[illegible] 66050146

เอกสารประกอบการสอน

คณิตศาสตร์สำหรับวิทยาการคอมพิวเตอร์

MATHEMATICS FOR COMPUTER SCIENCE

ผศ.ดร.กนกณัฏฐช์ วัฒนแจ่มศรี

ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ สจล.

Modular arithmetic

ผู้เขียนทำการทบทวน modular arithmetic ดังแสดงดังต่อไปนี้เพื่อใช้ในหัวข้อถัดไป

1. **Reflexivity:** a ≡ a (mod n)
2. **Symmetry**: ถ้า a ≡ b (mod n) แล้ว b ≡ a (mod n)
3. **Transitivity:** ถ้า a ≡ b (mod n) และ b ≡ c (mod n) แล้ว a ≡ c (mod n)
4. ถ้า a ≡ b (mod n) และ c ≡ d (mod n) แล้ว a+c ≡ b+d (mod n)
5. ถ้า a ≡ b (mod n) และ c ≡ d (mod n) แล้ว ac ≡ bc (mod n)
6. ถ้า a ≡ b (mod n) แล้ว $a^m \equiv b^m$ (mod n)
7. ถ้า ab ≡ ac (mod n) และ a และ n ไม่มีตัวประกอบร่วมนอกจาก 1 และ -1 (หรม ของ a และ n คือ 1 หรือ gcd(a,n) =1) (relatively prime) ดังนั้น b ≡ c (mod n)
8. **Fermat's litter theorem:** a^p ≡ a (mod p)
9. สำหรับจำนวนเฉพาะ p ใด ๆ ดังนั้น $(x+y)^p \equiv x^p + y^p \pmod p$
10. **Chinese remainder theorem:** สำหรับจำนวนเต็มบวก m_1 และ m_2 ที่ไม่มีตัวประกอบร่วมนอกจาก 1 และ -1 (relatively prime) และ a และ b เป็นจำนวนเต็มใดๆ จะมี x ที่

    x ≡ a (mod m_1) และ x ≡ b (mod m_2)

Simple Encryption

Simple Encryption เป็นการใส่รหัสแบบง่ายๆ เพื่อใช้ในการส่งข้อความและไม่ต้องการให้คนทั่วไปทราบว่าส่งข้อความอะไรไปยังผู้รับข้อความ ซึ่งได้มีมาหลายพันปี และมีวิธีการดังนี้

1. เปลี่ยนข้อความให้อยู่ในรูปอักษรพิมพ์ใหญ่
2. เปลี่ยนอักษรเป็นตัวเลขระหว่าง 1 ถึง 26
3. ใช้ modular function กันตัวเลขเหล่านั้น
4. แปลงข้อความกลับเป็นตัวอักษร

ตาราง 1. ตารางแสดงการ conversion ของ Letter ↔ Number

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

ตัวอย่าง 1 (Encryption)

จงทำการใส่รหัส "STOP THIEF" โดยกำหนดให้ encryption function คือ

$$\mathrm{f(a) = (3a + 9) mod 26} \tag{1}$$

วิธีทำ 1. STOP THIEF (อักษรพิมพ์ใหญ่)

2. 19, 20, 15, 16 20, 8, 9, 5, 6

3. 14, 17, 2, 5 17, 7, 10, 24, 1 (แทน a ในสมการ (1) ด้วยตัวเลขในข้อ 2.)

เช่น เลขตัวแรกคือ 19 ดังนั้น f(19) = (3(19)+9) mod 26 = 14

4. NQBE QGJXA

Decryption

Decryption เป็นการถอดรหัสหลังจากได้รับข้อความจากผู้ส่ง ซึ่งทำให้ทำนองเดียวกันกับ Encryption แต่ต้องใช้ฟังก์ชันผกผัน (inverse function) เช่น หาฟังก์ชัน g ซึ่งเป็น inverse function ของ $f(p) = (p + k) \bmod 26$ ดังนั้น $g(p) = f^{-1}(p) = (p - k) \bmod 26$

<u>Caesar cipher</u>

<u>Caesar cipher</u> เป็นวิธีหนึ่งในการใส่รหัสและถอดรหัส ซึ่งมีวิธีการที่คล้ายกับที่กล่าวข้างต้นแต่มีลำดับตัวเลขต่างไปโดยให้อักษร A เป็นศูนย์และอักษรถัดไปมีค่าเพิ่มขึ้นทีละ 1 ดังแสดงในตารางที่ 2 นี้

ตาราง 2. ตารางแสดงการ conversion ของ Letter ↔ Number โดยวิธีของ Caesar cipher

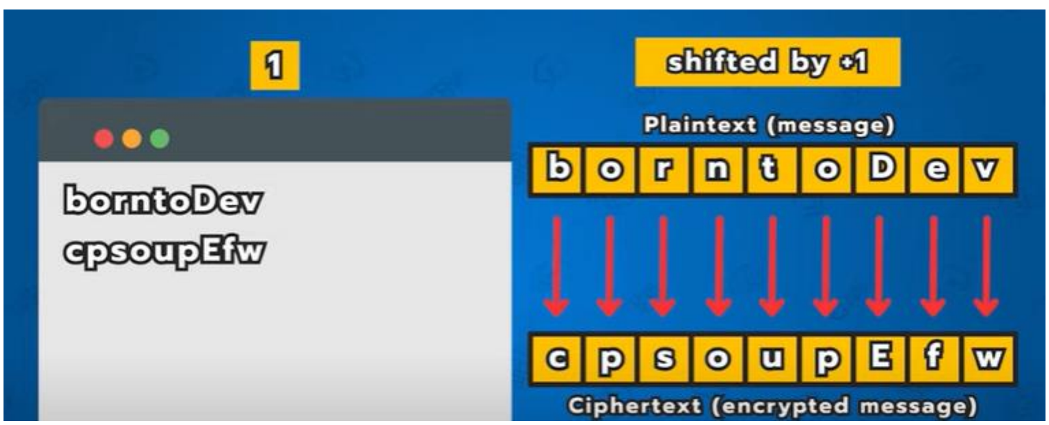
A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

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

Caesar cipher เป็น cipher ที่เรียกว่า shift cipher นั่นคือ ถ้าต้องการ shift อักษรไป 1 ตัว (**shifted by 1**) เราจะใช้ฟังก์ชัน

$$f(p) = (p + 1) \bmod 26$$

สำหรับการใส่รหัส ดังแสดงในรูปที่ 1 ดังนี้



รูปที่ 1: Caesar cipher (shifted by 1)

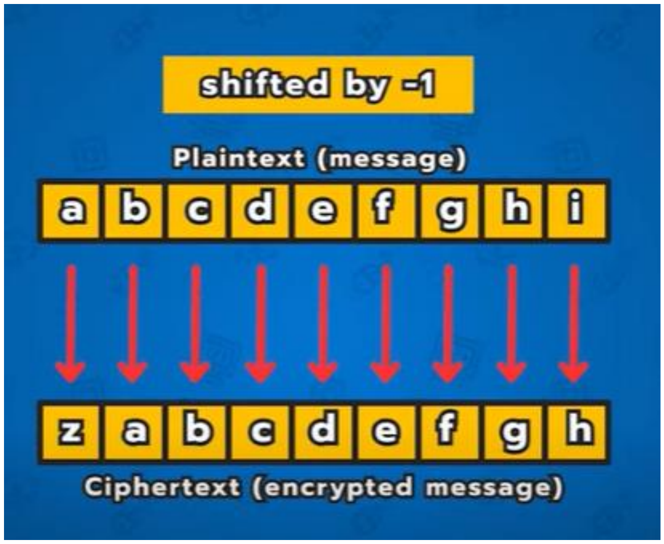
(ที่มา: [Encoding vs Encryption vs Hashing แตกต่างกันยังไง !? - สาระเดฟใน 3 นาที - YouTube])

และสำหรับการถอดรหัสเราจะใช้

$$f^{-1}(p) = (p - 1) \bmod 26$$

หรือการ *shift* กลับดังแสดงในรูปที่ *2* ดังนี้

ณัฏฐศิญา จตุรพนธกุล 66050146



รูปที่ 2: Caesar cipher (shifted back by 1)

(ที่มา: Encoding vs Encryption vs Hashing แตกต่างกันยังไง !? - สาระเดฟใน 3 นาที - YouTube)

ตัวอย่าง 2 จงทำการใส่รหัส “go cavaliers” และถอดรหัสโดยกำหนดให้ encryption function คือ

$$f(a) = (a + 3)\text{mod}26 \qquad \text{(shifted by 3)} \qquad (2)$$

<u>วิธีทำ</u> <u>Encrypt</u> “go cavaliers”

1. เปลี่ยนอักษรเป็นตัวเลข นั้นคือ

   g=6, o=14, c=2, a = 0, v=21, l=11, i=8, e=4, r=17, s=18 หรือ

   6, 14, 2, 0, 21, 0, 11, 8, 4, 17, 18

2. ใช้ฟังก์ชันในสมการที่ (2) กับตัวเลขแต่ละตัว

   เช่น f(6) = 9 mod 26 = 9 ทำเช่นนี้กับตัวเลขทุกตัวทำให้ได้ตัวเลขใหม่คือ

   9, 17, 5, 3, 24, 3, 14, 11, 7, 20, 21

3. ทำการเปลี่ยนตัวเลขกลับเป็นตัวอักษร ทำให้ได้อักษรต่อไปนี้

   jr wfdydolhuv

<u>Decrypt</u> “jr wfdydolhuv”

1. เปลี่ยนอักษร “jr wfdydolhuv” กลับไปเป็นตัวเลข ทำให้ได้

   9, 17, 5, 3, 24, 3, 14, 11, 7, 20, 21

   ใช้ inverse fuction ของ f กับตัวเลขในข้อ 1. นั่นคือ $f^{-1}(a) = (a-3) \bmod 26$ ทำให้ได้ลำดับ

   6, 14, 2, 0, 21, 0, 11, 8, 4, 17, 18

2. เปลี่ยนตัวเลขเป็นตัวอักษร ทำให้ได้

   “go cavaliers”

ตัวอย่าง 3 กำหนดให้ $f(p) = (p+13) \bmod 26$ จงใช้ Caesar cipher กับฟังก์ชันดังกล่าวในการใส่และถอดรหัส (Encrypt and Decrypt) ข้อความ DO NOT PASS GO (การใช้ฟังก์ชันนี้กับ Caesar cipher เรียกว่า shifted by 13)

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

วิธีทำ 1 เปลี่ยนอักษรเป็นตัวเลข

→ D = 3, O = 14 | N = 13, O = 14, T = 19 | P = 15, A = 0, S = 18, S = 18 | G = 6, O = 14

⇒ 3, 14, 13, 14, 19, 15, 0, 18, 18, 6, 14

2 ใช้ฟังก์ชัน จาก $f(p) = (p+13) \bmod 26$

$f(3) = (3+13) \bmod 26 = 16 \bmod 26 = 16$

$f(14) = (14+13) \bmod 26 = 27 \bmod 26 = 1$

$f(13) = (13+13) \bmod 26 = 26 \bmod 26 = 0$

$f(14) = (14+13) \bmod 26 = 27 \bmod 26 = 1$

$f(19) = (19+13) \bmod 26 = 32 \bmod 26 = 6$

$f(15) = (15+13) \bmod 26 = 28 \bmod 26 = 2$

$f(0) = (0+13) \bmod 26 = 13 \bmod 26 = 13$

$f(18) = (18+13) \bmod 26 = 31 \bmod 26 = 5$

$f(18) = (18+13) \bmod 26 = 31 \bmod 26 = 5$

$f(6) = (6+13) \bmod 26 = 19 \bmod 26 = 19$

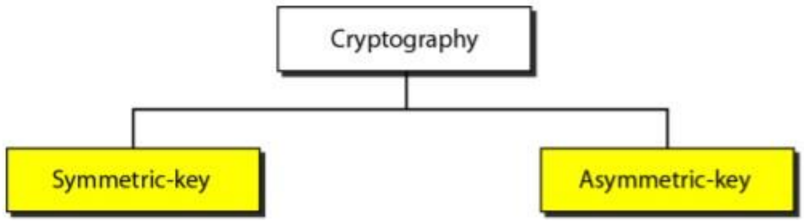
$f(14) = (14+13) \bmod 26 = 27 \bmod 26 = 1$

⇒ 16, 1, 0, 1, 6, 2, 13, 5, 5, 19, 1

Encrypt ⇒ QB ABG CNFF TB

Cryptography

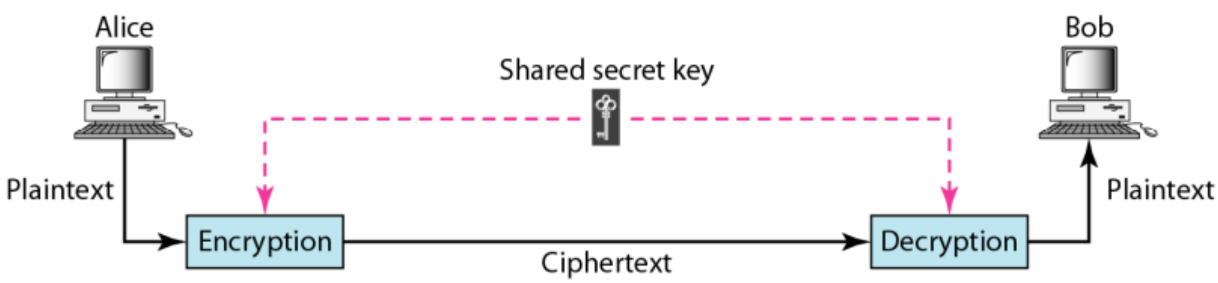
ก่อนจะกล่าวถึงหัวข้อ RSA ผู้เขียนจะกล่าวถึงการเข้ารหัสซึ่งมีสองแบบคือ symmetric-key cryptography และ asymmetric-key cryptography ดังแสดงในรูปที่ 3



รูปที่ 3

(ที่มา: https://www.cpe.ku.ac.th/~plw/dccn/presentation/ch30.pdf)

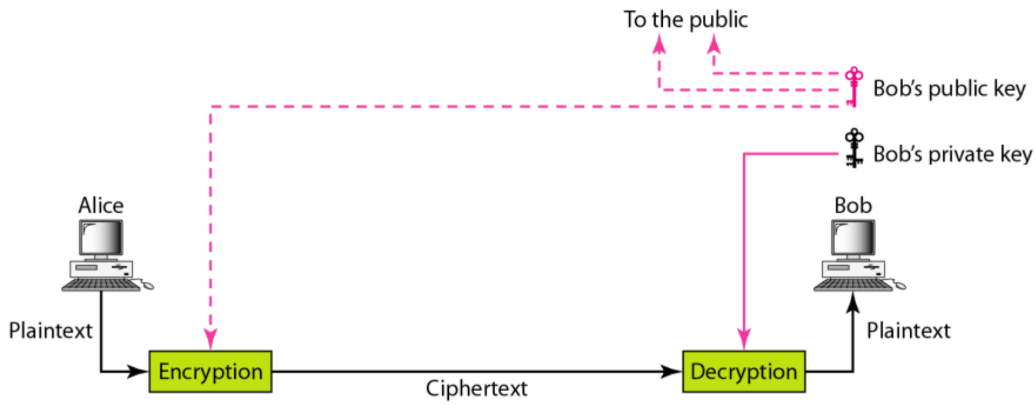
ซึ่ง symmetric-key cryptography นั้นมีการ share secret key (public key) ดังแสดงในรูปที่ 4



รูปที่ 4

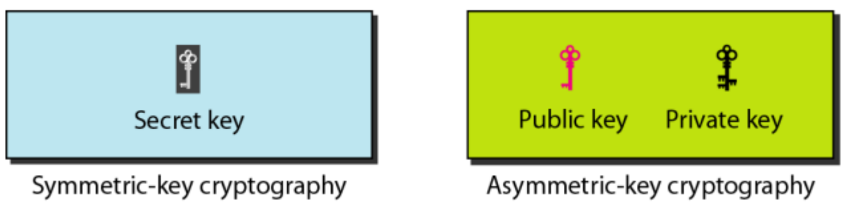
(ที่มา: https://www.cpe.ku.ac.th/~plw/dccn/presentation/ch30.pdf)

แต่สำหรับ asymmetric-key cryptography นั้นมีการ share secret key (public key) เฉพาะการ encryption แต่สำหรับ decryption นั้นจะเป็น private key คือจะถูกเก็บเป็นความลับ ดังแสดงในรูปที่ 5

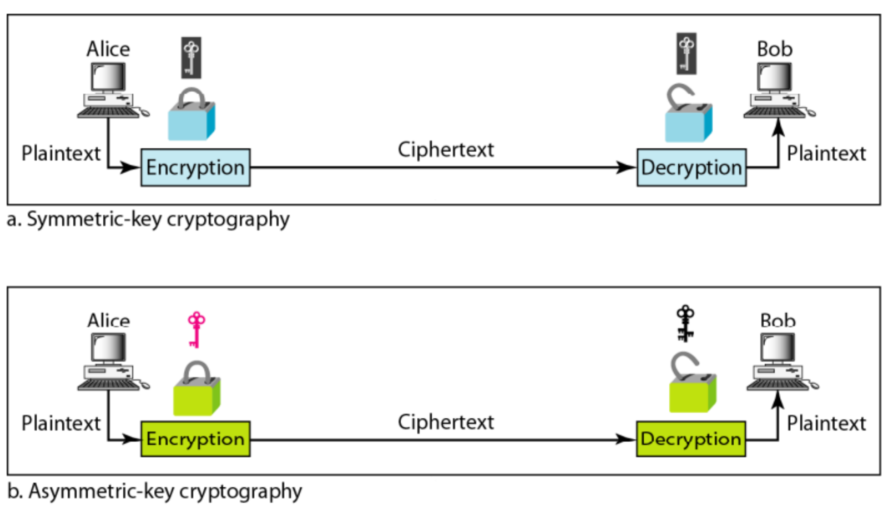


รูปที่ 5 (ที่มา: https://www.cpe.ku.ac.th/~plw/dccn/presentation/ch30.pdf)

รูปที่ 6 และ 7 เป็นการเปรียบเทียบให้เห็นภาพชัดเจนมากยิ่งขึ้นคือ symmetric-key cryptography จะมี key เดียว ที่ใช้ในการ lock และ unlock ข้อความ แต่ asymmetric-key cryptography มีสอง key ดังนี้



รูปที่ 6 (ที่มา: https://www.cpe.ku.ac.th/~plw/dccn/presentation/ch30.pdf)



รูปที่ 7 (ที่มา: https://www.cpe.ku.ac.th/~plw/dccn/presentation/ch30.pdf)

ตัวอย่างของ symmetric-key cryptography คือ Caesar cipher และตัวอย่างของ asymmetric-key cryptography คือ RSA ซึ่งจะกล่าวในหัวข้อถัดไป

RSA (Rivest, Shamir, Adleman) Cryptosystem

RSA เป็นการ encryption (sender) และ decryption (receiver) ข้อความ ซึ่ง RSA นั้นในการ encrypt ข้อความสามารถทำเป็นสาธารณะได้ (public key) แต่การ decryption จะถูกเก็บไว้เป็นความลับเพื่อความปลอดภัยของข้อมูล

RSA มีประโยชน์หลายอย่าง เช่น การซื้อของออนไลน์ของประชากรล้านคน การใช้บัตรเครดิตออนไลน์ให้มีความปลอดภัย ซึ่งรายละเอียดของบัตรเครดิตจำเป็นต้องเปิดเผยต่อผู้ขายแต่การ decryption จะรู้เฉพาะธนาคารที่เกี่ยวข้องกับการจ่ายเงินนั้น

การ encrypt และ decrypt โดยวิธี RSA

กำหนดให้ public เป็นน้ำเงิน และ private เป็นสีแดง

1. เลือกจำนวนเฉพาะมา 2 จำนวน

   ตัวอย่าง **p=5** และ **q =13**

2. ให้ n= **p x q**

   n = 5 x 13 = 65

3. ให้ **A = (p-1)(q-1)**

   A = 4 x 12 = 48

4. เลือก E ให้อยู่ในช่วง (1, A) โดยที่ E และ A ไม่มีตัวคูณร่วมนอกจาก 1 (**relatively prime**)

   หรือ หรม ของ E และ A เป็น 1 หรือ **gcd (E, A) = 1**

   เช่น E = 11

5. หาจำนวนเต็ม D ให้อยู่ในช่วง (1, A) โดยที่ A สามารถหาร (D x E) – 1 ลงตัว หรือ $E \cdot D \equiv 1 \; mod \; A$

   เช่น D=35 เพราะว่า (35 x 11) -1 = 384 = 8 x 48

Public key: n, E

Private key: p, q, D

ข้อสังเกตุ เนื่องจากเราทราบว่า *"ทุกๆ จำนวนเต็มบวกที่มากกว่า 1 สามารถเขียนให้อยู่ในรูปของผลคูณของจำนวนเฉพาะ"* ดังนั้นถ้าจำนวนเฉพาะนั้นมีค่ามาก มันยากที่จะแยกตัวประกอบ n ให้ได้ผลคูณของจำนวนเฉพาะนั้น ทำให้ RSA encryption ยากที่จะถอดรหัสได้

Public-key encryption

Public key คือคู่อันดับ (n,E) ซึ่งสามารถ share กับบุคคลอื่นได้ และสำหรับข้อความ (plaintext message) ที่ถูกเปลี่ยนเป็นตัวเลข M ต้องมีค่าอยู่ในช่วง $0 < M \leq n-1$ และ M จะถูกเข้ารหัส (encrypted) ด้วยข้อความเข้ารหัส (ciphertext message) C จากสูตรดังนี้

$$C \equiv M^E \text{ (mod n)}$$

โดยที่ $0 \leq \boldsymbol{C} \leq n-1$

Private-key encryption

Private key คือ เลข D ที่ถูกเก็บเป็นความลับ เราจะถอดรหัส (decrypt) ข้อความ (the ciphertext) C โดยใช้สูตร

$$M \equiv C^D \text{ (mod n)}$$

โดยที่ตัวเลข *p* และ *q* จะถูกเก็บเป็นความลับด้วย

วิธีการ RSA เมื่อ Bob ต้องการส่งข้อความหา Alice ดังนั้น Bob จะส่ง n และ E ให้ Alice

Set up:

a) Bob กำหนด p และ q (เช่นจำนวนเฉพาะที่มากกว่า 200 หลัก)
b) Bob คำนวณ n= pq และ เลือก E
c) Bob คำนวณ D
d) Bob publishes n และ E (public key)
e) Bob เก็บ D, p และ q เป็นความลับ

Encrypt:

- Alice ต้องการส่งข้อความ M หา Bob
- Alice คำนวณหา $C \equiv M^E$ (mod n) แล้วส่ง *C* ให้ *Bob*

Decrypt:

- Bob ใช้ข้อความเข้ารหัส (cipher text) C และ secret key D คำนวณหา $M \equiv C^D$ (mod n)

Note

- Encode คือ การแปลงข้อมูลจากแบบหนึ่ง ไปอีกแบบหนึ่ง เพื่อทำให้ระบบอื่นๆสามารถ '**เข้าใจและนำไปใช้** (Usability)' ต่อได้
- Encrypt คือ การแปลงข้อมูลจากแบบหนึ่ง ไปเป็นอีกแบบหนึ่ง โดยจะมีเพียงผู้ใช้ที่มีรหัสผ่าน (key) เท่านั้น ที่จะสามารถเข้าใจความหมายของข้อความต้นฉบับได้ '**จุดประสงค์เพื่อ ปกปิดและรักษาความลับ** (Confidentiality)' นั่นเอง
- Hash คือ การแปลงข้อมูลจากอีกแบบหนึ่ง สู่อีกแบบหนึ่งโดยไม่สามารถแปลงค่าที่ถูก Hash กลับมาเป็นข้อความต้นฉบับได้ โดยจุดประสงค์คือ ใช้เพื่อทำการ '**ยืนยันว่าไม่มีการเปลี่ยนแปลงข้อมูล** (Integrity)' ของข้อความนั้นๆ

ตัวอย่าง 4

Set up:

f) Bob กำหนด p = 43 และ q = 59 และเลือก E = 13

g) Bob คำนวณ n= pq = 43 x 59 = 2537

h) Bob คำนวณ D = 937

i) Bob publishes n= 2537 และ E = 13 (public key)

j) Bob เก็บ D=937, p=43 และ q=59 เป็นความลับ

Encrypt:

- Alice ต้องการส่งข้อความ **Stop** หา Bob โดยใช้ RSA

  S = 18, T = 19, O = 14, P = 15

  จัดกลุ่ม กลุ่มละ 4 ตัวเลข ดังนั้นจะได้ 1819 1415

- Alice คำนวณหา $C \equiv M^E$ (mod n)

  ดังนั้น $C \equiv 1819^{13} \bmod 2537 = 2081$ และ

$$C \equiv 1451^{13} \bmod 2537 \;=\; 2182$$

- Encrypted message คือ 2081 2182
- Alice ส่งข้อความเข้ารหัส (cypher text) 2081 2182 ให้ Bob

<u>Decrypt:</u>

- Bob คำนวณหา $M \equiv C^{D}\ (mod\ n) = 2081^{937}\ (\mathrm{mod}\ 2537) \;=\; 1819 \;\rightarrow\; S\,T$

  Bob คำนวณหา $M \equiv C^{D}\ (mod\ n) = 2182^{937}\ (\mathrm{mod}\ 2537) \;=\; 1415 \;\rightarrow\; O\,P$

<u>ตัวอย่าง 5</u> การคำนวณตัวเลขโดยใช้ modular arithmetic เมื่อ n=65 และ E =11

<u>การ encryption</u> เช่น ตัวเลขเข้ารหัสคือ 3 เราจะเอาเลข 3 ยกกำลัง E=11 และ หารด้วย n และทำการหาเศษเหลือ ดังนี้ $\left(C \equiv M^{E}\ (\text{mod } n)\right)$

1. $3^{11} \;=\; 177{,}147 = \;(2725\;\times 65) + 22$
2. ดังนั้น $3^{11} - \;(2725\;\times 65) = 22$
3. เศษเหลือ คือ C =22

ดังนั้น $22 \equiv 3^{11}\ (\mathrm{mod}65)$ หรือ $3^{11} \equiv 22\ (\mathrm{mod}65)$

<u>การ decryption</u> เช่น ตัวเลขรหัสคือ 22 (จาก encryption) เราจะเอาเลข 22 ยกกำลัง D=35 และ หารด้วย n=65 และทำการหาเศษเหลือ ดังนี้ $(M \equiv C^{D}\ (\text{mod } n))$

1 ในการคำนวณ $22^{35} = 9.6559 \times 10^{46}$ ซึ่งมีค่ามาก เราจะใช้สมบัติของ modular arithmetic เข้ามาช่วยในการคำนวณ เนื่องจาก 35 = 24+10+1

2 เนื่องจาก $22^{2} \equiv\; 29\ (\mathrm{mod}\ 65) \;\rightarrow\; 22^{10} \equiv 29^{5}(\mathrm{mod}65)$ และ $22^{12} \equiv 29^{6}(\mathrm{mod}65)$

3 เนื่องจาก $22^{12} \equiv 29^{6}(\mathrm{mod}65)$ และ $29^{6} \equiv\; 1\ (\mathrm{mod}\ 65) \;\rightarrow\; 22^{12} \equiv\; 1\ (\mathrm{mod}\ 65)$

4 ดังนั้น $\rightarrow\; 22^{24} \equiv\; 1\ (\mathbf{mod}\ 65)$

5 เนื่องจาก $22^{10} \equiv 29^{5}(\mathrm{mod}65)$ และ $29^{5} \equiv\; 9\ (\mathrm{mod}\ 65) \;\rightarrow\; 22^{10} \equiv 9\ (\mathbf{mod}65)$

6 เนื่องจาก $22^{35} = 22^{24} \times 22^{10} \times 22$ และ

7 $22^{24} \equiv\; 1\ (\mathbf{mod}\ 65)$ และ $22^{10} \equiv 9\ (\mathbf{mod}65)$ และ $22 \equiv 22\ (\mathbf{mod}65)$

8 ดังนั้น $22^{35} \equiv 1 \times 9 \times 22\ (\mathrm{mod}65)$

$$\equiv\; 198\ (\ \mathrm{mod}\ 65)$$

$$\equiv\; 3\ (\ \mathrm{mod}\ 65)$$

9 เศษเหลือคือ 3

ตัวอย่าง 6 Susan ต้องการส่งข้อความ HELP หา Bob โดยใช้ n=2537, E=13 และ Bob เก็บ D= 937 ดังในตัวอย่างข้างต้น จงใช้วิธี RSA ในการ encrypt และ decrypt ข้อความข้างต้น

วิธีทำ Encrypt

① Susan ต้องการส่งข้อความ "Help" หา Bob โดยวิธี RSA

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

ข้อมูลจะได้ว่า 74 11 15

② คำนวณหาจาก $\boxed{C \equiv M^E \pmod n}$

$\therefore C \equiv 74^{13} \pmod{2537}$

1) $C \equiv 74^2 \pmod{2537}$

$5476 \bmod 2537 = 402$

$\left.\begin{array}{l} \Rightarrow 402 \equiv 74^2 \bmod 2537 \\ \Rightarrow 74^2 \equiv 402 \bmod 2537 \end{array}\right\}$ ค่าเท่ากัน

2) $(74^2)^2 \bmod 2537 = 402^2 = 161{,}604$

$\left.\begin{array}{l} 74^4 \equiv 161{,}604 \bmod 2537 = 1{,}773 \\ \downarrow \text{แปลง} \\ \equiv 1{,}773 \bmod 2537 = 1{,}773 \end{array}\right\}$ เลขเท่ากัน

3) $74^5 \bmod 2537 = 74^4 \times 74 \bmod 2537$

$= (74^4 \bmod 2537)(74 \bmod 2537)$

$= 1{,}773 \times 74$

$74^5 \bmod 2537 = 131{,}202$

4) $74^6 \bmod 2537 = 74^5 \times 74 \bmod 2537$

$= (74^5 \bmod 2537)(74 \bmod 2537)$

$= 1{,}815 \times 74$

$74^6 \bmod 2537 = 134{,}310$

5) $74^{13} \bmod 2537 \equiv 421{,}281{,}704 \bmod 2537 = 169$

$\downarrow$ แปลง

$\equiv 169 \bmod 2537$

$74^{13} \bmod 2537 = 169$

$169 = 74^{13} \bmod 2537$

$C \equiv 11^3 \bmod 2537$

1) $11^6 \bmod 2537 = 735$

$\mapsto 735 \equiv 11^6 \bmod 2537$

$\mapsto 11^6 \equiv 735 \bmod 2537$

2) $(11^6)^2 \bmod 2537 = (735)^2 = 1{,}470$

$11^6 = 1{,}470 \bmod 2537$

3) $11^{13} \bmod 2537 = 11^{12} \times 11 \bmod 2537$

$= (11^{12} \bmod 2537)(11 \bmod 2537)$

$= 1{,}470 \times 11 = 16{,}170$

$11^{13} \bmod 2537 = 16{,}170$

$11^{13} = 16{,}170 \bmod 2537 = 948$

$\downarrow$ แปลง

$= 948 \bmod 2537 = 948$

$11^{13} \bmod 2537 = 948$

$\therefore 11^{13} \equiv 948 \bmod 2537$

$948 \equiv 11^{13} \bmod 2537$

③ C คือ 169 948 2116 (Encrypt message)

④ Susan ส่งข้อความเข้ารหัส 169 948 2116 ให้ Bob

Decrypt

① Bob ได้รับ cypher text จาก Susan

② คำนวณหาจาก $\boxed{M \equiv C^D \pmod n}$

③ $M \equiv 169^{937} \bmod 2537$

1) $169^{937} \bmod 2537 = 74$

$74 \equiv 169^{937} \bmod 2537$

$M \equiv 948^{937} \bmod 2537$

1) $948^{937} \bmod 2537 = 11$

$11 \equiv 948^{937} \bmod 2537$

M คือ 74 11 15 (Decrypt message)

④ Bob ถอดรหัสได้คำว่า "Help"

ณัฐฤดี จตุรสมบูล ๖๑๐๕๐๑๔๖

<u>แบบฝึกหัด</u>

1 จงหา a ในข้อต่อไปนี้ โดยที่ a เป็นจำนวนเต็มที่น้อยที่สุดเท่าที่จะเป็นไปได้ที่มากกว่าหรือเท่ากับ 0

a) $2468 \equiv a \ (mod\ 7)$

b) $2^{242} \equiv \mathrm{a(mod3)}$

c) $3^{245} \equiv \mathrm{a(mod5)}$

d) $654^{5} \equiv \mathrm{a(mod12)}$

2 กำหนดให้ $f(p) = (p+4)\mathbf{mod}\ 26$ จงใช้ Caesar cipher กับฟังก์ชันดังกล่าวในการใส่และถอดรหัส (Encrypt and Decrypt) ข้อความ WATCH YOUR STEP (การใช้ฟังก์ชันนี้กับ Caesar cipher เรียกว่า shifted by 4)

3 จงใช้ระบบ RSA ในการใส่และถอดรหัส (Encrypt and Decrypt) ข้อความ UPLOAD โดยที่ n = 53x61 และ E=17

<u>Links</u>

1. https://www.amsi.org.au/teacher_modules/pdfs/Maths_delivers/Encryption5.pdf
2. Microsoft PowerPoint - ch30.ppt [Compatibility Mode] (ku.ac.th)
3. https://engineering.thinknet.co.th/encode-encrypt-hash-%E0%B8%81%E0%B9%87%E0%B8%84%E0%B8%87%E0%B8%A1%E0%B8%B5%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1%E0%B8%AB%E0%B8%A1%E0%B8%B2%E0%B8%A2%E0%B9%80%E0%B8%AB%E0%B8%A1%E0%B8%B7%E0%B8%AD%E0%B8%99%E0%B9%86-%E0%B8%81%E0%B8%B1%E0%B8%99-a863e2af3621

<u>References</u>

[1] Kenneth H. Rosen, Discrete Mathematics and Its Applications, 7th edition, McGraw-Hill Companies, 2007.