Written by Thapanapong Rukkanchanunt

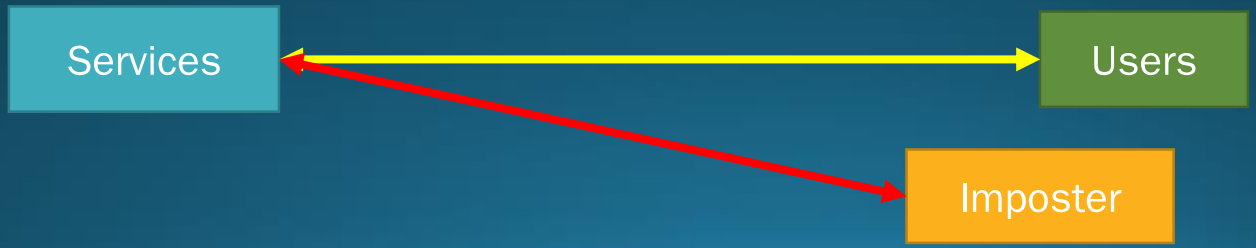
Network Security

Outline

- ความปลอดภัยในเครือข่ายคอมพิวเตอร์ (Internet Security)
- การเข้ารหัสข้อมูล (Encryption and Decryption)

Internet Security

- ความปลอดภัยในเครือข่ายคอมพิวเตอร์หมายถึงการรักษาข้อมูลที่ใช้ในการติดต่อระหว่างคอมพิวเตอร์ไม่ให้ถูกขโมย หรือหากข้อมูลถูกขโมยผู้ขโมยไปต้องไม่สามารถถอดรหัสของข้อมูลนั้นได้
- การป้องกันไม่ให้ข้อมูลรั่วไหลสามารถทำได้สองวิธี
  - Authentication การระบุตัวตนของผู้ที่รับข้อมูลนั้น
  - Authorization การให้อำนาจในการเข้าถึงข้อมูลของบุคคลในแต่ละระดับ



Authentication

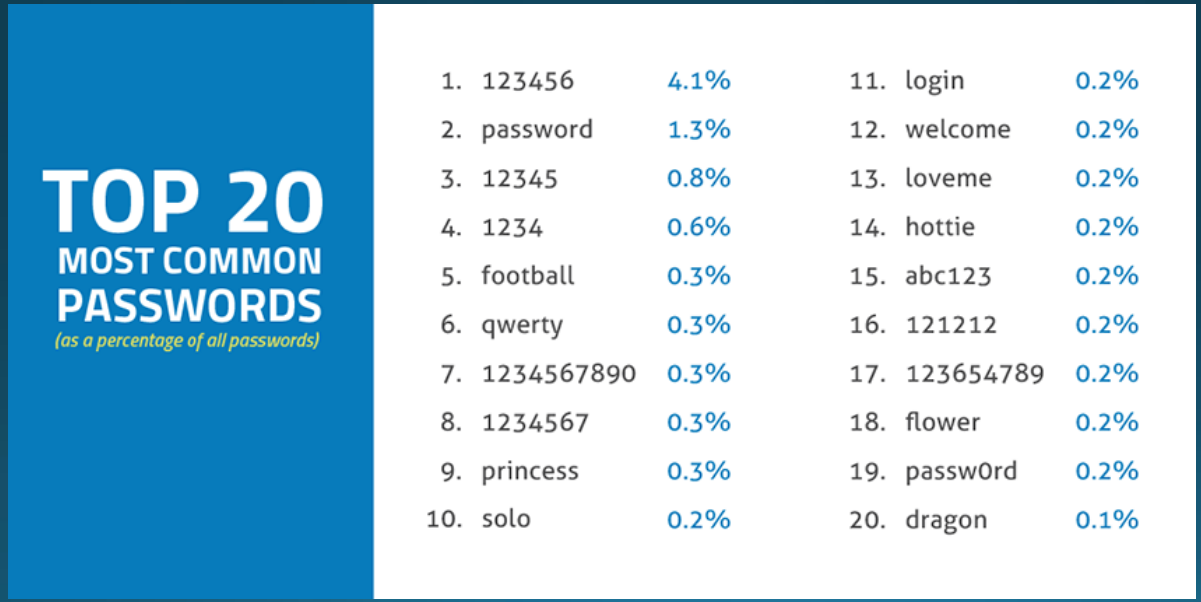
- การระบุตัวตน คือ การตรวจสอบว่าบุคคลที่พยายามจะเข้ามาเรียกใช้ข้อมูลจะต้องเป็นตัวจริงและไม่ได้ถูกคนอื่นแอบอ้างมา
- เทคนิคที่ใช้ในการระบุตัวตนแบ่งออกเป็นสามระดับ
  - ใช้สิ่งที่มี (Possession)
  - ใช้สิ่งที่รู้ (Memorization)
  - ใช้สิ่งที่เป็น (Physicality)

Possession

- ใช้สิ่งของที่ทำขึ้นมาเฉพาะเพื่อใช้ระบุตัวตน เช่น
  - ID Card / Credit Card มีแถบแม่เหล็กหรือลายน้ำที่ทำขึ้นมาเฉพะ
  - Authenticator เป็นอุปกรณ์ที่สุ่มเลขมาเพื่อใช้ประกอบรหัสผ่านในการเข้าสู่ระบบ

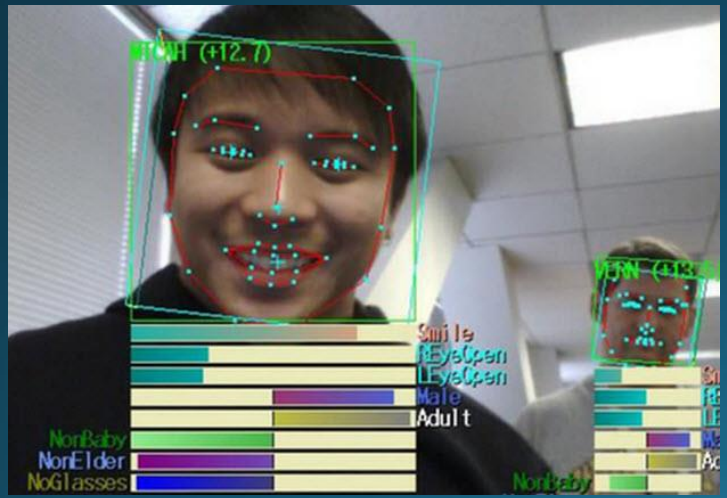
Memorization

- ใช้รหัสผ่านที่ผู้ใช้คิดขึ้นเอง



Physicality

- ใช้สิ่งที่เป็นเอกลักษณ์เฉพาะบุคคล (เป็นผลสืบเนื่องมาจาก DNA) เช่น ใบหน้า ม่านตา ลอยนิ้วมือ ฝ่ามือ เสียง หรือหลายอย่างรวมกัน



ข้อจำกัด

- ข้อจำกัดของ Possession ได้แก่
  - ถ้าบัตรโดนขโมยจะต้องรีบแจ้งระงับการใช้งานทันที
  - ปลอมแปลงบัตร
- ข้อจำกัดของ Memorization ได้แก่
  - รหัสผ่านง่ายเกินไป หรือถ้ารหัสผ่านยากเกินไปอาจจะจำรหัสผ่านไม่ได้
  - เสี่ยงต่อการดักรหัสผ่าน เมื่อใช้งานคอมพิวเตอร์สาธารณะ
- ข้อจำกัดของ Physicality
  - ต้องใช้อุปกรณ์เฉพาะในการตรวจจับเอกลักษณ์ดังกล่าว

Authorization

- การให้อำนาจในการเข้าถึงข้อมูลของบุคคลในแต่ละระดับมักจะคำนึงถึงความสำคัญหรือตำแหน่งของบุคคลนั้น ๆ เช่น
  - ผู้ใช้ A สามารถเห็นข้อมูลของตนเองได้แต่ไม่สามารถเห็นข้อมูลของผู้ใช้ B
  - ผู้ควบคุมระบบสามารถดูได้แค่ข้อมูลทั่วไปของผู้ใช้
- ปัญหาของการให้อำนาจแต่ละกลุ่มบุคคลได้แก่
  - ผู้ควบคุมระบบมีอำนาจในการเปลี่ยนแปลงรหัสผ่านของผู้ใช้ (อำนาจมากเกินไป)
  - ผู้ใช้ A ไม่สามารถเข้าไปแก้ไขชื่อของตนเองได้ (อำนาจไม่เพียงพอ)

Encryption and Decryption

- ในการส่งข้อมูลผ่านอินเตอร์เน็ต เราไม่สามารถรับประกันได้ว่าข้อมูลที่ส่งไปจะไม่ถูกดักระหว่างทาง ดังนั้นเราจึงจำเป็นต้องเข้ารหัสข้อมูล โดยข้อมูลที่ถูกเข้ารหัสแล้วนั้นสามารถถอดรหัสได้เฉพาะผู้ส่งและผู้รับเท่านั้น
- การเข้ารหัสสามารถจำแนกได้สองระบบคือ
  - การเข้ารหัสโดยใช้คีย์ลับ (Secret Key Cryptography)
  - การเข้ารหัสโดยใช้คีย์สาธารณะ (Public Key Cryptography)

Secret Key Cryptography

- ใช้คีย์ลับในการเข้ารหัสและถอดรหัสข้อมูล ซึ่งคีย์ลับอาจจะตกลงกันไว้ก่อนการส่งข้อมูล เนื่องจากการส่งคีย์ลับผ่านอินเตอร์เน็ตอาจจะไม่ปลอดภัย

Transposition Cipher

- เข้ารหัสข้อความด้วยการจัดเรียงใหม่ จำนวนคอลัมน์คือคีย์ลับ

Substitute Cipher

- เข้ารหัสข้อความด้วยเลื่อนตัวอักษรตามพจนานุกรม จำนวนครั้งในการเลื่อนเป็นคีย์ลับ เช่น เลื่อน A หนึ่งครั้งจะได้ B หรือ เลื่อน Z สองครั้งจะได้ B

จำนวนครั้งในการเลื่อน	ข้อความ
0	THIS IS A SECRET
1	UIJT JT B TFDSFU
10	?

One Time Pads Cipher

- เข้ารหัสข้อความคล้ายกับวิธี Substitute Cipher เพียงแต่ว่าแต่ละตัวอักษรจะถูกเลื่อนไปเป็นจำนวนไม่เท่ากัน ชุดจำนวนครั้งในการเลื่อนคือคีย์ลับ

T	H	I	S	I	S	A	S	E	C	R	E	T
+6	+2	-1	-5	+6	+2	-1	-5	+6	+2	-1	-5	+6
Z	J	H	N	O	U	Z	N	K	E	Q	Z	Z

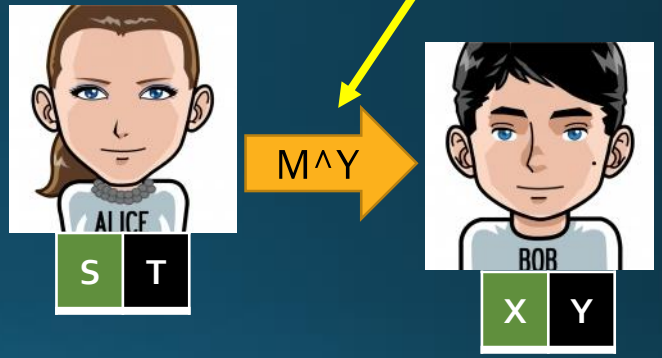
ชุดจำนวนครั้งในการเลื่อนคือ +6 +2 -1 -5

Public Key Cryptography

- แต่ละฝ่ายของการรับส่งข้อมูลจะมีสองคีย์ คีย์ลับและคีย์สาธารณะ
- คีย์ลับและคีย์สาธารณะจะต้องสัมพันธ์กัน ข้อความที่ถูกเข้ารหัสด้วยคีย์สาธารณะจะสามารถถูกถอดรหัสได้จากคีย์ลับที่สัมพันธ์กันเท่านั้น ในทางกลับกันข้อความที่ถูกเข้ารหัสด้วยคีย์ลับจะสามารถถูกถอดรหัสได้จากคีย์สาธารณะที่เป็นคู่กันเท่านั้น
- วิธีการนี้จะแบ่งออกเป็นสองช่วงคือ
  - Message Encryption เข้ารหัสข้อความ (ป้องกันการขโมย)
  - Digital Signature เซ็นข้อความ (ป้องกันการปลอมแปลง)

Message Encryption

- ถ้า Alice ต้องการจะส่งข้อมูลใน Bob Alice จะต้องทำตามขั้นตอนดังนี้
  - Alice มีคีย์ลับ S และคีย์สาธารณะ T
  - Bob มีคีย์ลับ X และคีย์สาธารณะ Y
  - Bob ประกาศ Y ให้ทุกคนในเครือข่ายรู้
  - Alice ส่งข้อความ M ให้ Bob โดยใช้ Y ในการเข้ารหัส
  - Bob ถอดรหัสโดยใช้ X



- เราจะพบว่าข้อความ M จะถูกถอดรหัสโดยใช้ X ได้อย่างเดียว ดังนั้นถึง Mallory จะได้ M เป็นก็ไม่สามารถถอดรหัสได้

Digital Signature

- ถ้า Mallory พยายามจะปลอมเป็น Alice โดยส่งข้อความ N ที่เข้ารหัสด้วย Y ไปให้ Bob Bob จะทราบได้อย่างไรว่าข้อความใดเป็น Alice
- Alice สามารถเซ็นข้อความได้ตามขั้นตอนดังนี้
  - Alice ประกาศ T ให้ทุกคนรู้
  - Alice ส่งข้อความ M ให้ Bob โดยใช้ Y และ S ในการเข้ารหัส
  - Bob ถอดรหัสข้อความโดยใช้ X และ T ถ้าข้อความไม่ผิดเพี้ยนแสดงว่าเป็นของ Alice

S T

M^Y^S

X Y

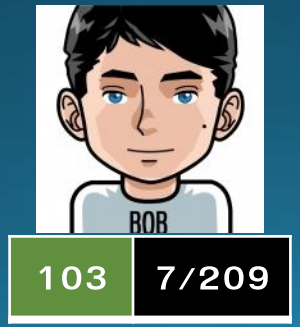
N^Y

การสร้างคีย์ด้วยวิธี RSA

- ในการสร้างคีย์ลับและคีย์สาธารณะด้วยวิธี RSA มีวิธีการดังนี้ (สำหรับ Bob)
  - Bob สุ่มจำนวนเฉพาะขึ้นมาสองตัวคือ p และ q และกำหนดให้ $n = pq$ และ $r = (p-1)(q-1)$
  - Bob เลือกจำนวน k ที่มีค่ามากกว่า r โดยที่
    - k ต้องหาร r แล้วเหลือเศษ 1
    - ไม่ใช่จำนวนเฉพาะหรือกำลังสองของจำนวนเฉพาะ
  - Bob แยกตัวประกอบ k ให้เป็นสองจำนวนคูณกันคือ e และ d
  - คีย์ลับของ Bob คือ d ส่วนคีย์สาธารณะคือ e และ n
  - จำนวนเฉพาะ p และ q จะถูกโยนทิ้งและไม่เปิดเผย
- ถ้า Alice ต้องการส่งข้อความ M ให้ Bob จะต้องเข้ารหัสโดย $C = M^e \bmod n$ (M ยกกำลัง e และหารเอาเศษด้วย n) Bob สามารถถอดรหัสได้ด้วย $M = C^d \bmod n$

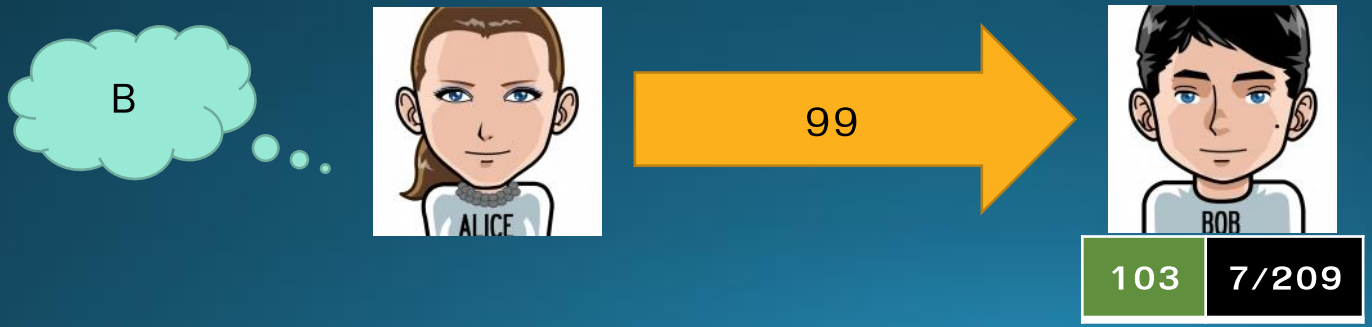
ตัวอย่างวิธี RSA

- Bob เลือกจำนวนเฉพาะ 11 และ 19 ดังนั้น n = 209 และ r = 180
- จำนวนที่หาร 180 และเหลือเศษ 1 ได้แก่ 181 361 541 721 901 1081 …
- เนื่องจาก 181 และ 541 เป็นจำนวนเฉพาะ ในขณะที่ 361 คือ 19 ยกกำลังสอง Bob จึงเลือก k เป็น 721 ซึ่งแยกตัวประกอบออกเป็น 7*103
- Bob เลือก e เป็น 7 และ d เป็น 103 (เลือก d > e จะได้เดาค่า d ได้ยาก)



ตัวอย่างวิธี RSA (2)

- ถ้า Alice ต้องการส่งตัวอักษร B ให้ Bob จะต้องแปลง B เป็นตัวเลขก่อน
- การแปลงตัวอักษรเป็นตัวเลข จะใช้ตาราง ASCII เป็นตัวเทียบ จะได้ว่า B = 66
- Alice เข้ารหัสโดยใช้คีย์สาธารณะของ Bob
  - $66^{7} \bmod 209 = 99$
- Bob ถอดรหัสข้อความ $99^{103} \bmod 209 = 66$ ซึ่งคือตัวอักษร B



วิธีการคำนวณเศษจากการหารเลขยกกำลัง

- Bob ต้องคำนวณค่า 99^{103} mod 209 ซึ่ง 99^{103} เป็นตัวเลขที่ใหญ่มากและเก็บในหน่วยความจำไม่ได้ ดังนั้น Bob จึงต้องใช้วิธีลัด

	99^2	หาร 209	เหลือเศษ 187	
	99^4	หาร 209	เหลือเศษ 187^2	
แต่	187^2	หาร 209	เหลือเศษ 66	
ดังนั้น	99^4	หาร 209	เหลือเศษ 66	(ลองกดเครื่องคิดเลขเพื่อตรวจสอบ)

- เราจะพบว่าการหารเอาเศษมีสมบัติถ่ายทอด

วิธีการคำนวณเศษจากการหารเลขยกกำลัง (2)

99^2	หาร 209	เหลือเศษ 187	
99^4	หาร 209	เหลือเศษ 66	
99^8	หาร 209	เหลือเศษ 176	(66^2 หาร 209 เหลือเศษ 176)
99^{16}	หาร 209	เหลือเศษ 44	(176^2 หาร 209 เหลือเศษ 44)
99^{32}	หาร 209	เหลือเศษ 55	(44^2 หาร 209 เหลือเศษ 55)
99^{64}	หาร 209	เหลือเศษ 99	(55^2 หาร 209 เหลือเศษ 99)
99^{96}	หาร 209	เหลือเศษ 99*55 หรือ 11	

วิธีการคำนวณเศษจากการหารเลขยกกำลัง (3)

99^{2}	หาร 209	เหลือเศษ 187
99^{4}	หาร 209	เหลือเศษ 66
99^{96}	หาร 209	เหลือเศษ 11
99^{100}	หาร 209	เหลือเศษ 11*66 หรือ 99
99^{102}	หาร 209	เหลือเศษ 99*187 หรือ 121
99^{103}	**หาร 209**	**เหลือเศษ 121*99 หรือ 66** **<<<< คำตอบ**

เพราะเหตุใด RSA จึงปลอดภัย

- ปกติแล้วเราจะเลือก p และ q เป็นจำนวนเฉพาะขนาดใหญ่ (หลายร้อยหลัก)
- ถ้าเรารู้ค่า e และ n เราไม่สามารถคำนวณค่า d ออกมาได้ เนื่องจากจำเป็นต้องรู้ค่า r
- แต่จะรู้ค่า r ก็ต้องทราบ p และ q จาก n ซึ่งวิธีเดียวที่จะแยกตัวประกอบให้เป็นจำนวนเฉพาะสองจำนวนคือต้องลองจำนวนเฉพาะทุกตัวที่เป็นไปได้
- ถ้า p และ q มีขนาด 128 bits (ค่าระหว่าง 1 ถึง 3.4×10^{38}) จำนวนเฉพาะที่อยู่ในช่วงนั้นจะมีอยู่ประมาณ 3.8×10^{36} จำนวน
- ถ้าคอมพิวเตอร์ของเราสามารถลองจำนวนเฉพาะหนึ่งล้านล้านจำนวนต่อวินาที คอมพิวเตอร์จะใช้เวลาประมาณ 1.2×10^{17} ปี ซึ่งยาวนานกว่าอายุของจักรวาล