# บทที่ 5 : การประยุกต์ใช้คริพโตกราฟี

## สธ412 ความมั่นคงของระบบสารสนเทศ

อาจารย์อภิพงศ์ ปิงยศ

apipong.ping@gmail.com

# ทบทวนการเข้ารหัสข้อมูล

- Secret Key Cryptography หรือ Symmetric Key
- Public Key Cryptography หรือ Asymmetric Key
- Hash Function ใช้ตรวจสอบความครบถ้วนของข้อมูล
- Steganography การอำพรางข้อมูล

# การประยุกต์ใช้

- Authentication
  - Password
  - Kerberos
- Mail Security
  - PGP
  - S/MIME

# Authentication


- **การพิสูจน์ทราบตัวตน (Authentication)** เป็นการยืนยันว่าสิ่งนั้นหรือคนนั้นคือของจริงไม่ใช่การลอกเลียนแบบ
- การพิสูจน์ตัวตนในรูปแบบดิจิตอล เช่น การล็อกอินเข้าสู่ระบบ ผู้ที่สื่อสารอาจเป็นผู้ใช้ คอมพิวเตอร์ หรืออาจเป็นโปรแกรมก็ได้

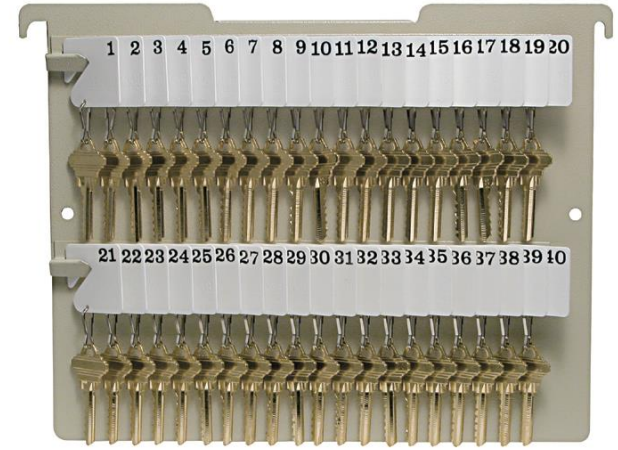
# Authentication : Password


- เกือบทุกระบบคอมพิวเตอร์ในปัจจุบันจะใช้รหัสผ่านเป็นอย่างน้อยในการป้องกันและพิสูจน์ทราบตัวตนผู้ที่จะล็อกอินเข้าใช้งานระบบ
- โดยทั่วไปรหัสผ่านมักจะไม่เก็บไว้ในรูปแบบเพลนเท็กซ์ แต่จะถูกเข้ารหัสไว้โดยอัลกอริทึมบางอย่าง เช่น Hash เพื่อไม่ให้ถูกขโมยไปได้อย่างง่ายดาย
- การแลกเปลี่ยนรหัสผ่านในเครือข่าย ปกติจะต้องมีการเข้ารหัสก่อนส่งผ่านเครือข่าย เพื่อป้องกันการถูกดักจับรหัสผ่าน

# Authentication : Kerberos


- **Kerberos (เคอร์เบรอส)** เป็นโปรโตคอลสำหรับ Authentication ก่อนที่จะมีการสื่อสารผ่านเครือข่ายระหว่างกัน
- ใช้การเข้ารหัสแบบ**ซีเคร็ทคีย์**
- ออกแบบและพัฒนาที่ Massachusetts Institute of Technology (MIT)

# Authentication : Kerberos [2]




- เป็นสถาปัตยกรรมแบบไคลเอนต์/เซิร์ฟเวอร์
- ทุก ๆ โฮสต์ที่อยู่บนเครือข่ายจะต้องมีซีเคร็ทคีย์เป็นของตนเอง
- ใช้ KDC (Key Distribution Center) เป็นศูนย์กลางหรือเซิร์ฟเวอร์ที่ทำหน้าที่จัดการและเก็บคีย์ของทุก ๆ โฮสต์ที่อยู่บนเครือข่ายเอาไว้
- หน้าที่ของ KDC มีสองแบบคือ AS (Authentication Server) และ TGS (Ticket-Granting Server)

# Authentication : Kerberos [3]

- ที่เปรียบเทียบกับสุนัข 3 หัว เพราะโปรโตคอลนี้ประกอบไปด้วย 3 ส่วน คือ
- หัวที่ 1 คือ Client
- หัวที่ 2 คือ Server
- หัวที่ 3 คือ KDC

# Kerberos Architecture



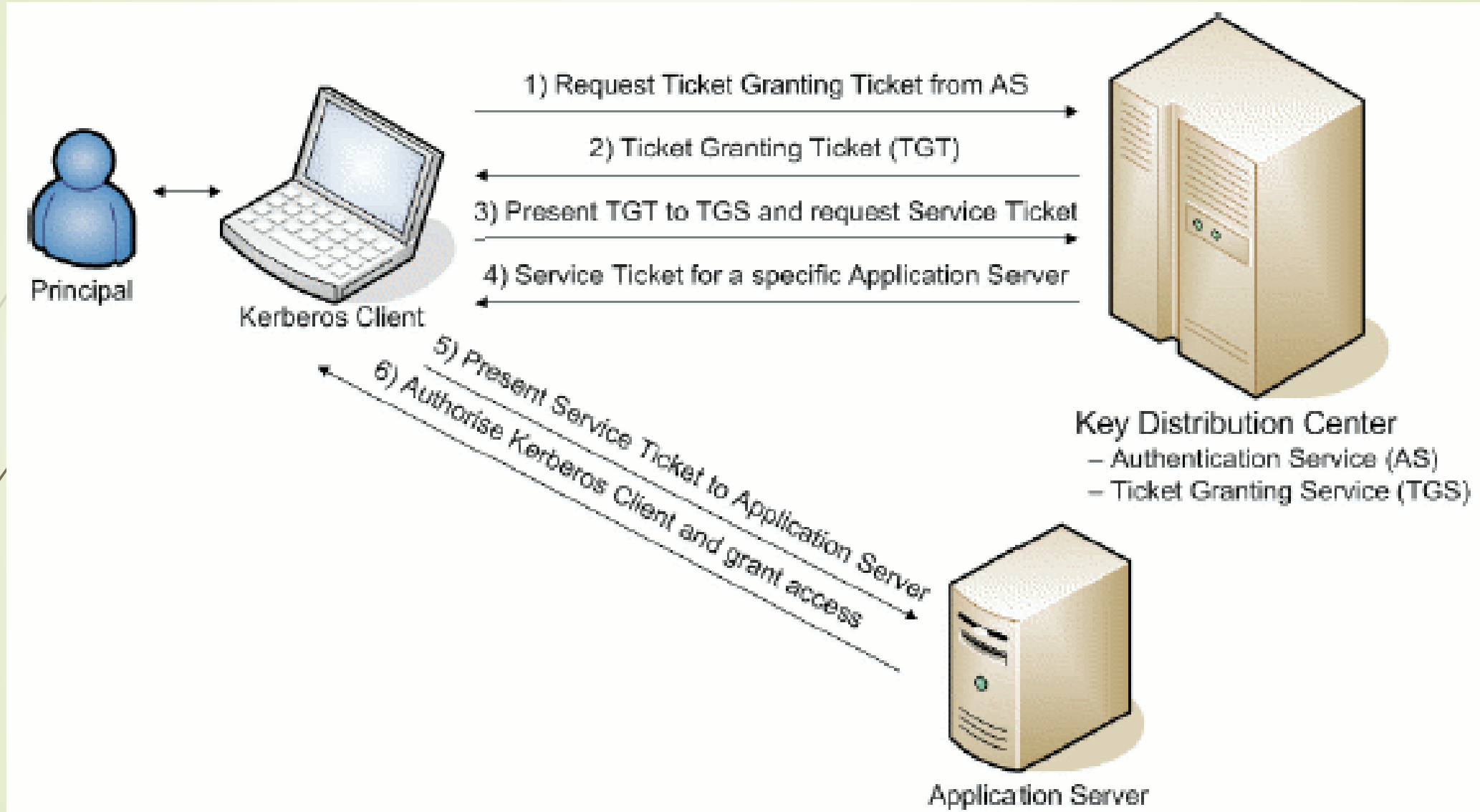



Figure 1: Java Kerberos System Architecture

# Mail Security

- การรับส่งอีเมลปกติจะไม่มีการเข้ารหัสข้อมูล ไม่ว่าจะใช้โปรโตคอลใดก็ตาม
- ในอดีตหากผู้ใช้ต้องการปกปิดข้อความในเมล ก็เป็นหน้าที่ของผู้ใช้เองที่ต้องหาทางปกปิดข้อมูลเหล่านั้น แต่ปัจจุบันผู้ให้บริการเมลมีการเข้ารหัสให้โดยอัตโนมัติแล้ว
- โปรโตคอลที่นิยมในการเข้ารหัสอีเมล์ เช่น PGP, S/MIME

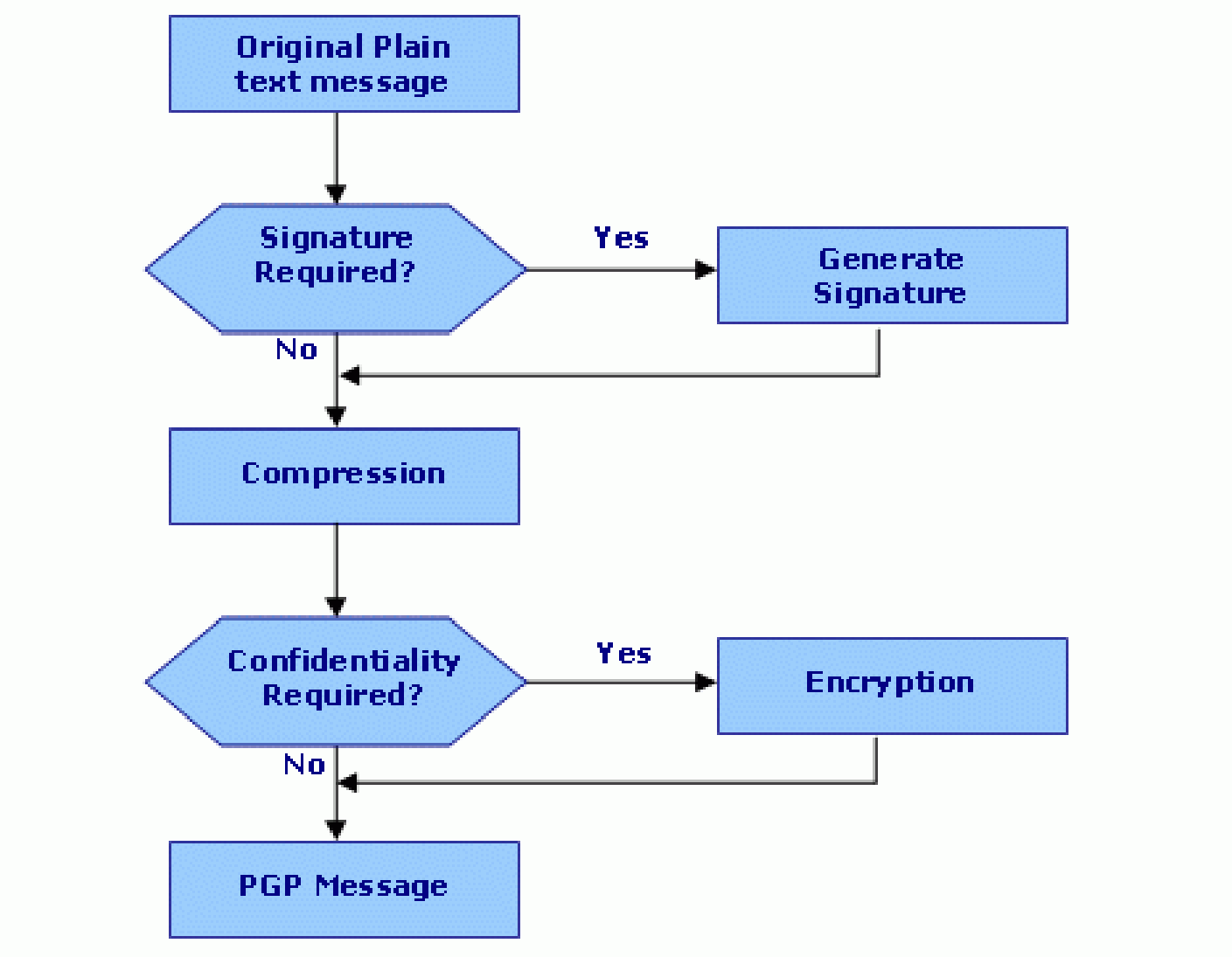
# Mail Security : PGP


- PGP (Pretty Good Privacy) เป็นวิธีการที่นิยมอย่างมากสำหรับการเข้ารหัสอีเมลที่มีความลับ
- ใช้วิธีการเข้ารหัสแบบพับลิกคีย์ โดยไคลเอนต์จะต้องเก็บพับลิกคีย์ซึ่งเป็นที่รู้จักโดยทั่วไปและเชื่อถือได้เอาไว้
- ถ้าอลิสต้องการพับลิกคีย์ของบ็อบ สามารถถามบ็อบผ่านทางอีเมล หรือโดยส่วนใหญ่จะดาวน์โหลดจากเซิฟเวอร์ที่ประกาศเอาไว้ล่วงหน้า

# Mail Security : PGP [2]

- PGP อาจถือได้ว่าเป็นการเข้ารหัสข้อมูลแบบลูกผสมครั้งแรก โดยใช้ทั้งซีเคร็ทคีย์และพับลิกคีย์
- เนื่องจากประสิทธิภาพของคอมพิวเตอร์ในยุคแรกไม่เพียงพอต่อการเข้ารหัสข้อความอีเมลลด้วยพับลิกคีย์ ดังนั้นจึงใช้ซีเคร็ทคีย์เข้ารหัสข้อความ และใช้พับลิกคีย์ในการเข้ารหัสคีย์ให้กลายเป็นเซสชันคีย์อีกทีหนึ่ง
- แต่ในปัจจุบันสามารถใช้พับลิกคีย์เข้ารหัสข้อความโดยตรงได้

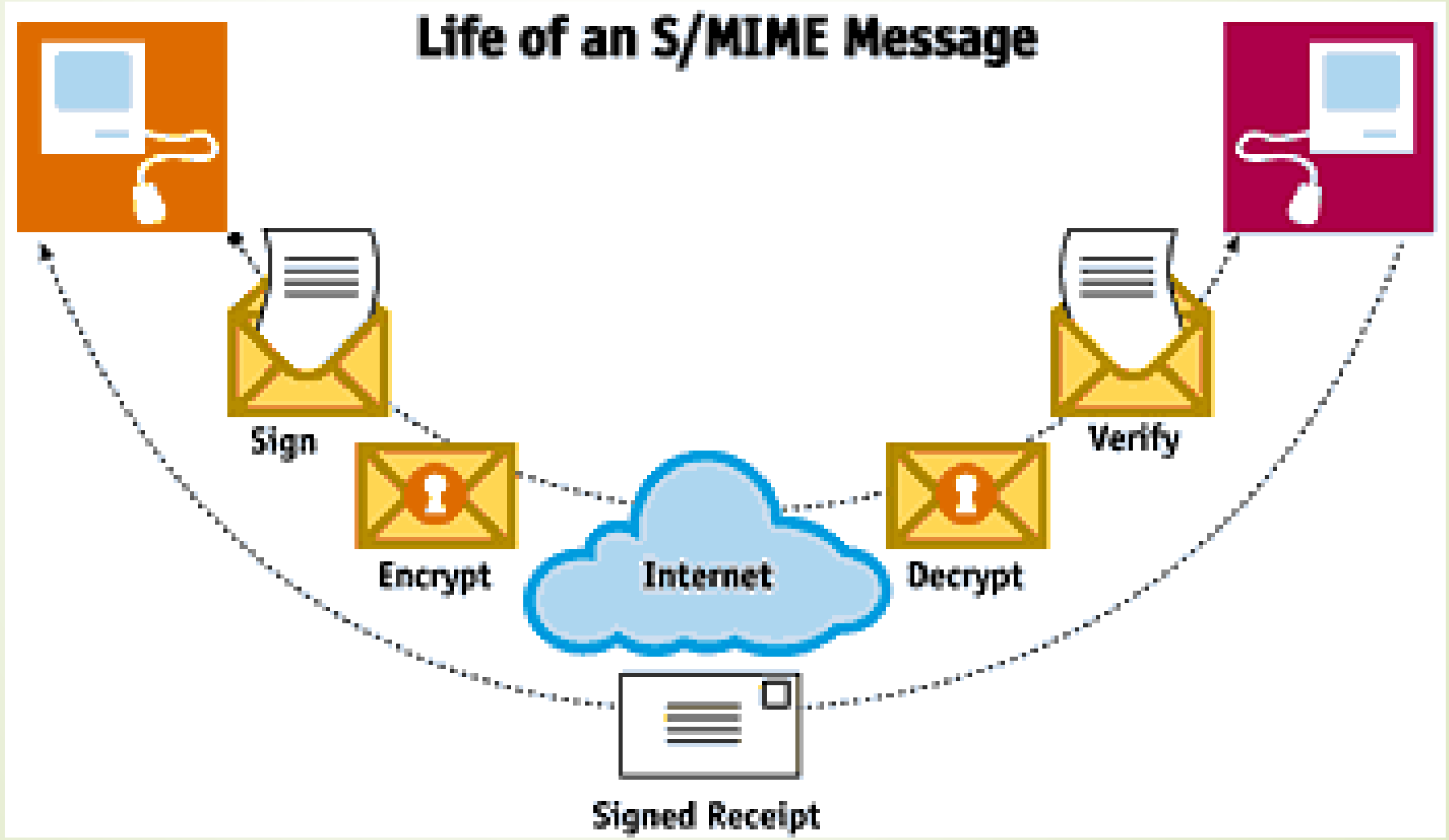
# PGP Architecture



# Mail Security : S/MIME

- **S/MIME (Secure / Multipurpose Internet Main Extensions)** เป็นมาตรฐานการเข้ารหัสเมลแบบพับลิกคีย์ และใช้ลายเซ็นดิจิตอลเพิ่มเติมเข้าไป
- ฟังก์ชันการทำงานของ S/MIME ได้ประยุกต์เข้ากับโปรแกรมอีเมลที่ใช้งานทั่วไป เช่น Outlook เป็นต้น (Native Encryption)

# การทำงานของ S/MIME อย่างง่าย [1]



# การทำงานของ S/MIME ในระบบไคลเอนต์/เซิร์ฟเวอร์