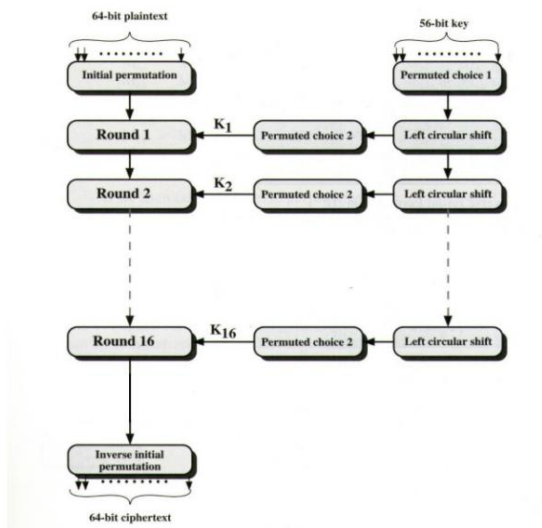


การบ้านครั้งที่ 3

1. จงศึกษาและอธิบายถึง การเข้ารหัส symmetric-Key cryptography แบบ DES,3DES,AES มีวิธีการและหลักการอย่างไร แต่ละวิธีแตกต่างกันอย่างไร พร้อมยกตัวอย่างประกอบ (อาจยกตัวอย่างโดยวิธีการเขียนโปรแกรมก็ได้)

1.1) DES (Data Encryption Standard)



เป็นอัลกอริทึมที่ใช้ในการเข้ารหัสและถอดรหัสแบบ Block Cipher ซึ่งจะทำให้การแบ่งข้อมูลออกเป็น Block แล้วนำไปทำการเข้ารหัส ทำการนำเข้าชุดข้อมูลแบบ บล็อกขนาด 64 bits และใช้กุญแจขนาด 56 bits มีจำนวนรอบการทำงานเท่ากับ 16 รอบ เพื่อสร้างกุญแจย่อยให้มีจำนวน 16 ดอก โดยระหว่างการเข้ารหัสนั้น แต่ละรอบการทำงานจะมีกุญแจขนาด 48 บิต

Input type: Text

Input text: (plain) Computer and Network Security !!

Function: DES

Mode: ECB (electronic codebook)

Key: (plain) abcdefg

Autodetect: ON | OFF

> Encrypt! > Decrypt!

Encrypted text:

00000000 18 89 1a d8 00 88 2b a9 9e 64 f8 fa 9c 92 14 c4 . . . 0 . 8 + 0 . d 0 ú . . Å
00000010 96 7c 19 8f d7 b8 87 55 0c 4e 75 b2 e5 fd 84 69 8 | . 8 × . . U . N u ² å ý . 1

[Download as a binary file] [?] Inactive

การเข้ารหัสแบบ DES

Input type: Text

Input text: (hex) 18 89 1a d8 00 88 2b a9 9e 64 f8 fa 9c 92 14 c4 96 7c 19 8f d7 b8 87 55 0c 4e 75 b2 e5 fd 84 69

Function: DES

Mode: ECB (electronic codebook)

Key: (plain) abcdefg

Autodetect: ON | OFF

> Encrypt! > Decrypt!

Decrypted text:

00000000 43 6f 6d 70 75 74 65 72 20 61 6e 64 20 4e 65 74 Computer and Net
00000010 77 6f 72 6b 20 53 65 63 75 72 69 74 79 20 21 21 work Security !!

[Download as a binary file] [?] Inactive

การถอดรหัสแบบ DES

1.2) 3DES (Triple DES)

จะใช้อัลกอริทึมเดียวกับ DES แต่จะใช้ 3 Keys และทำ DES 3 ครั้ง

ดังนั้น Keys ทั้งหมดจะมีความยาวเท่ากับ $56 \times 3 = 168$ bits อย่างไรก็ตาม FIPS PUB 46-3 อนุญาตให้ใช้ Keys ได้เพียงแค่ 2 Keys คือ กำหนดให้ K1 เท่ากับ K3 ดังนั้นความยาวจะเหลือเพียง 112 bits สรุปได้ว่า 3DES เป็นการเข้ารหัสที่ถูกพัฒนาจาก DES เพื่อเสริมความปลอดภัยและยังสามารถทำงานร่วมกับ DES ได้

Input type: Text

Input text: (plain) Computer and Network Security !!

Autodetect: ON | OFF

Function: 3DES

Mode: ECB (electronic codebook)

Key: (plain) abcdefg

Plaintext ☒ Hex

> Encrypt! > Decrypt!

Encrypted text:

00000000	18 89 1a d8 00 88 2b a9 9e 64 f8 fa 9c 92 14 c4	. . . 0 . 0 + 0 . d 0 0 0 . . 0
00000010	96 7c 19 8f d7 b8 87 55 0c 4e 75 b2 e5 fd 84 69	0 0 . 0 x . . U . N u 2 d y . i
00000020	51 97 9d 1f 12 ec 5b ff	Q . 0 . . i [y

[Download as a binary file] [?]

Inactive

การเข้ารหัสแบบ 3DES

Input type: Text

Input text: (hex) 18 89 1a d8 00 88 2b a9 9e 64 f8 fa 9c 92 14 c4 96 7c 19 8f d7 b8 87 55 0c 4e 75 b2 e5 fd 84 69 51 97 9d 1f 12 ec 5b ff

Autodetect: ON | OFF

Function: 3DES

Mode: ECB (electronic codebook)

Key: (plain) abcdefg

Plaintext ☐ Hex ☒

> Encrypt! > Decrypt!

Decrypted text:

00000000	43 6f 6d 70 75 74 65 72 20 61 6e 64 20 4e 65 74	C o m p u t e r a n d N e t
00000010	77 6f 72 6b 20 53 65 63 75 72 69 74 79 20 21 21	w o r k S e c u r i t y ! !
00000020	0d 0a 00 00 00 00 00 00

[Download as a binary file] [?]

Inactive

การถอดรหัสแบบ 3DES

1.3) AES (Advanced Encryption Standard)

การทำงานของ AES

- SubBytes เป็น Non-linear substitution แต่ละไบต์จะถูกแทนที่ด้วยไบต์ที่ได้จาก LUT
- ShiftRows เป็นการเลื่อนไบต์ในแต่ละแถว ซึ่งจะทำการเฉพาะแถวที่ 2 , 3 และ 4
- MixColumn เป็นการผสมรวม 4 ไบต์ภายในคอลัมน์
- AddRoundKey เป็นการนำ Cipher text และ Key ผสมกันจนเป็น Cipher text ใหม่

Input type: Text

Input text: (plain) Computer and Network Security !!

Autodetect: ON | OFF

Function: AES

Mode: ECB (electronic codebook)

Key: (plain) abcdefg

Plaintext ☒ Hex

> Encrypt! > Decrypt!

Encrypted text:

00000000	c9 51 28 a3 72 c9 38 0a 7b 01 0e 1f d8 11 16 5b	É Q (É r É 8 . { . . . 0 . . [
00000010	29 37 7e 37 bd e6 56 e1 09 2c 17 92 bc 0b 2b 38) 7 ~ 7 X m V á . , . . X . + 8

[Download as a binary file] [?]

Inactive

การเข้ารหัสแบบ 3DES

Input type: Text

Input text: (hex) c9 51 28 a3 72 c9 38 0a 7b 01 0e 1f d8 11 16 5b 29 37 7e 37 bd e6 56 e1 09 2c 17 92 bc 0b 2b 38

Autodetect: ON | OFF

Function: AES

Mode: ECB (electronic codebook)

Key: (plain) abcdefg

Plaintext ☐ Hex ☒

> Encrypt! > Decrypt!

Decrypted text:

00000000	43 6f 6d 70 75 74 65 72 20 61 6e 64 20 4e 65 74	C o m p u t e r a n d N e t
00000010	77 6f 72 6b 20 53 65 63 75 72 69 74 79 20 21 21	w o r k S e c u r i t y ! !

[Download as a binary file] [?]

Inactive

การถอดรหัสแบบ 3DES

2. จงศึกษาและอธิบายถึง การเข้ารหัส Asymmetric-Key cryptography แบบ RSA, Diffie Hellman มีวิธีการและหลักการอย่างไร แต่ละวิธีแตกต่างกันอย่างไร พร้อมยกตัวอย่างประกอบ (อาจยกตัวอย่างโดยวิธีการเขียนโปรแกรมก็ได้)

2.1) RSA

ขั้นตอนการทำ RSA

- (1) เลือก p และ q ซึ่งเป็นจำนวนเฉพาะที่มีค่าต่างกัน
- (2) ให้ $n = pq$
- (3) ให้ $m = (p-1)(q-1)$
- (4) เลือกค่า e โดยที่ $1 < e < m$ ซึ่งมี ห.ร.ม. ของ m และ e เท่ากับ 1
- (5) หาค่า d ที่ทำให้ $e \cdot d \bmod m$ เท่ากับ 1
- (6) จะได้ว่า Public Key คือ (e, n)
- (7) จะได้ว่า Private Key คือ (d, n)
- (8) ให้ M คือ ข้อความที่ยังไม่ถูกเข้ารหัส (ในรูปแบบของตัวเลข) โดยที่ $M < n$
- (9) สูตรคำนวณการเข้ารหัส (Encryption) คือ $C = M^e \bmod n$
- (9) สูตรคำนวณการถอดรหัส (Decryption) คือ $M = C^d \bmod n$

ตัวอย่าง

ให้ $p = 3$ และ $q = 5$ จะได้ $n = (3)(5) = 15$ และ $m = (3-1)(5-1) = 8$

เลือกค่า $e = 5$ โดยที่ $1 < e < m$ นั่นคือ $1 < 5 < 8$ ซึ่งมี ห.ร.ม. ของ m และ e เท่ากับ 1

จะได้ว่า $(5)(d) \bmod 8 = 1$ ดังนั้น $d = 13$

ดังนั้น Public Key คือ $(5, 15)$ และ Private Key คือ $(13, 15)$

ให้ $M = 13$ โดยที่ $M < n$ นั่นคือ $13 < 15$

สูตรคำนวณการเข้ารหัส (Encryption) คือ $C = M^e \bmod n$ นั่นคือ $C = 13^5 \bmod 15$ ดังนั้น $C = 13$

(9) สูตรคำนวณการถอดรหัส (Decryption) คือ $M = C^d \bmod n$ นั่นคือ $M = 13^{13} \bmod 15$ ดังนั้น $M = 13$

2.2 Diffie Hellman

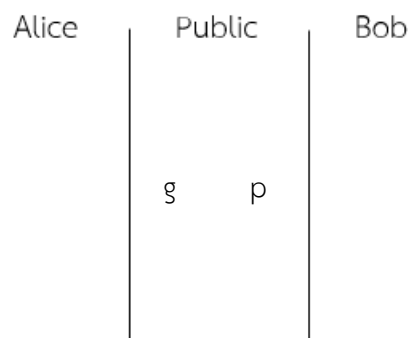
หลักการทำงานของ Diffie Hellman คือ การใช้คุณสมบัติของการ Modulo ดังนี้

$$(g^a \bmod p)^b \bmod p = g^{ab} \bmod p$$

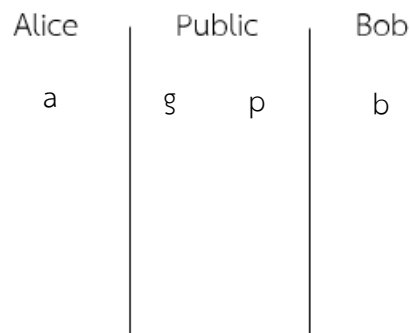
$$(g^b \bmod p)^a \bmod p = g^{ba} \bmod p$$

วิธีการทำงานของ Diffie Hellman

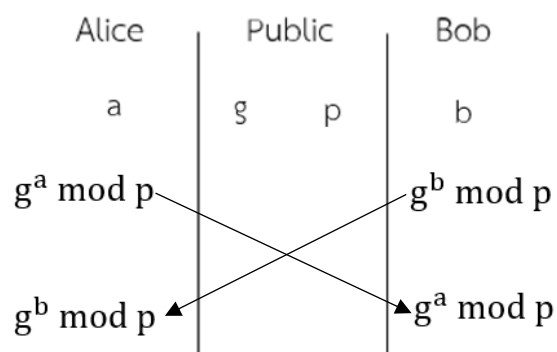
1. Alice และ Bob เลือกเลขจำนวนเฉพาะ g และ p โดยจะใช้ g และ p เป็นค่าเดียวกัน โดยค่าทั้งสองจะสามารถส่งผ่าน Public ได้ โดยปกติแล้ว p จะใหญ่ g มาก เพื่อความปลอดภัย



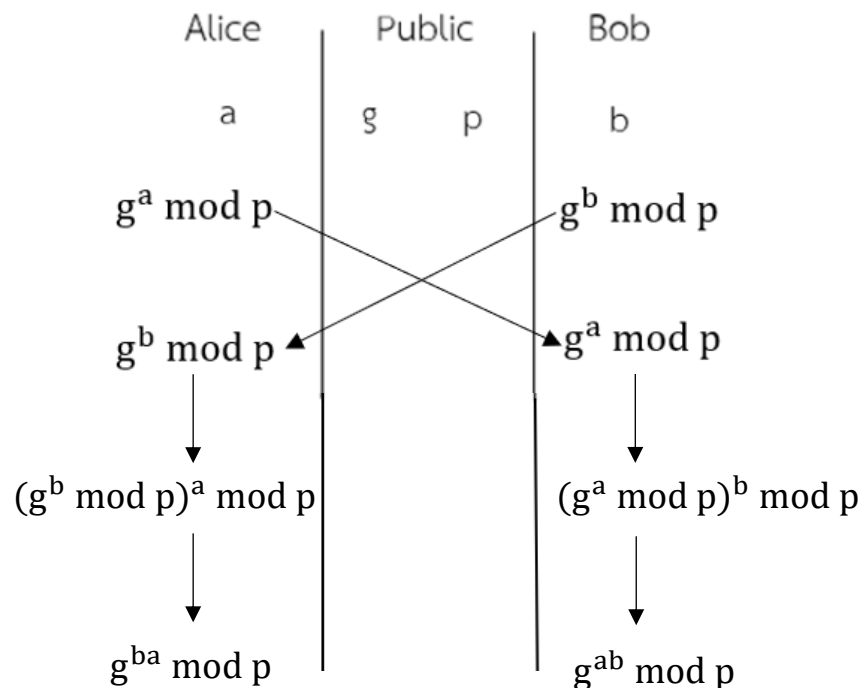
2. Alice และ Bob เลือกเลขขึ้นมา คน ละ 1 เลข โดยเก็บไว้เป็นความลับ



3. Alice ทำการคำนวณหา $g^a \bmod p$ และส่งค่าที่คำนวณได้ให้กับ Bob ผ่าน Public โดยที่ Bob ก็จะคำนวณ $g^b \bmod p$ และส่งค่าไปให้ Alice ด้วยเช่นเดียวกัน



4. Alice นำค่าที่ได้จาก Bob มายกกำลังด้วย a และ Modulo ด้วย p โดยที่ Bob ก็ทำเช่นเดียวกันกับตามเลขที่ตัวเองใช้เป็นความลับ



ค่าที่ทั้งสองส่งให้กัน เมื่อพิจารณาตามคุณสมบัติของการ Modulo จะทำให้ทั้งสองได้ค่าเดียวกัน เรียกว่า Shared-Secret หรือถูกใช้ในการเข้ารหัสและถอดรหัสในการสื่อสารต่อไป เมื่อเราใช้ค่า $g^{ab} \bmod p$ เป็นกุญแจสำหรับการเข้ารหัสแบบ Asymmetric-Key cryptography เราสามารถแลกค่า g และ p ได้อย่างเปิดเผยได้ โดยที่ a และ b ยังคงเป็นความลับของแต่ละฝ่ายได้

ตัวอย่างเช่น

- กำหนดให้ g และ p คือ 13 และ 97 ตามลำดับ และให้ Alice ถือ เลข $a = 3$ และ Bob ถือเลข $b = 11$ โดยที่เลข a และ b ที่ทั้งสองถือกันเป็นความลับต่อกัน
- ให้ Alice คำนวณค่าที่ได้จากการ Modulo นั่นคือ $g^a \bmod p = 13^3 \bmod 97 = 63$ ไปให้ Bob และ Bob ก็ส่งค่าที่ได้จากการ Modulo นั่นคือ $g^b \bmod p = 13^{11} \bmod 97 = 87$ ไปให้ Alice เช่นกัน
- หลังจากนั้น ให้ทำการเข้าสมการที่ได้กำหนดไว้ข้างต้น

$$(13^{11} \bmod 97)^3 \bmod 97 = 67 = 13^{(3)(11)} \bmod 97 = g^{ab} \bmod p$$

$$(13^3 \bmod 97)^{11} \bmod 97 = 67 = 13^{(11)(3)} \bmod 97 = g^{ba} \bmod p$$

จะเห็นว่า ทั้งสองจะได้รับ Keys เหมือนกัน คือ 67 นั่นเอง