การจัดการความมั่นคงปลอดภัยทางข้อมูล

Information Security Management

Chapter 7 : การใช้งานการเข้ารหัส (Using Encryption)

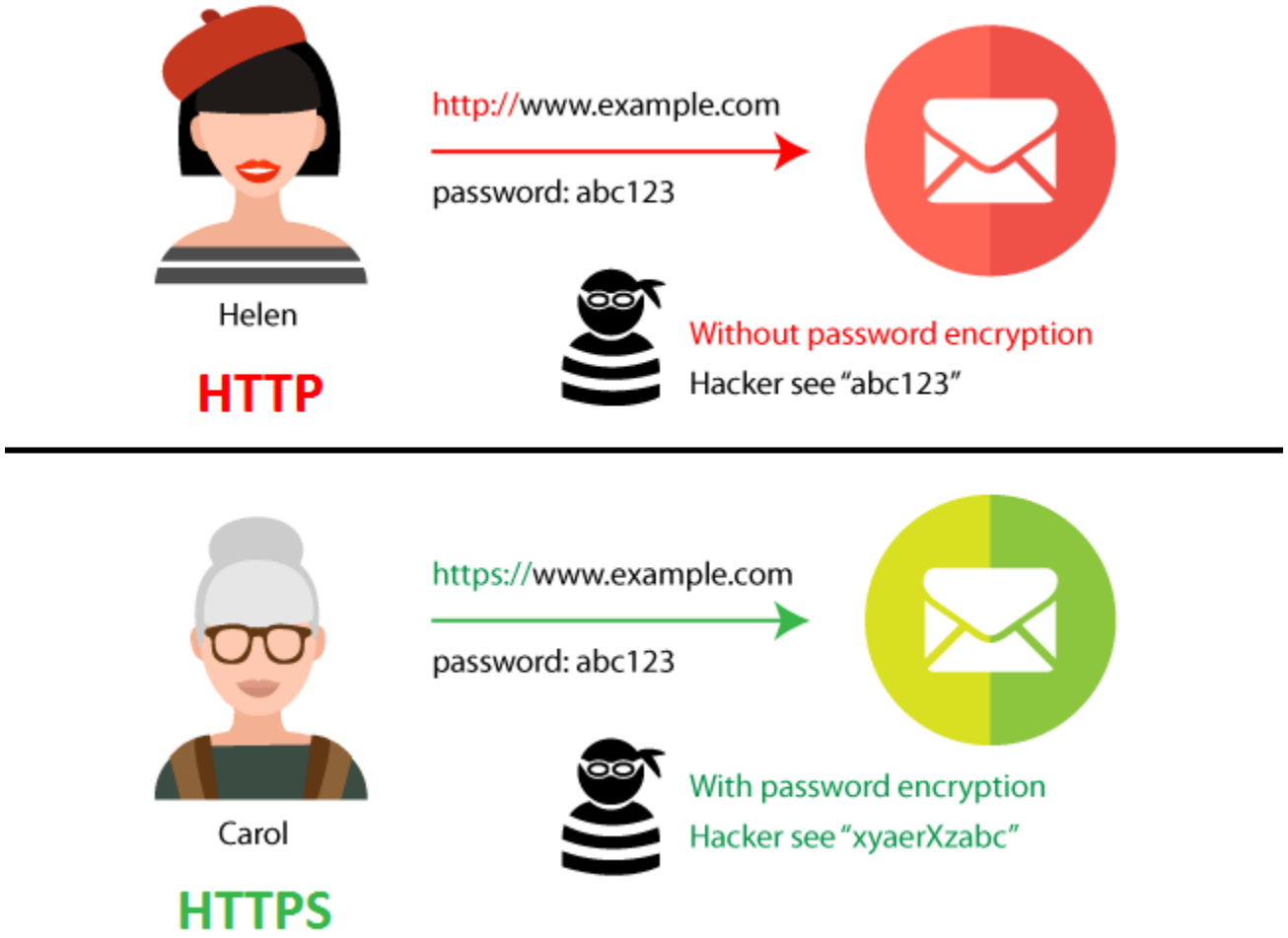
เนื้อหา

- Encode vs. Encryption vs. Hashing vs. Obfuscation
- Encryption : Symmetric Encryption vs. Asymmetric Encryption
- Encryption : Caesar cipher, Substitution Cipher, Vigenere Cipher
- Hashing : md5(), sha1()

Encode vs. Encryption vs. Hashing vs. Obfuscation

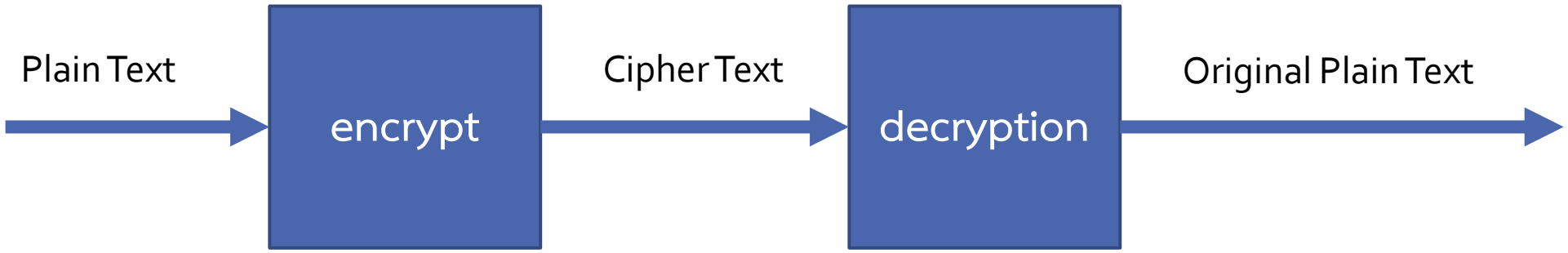
Packet Sniffing

Packet Sniffing : HTTP vs HTTPS



การเข้ารหัสข้อมูล

มีจุดประสงค์เพื่อรักษาความลับของข้อมูล ข้อมูลนั้นจะถูกเปิดอ่านโดยบุคคลที่ได้รับอนุญาตเท่านั้น หลักการของการเข้ารหัสข้อมูล คือ แปลงข้อมูล (Encrypt) ไปอยู่ในรูปของข้อมูลที่ไม่สามารถอ่านได้โดยตรง ข้อมูลจะถูกถอดกลับด้วยกระบวนการถอดรหัส (Decryption)



องค์ประกอบของรหัสลับ

- ข้อความต้นฉบับ (Plain text)
- อัลกอริทึมการเข้ารหัสลับ (Encryption Algorithm)
- กุญแจลับ (Key)
- ข้อความไซเฟอร์ (Ciphertext)
- อัลกอริทึมการถอดรหัสลับ (Decryption Algorithm)

Encode vs. Encryption vs. Hashing vs. Obfuscation

Encode

การแปลงข้อมูลจากแบบหนึ่ง ไปอีกแบบหนึ่ง เพื่อทำให้ระบบอื่น ๆ สามารถ “**เข้าใจและนำไปใช้ (Usability)**” ต่อได้

https://medium.com/@Mnosuk/บางอย่าง-คนสนิทกันดีเท่านั้นถึงจะเข้าใจกันได้-95c24a9c60ac

result = **encoder(**plaintext**)**;

https://medium.com/@Mnosuk/%E0%B8%9A%E0%B8%B2%E0%B8%87%E0%B8%AD%E0%B8%A2%E0%B9%88%E0%B8%B2%E0%B8%87-%E0%B8%84%E0%B8%99%E0%B8%AA%E0%B8%99%E0%B8%B4%E0%B8%97%E0%B8%81%E0%B8%B1%E0%B8%99%E0%B8%94%E0%B8%B5%E0%B9%80%E0%B8%97%E0%B9%88%E0%B8%B2%E0%B8%99%E0%B8%B1%E0%B9%89%E0%B8%99%E0%B8%96%E0%B8%B6%E0%B8%87%E0%B8%88%E0%B8%B0%E0%B9%80%E0%B8%82%E0%B9%89%E0%B8%B2%E0%B9%83%E0%B8%88%E0%B8%81%E0%B8%B1%E0%B8%99%E0%B9%84%E0%B8%94%E0%B9%89-95c24a9c60ac

Encode vs. Encryption vs. Hashing vs. Obfuscation

Encode

https://medium.com/@Mnosuk/บางอย่าง-คนสนิทกันดีเท่านั้นถึงจะเข้าใจกันได้-95c24a9c60ac

result = **json_encoder(**plaintext**)**;

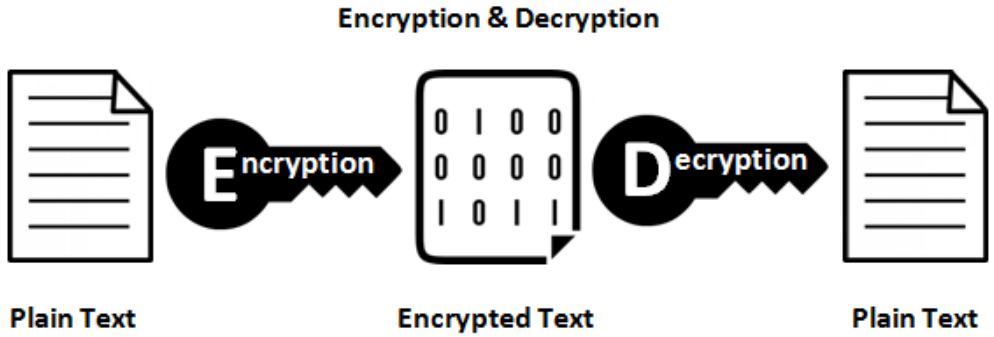
https://medium.com/@Mnosuk/%E0%B8%9A%E0%B8%B2%E0%B8%87%E0%B8%AD%E0%B8%A2%E0%B9%88%E0%B8%B2%E0%B8%87-%E0%B8%84%E0%B8%99%E0%B8%AA%E0%B8%99%E0%B8%B4%E0%B8%97%E0%B8%81%E0%B8%B1%E0%B8%99%E0%B8%94%E0%B8%B5%E0%B9%80%E0%B8%97%E0%B9%88%E0%B8%B2%E0%B8%99%E0%B8%B1%E0%B9%89%E0%B8%99%E0%B8%96%E0%B8%B6%E0%B8%87%E0%B8%88%E0%B8%B0%E0%B9%80%E0%B8%82%E0%B9%89%E0%B8%B2%E0%B9%83%E0%B8%88%E0%B8%81%E0%B8%B1%E0%B8%99%E0%B9%84%E0%B8%94%E0%B9%89-95c24a9c60ac

!!! ข้อควรระวังสูงสุด คือ การนำ Encode ไปเพื่อใช้ในการรักษาความลับ (Confidentiality) ของข้อมูล **ซึ่งมันไม่ได้**

Encode vs. Encryption vs. Hashing vs. Obfuscation

Encryption

การแปลงข้อมูลจากแบบหนึ่ง ไปเป็นอีกแบบหนึ่ง โดยที่มีรหัสผ่าน (key) เท่านั้น ที่จะสามารถเข้าใจความหมายของข้อความต้นฉบับได้ จุดประสงค์เพื่อ **ปกปิดและรักษาความลับ (Confidentiality)**



https://cryptii.com/

Bomber tomorrow morning

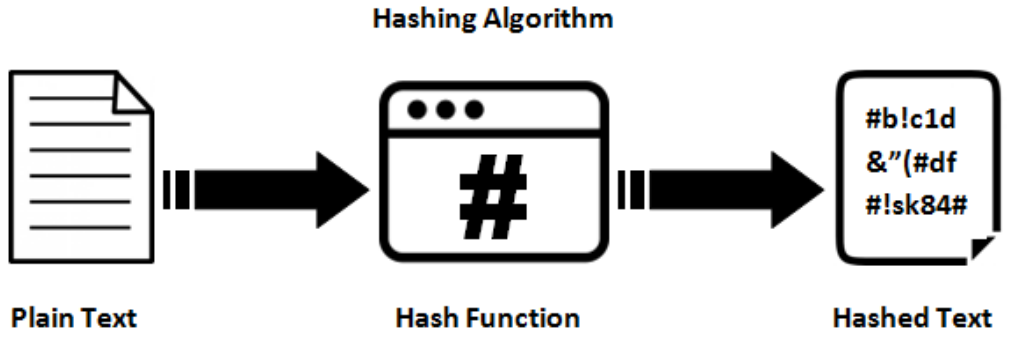
wgbap fudtw hkqcu ndute z

Encode vs. Encryption vs. Hashing vs. Obfuscation

Hashing

การแปลงข้อมูลจากอีกแบบหนึ่ง สู่อีกแบบหนึ่งโดยไม่สามารถแปลงค่าที่ถูก Hash กลับมาเป็นข้อความต้นฉบับได้ โดยจุดประสงค์คือ ใช้เพื่อทำการ **ยืนยันว่าไม่มีการเปลี่ยนแปลงข้อมูล - (Integrity)**

เช่น md5(), sha1(), hash()



id	username	password	real_password
1	mnosuk	098cbc1fbd44085ab94d0748e1c38e88	notenarak
2	jbp	e10adc3949ba59abbe56e057f20f883e	123456
3	ajaja	8f62947554d1aec182f604ea95dc89d4	AjajaLoveYouAll
4	aofleejay	e9ae38c35488f4d4d7975a47a23f7fe1	mooping

Encode vs. Encryption vs. Hashing vs. Obfuscation

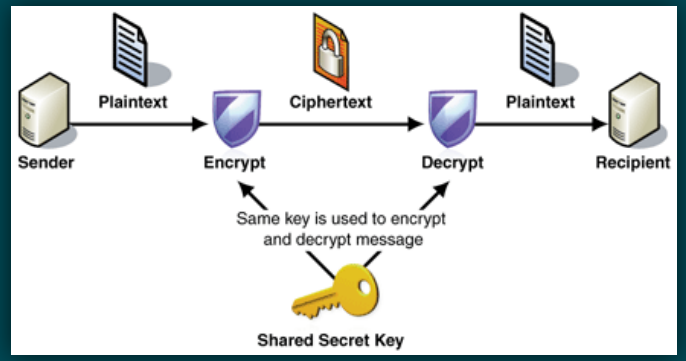
Obfuscation

การทำให้ข้อมูลนั้นอ่านได้ยาก เพื่อให้ยากต่อการแกะ (Attack) หรือการ Copy ข้อมูล มักใช้ในการหลบเลี่ยงการตรวจจับของ Antivirus, การทำให้สามารถอ่านได้ยากเมื่อถูก Reverse Engineer

https://javascriptobfuscator.com/

Symmetric Encryption vs. Asymmetric Encryption

Symmetric Vs. Asymmetric Encryption



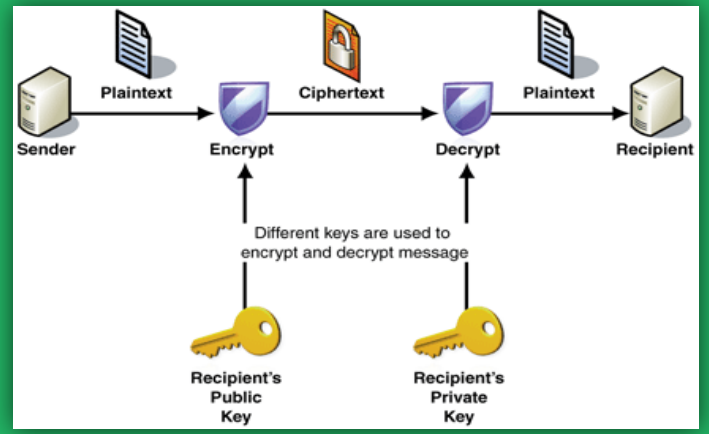
SYMMETRIC

(Secret Key)

VS

ASYMMETRIC

(Public Key)

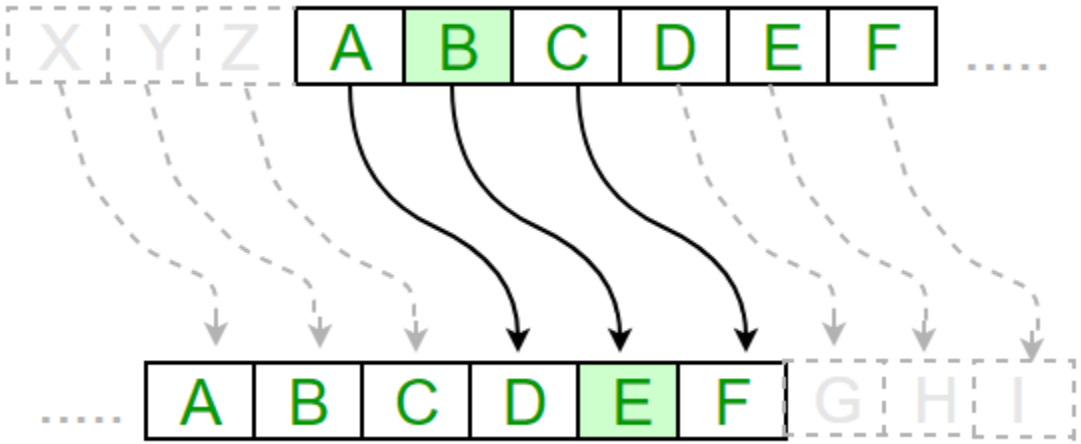


- Vigenere Cipher
- CBC
- DES
- DES
- CTR

- ElGamal
- RSA
- การเข้ารหัสลับเส้นโค้งเชิงวงรี
- Digital Signature Algorithm (DSA)

Caesar Cipher

คิดค้นโดยกษัตริย์ Julius Caesar เพื่อสื่อสารับทหารในกองทัพ และป้องกันไม่ให้ข่าวสารรั่วไหลไปถึงศัตรู โดยหลักการ คือ ทำการเลื่อน (Shift) ตัวอักษรไป 3 ตำแหน่งจากตำแหน่งเดิม



Caesar Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M
D	E	F	G	H	I	J	K	L	M	N	O	P
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	R	S	T	U	V	W	X	Y	Z	A	B	C

ตัวอย่าง

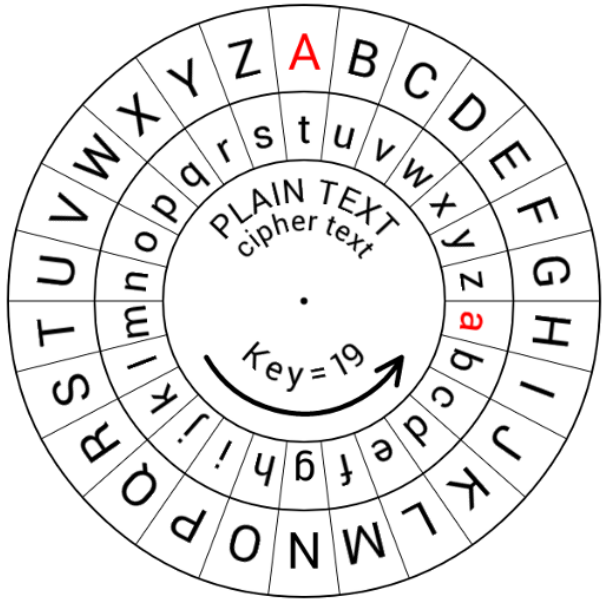
Plain text : **You are so beautiful to me.**

Cipher text : **BRX DUH VR EHDXWLIXO WR PH.**

ส่วนจะเอาช่องว่าง และ Punctuation marks ต่างๆ ออกหรือไม่ก็ได้ แต่จะทำให้เดาข้อความได้ยากขึ้น

Caesar Cipher

นำไปประยุกต์ใช้งาน สามารถนำมาเปลี่ยน Key ได้ทำให้มี key 2-26



Caesar Cipher Wheel

	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Caesar Cipher

การแกะรหัสของ Caesar cipher นำมาซึ่งการโจมตีได้ง่ายโดยไม่จำเป็นต้องรู้ Key ซึ่งเรียกการโจมตีนี้ว่า Brute Force Attack ซึ่งทำการไล่สุ่ม Key เพียง 24 ครั้งเท่านั้น

```
Encrypted message: JXKHITQO
Decrypted message: SECRET MESSAGE
Brute Force attack:
Recovered message (key= 0): HDVB WR EUHDN
Recovered message (key= 1): GCUA VQ DTGCM
Recovered message (key= 2): FBTZ UP CSFBL
Recovered message (key= 3): EASY TO BREAK
Recovered message (key= 4): DZRX SN AQDZJ
Recovered message (key= 5): CYQW RM ZPCYI
Recovered message (key= 6): BXPV QL YOBXH
Recovered message (key= 7): AWOU PK XNAWG
Recovered message (key= 8): ZVNT OJ WMZVF
Recovered message (key= 9): YUMS NI VLYUE
Recovered message (key=10): XTLR MH UKXTD
Recovered message (key=11): WSKQ LG TJWSC
Recovered message (key=12): VRJP KF SIVRB
Recovered message (key=13): UQIO JE RHUQA
Recovered message (key=14): TPHN ID QGTPZ
Recovered message (key=15): SOGM HC PFSOY
Recovered message (key=16): RNFL GB OERNX
Recovered message (key=17): QMEK FA NDQMW
Recovered message (key=18): PLDJ EZ MCPLV
Recovered message (key=19): OKCI DY LBOKU
Recovered message (key=20): NJBH CX KANJT
Recovered message (key=21): MIAG BW JZMIS
Recovered message (key=22): LHZF AV IYLHR
Recovered message (key=23): KGYE ZU HXKGQ
Recovered message (key=24): JFXD YT GWJFP
Recovered message (key=25): IEWC XS FVIEO
```

Substitution Cipher

ระบบรหัสลับแบบสับเปลี่ยน (Substitution Cipher) คือ การสับเปลี่ยนแต่ละตัวอักษรใน plaintext ด้วยตัวอักษรอื่น ตามตารางที่กำหนด เช่น A แทนด้วย T, B แทนด้วย P

A	B	C	D	E	F	G	H	I	J	K	L	M
T	P	Y	B	M	H	U	Q	X	C	J	I	V
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
O	A	N	R	E	K	D	G	S	F	W	L	Z

Substitution Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M
T	P	Y	B	M	H	U	Q	X	C	J	I	V
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
O	A	N	R	E	K	D	G	S	F	W	L	Z

ตัวอย่าง

Plain text : **You are so beautiful to me.**

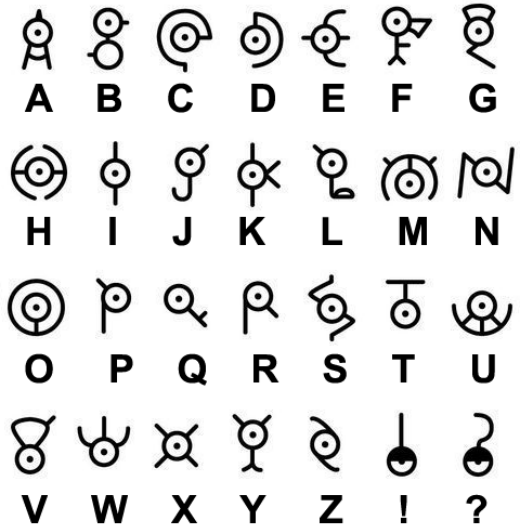
Cipher text : **LAG TEM KA PMTGDXHGI DA VM.**

ส่วนจะเอาช่องว่าง และ Punctuation marks ต่างๆ ออกหรือไม่ก็ได้ แต่จะทำให้เดาข้อความได้ยากขึ้น

Substitution Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M
T	P	Y	B	M	H	U	Q	X	C	J	I	V
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
O	A	N	R	E	K	D	G	S	F	W	L	Z

นำไปประยุกต์ใช้งาน



การสุ่มจับคู่ตัวอักษรเป็นชุด

Array = ((A,V),(D,X),(H,B),(I,G),(K,J),(M,C),(O,Q),(R,L),(S,N),(U,E),(W,F),(Y,P),(Z,T))

Vigenere Cipher

Plain text : ATTACKATDAWN

Key : LEMON

Cipher text : LXFOPVEFRNHR

	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

ขั้นตอนการทำ Vigenere Cipher

1. ความสัมพันธ์ระหว่างตัวอักษรและตัวเลข

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

ขั้นตอนการทำ Vigenere Cipher

2. เลือกขนาดของ Key และคำ Keyword

Sender

Key

M = 5

Keyword = “LEMON”

Receiver

ขั้นตอนการทำ Vigenere Cipher

3. สร้าง Private Key

Key

M = 5

Keyword = “LEMON”

L	E	M	O	N
11	4	12	14	13

Sender

Private Key = (11,4,12,14,13)

Receiver

ขั้นตอนการทำ Vigenere Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

4. ผู้ส่งทำการเข้ารหัสข้อความที่ต้องการส่ง

Message = “ATTACK AT DAWN”

Sender

Message	A	T	T	A	C	K	A	T	D	A	W	N
M	0	19	19	0	2	10	0	19	3	0	22	13
Private Key	L	E	M	O	N	L	E	M	O	N	L	E
P	11	4	12	14	13	11	4	12	14	13	11	4
C = M+P MOD26	11	23	5	14	15	21	4	5	17	13	7	17
Ciphertext	L	X	F	O	P	V	E	F	R	N	H	R

Ciphertext : LXFOPVEFRNHR

ขั้นตอนการทำ Vigenere Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

5. ผู้รับทำการถอดรหัสข้อความที่ได้รับมา

Receiver

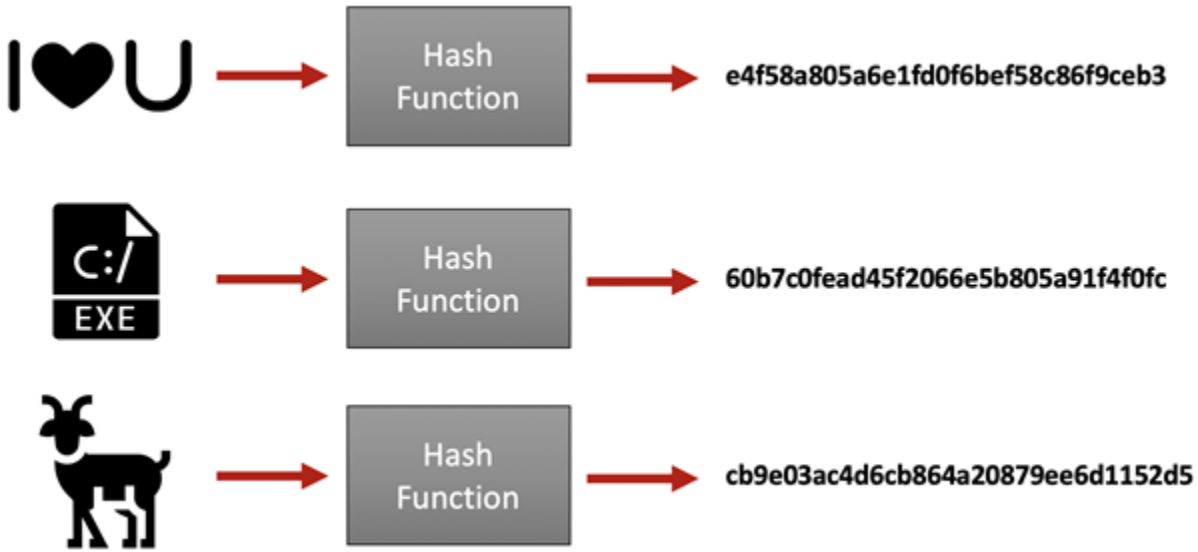
Ciphertext : LXFOPVEFRNHR

Ciphertext	L	X	F	O	P	V	E	F	R	N	H	R
M	11	23	5	14	15	21	4	5	17	13	7	17
Private Key	L	E	M	O	N	L	E	M	O	N	L	E
P	11	4	12	14	13	11	4	12	14	13	11	4
C = M-P MOD26	0	19	19	O	2	10	0	19	3	0	22	13
SendMessage	A	T	T	A	C	K	A	T	D	A	W	N

Message = “ATTACK AT DAWN”

Hashing

Hashing เป็นการเอาข้อมูลที่ไม่ว่าจะมีความยาวแค่ไหนก็ตาม มาผ่าน Formula (Algorithm) และได้ผลออกมาเป็น Hash Value ซึ่งจะมีความยาวเท่าเดิมเสมอ ขึ้นอยู่กับ Formula ที่เราใช้ว่าเป็นอะไร เช่น AES, ECC, MD5 เป็นต้น



Hashing Function

มาตรฐาน Hash Function ที่มีการใช้งานกันอยู่ในปัจจุบัน เช่น Message Digest Algorithm (MD5), Secure Hash Algorithm (SHA-1, SHA-2)

หมายเหตุ ความแตกต่างของแต่ละมาตรฐานอยู่ที่ Algorithm และ Fixed Length Output ที่ได้หลังจากผ่านกระบวนการ Hashing

Replace	With	State Size	Output Size
MD5	Skein-256-128	256	128
	Skein-512-128	512	128
SHA-1	Skein-256-160	256	160
	Skein-512-160	512	160
SHA-224	Skein-256-224	256	224
	Skein-512-224	512	224
SHA-256	Skein-256-256	256	256
	Skein-512-256	512	256
SHA-384	Skein-512-384	512	384
	Skein-1024-384	1024	384
SHA-512	Skein-512-512	512	512
	Skein-1024-512	1024	512

ความปลอดภัย เมื่อใช้ Hashing Function

1.php

```php
<?php
$pass = "1234";
echo md5($pass);

echo "<br>";

$pass = "12345";
echo md5($pass);
?>
```

81dc9bdb52d04dc20036dbd8313ed055
827ccb0eea8a706c4c34a16891f84e7b

```php
$pass = "1234";
echo sha1($pass);

echo "<br>";

$pass = "12345";
echo sha1($pass);
```

7110eda4d09e062aa5e4a390b0a572ac0d2c0220
8cb2237d0679ca88db6464eac60da96345513964

ความปลอดภัย เมื่อใช้ Hashing Function