บทที่ 4 : Cryptography & Steganography Part3

สธ412 ความมั่นคงของระบบสารสนเทศ

อาจารย์อภิพงศ์ ปิงยศ

apipong.ping@gmail.com

Agenda

Digital Certificate

Hash Functions

Digital Envelope

Steganography

Digital Certificate

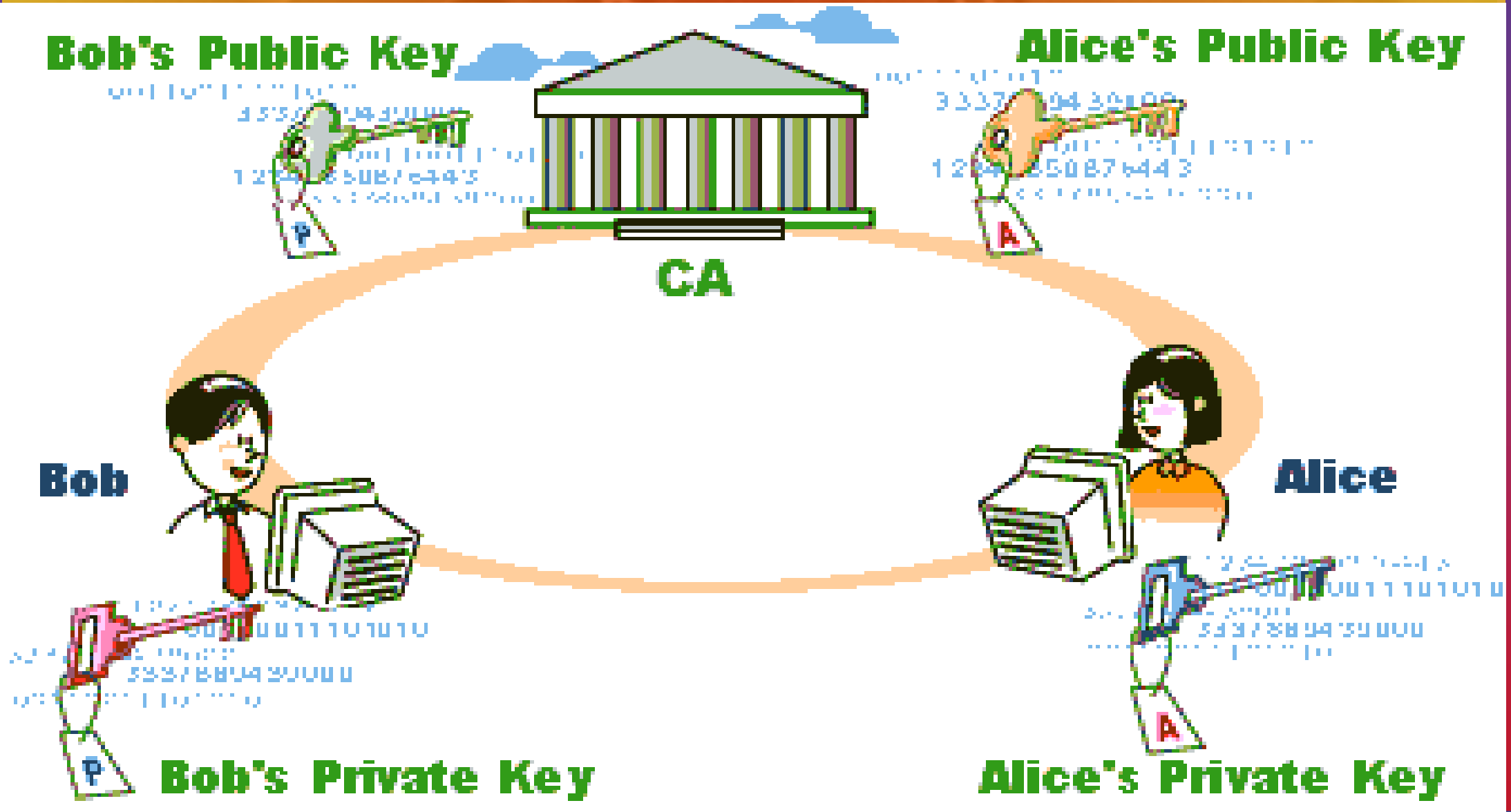
- การรักษาความปลอดภัยไม่ได้ขึ้นอยู่กับอัลกอริทึม และคีย์ที่ใช้เข้ารหัสเท่านั้น แต่ขึ้นอยู่กับการสร้าง แจกจ่าย และจัดการคีย์ด้วย
- **จุดอ่อนของการใช้คีย์**คือจะแน่ใจได้อย่างไรว่าคีย์ที่ได้มาไม่ได้เป็นคีย์ของบุคคลที่สาม

Digital Certificate

แก้ปัญหาโดย

- **ซีเคร็ทคีย์**จะใช้ **Key Distribution Center (KDC)** ซึ่งทำหน้าที่แจกจ่ายคีย์อย่างปลอดภัย เช่นในระบบ Kerberos
- **พับลิกคีย์จะ**ให้ความไว้วางใจกับระบบจัดการคีย์ Public Key Infrastructure (PKI) โดยมี **Certificate Authority (CA)** เป็นผู้รับรอง Digital Certificate

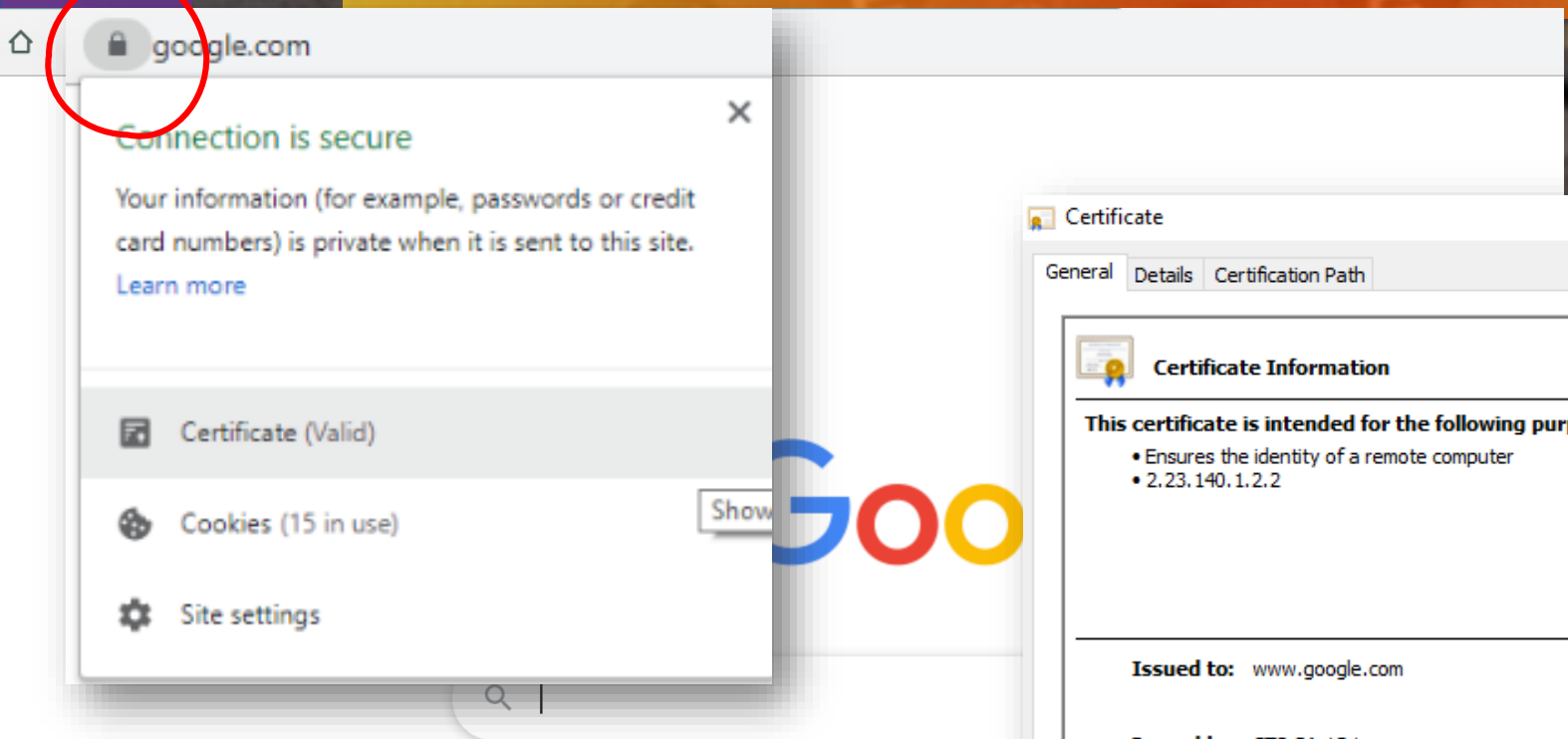
การใช้ Digital Certificate

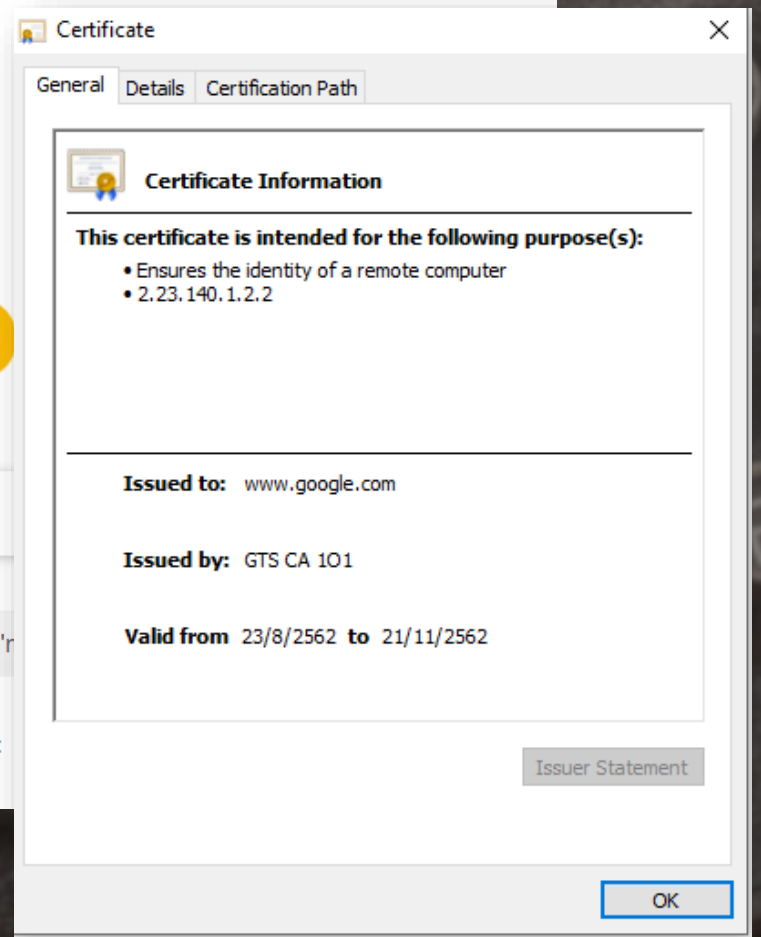


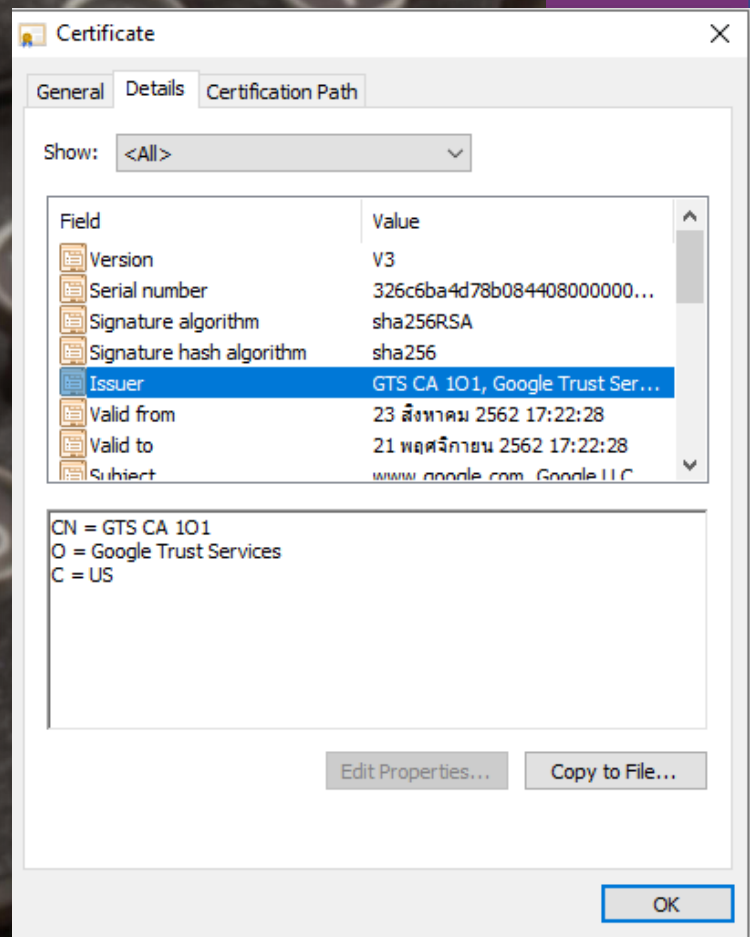
Certificate Authority

- ตรวจสอบความมีตัวตนของบุคคลหรือระบบนั้นๆ
- เมื่อตรวจสอบแล้วก็จะสร้างใบรับรองให้กับผู้ที่ร้องขอ
- ใบรับรองประกอบไปด้วยพับลิกคีย์ของบุคคลนั้น+หมายเลขเฉพาะที่ระบุบุคคลหรือระบบนั้นๆ
- ข้อมูลดังกล่าวจะถูกเข้ารหัสแบบ Digital Signature
- เมื่อมีการสื่อสารกัน จะมีการแลกเปลี่ยน Digital Certificate ที่ถอดรหัสโดยพับลิกคีย์ของ CA

Digital Certificate







ข่าวในวงการ Digital Certificate

กูเกิลลงโทษ Symantec ฐานออกใบรับรองไม่ถูกต้อง เตรียมไม่รับใบรับรองหากไม่เปิดเผยข้อมูลการออกใบรับรอง

By: lew on 29 October 2015 - 17:18 Tags: Google Security Symantec Digital Certificate

เมื่อเดือนกันยายนที่ผ่านมาไซแมนเทคออกใบรับรองให้กับโดเมน Google.com โดยไม่ได้รับอนุญาต แม้จะระบุว่าเป็นการทดสอบระบบและไล่พนักงานที่เกี่ยวข้องออกไปแล้ว แต่การออกใบรับรองเช่นนี้ผิดไปจากข้อตกลงการรักษาความปลอดภัยของหน่วยงานรับรอง (Certification Authority - CA) และวันนี้ทางกูเกิลก็ประกาศมาตรการเพิ่มข้อจำกัดของไซแมนเทคในการออกใบรับรองในอนาคต

ไซแมนเทครายงานการตรวจสอบภายใน พบว่ามีใบรับรองที่ออกโดยไม่ได้รับอนุญาตอีก 164 ใบ และมีอีก 2,458 ใบที่รับรองโดเมนที่ไม่เคยมีการจดทะเบียนจริง

กูเกิลประกาศมาตรการเป็นการลงโทษไซแมนเทคว่าหลังจากวันที่ 1 มิถุนายน 2016 **ใบรับรองทุกใบที่ออกโดยไซแมนเทค**จะต้องผ่านกระบวนการเปิดเผยข้อมูล (Certificate Transparency - CT) หากใบรับรองใหม่ไม่ผ่านกระบวนการนี้อาจจะ**มีปัญหา**กับสินค้าของกูเกิล

นอกจากมาตรการที่จะมีผลกระทบไปถึงลูกค้าของไซแมนเทคแล้ว ทางกูเกิลยังขอให้ไซแมนเทคส่งรายงานวิเคราะห์หาสาเหตุว่าทำไมจึงมีการออกใบรับรองเหล่านี้ออกมาได้ พร้อมรายงานความผิดพลาดอย่างละเอียดว่ามีความผิดพลาดที่จุดใดบ้าง นอกจากนี้ยังขอให้ไซแมนเทคดำเนินการตรวจสอบโดยผู้ตรวจสอบภายนอกยืนยันว่าพนักงานของไซแมนเทคเข้าถึงกุญแจลับไม่ได้อีก และกระบวนการป้องกันและตรวจสอบย้อนกลับเป็นไปตามมาตรฐาน

มาตรการเหล่านี้คล้ายกับมาตรการที่กูเกิลประกาศกับ CNNIC ที่ออกใบรับรองผิดพลาดเช่นเดียวกัน

ที่มา - Google Online Security, ArsTechnica

ไซแมนเทคขายกิจการออกใบรับรองและความปลอดภัยเว็บให้ DigiCert

By: lew on 4 August 2017 - 10:49 Tags: Symantec Digital Certificate

ไซแมนเทคประกาศขายกิจการการออกใบรับรองและความปลอดภัยเว็บให้กับ DigiCert ด้วยเงินสด 950 ล้านดอลลาร์ และหุ้นของ DigiCert อีก 30%

ธุรกิจออกใบรับรองดิจิตอลของไซแมนเทคมีปัญหาในช่วงหลัง จากการออกใบรับรองผิดพลาดจำนวนมากจนกระทั่งผู้ผลิตเบราว์เซอร์กำหนดเส้นตายในการหยุดรับรองใบรับรองจากไซแมนเทค ล่าสุดมอซิลล่าประกาศว่าจะปรับระยะเวลาการยกเลิกรองรับใบรับรองจากไซแมคเทคให้ตรงกับโครม โดยจะเหลื่อมกันเล็กน้อยขึ้นกับช่วงเวลาที่ออกเวอร์ชั่นใหม่

ไซแมนเทคระบุว่าการขายครั้งนี้จะทำให้บริษัทมุ่งเป้าไปยังระบบความปลอดภัยสำหรับองค์กรได้ดีขึ้น

ที่มา - Symantec

CA จีน WoSign ออกใบรับรองโดยไม่ได้รับอนุญาต, อาจจะออกใบรับรอง SHA-1 ย้อนหลัง

By: lew on 29 August 2016 - 13:03 Tags: China Digital Certificate Security PKI

WoSign หน่วยงานออกใบรับรองจากจีนที่เพิ่งประกาศสนับสนุนการเปิดเผยการออกใบรับรองเมื่อกลางปีที่ผ่านมา กำลังถูกร้องเรียนว่าละเมิดข้อกำหนดความปลอดภัยของการทำหน้าที่หน่วยงานออกใบรับรองหลายประการ

เหตุการณ์เริ่มต้นตั้งแต่ปีที่แล้ว ที่ WoSign อนุญาตให้ยืนยันความเป็นเจ้าของโดเมนโดยใช้ "พอร์ตใดๆ" ในเครื่อง ทำให้ผู้ใช้ที่มีสิทธิ์ระดับต่ำสามารถใช้พอร์ตหมายเลขสูงๆ ขอใบรับรองของเครื่องออกมาได้ อย่างไรก็ดี ก่อนหน้านี้กระบวนการของ WoSign ไม่ได้ละเมิดข้อกำหนดการเป็น CA ก่อนการแก้ไขที่ 169

ความผิดพลาดต่อมาคือการออกใบรับรองสำหรับโดเมนหลัก ให้กับผู้ครอบครองโดเมนย่อย (subdomain) ทำให้ผู้ใช้โดเมนย่อยของ github.com สามารถออกใบรับรองของ github.com เองได้ มีหน่วยงานจำนวนมากได้รับผลกระทบจากเหตุการณ์นี้ บางมหาวิทยาลัยเช่น ucf.edu ใบรับรองยังไม่ถูกยกเลิกหลังจากเหตุการณ์ผ่านไปเกือบปี จนกระทั่งกูเกิลต้องแจ้งไปทาง WoSign เอง

เหตุการณ์สุดท้ายคือมีผู้พบว่าหากใช้บริการ StartEncrypt แล้วเลือกหน่วยงานออกใบรับรองเป็น "WoSign CA Free SSL Certificate G2" จะได้ใบรับรองที่มีฟิลด์ notBefore เป็นวันที่ 20 ธันวาคม 2015 แม้ว่าจะขอใบรับรองหลังจากนั้นก็ตาม เรื่องนี้ทำให้มองได้ว่า WoSign พยายามหลอกเบราว์เซอร์ที่ไม่ยอมรับใบรับรอง SHA-1 ที่ออกหลังจากวันที่ 20 ธันวาคมที่ผ่านมา

Richard Wang ตัวแทนของ WoSign เข้ามาตอบคำถาม ระบุว่ากำลังอัพโหลดใบรับรองที่ออกผิดพลาดทั้งหมดเข้าไปยัง CT log เมื่อถูกถามว่าทำไมเหตุการณ์ออกใบรับรองผิดพลาดเช่นนี้ไม่ถูกรายงานในการรายงานการตรวจสอบ เขาระบุว่าเหตุการณ์เหล่านี้ "เทคนิค" เกินไปที่ผู้ตรวจสอบจะตรวจพบ

Wang สัญญาว่า WoSign จะปรับปรุงไม่ให้เกิดปัญหาเหล่านี้อีกในอนาคต

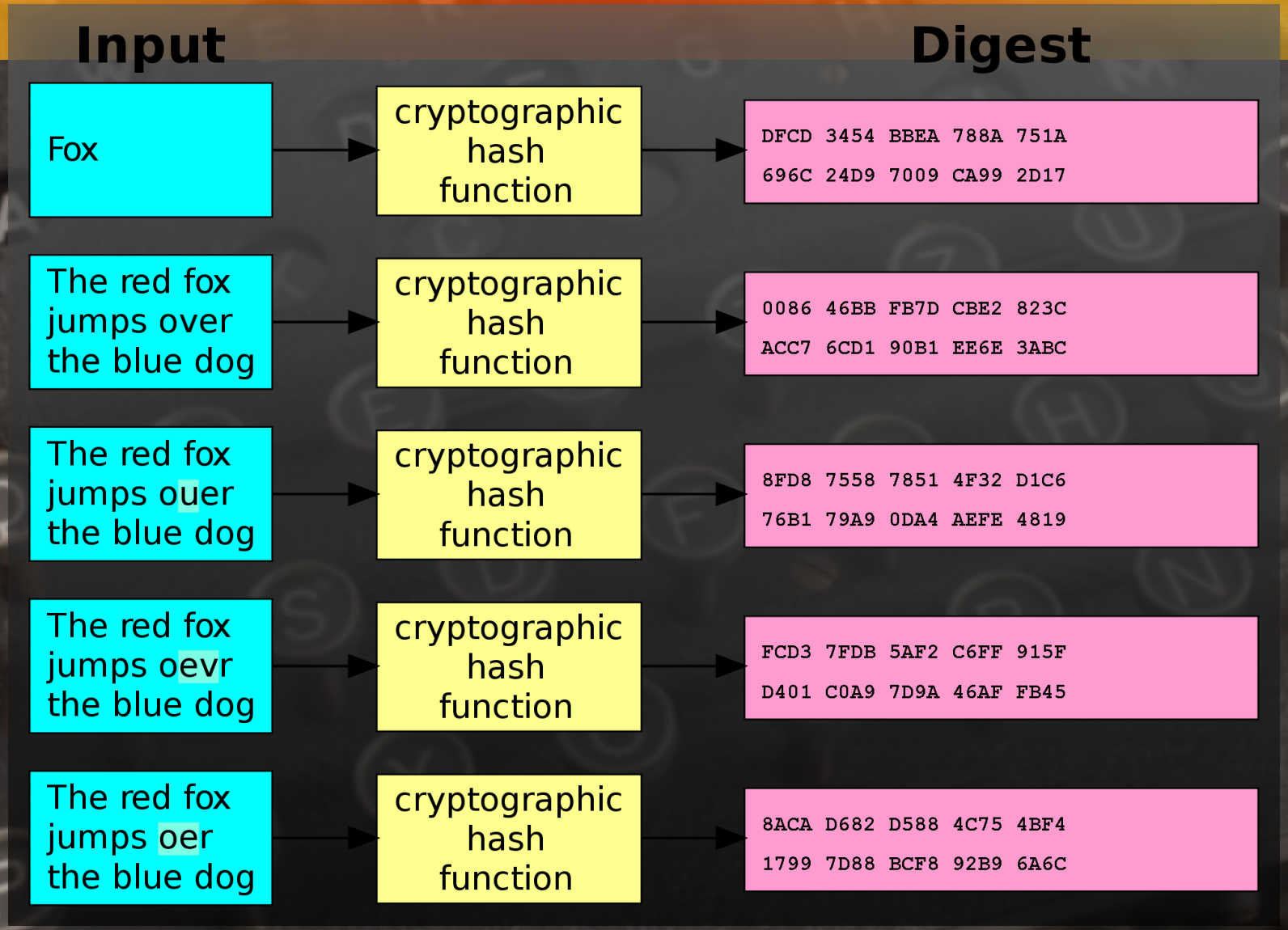
ส่วนตัวผมเองคงถอด WoSign ออกจากเครื่องก่อน

ที่มา - mozilla.dev.security.policy

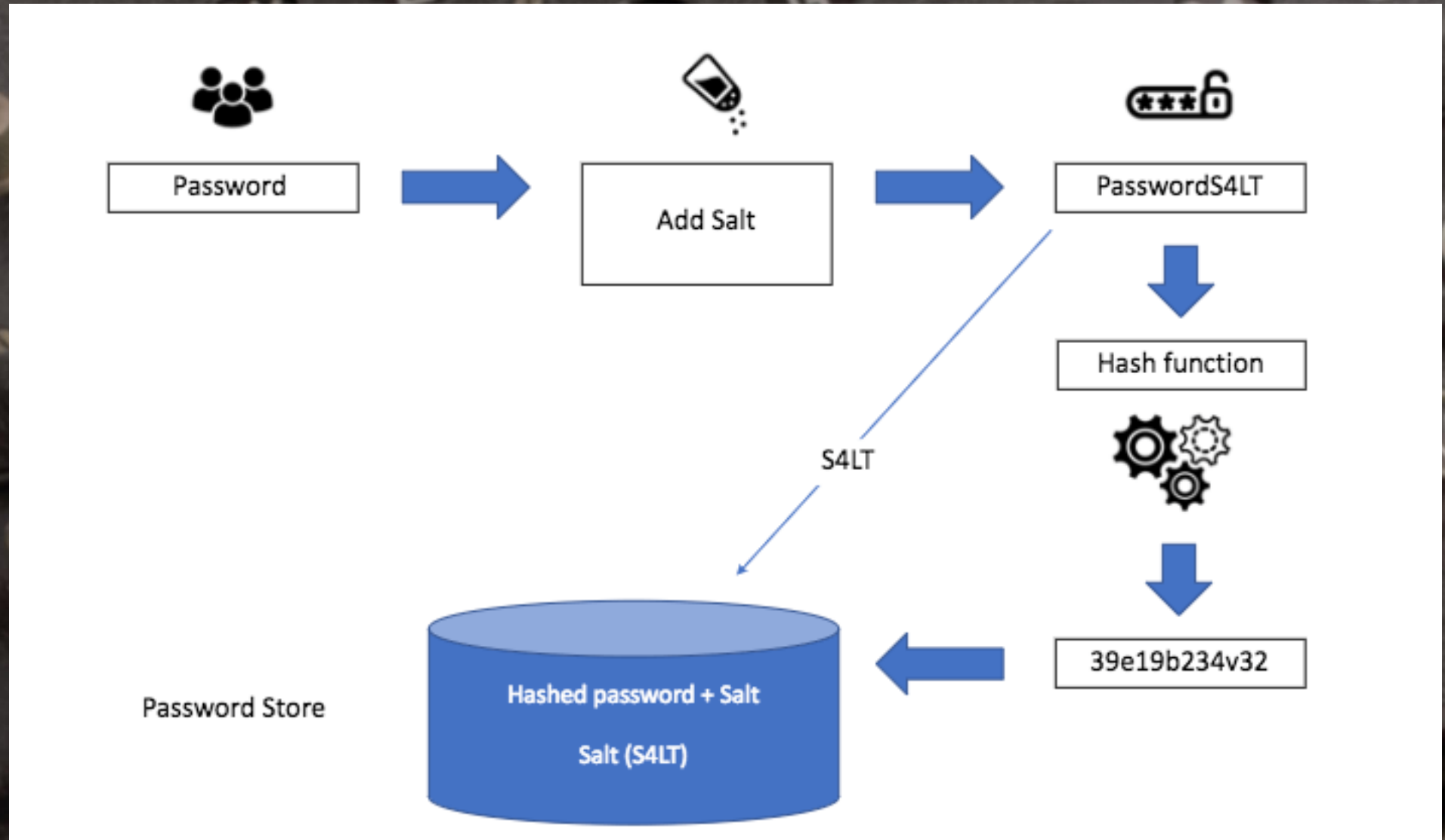
Hash Functions

- เป็นอัลกอริทึมการเข้ารหัสข้อมูลโดย**ไม่ใช้คีย์**
- ค่าแฮชที่คำนวณได้มีความยาวคงที่ ซึ่งไม่สามารถคำนวณหาเนื้อหาและความยาวของข้อความเดิมได้
- **ใช้ตรวจสอบดูว่าไฟล์นั้นมีการเปลี่ยนแปลงหรือไม่ (คุณสมบัติด้าน Integrity)**
- นิยมใช้ในระบบปฏิบัติการเพื่อเข้ารหัส Password ในการล็อกอินเข้าระบบ โดยใช้ Hash+Salt เพื่อเพิ่มความแข็งแกร่ง

ตัวอย่างแฮชฟังก์ชัน



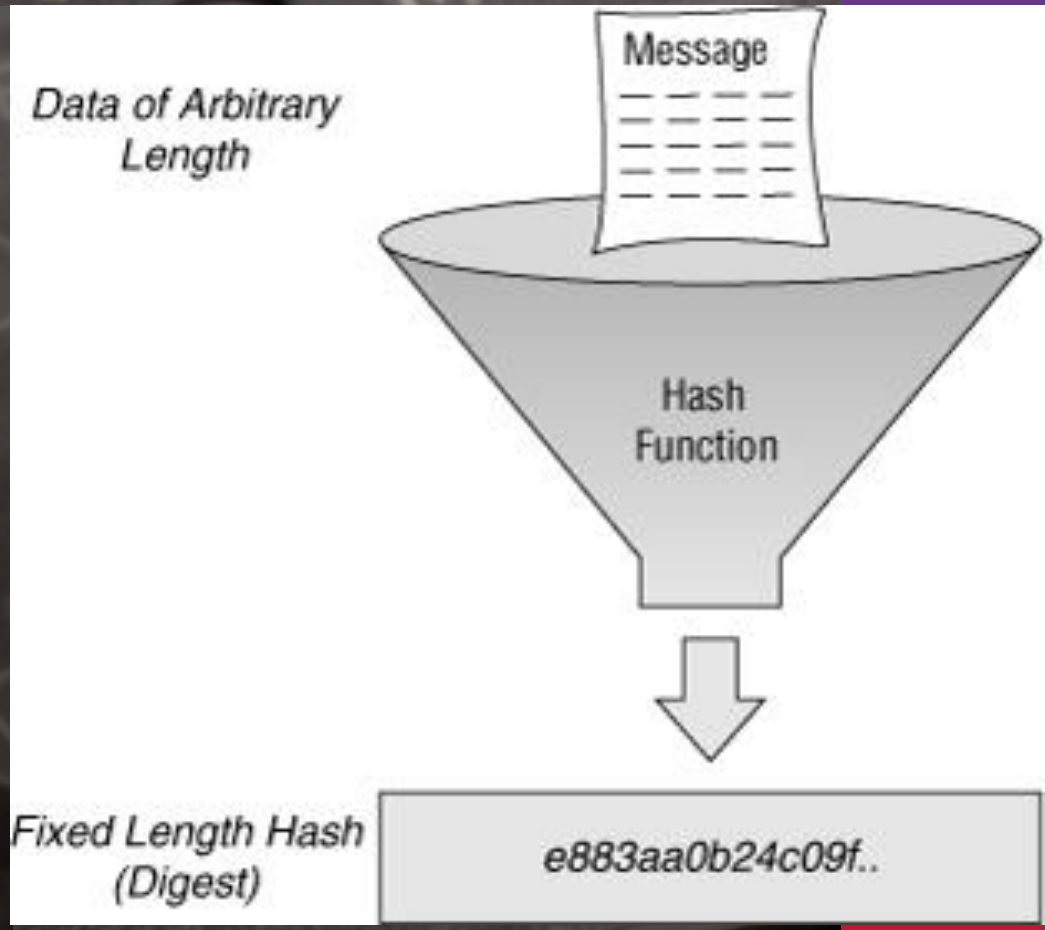
Hash + Salt


Password
Add Salt
PasswordS4LT
Hash function
S4LT
39e19b234v32
Password Store
Hashed password + Salt
Salt (S4LT)

Hash Functions : มาตรฐานแฮชฟังก์ชัน

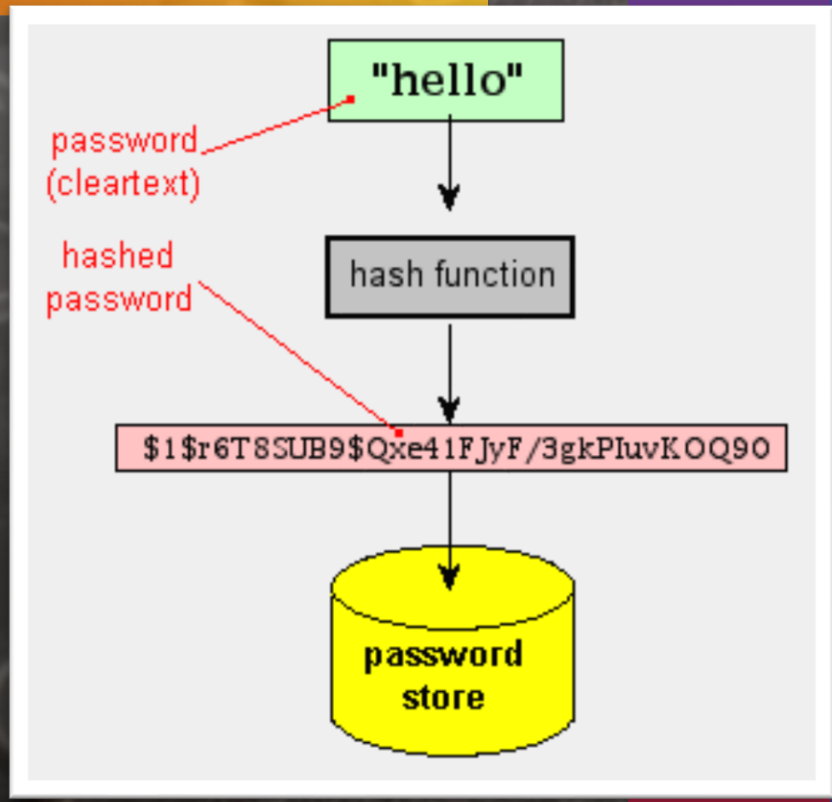
แฮชฟังก์ชันที่นิยมใช้มีดังนี้

- Message Digest (MD)
- * Secure Hash Algorithm (SHA)
- RIPEMD
- HAVAL
- Whirlpool

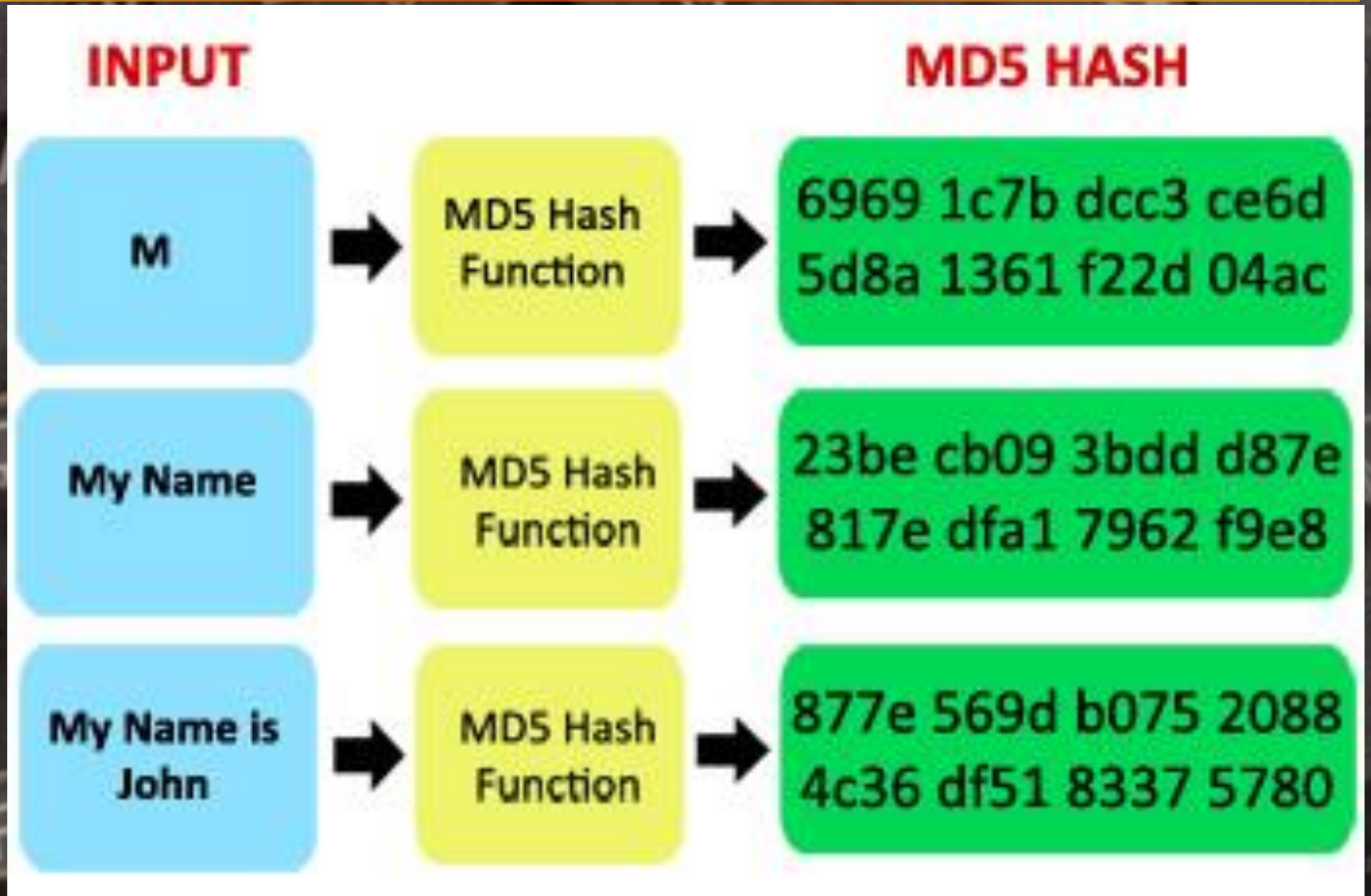


Hash Functions : Message Digest (MD)

- Message Digest เป็นฟังก์ชันที่สร้างค่าแฮชที่มีความยาวคงที่ จากข้อความที่มีความยาวเท่าไรก็ได้
- **MD2** : ออกแบบสำหรับระบบที่มีหน่วยความจำน้อย เช่น สมาร์ทการ์ด
- **MD4** : คล้ายกับ MD2 แต่ถูกออกแบบเพื่อให้ทำงานได้เร็วยิ่งขึ้น
- **MD5** : มีการใช้งานอย่างแพร่หลายในอดีต ถูกค้นพบจุดอ่อนโดยนักเข้ารหัสชาวเยอรมัน Hans Dobbertin ในปี 1996 ปัจจุบันไม่นิยมแล้ว
- MD6 : ออกแบบและตีพิมพ์ในปี 2008 ค่าแฮชขนาด 512 บิต



MD5 Example


INPUT
MD5 HASH
M
MD5 Hash Function
6969 1c7b dcc3 ce6d 5d8a 1361 f22d 04ac
My Name
MD5 Hash Function
23be cb09 3bdd d87e 817e dfa1 7962 f9e8
My Name is John
MD5 Hash Function
877e 569d b075 2088 4c36 df51 8337 5780

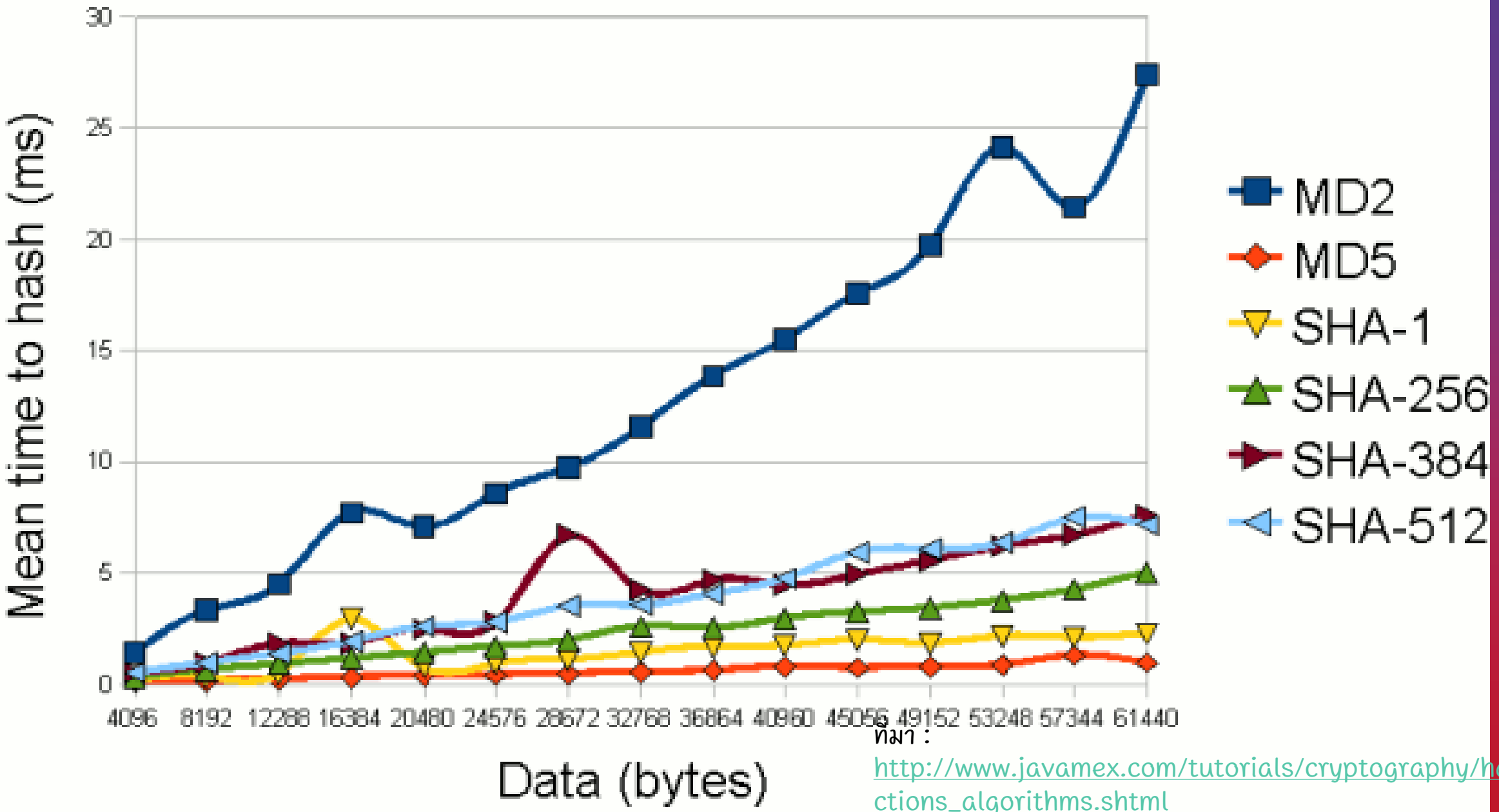
Hash Functions :
Secure Hash Algorithm (SHA)

- มีอยู่หลายเวอร์ชัน โดยใช้ค่าแฮชที่มีความยาวแตกต่างกัน
- เช่น **SHA-1**, SHA-1 plus, **SHA-256**, SHA-384 และ SHA-512
- สร้างแฮชที่มีมีความยาว 160, 256, 384 และ 512 ตามลำดับ
- ยิ่งความยาวของข้อความที่ถูกแฮชมากขึ้น ยิ่งทำให้ถูกแครกได้ยากขึ้น
- เป็นการแฮชที่ได้รับความนิยมมากที่สุด

=

```
79054025
255fb1a2
6e4bc422
aef54eb4
```

Speed of secure hash functions



ที่มา : http://www.javamex.com/tutorials/cryptography/hash_functions_algorithms.shtml

รู้หมือไร่?

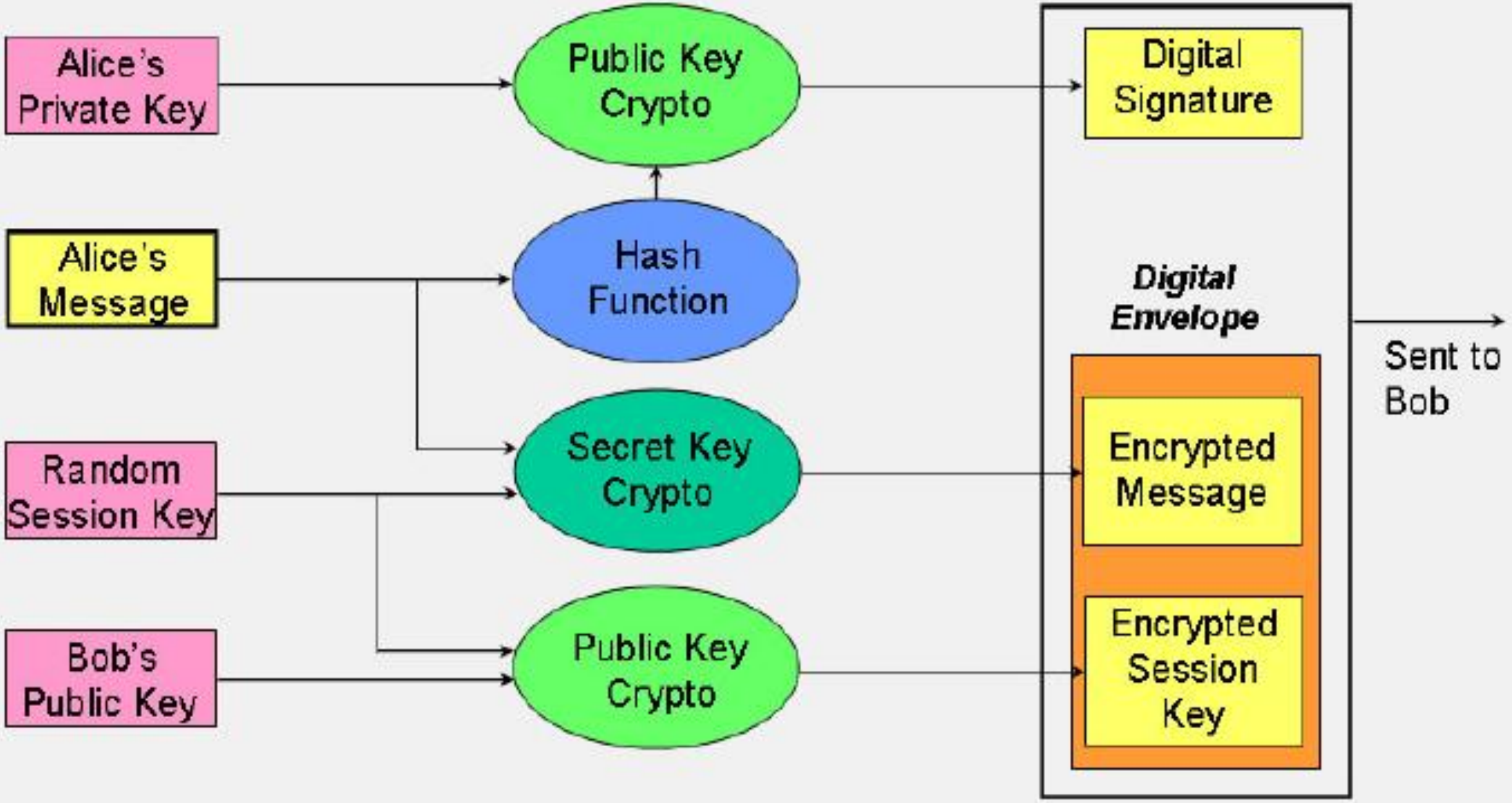
แฮชฟังก์ชันในภาษาโปรแกรมมิ่งต่าง ๆ และระบบปฏิบัติการ Linux นิยมใช้แฮชฟังก์ชันที่ชื่อว่า

“bcrypt”

ซึ่งพัฒนามาจาก Blowfish Cipher

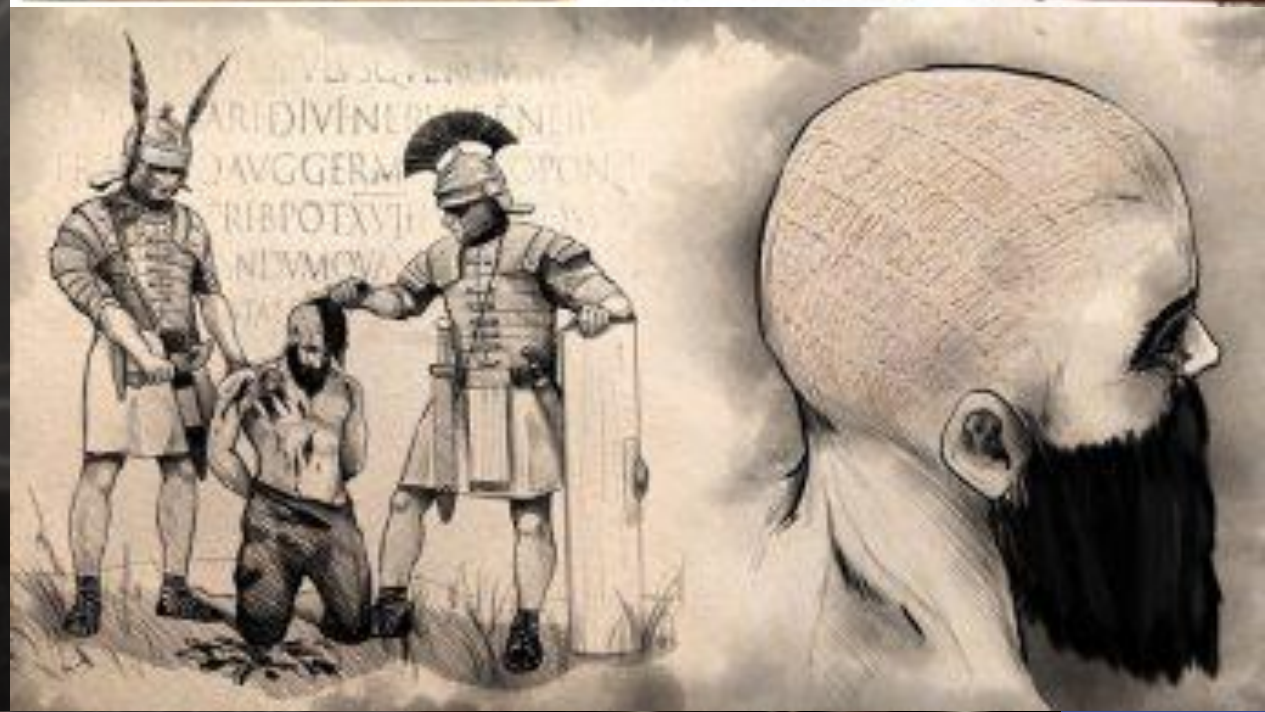
Digital Envelope

- **รูปแบบการเข้ารหัสแบบไหนดีที่สุด?**
- การเข้ารหัสแต่ละรูปแบบมีจุดประสงค์การใช้งานที่แตกต่างกัน จึงต้องมีการใช้งานร่วมกันจึงจะได้ผลลัพธ์ที่ดีที่สุด
- **แฮชฟังก์ชัน**เหมาะสำหรับการรักษาความคงสภาพของข้อมูลและการหลีกเลี่ยงการเก็บข้อมูลที่เป็น Plaintext
- การเข้ารหัสแบบ**ซีเคร็ทคีย์**เหมาะสำหรับการเข้ารหัสข้อมูล โดยอาจสร้าง**เซสชั่นคีย์**ด้วย**พับลิกคีย์**อีกชั้นในการส่งข้อมูลแต่ละครั้ง เพื่อการแลกเปลี่ยนคีย์ที่ปลอดภัยยิ่งขึ้น


Alice's Private Key
Public Key Crypto
Digital Signature
Alice's Message
Hash Function
Digital Envelope
Sent to Bob
Random Session Key
Secret Key Crypto
Encrypted Message
Bob's Public Key
Public Key Crypto
Encrypted Session Key

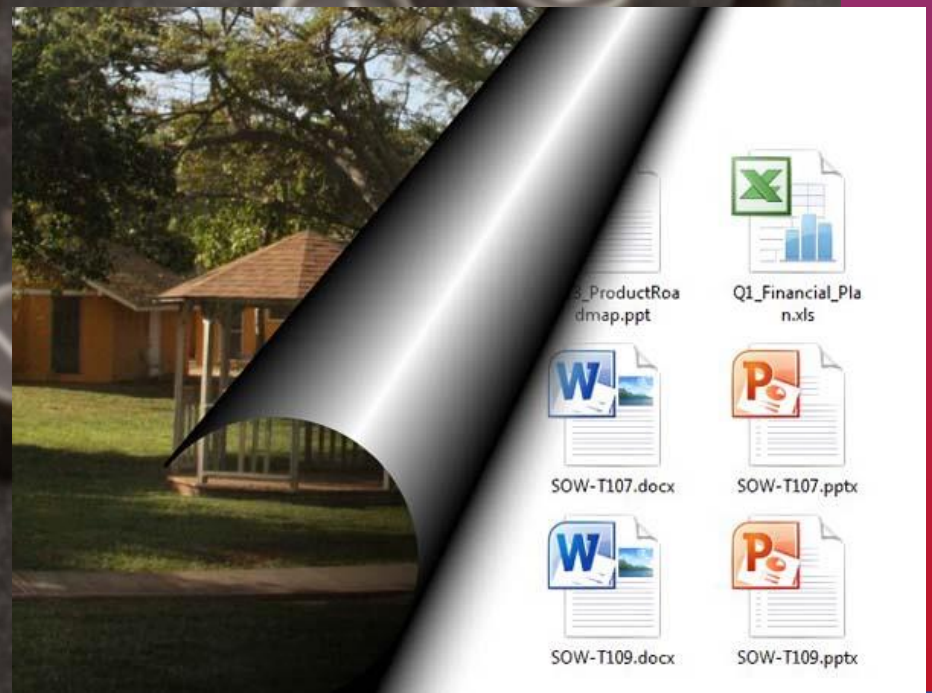
การอำพรางข้อมูล Steganography

- ประวัติศาสตร์มีการบันทึกเอาไว้ว่ามีการอำพรางข้อมูลในอดีตกาลมานานแล้ว
- โดยครั้งแรกเกิดขึ้นตั้งแต่สมัยกรีกโบราณ อำพรางข้อมูลโดยแกะสลักข้อความลงบนแผ่นไม้แล้วใช้ขี้ผึ้งเททับก่อนที่จะส่งข้อความนี้ไป
- หรือการสักข้อความลงบนหนังศีรษะแล้วรอให้ผมขึ้นเต็มหัวก่อนค่อยออกเดินทาง



Steganography

- เป็นศาสตร์และศิลป์ในการอำพรางข้อมูล โดยการฝังข้อมูลไปกับสิ่งอื่น ซึ่งดูเผินๆ เหมือนไม่มีอะไร
- จุดประสงค์เพื่อไม่ให้ผู้ที่ไม่มีส่วนเกี่ยวข้องรู้ว่ามีข้อมูลนั้นอยู่ ต่างจากการเข้ารหัสข้อมูลทั่วไปที่ความมีอยู่ของข้อมูลจะไม่ถูกซ่อน
- อาจใช้ร่วมกับการเข้ารหัสด้วย เพราะข้อมูลที่อำพรางอาจถูกจับได้ แต่ก็ยังไม่สามารถถอดรหัสได้ถ้าไม่มีคีย์



Steganography

- การตรวจจับนั้นจำเป็นต้องรู้อัลกอริทึมที่ใช้ในการอำพรางข้อมูล
- ยากต่อการตรวจจับและถอดรหัสได้ เพราะเป็นการวิเคราะห์ในระดับบิต
- เป็นวิธีที่ใช้สำหรับส่งข้อความที่ต้องการปกปิดไปยังผู้รับผ่านช่องทางที่ไม่มีความปลอดภัยเลย

Steganography example

ภาพที่มีข้อมูลอำพรางข้างใน

ภาพที่ถอดได้จากการซ่อน

โปรแกรมสำหรับการอำพราง

- มีเครื่องมือสำหรับอำพรางข้อมูลมากมายบนอินเทอร์เน็ต นักศึกษาสามารถค้นหาได้โดยใช้คีย์เวิร์ด “Steganography Tools”
- ตัวอย่างเดโมวีดีโอการอำพรางข้อมูล https://www.youtube.com/watch?v=mxDGKolrv_0