไวรัสจะแพร่กระจายตัวเองอย่างรวดเร็วไปยังทุกไฟล์ภายในคอมพิวเตอร์ หรืออาจจะทำให้ไฟล์เอกสารติดเชื้ออย่างช้าๆ

ตัวอย่างไวรัสที่พบบ่อย

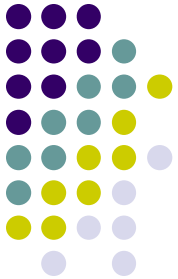
ไวรัส	รายละเอียด
Hacked by Godzilla	ไม่สามารถดับเบิ้ลคลิกเปิดไดร์ฟต่างๆ ได้ และมีข้อความปรากฏบน Title Bar ของ Internet Explorer ว่า “Hacked By Godzilla”
Apology-B	ส่งอีเมลล์ที่มีไวรัสตามอีเมลล์ที่ผู้ใช้ส่งออกไป
KuKworm	แนบตัวเองไปกับอีเมลล์ที่ถูกส่งออกไป
Love Bug	สร้างตัวเองขึ้นมาใหม่ผ่านโปรแกรม Microsoft Outlook หรือเปลี่ยนชื่อไฟล์
Stages-A	ทำสำเนาตัวเองไปบนเน็ตเวิร์กไดรฟ์
Thus	ลบไฟล์ข้อมูลเมื่อถึงวันที่ 13 ธันวาคม

ภัยคุกคามด้านความปลอดภัย



- **Worm** เป็นไวรัสคอมพิวเตอร์ชนิดหนึ่งที่ติดต่อกันทางอินเทอร์เน็ท แพร่กระจายได้อย่างรวดเร็วโดยคัดลอกตัวเองซ้ำแล้วใช้ระบบเครือข่ายเป็นสื่อในการแพร่กระจายซึ่งจะแพร่กระจายได้อย่างรวดเร็วและทำความเสียหายรุนแรงกว่าไวรัสมาก

ภัยคุกคามด้านความปลอดภัย

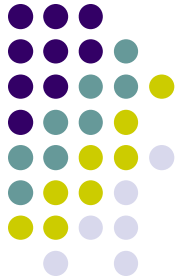


Trojan Horses

เป็นไวรัสที่สามารถหลบเลี่ยงการตรวจหาได้และสามารถหลอกผู้ใช้ให้คิดว่าเป็นโปรแกรมธรรมดาทั่วไป เมื่อเรียกใช้งานโปรแกรม ไวรัสนี้จะทำงานโดยดักจับรหัสผ่านต่าง ๆ และส่งกลับให้ผู้สร้าง เพื่อเจาะระบบป้องกันเข้าสู่เครือข่าย

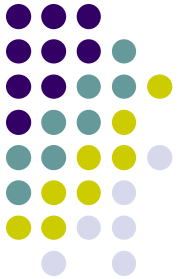
<u>การป้องกัน</u> อาจมีเครื่องให้บริการหลายตัวเพื่อทำหน้าที่แทนกัน

คุกกี้ (Cookie) เป็นอย่างไร



- **คุกกี้ (Cookie)** เป็นการบันทึกค่าต่างๆ ที่มีขนาดเล็กของ Web Server ลงยัง Browser เพื่อทำการให้ Browser จดจำค่าต่างๆ ในการใช้งานบน Web Server และเมื่อ Browser มีการเรียกใช้งาน Web Server อีกครั้ง Web Server สามารถที่จะทำการตรวจสอบข้อมูลในคุกกี้ว่าก่อนนี้ Browser นี้มีการเรียกใช้งาน Web Server อะไรไปบ้าง

ภัยคุกคามด้านความปลอดภัย



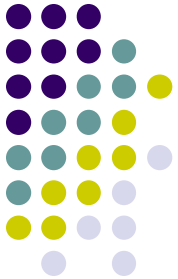
2. การเข้าสู่เครือข่ายโดยไม่ได้รับอนุญาต (Unauthorized Access)

เป็นภัยคุกคามด้วยการเข้าไปยังเครือข่ายโดยไม่ได้รับอนุญาต ซึ่งอาจมีจุดประสงค์ในการโจรกรรมข้อมูล แบ่งเป็น 2 ประเภท คือ

- **Passive Unauthorized Access** เป็นการลอบฟังข้อมูลที่ส่งผ่านเครือข่ายโดย Hacker จะไม่ทำอะไรต่อระบบ โดยข้อมูลที่ลอบฟังส่วนมากเป็นรหัสผ่านเพื่อเข้าสู่เครือข่ายองค์กร

- **Active Unauthorized Access** เป็นภัยคุกคามโดยมีวัตถุประสงค์เพื่อเปลี่ยนแปลงข้อมูล เช่น ข้อมูลเงินฝากธนาคาร โดยการใช้วิธี **“Spoofing”**

ภัยคุกคามด้านความปลอดภัย

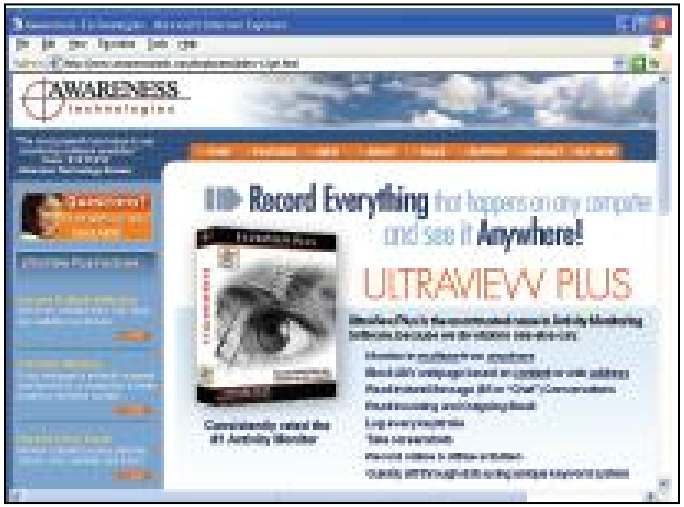


3. การโจรกรรมและการปลอมแปลง (Theft and Fraud)

เป็นภัยคุกคามที่เกิดจากการโจรกรรมซอฟแวร์หรือเปลี่ยนแปลงข้อมูลที่ทำให้องค์กรเสียหาย เช่น พนักงานคัดลอกซอฟแวร์ที่ถูกกฎหมายของบริษัทเพื่อนำกลับไปใช้ที่บ้าน หรือนำไปให้คนอื่น แต่ตัวซอฟแวร์ที่คัดลอกมาไม่ได้สามารถคัดลอกลิขสิทธิ์ (License) ได้ ทำให้ซอฟแวร์นั้นกลายเป็นผิดกฎหมายไปในที่สุด

สิทธิส่วนบุคคล

- **การแอบดูการทำงานของลูกจ้าง การแอบดูไฟล์หรืออีเมล์**
  - ใช้โปรแกรมสนู้ปแวร์ (snoopware)
- **การตรวจสอบเนื้อหาโดยผู้ให้บริการ**
  - กลั่นกรองและปฏิเสธข้อมูล
  - ยกเลิกรหัสผู้ใช้



อินเทอร์เน็ตและเว็บ

- **ความลวงของการไม่มีตัวตน (illusion of anonymity)**
  - การไม่ใช้ชื่อ-นามสกุลหรือข้อมูลส่วนตัวจริง
  - ไม่สนใจในภาวะส่วนตัวเมื่อท่องอินเทอร์เน็ต หรือส่งจดหมายอิเล็กทรอนิกส์
- **ไฟล์ประวัติ (history file)**
- **คุกกี้ (cookies)**
  - คุกกี้แบบดั้งเดิม (traditional cookies)
  - คุกกี้แอ็ดเน็ตเวิร์ก หรือคุกกี้แอ็ดแวร์
    (ad network cookies หรือ adware cookies)
- **โปรแกรมสายลับ (spyware)**
- **โปรแกรมต่อต้านหรือกำจัดโปรแกรมสายลับ**
  (anti-spyware program หรือ spy removal program)

ภัยอื่นๆ

- **ภัยธรรมชาติ**
  - ไฟไหม้
  - น้ำท่วม
  - พายุ
  - แผ่นดินไหว
  - ฯลฯ

- **การต่อสู้กันของพลเมือง และการก่อการร้าย**
  - สงคราม
  - จลาจล
  - กบฏ
  - ก่อการร้าย

- **ความผิดพลาดทางด้านเทคโนโลยี**
- **แรงดันไฟกระชาก** (voltage surge)
  - เครื่องป้องกันกระแสไฟกระชาก (surge protector)
- **ความผิดพลาดจากมนุษย์**

ตารางสรุปฐานความผิดและโทษตามร่างพระราชบัญญัติการกระทำความผิดทางคอมพิวเตอร์

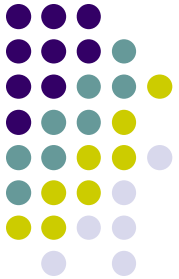
มาตรา	ฐานความผิด	โทษจำคุก สูงสุด	โทษปรับสูงสุด (บาท)
5	เข้าถึงคอมพิวเตอร์โดยมิชอบ	1 เดือน	1,000 บาท
6	การเปิดเผยมาตรการป้องกันการเข้าถึง	6 เดือน	10,000 บาท
7	เข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ	1 ปี	20,000 บาท
8	การดักข้อมูลคอมพิวเตอร์	3 ปี	60,000 บาท
9	การรบกวนข้อมูลคอมพิวเตอร์	5 ปี	100,000 บาท
10	การรบกวนระบบคอมพิวเตอร์	5 ปี	100,000 บาท

ตารางสรุปฐานความผิดและโทษตามร่างพระราชบัญญัติการกระทำความผิดทางคอมพิวเตอร์

มาตรา	ฐานความผิด	โทษจำคุก สูงสุด	โทษปรับสูงสุด (บาท)
11	การกระทำต่อความมั่นคง		
	- ก่อความเสียหายแก่ข้อมูลฯ	1 ปี – 10 ปี	2 หมื่นบาท – 2 แสนบาท
	- กระทบต่อความมั่นคง	3 ปี – 15 ปี	6 หมื่นบาท- 3 แสนบาท
	- อันตรายแก่ร่างกายหรือชีวิต	ประหารชีวิต / จำคุกตลอดชีวิต / 10 ปี-20 ปี	

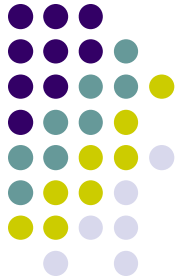
ตารางสรุปฐานความผิดและโทษตามร่างพระราชบัญญัติการกระทำความผิดทางคอมพิวเตอร์

มาตรา	ฐานความผิด	โทษจำคุก สูงสุด	โทษปรับสูงสุด (บาท)
12	การจำหน่าย/เผยแพร่ชุดคำสั่ง	1 ปี	2 หมื่นบาท
13	การเผยแพร่เนื้อหาอันไม่เหมาะสม	2 ปี - 5 ปี	4 หมื่นบาท – 1แสนบาท
14	ความรับผิดของผู้ให้บริการ	2 ปี - 5 ปี	4 หมื่นบาท – 1 แสนบาท
15	การตัดต่อภาพผู้อื่น	3 ปี	6 แสนบาท



การควบคุมและรักษาความปลอดภัย

การรักษาความปลอดภัยของข้อมูล



- การควบคุมและรักษาความปลอดภัยในองค์กรมี 2 วิธีคือ
  1. **การรักษาความปลอดภัยให้กับเครือข่ายองค์กร**
  2. **รักษาความปลอดภัยให้กับข้อมูลที่ส่งผ่านเครือข่าย**

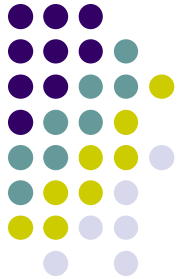
การควบคุมและรักษาความปลอดภัย

1. การรักษาความปลอดภัยให้กับเครือข่ายองค์กร

1.1 ควบคุมการเข้าถึงทางกายภาพ (Physical Access Control)

- การล็อกห้องคอมพิวเตอร์อย่างแน่นหนาเมื่อไม่มีการใช้งานแล้ว
- การใช้ยามเฝ้าหรือติดโทรทัศน์วงจรปิด
- การใช้ Back-Up Disk สำหรับการทำข้อมูลสำรองอย่างสม่ำเสมอ และไม่เก็บไว้ในที่เดียวกันกับระบบคอมพิวเตอร์นั้น ๆ
- ติดตั้งระบบดับเพลิง

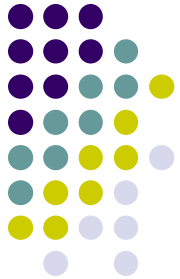
การควบคุมและรักษาความปลอดภัย



Biometrics เป็นวิธีที่ใช้ลักษณะเฉพาะตัวของแต่ละบุคคลที่แตกต่างกันไป เช่น

- การพิสูจน์บุคคลด้วยลายนิ้วมือ
- การพิสูจน์บุคคลด้วยเรตินา
- การพิสูจน์บุคคลด้วยลายเซ็นอิเล็กทรอนิกส์
- การพิสูจน์บุคคลด้วยอุณหภูมิ
- การพิสูจน์บุคคลด้วยเสียง

การควบคุมและรักษาความปลอดภัย



1.2 ควบคุมการเข้าถึงทางตรรกะ คือการรักษาความปลอดภัยด้วยการใช้ลักษณะเฉพาะตัวของแต่ละบุคคลหรือใช้อุปกรณ์มาช่วย

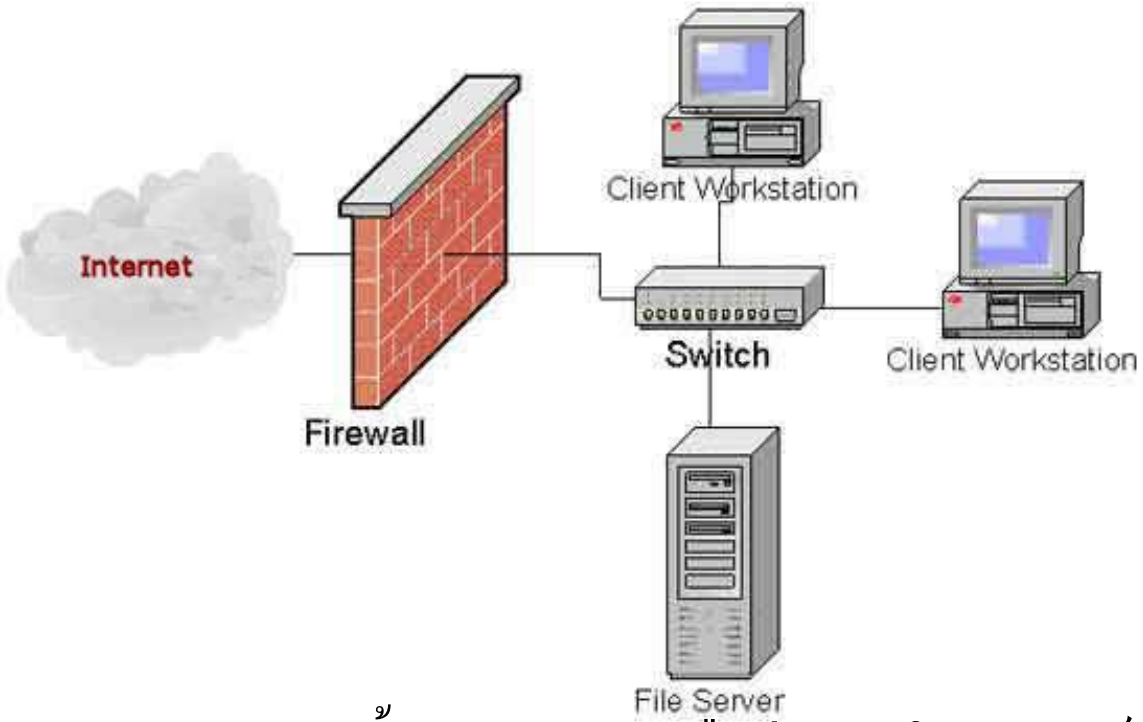
- **การเก็บประวัติส่วนตัวผู้ใช้(User profiles)** นิยมใช้กันมากที่สุด

ข้อมูลผู้ใช้ประกอบด้วย

- ชื่อผู้ใช้
- รหัสผ่าน
- สิทธิการใช้งาน

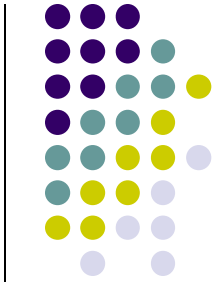
การควบคุมและรักษาความปลอดภัย

- **Firewall** เป็นการติดตั้งโปรแกรมคอมพิวเตอร์บนคอมพิวเตอร์หรือเครื่องเราท์เตอร์ที่มีหน้าที่จัดการ ควบคุมการเชื่อมต่อจากภายนอกสู่ภายในองค์กร และจากภายในองค์กรสู่ภายนอกองค์กร



แสดงการติดตั้ง firewall กับเครือข่ายภายในขององค์กร

การควบคุมและรักษาความปลอดภัย



1.3 ตรวจสอบการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต (Detecting Unauthorized Access)

- **การตรวจสอบการใช้งาน (Audit Logs)**

  เก็บรายละเอียดการใช้งานของผู้ใช้แต่ละคน

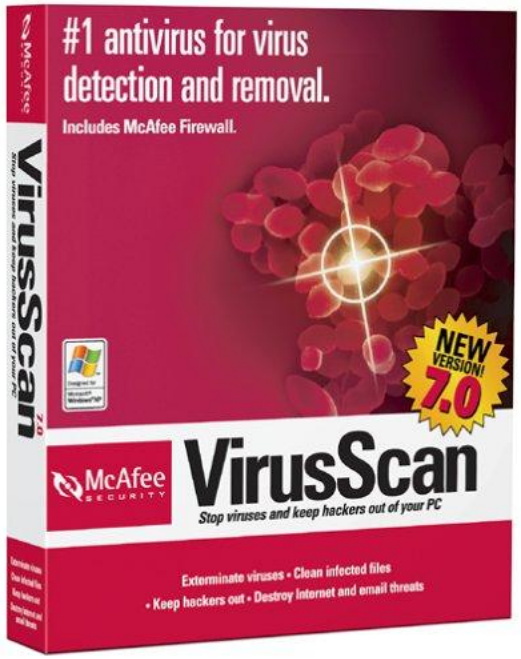
- **สร้างเซิร์ฟเวอร์ลวง (Entrapment Server)**

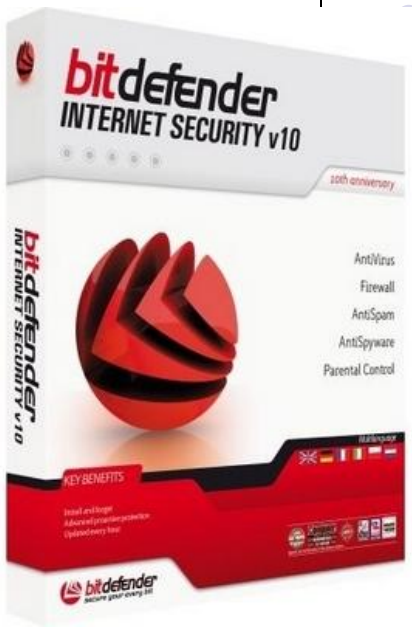
  ใช้ตรวจหาผู้บุกรุกต่อเครือข่ายภายในองค์กร โดยการสร้างเครื่องให้บริการลวง

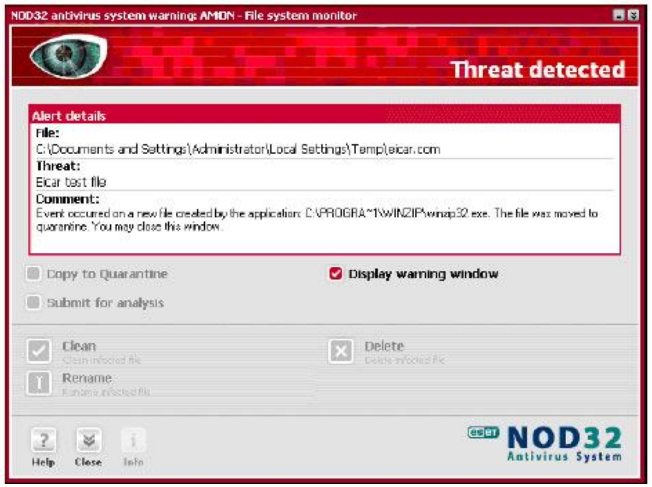
1.4 ป้องกันภัยคุกคามจากไวรัส

- ใช้โปรแกรมป้องกันไวรัส
- ใช้ Anti Virus Card

โปรแกรมตรวจหาหรือทำลายไวรัส







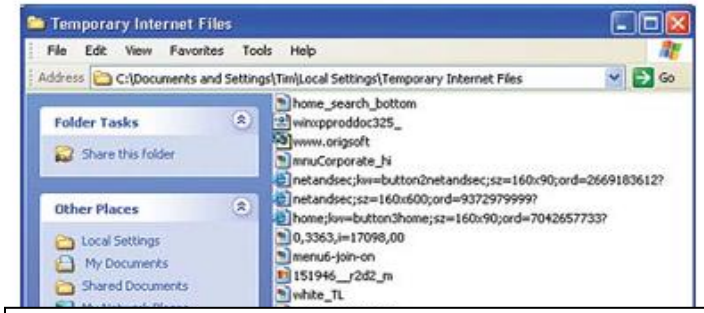
2012 Compare The Best Antivirus Software Products

Displaying 1 to 10 of 25 « Previous 10 | Next 10 »

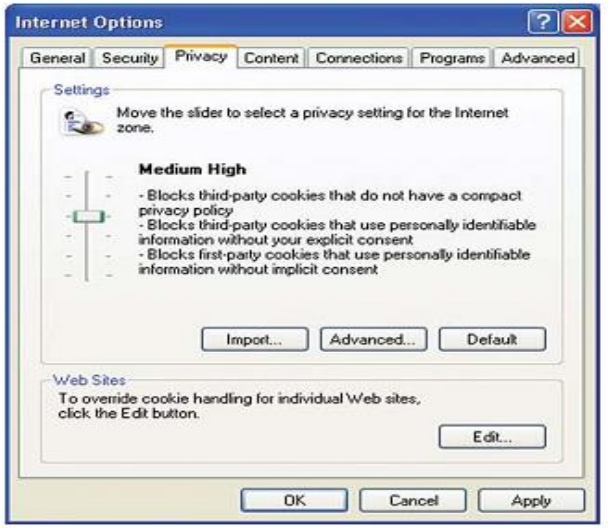
Rank	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
★★★★ Excellent ★★★☆ Very Good ★★☆☆ Good ★☆☆☆ Fair ☆☆☆☆ Poor	Bitdefender Antivirus Plus	Kaspersky Anti-Virus	Panda Antivirus Pro	F-Secure Anti-Virus	AVG Anti-Virus	Avast! Pro Antivirus	G Data AntiVirus	BullGuard Antivirus	Avira AntiVir Premium	ESET NOD32 Antivirus
										
Reviewer Comments	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review
Lowest Price	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now
	$29.95	$59.95	$39.99	$39.99	$34.99	$39.99	$29.95	$29.95	$23.49	$39.99
Overall Rating	★★★★	★★★★	★★★½	★★★½	★★★½	★★★☆	★★★☆	★★★☆	★★★☆	★★★☆
Ratings										
Performance	★★★★	★★★★	★★★½	★★★½	★★★☆	★★★☆	★★★½	★★★☆	★★★☆	★★★☆
Features	★★★★	★★★★	★★★½	★★☆☆	★★★★	★★★★	★★★☆	★★★★	★★★½	★★★★
Help & Support	★★★★	★★★★	★★☆☆	★★★★	★★★★	★★★☆	★★★☆	★★★★	★★★★	★★★☆
Proportion of people who buy the product	92.54%	4.17%	0.79%	0.00%	1.78%	0.49%	0.00%	0.00%	0.00%	0.23%
Special Offers										
Discounts	10% Discount									
Number of PCs Protected										
PCs per License	3	3	3	3	1	1	1	1	1	1
Windows 7 Performance										
Protection Score	100%	100%	83%	92%	83%	83%	92%	75%	67%	58%
Repair Score	83%	75%	92%	83%	58%	42%	75%	50%	67%	42%
Usability Score	92%	83%	83%	83%	92%	83%	67%	75%	75%	83%
Windows XP Performance										
Score	100%	92%	92%	92%	92%	83%	92%	83%	58%	67%

การป้องกันการฝังตัวของคุ้กกี้

1. เลือก Tools จากแถบเมนู
   เลือก Internet Options
2. เลือก Settings จากแท็บ General
   เลือก View files

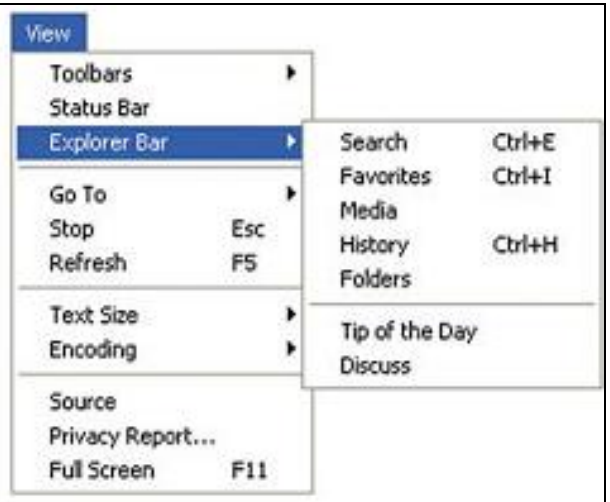


1. เลือก Tools จากเมนูบาร์
   เลือก Internet Options
2. เลือกแท็บ Privacy
   ปรับแถบเลื่อนไปตามระดับการป้องกันที่ต้องการ
   คลิก Apply และ OK

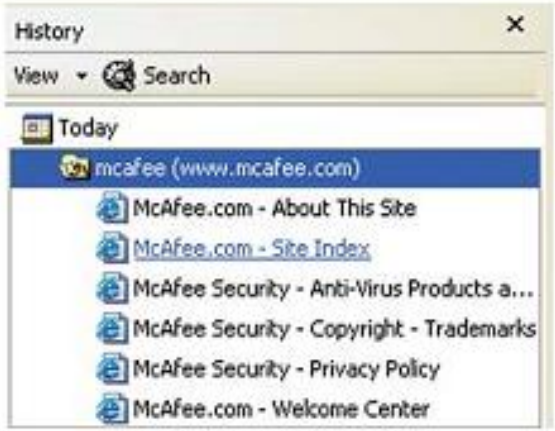


การเรียกดูไฟล์ประวัติ

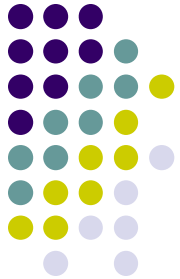
1. คลิกที่ปุ่ม Start
   เลือก view จากแถบเมนู
   เลือก Explorer



2. เลือก History



การควบคุมและรักษาความปลอดภัย



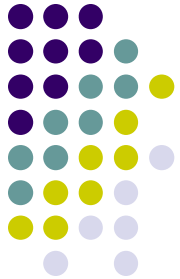
1.5 การใช้นโยบายในการควบคุม (Policies)

หน่วยงานต้องกำหนดให้แน่นอนว่า ผู้ใช้ใดสามารถเข้าถึงข้อมูลส่วนใดได้บ้าง และใครมีสิทธิที่จะเปลี่ยนแปลงแก้ไขข้อมูล รวมถึงต้องกำหนดแผนป้องกันและกู้ภัยที่อาจเกิดขึ้นได้ด้วย

1.6 การป้องกันภัยคุกคามในเครือข่ายไร้สาย (Wireless Security)

- ติดตั้ง Firewall ให้กับ gateway ของเครือข่ายไร้สาย
- เลือกใช้สัญญาณดิจิตอลในการส่งข้อมูลผ่านโทรศัพท์มือถือ

การควบคุมและรักษาความปลอดภัย



2. รักษาความปลอดภัยให้กับข้อมูลที่ส่งผ่านเครือข่าย

2.1 การรักษาความลับของข้อมูล (Confidentiality)

- ใช้เทคนิคการ Encryption

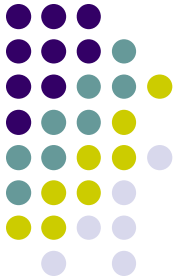
2.2 การรักษาความถูกต้องของข้อมูล (Integrity)

- ใช้เทคนิคที่เรียกว่า Hashing

2.3 การระบุตัวตน (Authentication)

- Digital Signature
- Password
- เครื่องมือตรวจวัดทางกายภาพ

การควบคุมและรักษาความปลอดภัย



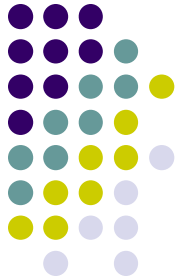
2.4 การป้องกันการปฏิเสธหรืออ้างความรับผิดชอบ (Non-Repudiation)

- Digital Signature
- การบันทึกเวลา
- การรับรองการให้บริการ

2.5 การระบุอำนาจหน้าที่ (Authorization)

- Password
- Firewall
- เครื่องมือตรวจวัดทางกายภาพ

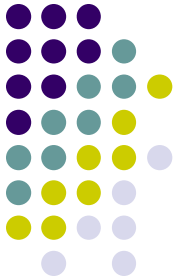
การควบคุมและรักษาความปลอดภัย



ความปลอดภัยของเว็บไซต์สังเกตได้จากหลายๆปัจจัย ดังต่อไปนี้

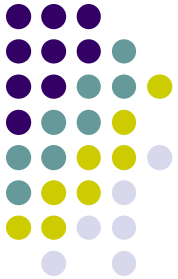
1. ชื่อเสียงของเว็บไซต์
2. เว็บไซต์จะต้องสนับสนุนระบบ SSL (Secure Socket Layer)
3. เว็บไซต์ควรจะได้รับการรับรองเรื่องความปลอดภัย
4. นโยบายส่งเสริมความมั่นใจหลังการขาย

การรักษาความปลอดภัยบนเครือข่ายอินเทอร์เน็ต (Internet Security)



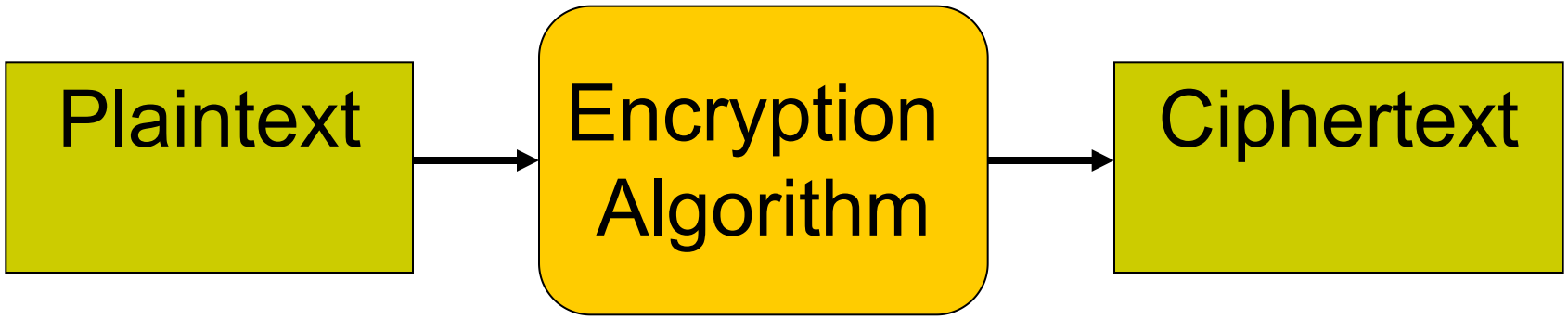
การรักษาความปลอดภัยของข้อมูลที่ส่งผ่านเครือข่ายอินเทอร์เน็ตที่นิยมใช้งานมากที่สุดคือ **“การเข้ารหัส (Encryption)”** โดยเว็บไซต์ที่ใช้วิธีการเข้ารหัสเพื่อป้องกันข้อมูลจะใช้ Digital Certification ร่วมกับ Security Protocal เพื่อทำให้มีความปลอดภัยสูงขึ้น

การเข้ารหัส (Encryption)

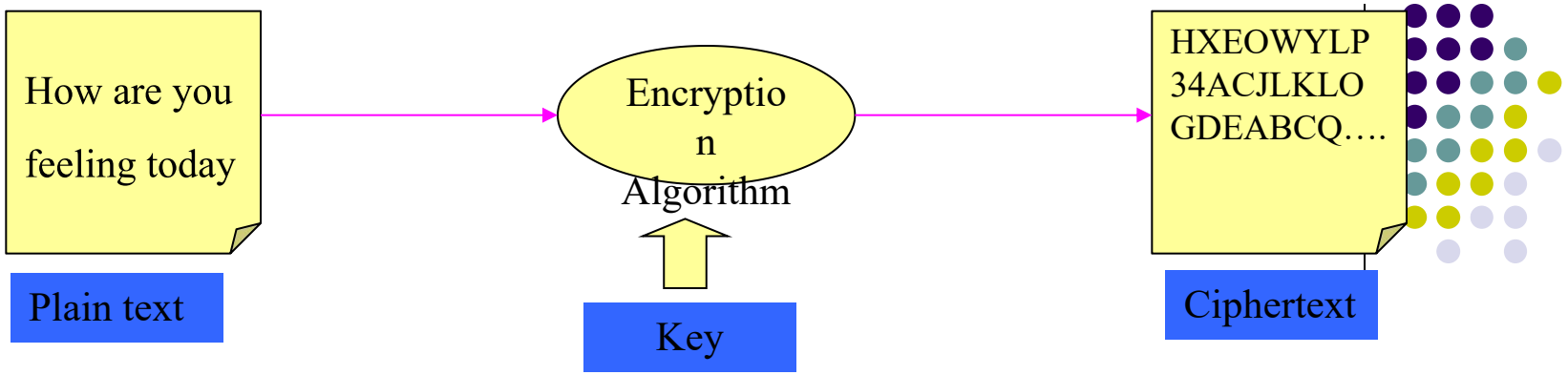


การเข้ารหัสเป็นวิธีป้องกันข้อมูลจากการโจรกรรมในขณะที่มีการรับและส่งข้อมูลผ่านทางเครือข่าย โดยข้อมูลทั้งหมดจะถูกแปลงเป็นรหัสที่ไม่สามารถอ่านได้ด้วยวิธีปกติ เรียกว่า **การเข้ารหัส(Encryption)** ดังนั้น แม้ว่าจะมีการโจรกรรมข้อมูลไปได้ แต่หากไม่สามารถ**ถอดรหัส (Decryption)** ก็ไม่สามารถเข้าใจข้อมูลเหล่านั้นได้

การเข้ารหัส (Encryption)

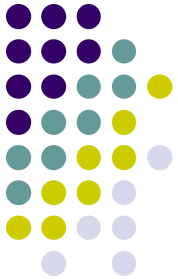


แสดงการเข้ารหัส



- คริพโตกราฟี (Cryptography)
  - Plain text คือ ข้อมูลต้นฉบับซึ่งเป็นข้อความที่สามารถอ่านแล้วเข้าใจ
  - Encryption Algorithm คือ ขั้นตอนวิธีในโปรแกรมคอมพิวเตอร์ที่ใช้ในการแปลงข้อมูลต้นฉบับเป็นข้อมูลที่ได้รับการเข้ารหัส
  - Ciphertext คือ ข้อมูลหรือข่าวสารที่ได้รับการเข้ารหัส ทำให้อ่านไม่รู้เรื่อง
  - Key คือ เป็นกุญแจที่ใช้ร่วมกับ อัลกอริทึมในการเข้ารหัส และถอดรหัส

การเข้ารหัส (Encryption)



มีด้วยกัน 2 ลักษณะ คือ

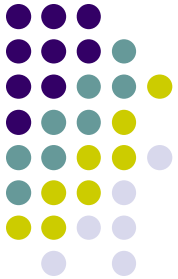
1. การเข้ารหัสแบบสมมาตร (Symmetric Encryption)

วิธีนี้ทั้งผู้รับและผู้ส่งข้อความจะทราบคีย์ที่เหมือนกันทั้งสองฝ่ายในการรับหรือส่งข้อความ

2. การเข้ารหัสแบบไม่สมมาตร (Asymmetric Encryption)

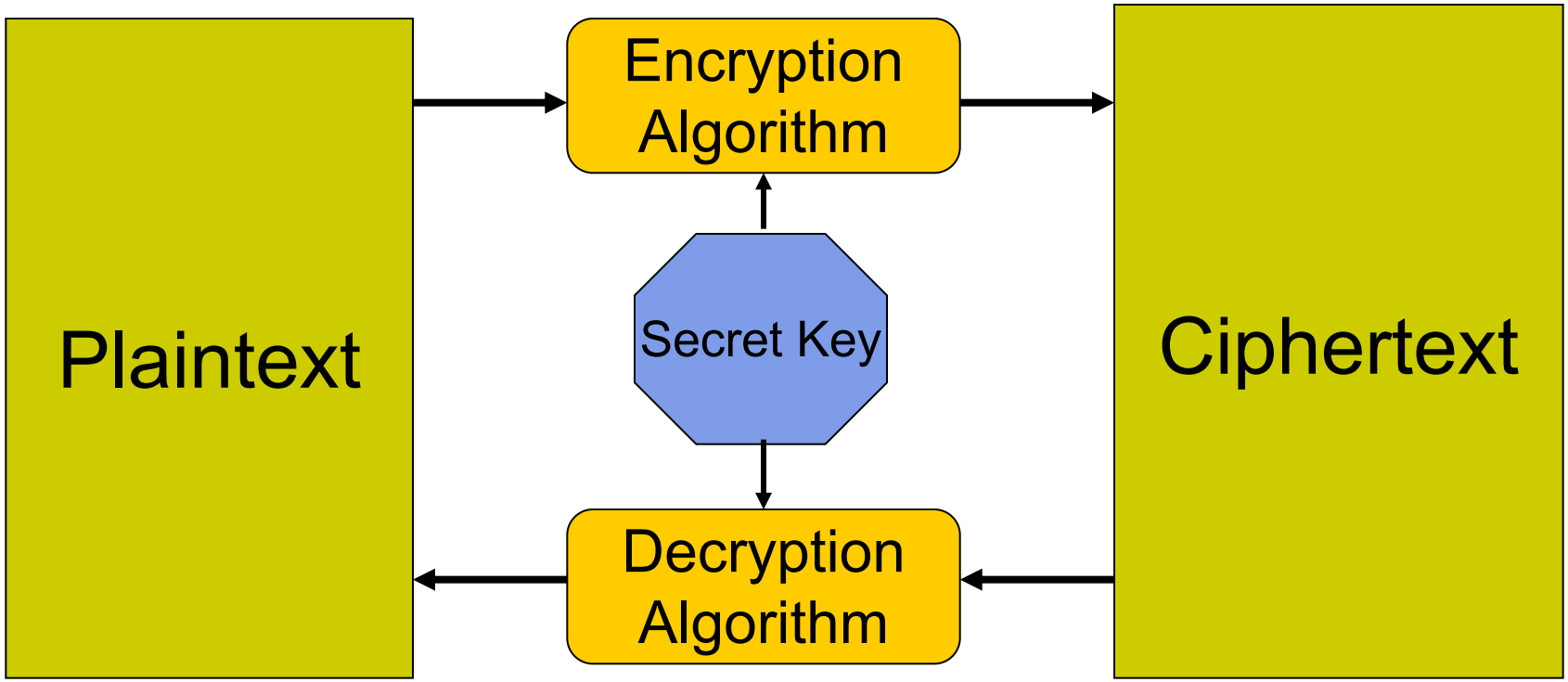
ใช้แนวคิดของการมีคีย์เป็นคู่ ๆ ที่สามารถเข้าและถอดรหัสของกันและกันเท่านั้นได้ โดยคีย์แรกจะมีอยู่ที่เฉพาะเจ้าของคีย์ เรียกว่า Private key และคู่ของคีย์ดังกล่าวที่ส่งให้ผู้อื่นใช้ เรียกว่า Public key

1. การเข้ารหัสแบบสมมาตร (Symmetric Encryption)



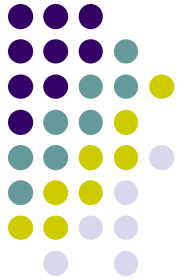
- **การเข้ารหัสแบบสมมาตร (Symmetric Encryption)**
  - เป็นการใช้อัลกอลิทึม หรือกุญแจในการเข้ารหัสดอกเดียวกัน ทั้งฝ่ายรับและฝ่ายส่ง
  - วิธีนี้ ทั้งผู้รับและผู้ส่งข้อความจะทราบคีย์ที่เหมือนกันทั้งสองฝ่ายในการรับหรือส่งข้อความ
  - ซึ่งหากมีขโมยนำกุญแจดอกนี้ไปได้ ก็สามารถถอดรหัสข้อมูลของเราได้

การเข้ารหัสแบบสมมาตร (Symmetric Encryption)



แสดงการเข้ารหัสแบบทางเดียวด้วยกุญแจลับ (Secret key encryption)

การเข้ารหัสแบบสมมาตร Symmetric Encryption



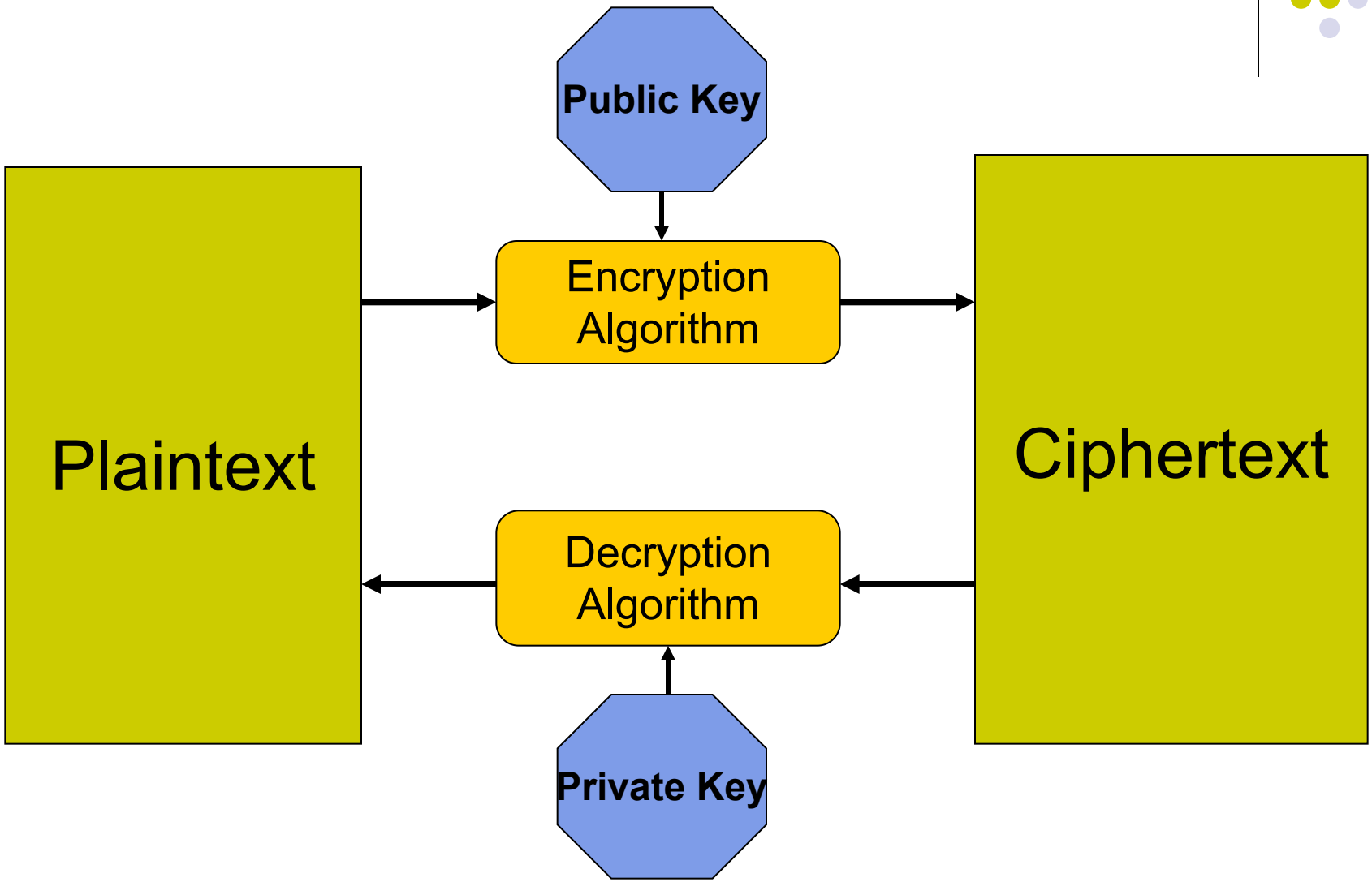
การเข้ารหัสแบบสมมาตรนี้ ก่อให้เกิดปัญหา 2 ส่วน คือ

- **ปัญหา Authentication** เนื่องจากผู้อื่นอาจทราบรหัสลับด้วยวิธีใดก็ตามแล้วปลอมตัวเข้ามาส่งข้อความถึงเรา
- **ปัญหา Non-repudiation** คือ ไม่มีหลักฐานใดที่พิสูจน์ได้ว่าผู้ส่งหรือผู้รับได้กระทำรายการจริง ๆ

2. การเข้ารหัสแบบไม่สมมาตร (Asymmetric Encryption)

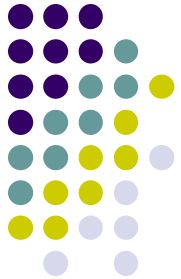
- **การเข้ารหัสแบบไม่สมมาตร (Asymmetric Encryption)**
  - ใช้แนวคิดของการมีคีย์เป็นคู่ ๆ ที่สามารถเข้าและถอดรหัสของกันและกันเท่านั้นประกอบด้วย กุญแจ 2 ดอก คือ
    - กุญแจสาธารณะ (Public key) ใช้สำหรับการเข้ารหัส
    - กุญแจส่วนตัว (Private key) ใช้สำหรับการถอดรหัส
  - ที่สำคัญกุญแจที่เข้ารหัสจะนำมาถอดรหัสไม่ได้ ซึ่ง Public key จะแจกจ่ายไปยังบุคคลต่างๆ ที่ต้องการสื่อสาร ส่วน Private Key จะเก็บไว้ส่วนตัวไม่เผยแพร่ให้ใคร

การเข้ารหัสแบบไม่สมมาตร (Asymmetric Encryption)



แสดงการเข้ารหัสด้วยกุญแจสาธารณะ(Public key)

การเข้ารหัสแบบไม่สมมาตร (Asymmetric Encryption)



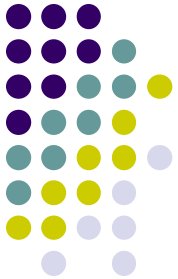
ประโยชน์ของระบบการเข้ารหัสแบบไม่สมมาตร มีดังนี้

1. ใช้รักษาความลับของข้อความที่จะจัดส่งไป

2. แก้ปัญหาการ Authenticate คือ ตรวจสอบว่าบุคคลที่ส่งข้อความเข้ามาเป็นผู้ส่งเองจริง ๆ ซึ่งทำได้โดยใช้วิธีการเข้ารหัสด้วยคีย์ส่วนตัว

** การใช้คีย์ส่วนตัวเข้ารหัสข้อความเปรียบได้กับการเซ็นชื่อของเราบนเอกสารที่เป็นกระดาษเพื่อรับรองว่าข้อความนี้เราเป็นผู้ส่งจริง

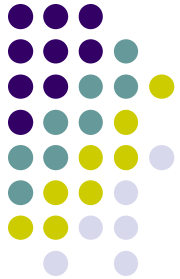
การรักษาความปลอดภัยบนเครือข่ายอินเทอร์เน็ต (Internet Security)



การรักษาความปลอดภัยของข้อมูลที่ส่งผ่านเครือข่ายอินเทอร์เน็ตที่นิยมใช้งานมากที่สุดคือ **“การเข้ารหัส (Encryption)”** โดยเว็บไซต์ที่ใช้วิธีการเข้ารหัสเพื่อป้องกันข้อมูลจะใช้ Digital Certification ร่วมกับ Security Protocal เพื่อทำให้มีความปลอดภัยสูงขึ้น โดยโปรโตคอลที่นิยมใช้งานมี 3 ชนิด คือ

- **Secure Socket Layer (SSL)**
- **Secure Hypertext Transport Protcocal S-HTTP**
- **Secure Electronic Transaction (SET)**

SSL (Secure Socket Layer)



เป็นโปรโตคอลที่พัฒนาโดย Netscape ใช้สำหรับตรวจสอบและเข้ารหัสด้วยกุญแจสาธารณะแก่ข้อมูล ก่อนที่ข้อมูลจะถูกส่งออกไปบนเครือข่ายอินเทอร์เน็ต โดยจะนำข้อมูลมาเข้ารหัสและถอดรหัสด้วยเทคนิค Cryptography และใบรับรองอิเล็กทรอนิกส์(Digital Certificates) และมีการทำงานที่ TCP/IP จะใช้ SSL ในการทำระบบรักษาความปลอดภัย

ส่วนการใช้งานในเว็บไซต์ เมื่อผู้ใช้ต้องการติดต่อมายัง Server ผู้ใช้จะต้องทำการเรียก Web Browser โดยในช่อง URL จะมีโปรโตคอลเป็น **https://** แทน **http://** เป็นตัวบอกว่าต้องการใช้ SSL ในการติดต่อ Server

SSL (Secure Socket Layer)

เราจะทราบได้อย่างไรว่าเว็บไซต์ที่เราเข้าไปเยี่ยมชมนั้นเป็นระบบ SSL หรือไม่ก็คงต้องสังเกตจาก Icon Security หรือ URL ที่แสดงผลอยู่บนเว็บบราวเซอร์

โดยกลไกการรักษาความปลอดภัย มีดังนี้

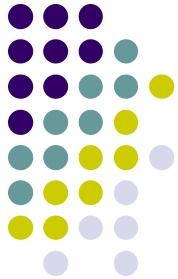
1) ความปลอดภัยของข้อความ (Message Privacy)

2) ความสมบูรณ์ของข้อความ (Message Integrity)

3) ความน่าเชื่อถือ (Matual Authentication)

4) ใบรับรองดิจิตอล (Digital Certificate)

Secure Hypertext Transport Protocal S-HTTP

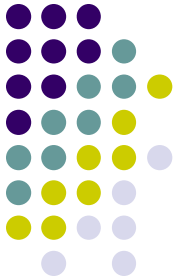


เป็นส่วนของโปรโตคอล HTTP ทำหน้าที่ตรวจสอบสิทธิผู้ใช้ ซึ่งจะเข้ารหัสการลง **Digital Signature**

ระบบนี้จะอนุญาตให้ผู้ใช้และเครื่องให้บริการติดต่อกันได้เมื่อทั้ง 2 ฝ่ายมี Digital Certificate

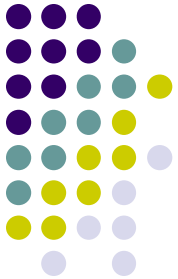
ระบบรักษาความปลอดภัยรูปแบบนี้ยุ่งยากกว่า SSL แต่มีความปลอดภัยมากกว่า นิยมใช้ในธุรกิจการเงิน

ระบบ *Secure Electronic Transaction* (SET)



ระบบ SET หรือ Secure Electronic Transaction เป็นระบบเพื่อใช้สำหรับตรวจสอบการชำระเงินด้วยบัตรเครดิตอย่างปลอดภัยบนอินเทอร์เน็ต ซึ่งได้รับการสนับสนุนเริ่มต้นโดย MasterCard, Visa, Microsoft, Netscape และ อื่น ๆ ด้วยการสร้างรหัส SET ซึ่งเป็นการเข้ารหัสด้วยกุญแจสาธารณะ

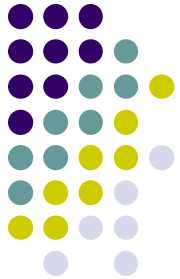
ระบบ *Secure Electronic Transaction* (SET)



ระบบ SET นี้ถูกออกแบบมาเพื่อใช้กับกิจกรรมการทำพาณิชย์-อิเล็กทรอนิกส์ โดยระบบนี้สามารถรักษาความลับของข้อมูลข่าวสารที่ถูกส่งผ่านระบบเครือข่ายคอมพิวเตอร์ได้เป็นอย่างดี และรับประกันความถูกต้องโดยไม่มีการปลอมแปลงของข้อมูลที่เกี่ยวกับการเบิกจ่ายเงินได้เป็นอย่างดีด้วย

นอกจากนี้ยังสามารถที่จะบ่งชี้ชัดได้ว่าใครเป็นผู้ซื้อและผู้ค้าได้อย่างถูกต้องโดยไม่มีการปลอมแปลง

เปรียบเทียบ SET กับ SSL



ระบบ SET

ข้อดี

1. ใช้วิธีการเข้ารหัสลับที่ดีกว่าจึงให้ความปลอดภัยสูงกว่า
2. ร้านค้าสามารถพิสูจน์ทราบลูกค้าได้ทันทีว่าเป็นผู้ได้รับอนุญาตในระบบหรือไม่และมีเครดิตเพียงพอในการซื้อหรือไม่
3. สามารถปกปิดความลับหรือข้อมูลการทำธุรกิจของลูกค้าจากร้านค้าและจากธนาคารผู้ออกบัตรได้

ข้อเสีย

1. ยังไม่มีการทดสอบและทดลองใช้อย่างเพียงพอ
2. ยังไม่มีการนำไปใช้เชิงธุรกิจในวงกว้างมากนัก

ระบบ SSL

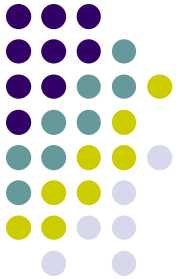
ข้อดี

1. ลงทุนน้อยหรือแทบไม่มีเลย เพราะปัจจุบันใช้ในวงกว้าง
2. สามารถควบคุมการเข้าถึงข้อมูลส่วนต่าง ๆ ภายในระบบของผู้ใช้ได้หลังจากที่ผู้ใช้ได้รับอนุญาตให้เข้ามาในระบบ
3. สามารถใช้ข้อมูลร่วมกันได้ระหว่างสองจุด
4. มีระบบป้องกันและตรวจสอบความถูกต้องของข้อมูลได้

ข้อเสีย

1. ใช้วิธีการเข้ารหัสที่ล้าสมัย ความปลอดภัยไม่เพียงพอ
2. ทำการสื่อสารอย่างปลอดภัยได้เพียงสองจุด แต่ระบบพาณิชย์อิเล็กทรอนิกส์ที่ใช้บัตรต้องใช้มากกว่าสองจุดในเวลาเดียวกัน
3. มีความเสี่ยงสูงเนื่องจากไม่มีการรับรองทางอิเล็กทรอนิกส์ระหว่างทุกฝ่ายที่ทำการซื้อขายในขณะนั้น และความเสี่ยงในการรั่วไหลของข้อมูลลูกค้า

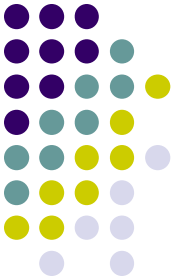
ลายเซ็นดิจิตอล (Digital Signature)



ลายเซ็นดิจิตอล หรือ ลายเซ็นอิเล็กทรอนิกส์ (Electronic Signature)

เป็นข้อมูลที่แนบไปกับข้อความที่ส่งไป เพื่อเป็นการแสดงตัวตน (Authentication) ว่าผู้ส่งข้อความเป็นใคร ใช้กับการพิสูจน์ความถูกต้องของเอกสารตามกฎหมาย เช่น ด้านการเงิน การทำสัญญา และเอกสารอื่นๆ ว่าเป็นของแท้นั้น สามารถทำได้โดยการตรวจสอบความถูกต้องของลายเซ็นของผู้มีอำนาจอนุมัติ

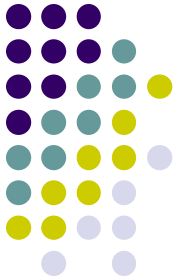
ลายเซ็นดิจิตอล (Digital Signature)



ข้อความที่ประทับลายเซ็นไปยังอีกฝ่ายหนึ่งในลักษณะต่อไปนี้

1. ผู้รับสามารถพิสูจน์เอกลักษณ์ของผู้ที่อ้างนั้นว่าเป็นคนส่งข่าวสารจริงๆ
2. ผู้ส่งไม่สามารถบอกปัดสิ่งที่เขียนลงไปในข้อความ
3. ผู้รับไม่สามารถที่จะประกอบและเปลี่ยนแปลงข้อความที่ตนส่งมาด้วยตนเองได้

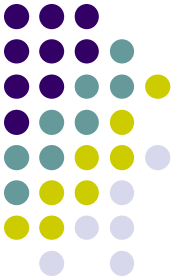
ลายเซ็นดิจิตอล (Digital Signature)



- ประโยชน์ของลายเซ็นดิจิตอล (Digital signature) มีดังนี้

  1. ยากแก่การปลอมแปลงลายเซ็น
  2. ข้อความในเอกสารไม่ถูกลักลอบอ่านและแก้ไข
  3. ระยะทางไม่เป็นอุปสรรคในการตรวจสอบความถูกต้อง
  4. สำเนาของเอกสารมีสถานะเทียบเท่ากับเอกสารต้นฉบับ
  5. มีบุคคลที่สาม (Certifies) หรือองค์กรกลาง [Certification Authority (CA)] เป็นผู้รับรองความถูกต้องของลายเซ็น (Certificate)

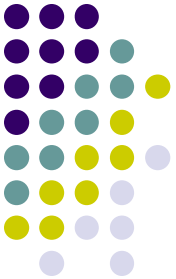
ใบรับรองอิเล็กทรอนิกส์ -Certification Authority (CA)



- **Certification Authority (CA) คืออะไร มีหน้าที่อย่างไร**
- CA หรือ Certificate Authority คือผู้ประกอบกิจการ ออกใบรับรองอิเล็กทรอนิกส์ และเป็นที่เชื่อถือ ซึ่งเปรียบเสมือนบัตรประจำตัวที่ใช้ในการระบุตัวบุคคล ซึ่งใบรับรองอิเล็กทรอนิกส์ดังกล่าวนั้น จะถูกนำมาใช้ในการยืนยันตัวบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์เพื่อสร้างให้เกิดความมั่นใจ และเพิ่มความปลอดภัยของข้อมูล โดยอาศัยเทคโนโลยีที่เรียกว่าเทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure - PKI)

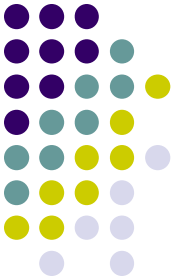
ทำไมต้องใช้ใบรับรองอิเล็กทรอนิกส์

Certification Authority (CA)

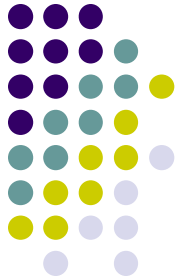


- ตัวอย่างเช่น การที่เรารับอีเมล์จากบุคคลหนึ่งๆ จะเป็นเพื่อนหรือใครก็ตาม เราจะสามารถมั่นใจได้อย่างไรว่าอีเมล์ที่เราได้รับไม่ได้ถูกปลอมแปลง หรือถูกแก้ไขให้บิดเบือนไปในระหว่างทางที่ส่งมาถึงเรา หรือถูกดักอ่านข้อความระหว่างทางที่ส่งไปยังผู้รับ

ทำไมต้องใช้ใบรับรองอิเล็กทรอนิกส์ Certification Authority (CA)



- การใช้ใบรับรองอิเล็กทรอนิกส์ ผู้ใช้จะสามารถมั่นใจได้ว่า
  - ข้อมูลต่างๆ ที่ได้รับมีความถูกต้อง ครบถ้วน ไม่ถูกเปลี่ยนแปลงแก้ไข
  - สามารถพิสูจน์ และยืนยันตัวบุคคลได้ ว่าเป็นบุคคลผู้ที่เราติดต่อด้วยจริง
  - สามารถรักษาความลับของข้อมูลได้ หากเป็นข้อมูลที่ต้องการให้ผู้รับเท่านั้นที่สามารถอ่านอีเมล์ฉบับนั้นๆได้ ซึ่งกรณีนี้จะต้องมีการใช้ใบรับรองอิเล็กทรอนิกส์ในการเข้ารหัสก่อนทำการส่งอีเมล์ไปยังผู้รับ



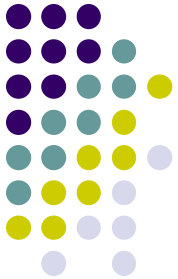
ตัวอย่างองค์กรที่ใช้ CA

- http://www.ca.tot.co.th/faq.php

ทดลองสมัครและติดตั้งใบรับรองอิเล็กทรอนิกส์สำหรับบุคคล

http://gca.thaigov.net/

แบบฝึกหัด



1. Hacker กับ Cracker แตกต่างกันอย่างไร
2. ให้นักศึกษาหาชื่อไวรัสคอมพิวเตอร์ในปัจจุบันมาอย่างน้อย 3 โปรแกรม โดยให้ระบุอาการของเครื่องเมื่อถูกไวรัสดังกล่าวเข้าสู่ระบบ
3. จงอธิบายการควบคุมและรักษาความปลอดภัยแบบ Biometrics
4. การเข้ารหัสแบบสมมาตร กับ การเข้ารหัสแบบไม่สมมาตร แตกต่างกันอย่างไร
5. โปรโตคอล SET ใช้รักษาความปลอดภัยให้กับสิ่งใด และมีข้อดีอย่างไร
6. เหตุใดจึงควรใช้ลายเซ็นดิจิตอลในการส่งข้อความไปให้กับผู้รับ