ทรงฤทธิ์ กิติศรีวรพันธุ์

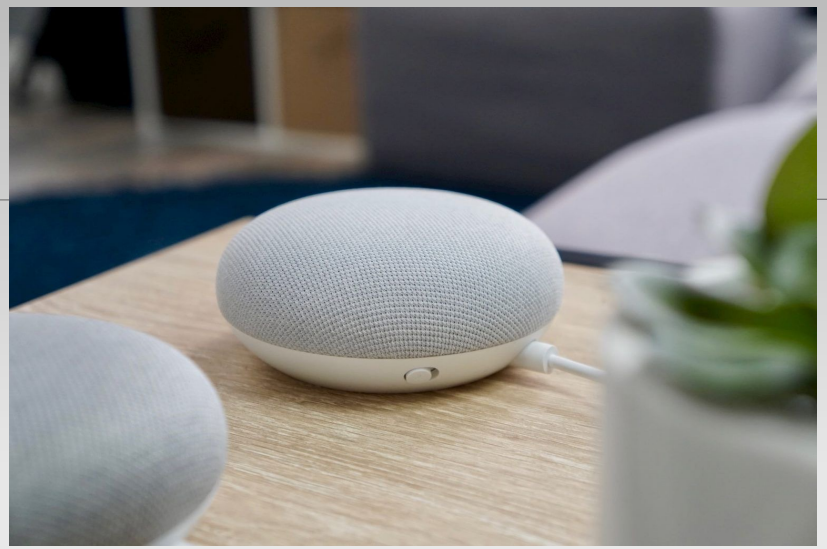
Email : songrit@npu.ac.th

สาขาวิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนครพนม

D3: Cryptography (เทคโนโลยีรหัสลับ)

ข่าวสารด้านความปลอดภัย

- source: thehackernews.com



PyTorch Machine Learning Framework Compromised with Malicious Dependency

Jan 02, 2023 Ravie Lakshmanan

The maintainers of the PyTorch package have warned users who have installed the nightly builds of the library between December 25, 2022, and December 30, 2022, to uninstall and download the latest versions following a dependency confusion attack.

Turning Google smart speakers into wiretaps for $100k

Dec 26, 2022

Summary

I was recently rewarded a total of $107,500 by Google for responsibly disclosing security issues in the Google Home smart speaker that allowed an attacker within wireless proximity to install a "backdoor" account on the device, enabling them to send commands to it remotely over the Internet, access its microphone feed, and make arbitrary HTTP requests within the victim's LAN (which could potentially expose the Wi-Fi password or provide the attacker direct access to the victim's other devices). These issues have since been fixed.

(Note: I tested everything on a Google Home Mini, but I assume that these attacks worked similarly on Google's other smart speaker models.)

https://downrightnifty.me/blog/2022/12/26/hacking-google-home.html

Time-of-Check/Time-of-Use Attacks

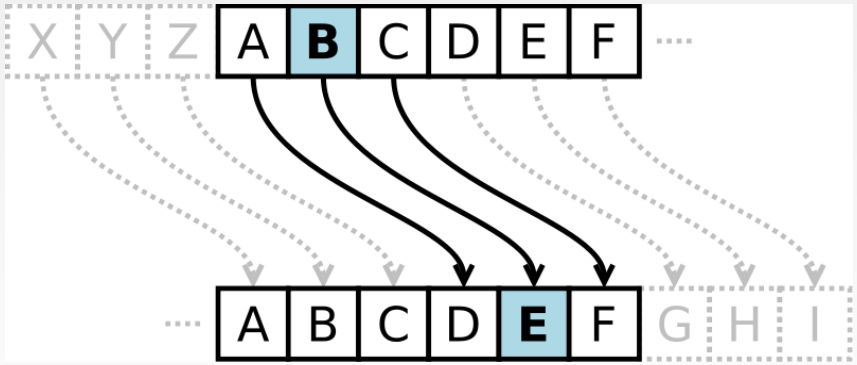
- Time-of-Check (TOC) to Time-of-Use (TOU)
  - TOCTOU
  - หรือเรียกว่า Race Condition
- Software bug caused by a race condition
  - Checking of the state of aprt of a system

Topic

- **The History of Cryptography**
- Encryption methodologies
- Cryptanalysis
- Key management
- Applications and uses of cryptography

What Is Cryptography

- Cryptography is the science of hiding information in plain sight, in order to conceal it from unauthorized parties.
  - Substitution cipher first used by Caesar for battlefield communications



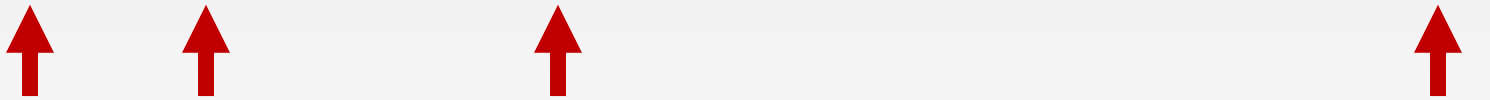
Cryptography begin

- 2000 B.C. ในอียิปต์ (โบราณ)
- พบบันทึกในสุสานฟาโรห์ (พีระมิด)
- Encryption history
  - Hebrew (600 B.C.) -- ATBASH
  - Spartans (400 B.C.) – Scytale
  - Greeks (440 B.C.)– Steganography
  - Roman (60 B.C.)– Caesar Cipher

การเข้ารหัสแบบ ATBASH (แอดบาสซ์)

- คิดค้นขึ้นโดยชาวฮิบรู เมื่อ 500-600 ปีก่อนคริสตกาล
- อัลกอริทึม
  - แทนที่ตัวอักษรแรก ด้วยตัวอักษรตัวสุดท้าย และไล่ไปตามลำดับ

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A



Cipher
ไซเฟอร์

HXRVMXV →

Plaintext
เพนเท็กซ์

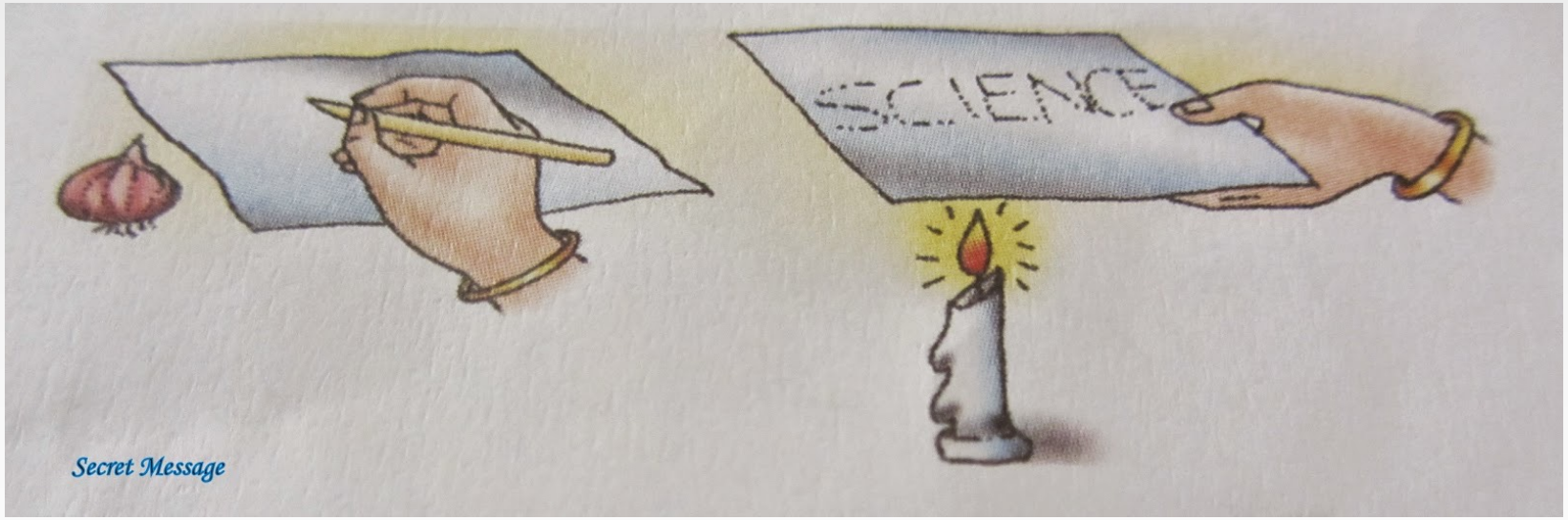
การเข้ารหัสแบบ Scytale (ไซเทล)

- รัฐสปาร์ตา รัฐของชนเผ่าดอเรียน
- หนึ่งในชนเผ่าสำคัญของกรีกโบราณ
- ยึดครองดินแดนต่าง ๆ ด้วยการทำสงคราม
- อักอริทึม
  - เข้ารหัส (encryption)
    - แผ่นหนังพันรอบท่อนไม้ แล้วเขียนข้อความที่ต้องการ
    - เมื่อคลี่แผ่นหนังจะได้ข้อความที่สลับกัน อ่านยาก
  - ถอดรหัส (decryption)
    - นำแผ่นหนังพันรอบท่อนไม้ อ่านข้อความจากซ้ายไปขวา

ตัวอย่าง SCYTALE Cipher

Steganography

- พบหลักฐาน ถูกใช้ครั้งแรกโดย ชาวกรีก เมื่อ 440 ปีก่อนคริสตกาล
- ซ่อนข้อความ(Hidden) แทนการใช้ช่องทางปกติในการอ่าน
- ไม่ให้อ่านได้โดยตรง



Caesar Cipher

- ที่โรม จูเลียส ซีซาร์ (44 ปีก่อนคริสตกาล) พัฒนาวีธีเข้ารหัสสำหรับใช้ส่งข้อความระหว่างกัน
- อัลกอริทึม
  - Encryption
    - คล้ายกับ ATBASH แต่เลื่อนตัวอักษรไป 3 ตัว เช่น A กลายเป็น D
  - Decryption
    - ถอยตัวอักษรกลับ 3 ตัว เช่น ถอด D ได้ อักษร A

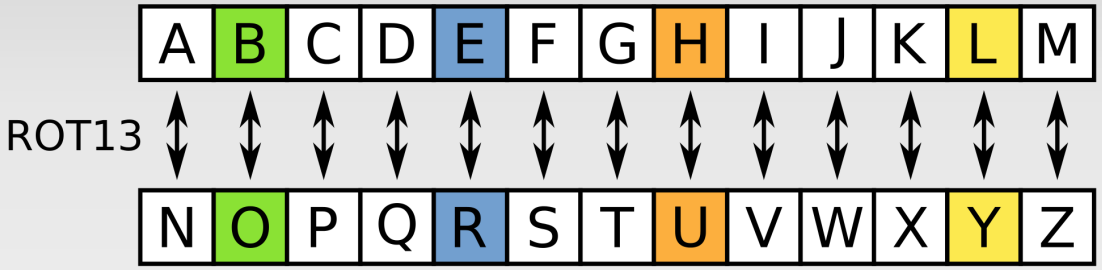
- Standard Alphabet :ABCDEFGHIJKLMNOPQRSTUVWXYZ
- Cryptographic Alphabet :DEFGHIJKLMNOPQRSTUVWXYZABC

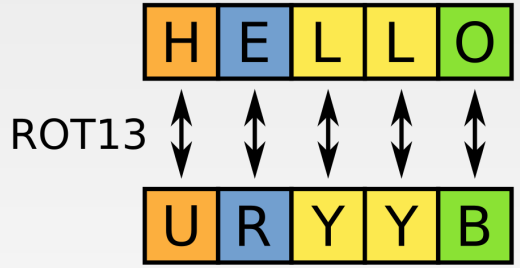
Plaintext :LOGICALSECURITY

Ciphertext :ORJLFDOVHFXULWB

ROT13

- พัฒนาในยุคหลัง ประมาณ 2000ปี หลังจาก Caesar Cipher
- พัฒนาเมื่อปี ค.ศ. 1980
- อัลกอริทึม
  - การเข้าและถอดรหัสคล้าย Caesar Cipher
  - แต่เปลี่ยนจากการเลื่อน 3 ตัวอักษร เป็น 13 ตัวอักษร





ต่อยอด Caesar Cipher

- ATBASH เข้ารหัสด้วยการเลื่อนตัวอักษร 25 ตัวอักษร (A → Z)
- Caesar เข้ารหัสด้วยการเลื่อนตัวอักษร 3 ตัวอักษร (A → D)
- ROT13 เข้ารหัสด้วยการเลื่อนตัวอักษร 13 ตัวอักษร (A → N)
- ความต้องการ
  - ถ้าต้องการส่งข้อความโดยระบุผู้รับ (คนที่รู้กุญแจถอดรหัส) จะทำอย่างไร
  - **Solution** : เลื่อนตัวอักษร k ตัว จำนวนตัวอักษรที่เลื่อน คือกุญแจถอดรหัส
    - รู้เฉพาะ ผู้ส่ง และ ผู้รับ

$$C = E_k(M)$$

Encryption

$$M = D_k(C)$$

Decryption

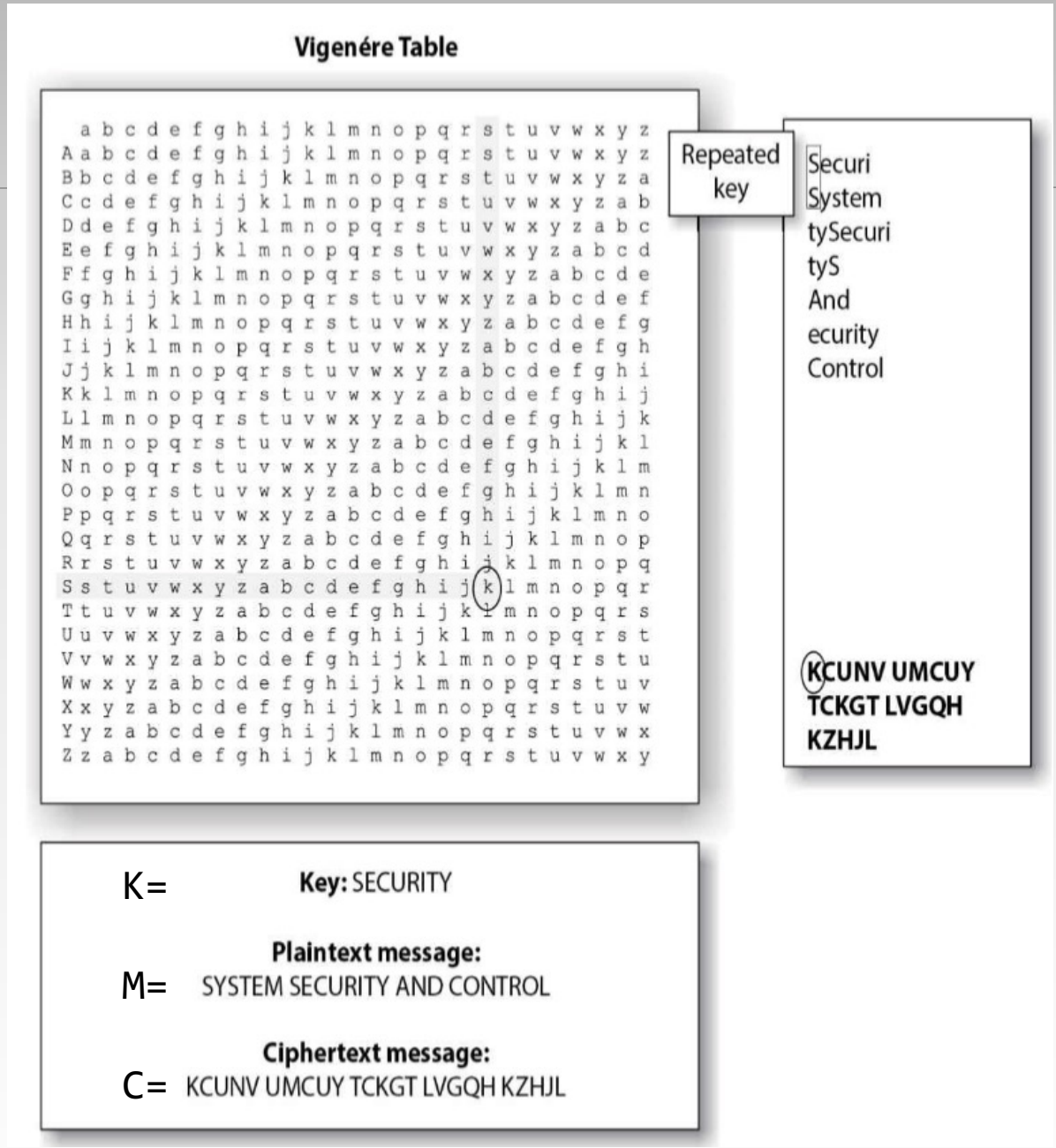
Encryption Terms and Operations

- **Plaintext (M)** – an original message
- **Ciphertext (C)** – an encrypted message
- **Encryption(E_K)** – the process of transforming plaintext into ciphertext (also *encipher*)
- **Decryption(D_K)** – the process of transforming ciphertext into plaintext (also *decipher*)
- **Encryption key(K)** – the text value required to encrypt and decrypt data

Vigenère Cipher

- In the 16th century in France, **Blaise de Vigenère** developed a **substitution cipher** for Henry III
- แบลส เดอ วิเจแนร์
- ใช้แนวคิด Caesar cipher
  - เพิ่มการเปลี่ยน key ในการเข้าและถอดรหัส
  - ครั้งแรกของการ เข้ารหัสด้วยการระบุกุญแจรหัสลับ

$$C = E_k(M)$$



แบ่งกลุ่ม Ciphers

- Transposition Ciphers
  - สลับตำแหน่ง
  - เช่น **Rail fence** cipher สลับจากการเขียนซ้ายไปขวา เป็นบนลงล่าง

- Substitution Ciphers
  - Caesar cipher
- Monoalphabetic Ciphers
- Polyalphabetic Ciphers

Monoalphabetic Cipher

- One alphabetic character is substituted or another
  - Caesar right-three shift:

A	B	C	D	E	F	G	H	I	J	…	Z
D	E	F	G	H	I	J	K	L	M	…	C

  - Or a more random scheme:

A	B	C	D	E	F	G	H	I	J	…	Z
W	E	R	T	B	N	P	Q	C	U	…	X

- Subject to *frequency analysis* attack

Polyalphabetic Cipher

- Two or more substitution alphabets

Plaintext	A	B	C	D	E	F	G	H	I	…	Z
Alpha 1	W	E	R	T	B	N	P	Q	C	…	X
Alpha 2	R	B	I	K	Q	D	X	U	N	…	E
Alpha 3	V	B	D	R	H	W	A	X	I	…	U
Alpha 4	M	U	T	X	D	G	P	O	W	…	F
Alpha 5	Y	D	V	B	J	I	K	E	Z	…	O

Polyalphabetic Cipher (cont.)

Plaintext	A	B	C	D	E	F	G	H	I	…	Z
Alpha 1	W	E	R	T	B	N	P	Q	C	…	X
Alpha 2	R	B	I	K	Q	D	X	U	N	…	E
Alpha 3	V	B	D	R	H	W	A	X	I	…	U
Alpha 4	M	U	T	X	D	G	P	O	W	…	F
Alpha 5	Y	D	V	B	J	I	K	E	Z	…	O

- CAGED becomes RRADB
- Not subject to *frequency attack*

Running-key Cipher

- Plaintext letters converted to numeric (A=0, B=1, etc.)
- Plaintext values “added” to key values giving ciphertext

Running-key Cipher

- Modulo arithmetic is used to keep results in range 0–26
  - Add 26 if results < 0; subtract 26 if results > 26

Plaintext	A	T	T	A	C	K	A	T	O	N	C	E	V	I	A	N
Key	S	E	C	R	E	T	S	E	C	R	E	T	S	E	C	R
Plaintext	0	19	19	0	2	10	0	19	14	13	2	4	21	8	0	13
Key	18	4	2	17	4	19	18	4	2	17	4	19	18	4	2	17
Sum	18	23	21	17	6	3	18	23	16	4	7	23	11	12	2	4
Ciphertext	S	X	V	R	G	D	S	X	Q	E	H	X	L	M	C	E

Crack classic cryptosystems

- **Statistical ciphertext-only attack**
- EXAMPLE: Consider the ciphertext "**KHOOR ZRUOG**." We first compute the fre- quency of each letter in the ciphertext:
- ตัวอักษรปรากฏในหนังสือ บ่อย (ความถี่) ไม่เท่ากัน
- บางตัวอักษร พบบ่อย เช่น อักษรที่ทำหน้าที่เป็น สระ (a,e,i,o) ตัวอักษร (t,h)

a	0.080	h	0.060	n	0.070	t	0.090
b	0.015	i	0.065	o	0.080	u	0.030
c	0.030	j	0.005	p	0.020	v	0.010
d	0.040	k	0.005	q	0.002	w	0.015
e	0.130	l	0.035	r	0.065	x	0.005
f	0.020	m	0.030	s	0.060	y	0.020
g	0.015					z	0.002

Statistical ciphertext-only attack

- "**KHOOR ZRUOG**." `G 0.1 H 0.1 K 0.1 O 0.3 R 0.2 U 0.1 Z 0.1`
- f(c) ได้จากตารางความถี่ตัวอักษร
- p(c–i) ได้จากจำนวน

$$\phi(i) = \sum_{0 \le c \le 25} f(c)p(c-i)$$

$$\phi(i) = 0.1p(6-i) + 0.1p(7-i) + 0.1p(10-i) + 0.3p(14-i) + 0.2p(17-i) + 0.1p(20-i) + 0.1p(25-i)$$

Statistical ciphertext-only attack

- i=3 , “WTAAD LDGAS”
- i=6 , “EBIIL TLOIA”
- i=10 ,“HELLO WORLD”

i	$\phi(i)$	*i*	$\phi(i)$	*i*	$\phi(i)$	*i*	$\phi(i)$
0	0.0482	7	0.0442	13	0.0520	19	0.0315
1	0.0364	8	0.0202	**14**	**0.0535**	20	0.0302
2	0.0410	9	0.0267	15	0.0226	21	0.0517
3	**0.0575**	**10**	**0.0635**	16	0.0322	22	0.0380
4	0.0252	11	0.0262	17	0.0392	23	0.0370
5	0.0190	12	0.0325	18	0.0299	24	0.0316
6	**0.0660**					25	0.0430

Topic

- The History of Cryptography
- **Encryption methodologies**
- Cryptanalysis
- Key management
- Applications and uses of cryptography

เทคนิคเข้ารหัสสมัยใหม่

- กุญแจลับ ไม่จำเป็นต้องมีความยาวเท่ากับข้อความ
- ความยาว Ciphertext ไม่จำเป็นต้องเท่ากับความยาว Plaintext
- ขั้นตอนเข้ารหัส

Definitions

- **Encryption** is a method of transforming readable data, called **plaintext**, into a form that appears to be random and unreadable, which is called **ciphertext**.
- **Plaintext** is in a form that can be understood either by a person (a document) or by a computer (executable code).
- **Ciphertext**, neither human nor machine can properly process it until it is decrypted
- **Cryptosystem**, A system or product that provides encryption and decryption
- **Algorithm**, the set of rules also known as the cipher, dictates how enciphering and deciphering take place

Encryption

- key (cryptovaiable)
- keyspace หมายถึง จำนวนของกุญแจที่เป็นไปได้
  - ถ้า keyspace น้อยจะทำให้เกิดการใช้ key ซ้ำ
  - เกิดการถอดรหัสได้
  - กุญแจขนาด 2 บิท มี keyspace $2^2 = 4$ จำนวน , กุญแจขนาด 512 มี keyspace = 2^{512}

Cryptosystem

- Software
- Protocols
- Algorithms
- Keys
- ตัวอย่าง Cryptosystem
  - TLS
  - PGP
  - RC4
  - AES

The Strength of the Cryptosystem

- ความแข็งแรงของ Cryptosystem เป็นการทดสอบความปลอดภัยของ algorithm สำหรับเข้าและถอดรหัส
- กล่าวถึง Strength ของ Cryptosystem จะสนใจ
  - ความยากของการได้ key
  - ความยากของการได้ Plaintext
- การได้ key วัดจากขนาดของ keyspace
- การ breaking cryptosystem ใช้วิธี brute-force attack
  - Pentium Core i5 ได้กุญแจใน 3 ชั่วโมงถือว่าไม่ปลอดภัย
  - cryptosystem ที่ปลอดภัย เป็นการกล่าวถึงการใช้ซุปเปอร์คอมพิวเตอร์ brute-force attack ต้องใช้เวลา มากกว่า 1.2ล้านปี

Cryptosystem สมัยใหม่

- **One-Time Pad**
- Ciphers สมัยใหม่
  - Block Ciphers
  - Stream Ciphers

One-time Pad

- Works like running key cipher, except that key is length of plaintext, and is used only once
- Highly resistant to cryptanalysis

Plaintext	A	T	T	A	C	K	A	T	O	N	C	E	V	I	A	N
Key	X	V	G	J	E	R	I	O	Q	W	J	P	E	K	A	F
Plaintext	0	19	19	0	2	10	0	19	14	13	2	4	21	8	0	13
Key	23	21	6	9	3	17	8	14	16	22	9	15	4	10	0	5
Sum	23	14	25	9	5	1	8	7	4	9	11	19	25	18	0	18
Ciphertext	X	O	Z	J	F	B	I	H	E	J	L	T	Z	U	A	U

Cryptosystem สมัยใหม่

- One-Time Pad
- **Ciphers สมัยใหม่**
  - Block Ciphers
  - Stream Ciphers

Block Ciphers

- Encrypt and decrypt a block of data at a time
  - Typically 128 bits
- Typical uses for block ciphers
  - Files, e-mail messages, text communications, web
- Well known encryption algorithms
  - DES, 3DES, AES, CAST, Twofish, Blowfish, Serpent

Block Cipher Modes of Operation

- Electronic Code Book (ECB)
- Cipher-block chaining (CBC)
- Cipher feedback (CFB)
- Output feedback (OFB)
- Counter (CTR)

Initialization Vector (IV)

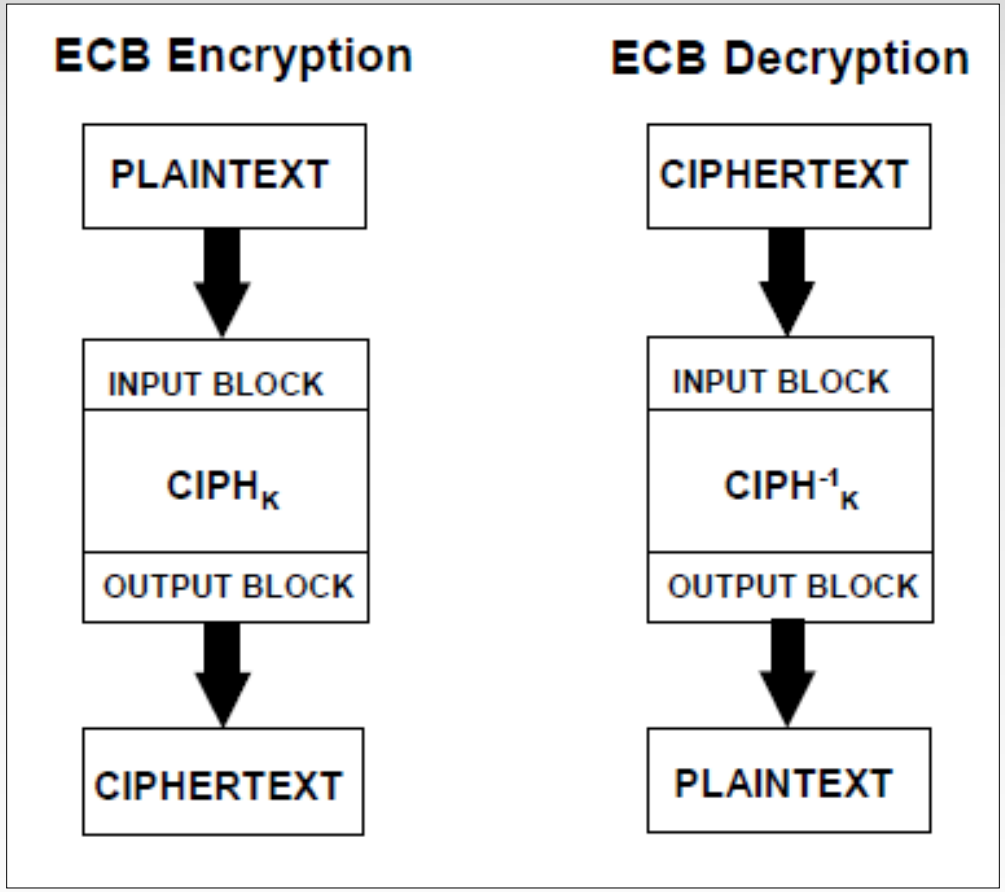
- Starting block of information needed to encrypt the first block of data
- IV must be random and should not be re-used
  - WEP wireless encryption is weak because it re-uses the IV, in addition to making other errors

Block Cipher: Electronic Code Book

- Electronic Code Book (ECB)
- Simplest block cipher mode
- Each block encrypted separately
  - Like plaintext encrypts to like ciphertext
  - Vulnerable to a *dictionary attack*
  - WEP does this

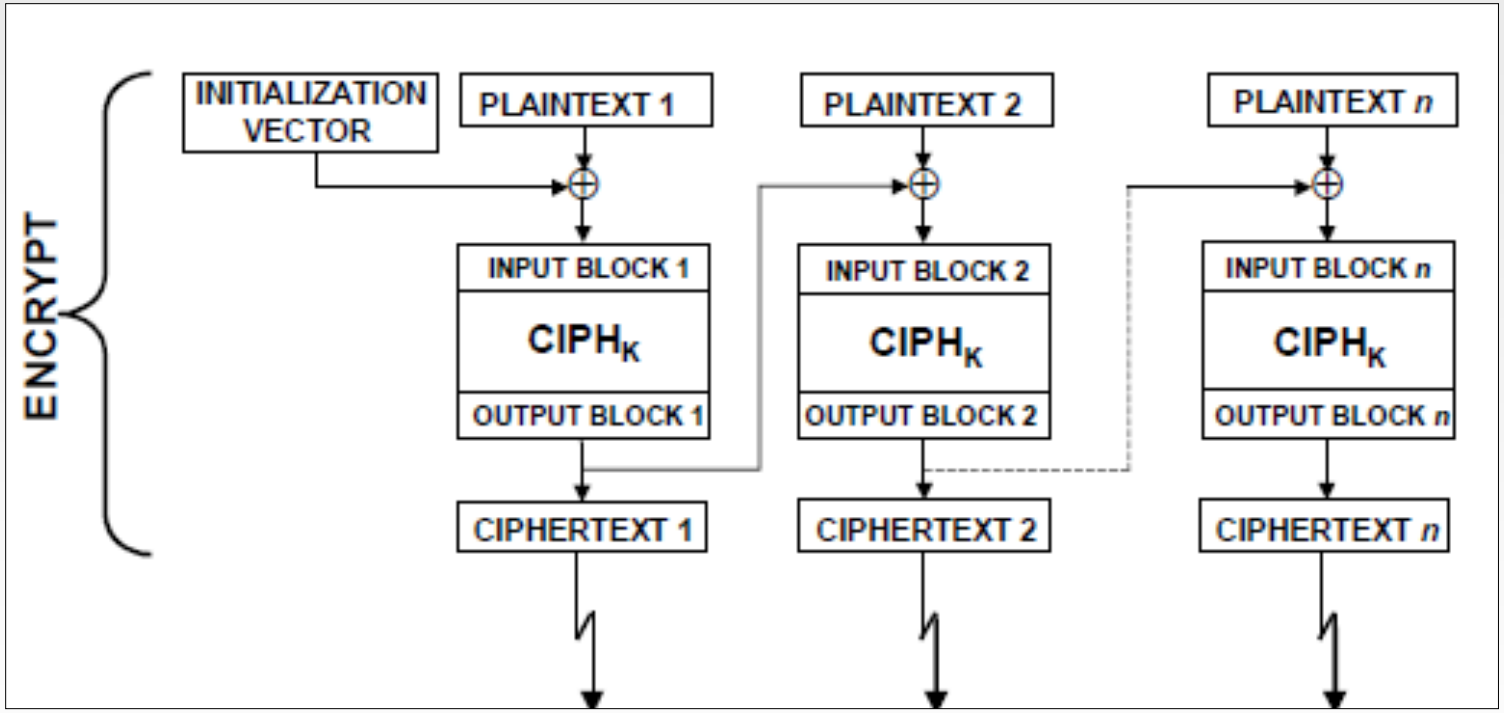
ECB Mode

- Images from NIST



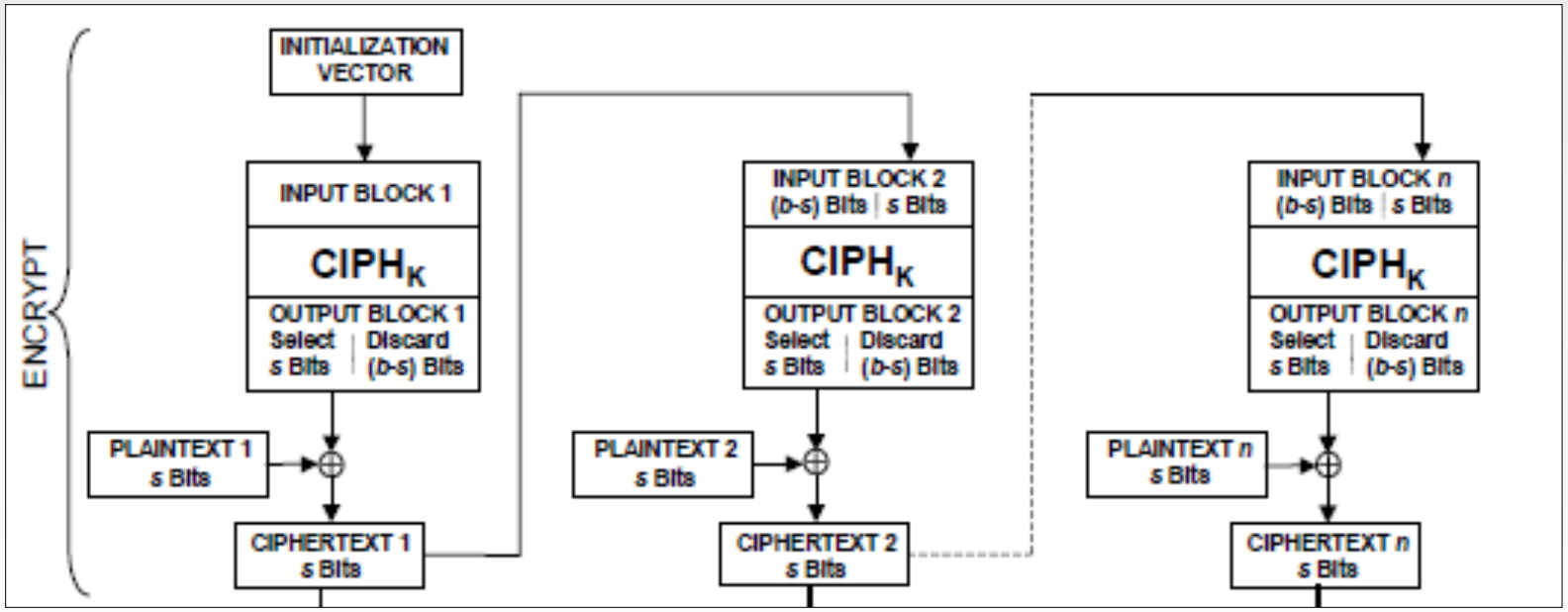
Block Cipher: Cipher-block Chaining (CBC)

- Ciphertext output from each encrypted plaintext block is used in the encryption for the next block
  - ต้องการ IV (initialization vector) สำหรับ block แรก



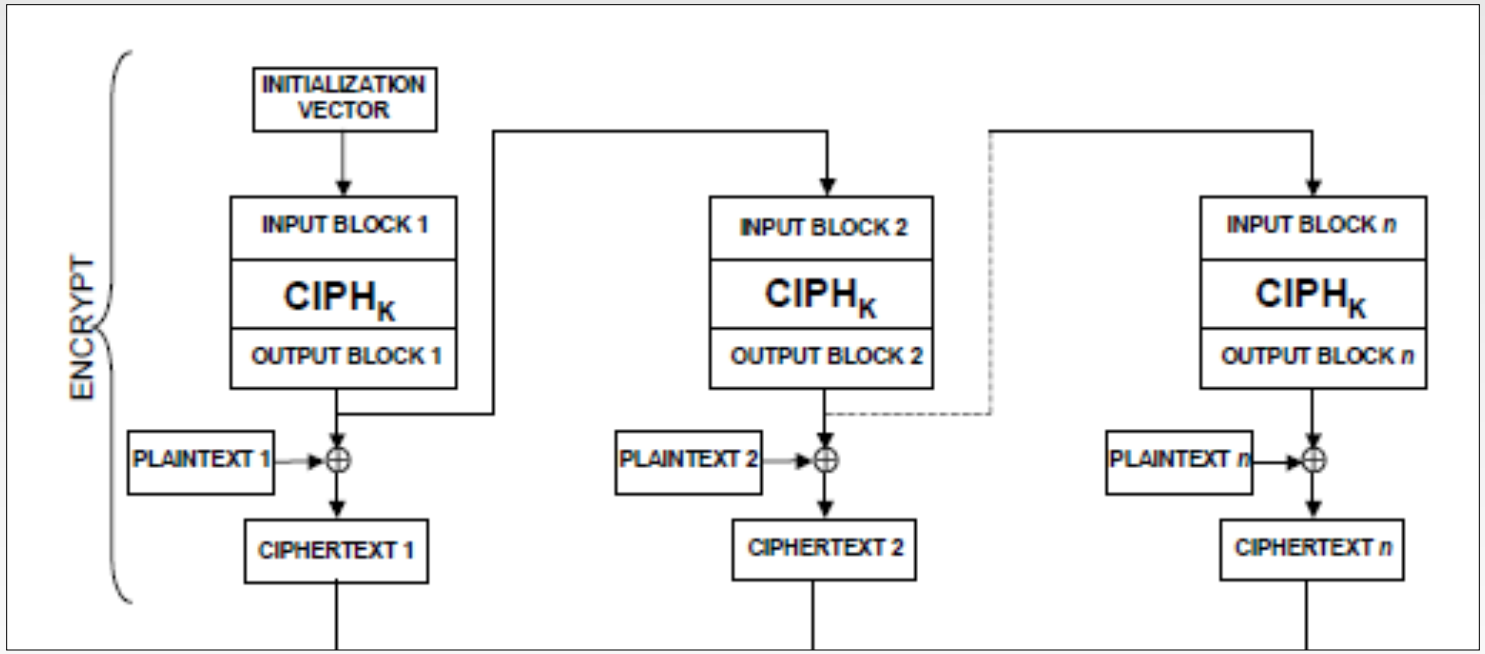
Block Cipher: Cipher Feedback (CFB)

- Plaintext for block N is XOR'd with the ciphertext from block N–1.
- In the first block, the plaintext XOR'd with the encrypted IV



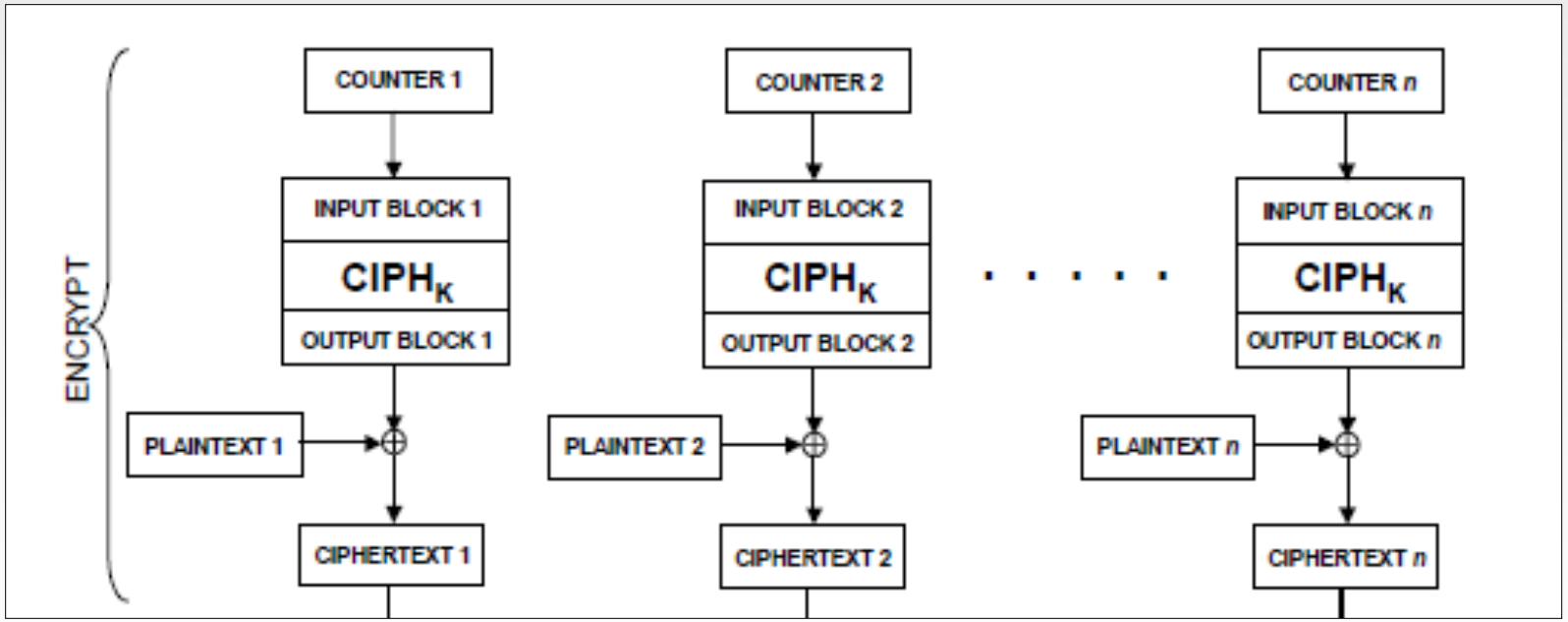
Block Cipher: Output Feedback (OFB)

- Plaintext is XOR'd with the encrypted material in the previous block to produce ciphertext



Block Cipher: Counter (CTR)

- Uses a "nonce" (a random number that is used once) that is concatenated with a counter or other simple function, to create a series of keys
  - Allows parallel computation



Exam

Which cipher mode uses no IV or nonce?

A. Electronic Code Book (ECB)

B. Cipher-block chaining (CBC)

C. Cipher feedback (CFB)

D. Output feedback (OFB)

E. Counter (CTR)

A. Electronic Code Book (ECB) no IV

Exam

Which mode calculates each block separately, so they can all be encrypted at once?

A. Cipher-block chaining (CBC)

B. Cipher feedback (CFB)

C. Output feedback (OFB)

D. Counter (CTR)

E. More than one of the above

D. Counter (CTR) is faster because each block separately and it allows parallel processing

Stream Ciphers

- Used to encrypt a continuous stream of data, such as an audio or video transmission
  - A stream cipher is a substitution cipher that typically uses an exclusive-or (XOR) operation that can be performed very quickly by a computer.
- Most common stream cipher is RC4
- Other stream ciphers
  - A5/1, FISH, Phelix1, ISAAC, MUGI, Panama, Phelix, Pike, Sapphire-II. SEAL, SOBER-128, and WAKE

Stream Ciphers (cont.)

- Encryption: simple XOR with key:

Ciphertext	1	0	1	1	1	0	1	0	0	0	1	0	0	1	1	0
Key	0	1	1	0	1	0	0	1	0	1	1	0	1	0	1	0
Plaintext	1	1	0	1	0	0	1	1	0	1	0	0	1	1	0	0

- Decryption: simple XOR with the same key:

Plaintext	1	1	0	1	0	0	1	1	0	1	0	0	1	1	0	0
Key	0	1	1	0	1	0	0	1	0	1	1	0	1	0	1	0
Ciphertext	1	0	1	1	1	0	1	0	0	0	1	0	0	1	1	0

Exam

Which of these is considered unbreakable?

A. Transposition cipher

B. Monoalphabetic cipher

C. Polyalphabetic cipher

D. Running-key cipher

E. One-time pad

E. One-time pad

Exam

Which of these rearranges the letters in a message without changing them?

A. Transposition cipher

B. Monoalphabetic cipher

C. Polyalphabetic cipher

D. Running-key cipher

E. Block cipher

A. Transposition cipher

Exam

Which of these is a stream cipher?

A. 3DES

B. AES

C. CAST

D. RC4

E. Twofish

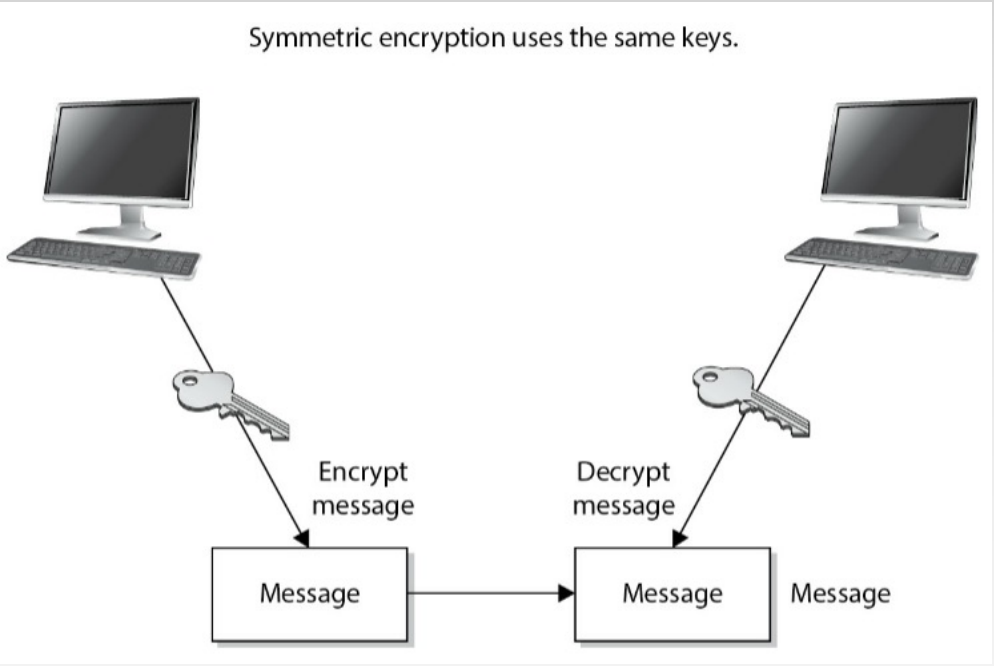
D. RC4 is stream cipher

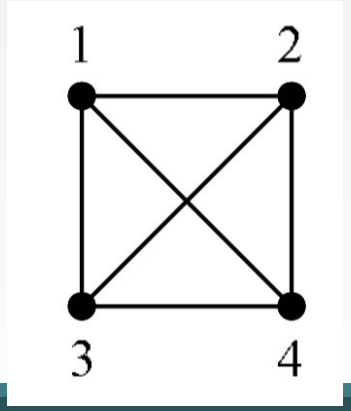
Types of Encryption Keys

- Symmetric key
  - A common secret that all parties must know
  - Difficult to distribute key securely
  - Used by DES, 3DES, AES, Twofish, Blowfish, IDEA, RC5
- Asymmetric key
  - Public / private key
  - Openly distribute public key to all parties
  - Keep private key secret
  - Anyone can use your public key to send you a message
  - Used by RSA. El Gamal, Elliptic Curve

Symmetric cryptography

- ผู้ส่งและผู้รับใช้กุญแจเดียวกัน
- ข้อดี
  - เข้ารหัสและถอดรหัสได้เร็ว
- ข้อเสีย
  - การแจกจ่ายคีย์ให้ปลอดภัยทำได้ยาก
  - เช่น มีผู้ใช้ 4 คนต้องการสื่อสารอย่างปลอดภัย
  - ต้องใช้คีย์ทั้งหมด 6 คีย์





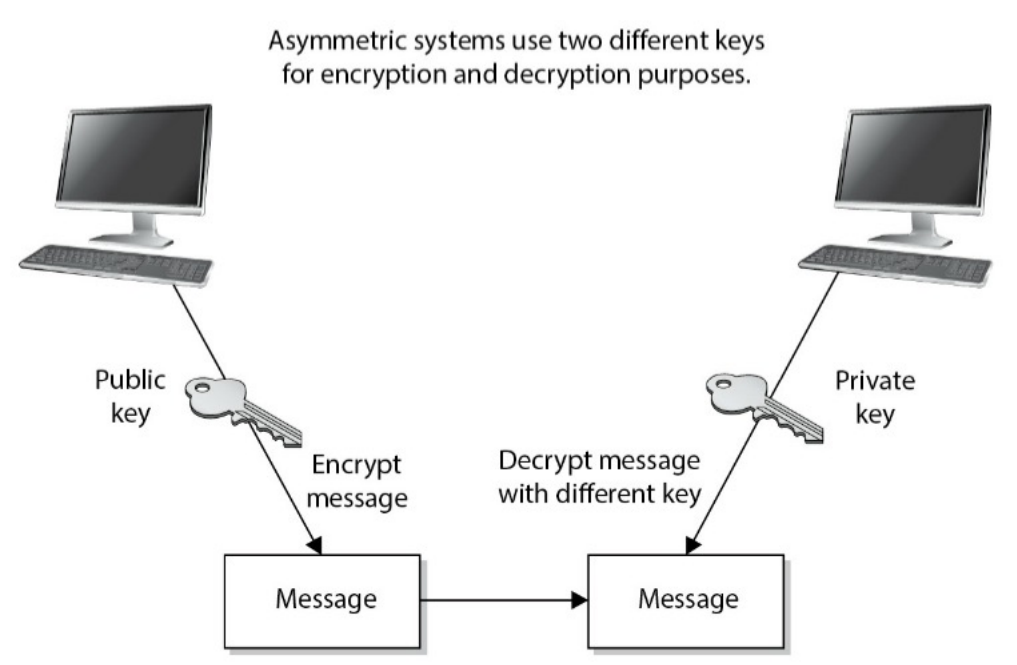
$$\frac{N(N-1)}{2} = \text{number of keys}$$

ตัวอย่าง Symmetric algorithms

- Data Encryption Standard (DES)
- Triple-DES (3DES)
- Blowfish
- Internation Data Encryption Algorithm (IDEA)
- RC4, RC5, and RC6
- Advanced Encryption Standard (AES)

Asymmetric cryptography

- แก้ปัญหาการแจกจ่ายคีย์ ด้วยการสร้างระบบ
  - Public-Private Key
  - มีกุญแจที่ใช้แจกใครก็ได้ (Public Key)
  - มีกุญแจที่มีเพียงดอกเดียว (Private Key)
  - เข้ารหัสและถอดรหัส จะต้องใช้คีย์ตรงข้ามกันเสมอ
  - เข้าด้วย Public ต้องถอดด้วย Private
  - ถ้าเข้าด้วย Private จะต้องถอดด้วย Public เท่ากัน
- ข้อดี
  - ไม่มีปัญหาการแจกจ่ายกุญแจ
- ข้อเสีย
  - ทำงานช้า
  - ต้องการหน่วยประมวลผลความเร็วสูง



Asymmetric Encryption Uses

- Encrypt message with recipient's public key
  - Only recipient can read it, using his or her **private key**
  - Provides **confidentiality**
- Sign message
  - Hash message, encrypt hash with your private key
  - Anyone can verify the signature using your **public key**
  - Provides **integrity** and **non-repudiation** (sender cannot deny authorship)
- Sign and encrypt
  - Both of the above

การประยุกต์ Asymmetric Encryption

- เจาะจงผู้รับ
- ต้องการยืนยันผู้ส่ง
  - ข้อความเปิดเผย
  - ข้อความเข้ารหัส (เจาะจงผู้รับ และ ยืนยันผู้ส่ง)

ต้องการเจาะจงผู้รับ

- Encrypt message with recipient's public key
- ขั้นตอน
  - รับกุญแจ Public key จาก อินเทอร์เน็ต ที่เจ้าของกุญแจเป็นผู้โพสเอง
  - นำข้อความ (Plaintext) ที่ต้องการส่ง เข้ารหัสด้วย Public key
  - ส่งข้อความนั้นไปหาผู้รับ
  - ผู้รับจะถอดรหัสได้ ต้องเป็นผู้ที่มี Private Key คู่กับ Public Key ที่ใช้เข้ารหัส

ต้องการยืนยันผู้ส่ง

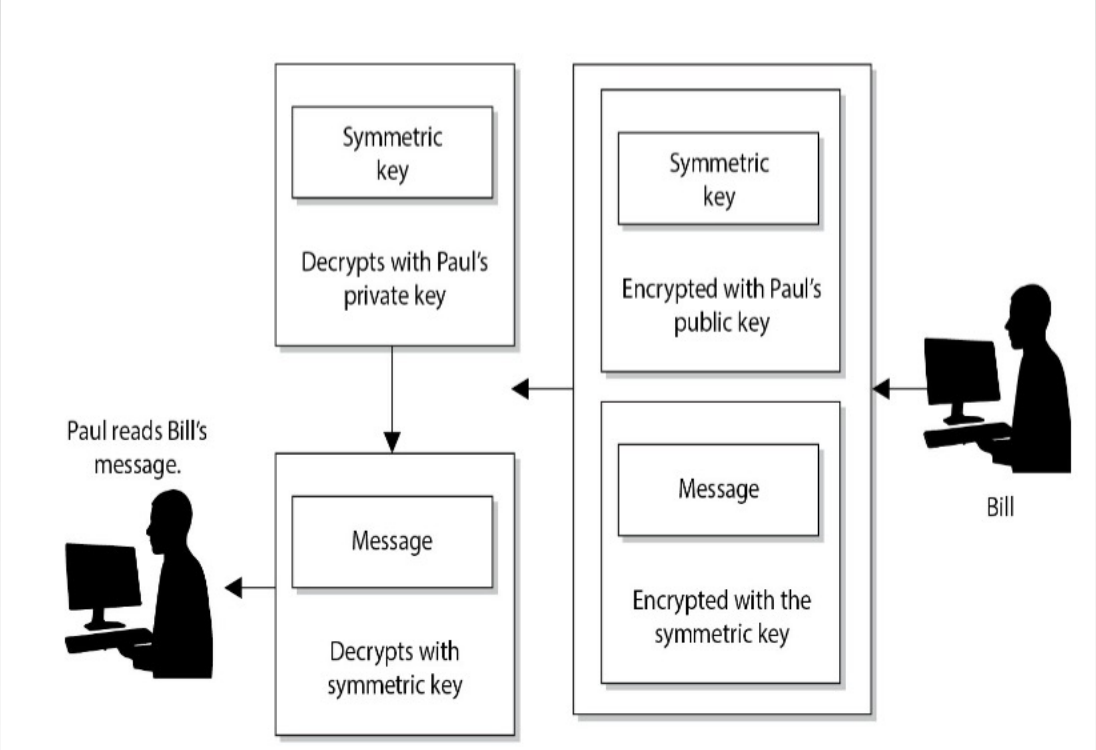
- ข้อความเปิดเผย ทุกคนมีสิทธิ์อ่าน
- ต้องการระบุว่า ผู้ใดเป็นผู้เขียน
- P แทน Plaintext, M แทน Message digest
- ขั้นตอน
  - ใช้ Message Digest (เข้ารหัสทางเดียว) เพื่อหา Signature ของข้อความ
  - P="Hello" , M=SHA256(P)
  - ใช้ Private key ของผู้ส่งเข้ารหัส M ได้ H = $E_{priv}(M)$
  - ส่งข้อความ P|H ไปให้ผู้รับ
  - ผู้รับทำ SHA256(P) ได้ M'
  - ผู้รับใช้ Public key ของผู้ส่งถอด M= $D_{pub}(H)$
    - ถ้า M' == M ถือว่าเป็นผู้ส่งตัวจริง

ต้องการยืนยันผู้ส่ง

- ข้อความเข้ารหัส ให้เฉพาะผู้รับมีสิทธิอ่านข้อความ
- ขั้นตอน
  - A ต้องการส่งข้อความหา B
    1. นำข้อความ M เข้ารหัสด้วย Private key ของผู้ส่ง $C1 = E^{A}_{priv}(M)$
    2. นำ C1 เข้ารหัสด้วย Public key ของผู้รับ $C2=E^{B}_{pub}(C1)$
    3. ส่งข้อความ C2 ไปให้ B
  - เมื่อ B ได้รับ
    1. ใช้ Private key ของตนถอดรหัส $C1 = D^{B}_{priv}(C2)$
    2. ใช้ Public key ของ A ถอดรหัส $M = D^{A}_{pub}(C1)$

Hybrid Encryption Method

- ใช้ Asymmetric ร่วมกับ Symmetric
- Asymmetric ดีตรงแจกกุญแจ แต่เข้ารหัสช้า
- Symmetric ดีตรงเข้ารหัสได้เร็ว แต่เสียตรงการแจกกุญแจ
- ส่ง session keys แทน



Topic

- The History of Cryptography
- Encryption methodologies
- **Cryptanalysis**
- Key Management
- Applications and uses of cryptography

Cryptanalysis

- Frequency analysis
  - Analyzing frequency of characters in ciphertext
- Birthday attacks
  - Collisions in a hash function can be found in approximately sqrt(N) attempts, where N is the number of possible hash values
  - So SHA-1, 160 bits long, will have a collision in 2^80 values

Cryptanalysis

- Ciphertext only attack
  - Attacker has only ciphertext
- Chosen plaintext attack
  - Attacker is able to see encryption of selected plaintext
- Chosen ciphertext attack
- Known plaintext attack

Cryptanalysis (cont.)

- Man in the middle attack
  - Effective against Diffie-Hellman Key Exchange
  - Real public key is replaced by fake one
- Replay attack
  - Effective against SMB, any non-secure cookie-based authentication, almost all Web 2.0 sites

Topic

- The History of Cryptography
- Encryption methodologies
- Cryptanalysis
- Key management
- **Applications and uses of cryptography**

Uses for Cryptography

- File encryption
  - PGP and GPG
  - WinZip (version 9 uses AES)
  - EFS (encrypting file system) for Windows
  - Crypt tool for Unix
- Encrypted volumes and disks
  - Truecrypt for Windows, Mac, Unix
  - Bitlocker for Windows Vista
  - PGP Disk
  - SafeBoot

Uses for Cryptography (cont.)

- E-mail
  - PGP / GPG – asymmetric key (public key crypto)
  - S/MIME (Secure / Multipurpose Internet Mail Extensions) – certificate based
  - PEM (Privacy Enhanced Mail) – not widely used, requires a single global PKI (which was never implemented)
  - MOSS (MIME Object Security Services) – not widely used

Uses for Cryptography (cont.)

- Protecting network communications
  - SSH
    - Replacement for telnet, rsh, rlogin
    - Secure FTP
  - IPsec
    - Encrypts all packets between established pairs of hosts
    - Used for VPNs (Virtual Private Networks)
  - SSL/TLS
    - Protects web browser traffic

Uses for Cryptography (cont.)

- Web browsing – protects session contents from eavesdropping
  - SSL / TLS (Secure Sockets Layer / Transport Layer Security)
    - https: in URL
    - 40–512 bit encryption with secure key exchange
    - Server authentication common, client authentication rare
  - SET (Secure Electronic Transaction)
    - Not widely used

Topic

- The History of Cryptography
- Encryption methodologies
- Cryptanalysis
- **Key management**
- Applications and uses of cryptography

Key Management

- Key creation
  - Process and results must be protected
- Key protection and custody
  - Secured keys in control by the fewest number of persons

Key Management (cont.)

- Key rotation
  - Periodic update of encryption keys
- Key destruction
  - Securely destroy, to protect encrypted data to be retired
- Key escrow
  - Keys held by a trusted third party

Message Digests and Hashing

- Message digest or hash
  - The result of a one-way function on a file or message
  - Fixed-length result regardless of message size
  - Impossible (or very difficult) to derive original message from digest
  - No other message should produce the same digest (such pairs are *collisions*)
  - Algorithms
    - MD-5, SHA-1, HMAC

Digital Signatures

- Message digest that is cryptographically combined with signer's private key
  - Requires public key cryptography
  - Verifies message integrity
  - Verifies identity of signer
  - Algorithms: DSA, El Gamal, Elliptic Curve DSA

Non-repudiation

- Inability for a user to repudiate (deny) an action, because of the methods used to permit or authorize the action
  - Digital signature
    - Verifies integrity of transaction
    - Verifies identity of person performing transaction
  - Password required to use digital signature

Public Key Infrastructure (PKI)

- Online facility
  - Storage of users' public encryption keys
  - Fast lookup via an API that makes use automatic
  - PKI platforms
    - LDAP
    - Microsoft Active Directory

Encryption Alternatives

- Steganography
  - Data hidden in image files, subtle changes that the eye won't see; can be encrypted as well
  - Many "stego" tools available
- Watermarking
  - Like a digital signature – a visible or invisible mark that claims ownership

Which of these is an asymmetric algorithm?

A. DES
B. AES
C. RSA
D. Twofish
E. RC5