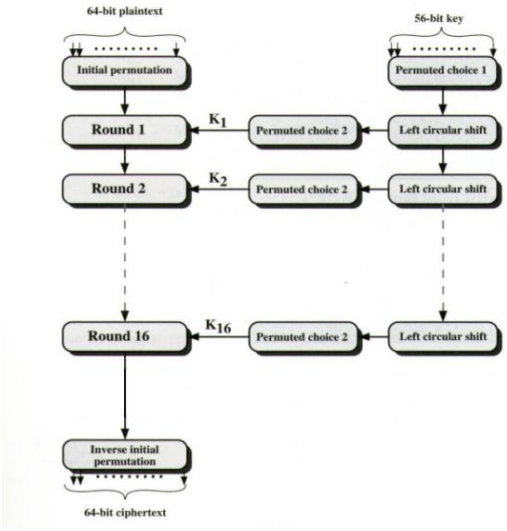
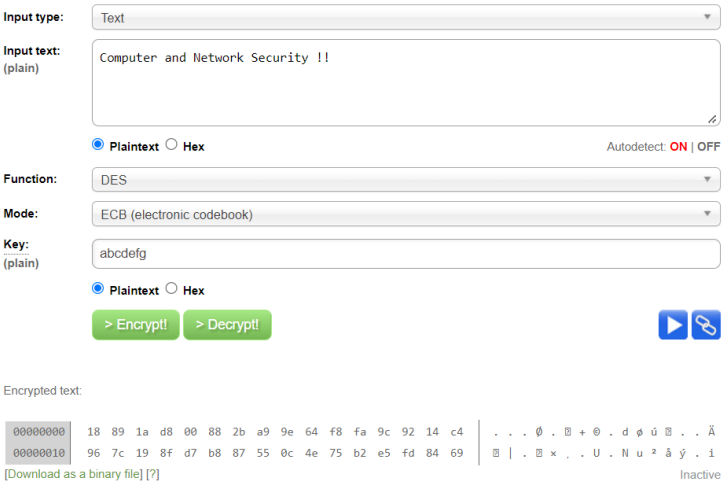
การบ้านครั้งที่ 3

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

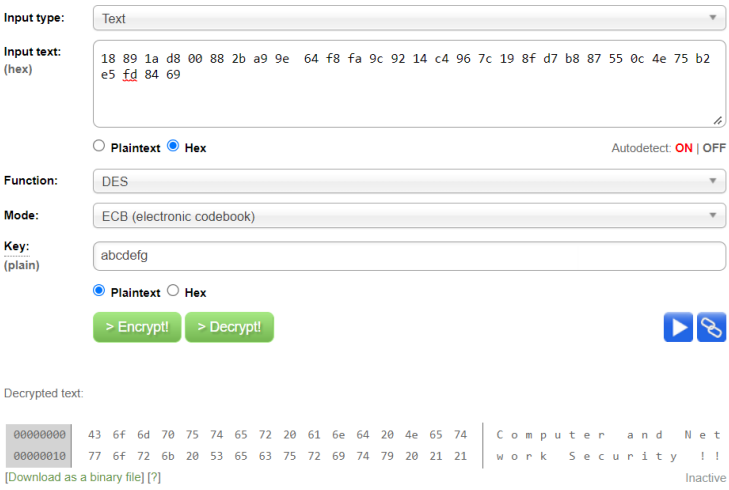
1.1) DES (Data Encryption Standard)



เป็นอัลกอริทึมที่ใช้ในการเข้ารหัสและถอดรหัสแบบ Block Cipher ซึ่งจะทำการแบ่งข้อมูลออกเป็น Block แล้วนำไปทำการเข้ารหัส ทำการนพเข้าชุดข้อมูลแบบบล็อกขนาด 64 bits และใช้กุญแจขนาด 56 bits มีจำนวนรอบการทำงานเท่ากับ 16 รอบ เพื่อสร้างกุญแจย่อยให้มีจำนวน 16 ดอก โดยระหว่างการเข้ารหัสนั้นแต่ละรอบการทำงานจะมีกุญแจขนาด 48 บิต



การเข้ารหัสแบบ DES

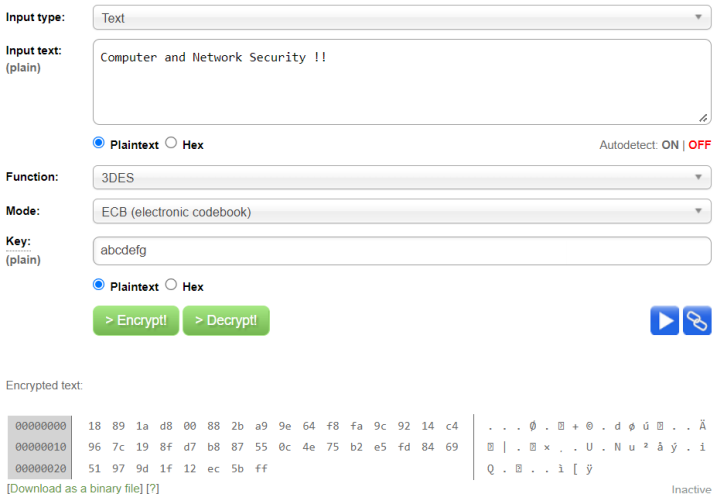


การถอดรหัสแบบ DES

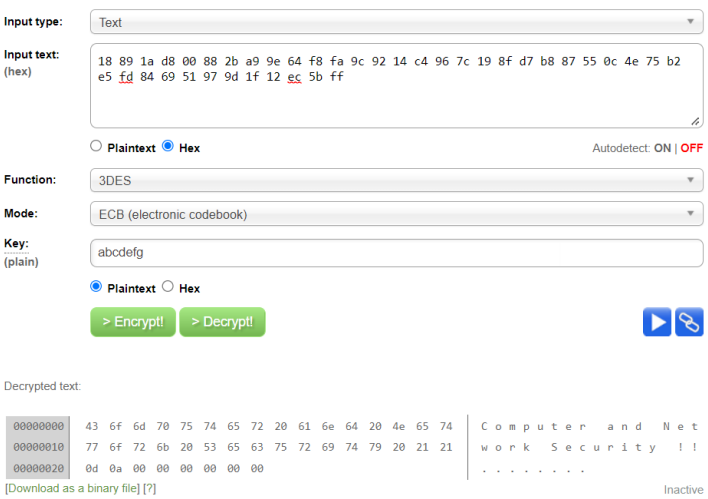
1.2) 3DES (Triple DES)

จะใช้อัลกอริทึมเดียวกับ DES แต่ละใช้ 3 Keys และทำ DES 3 ครั้ง

ดังนั้น Keys ทั้งหมดจะมีความยาวเท่ากับ 56 x 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



การเข้ารหัสแบบ 3DES



การถอดรหัสแบบ 3DES

1.3) AES (Advanced Encryption Standard)

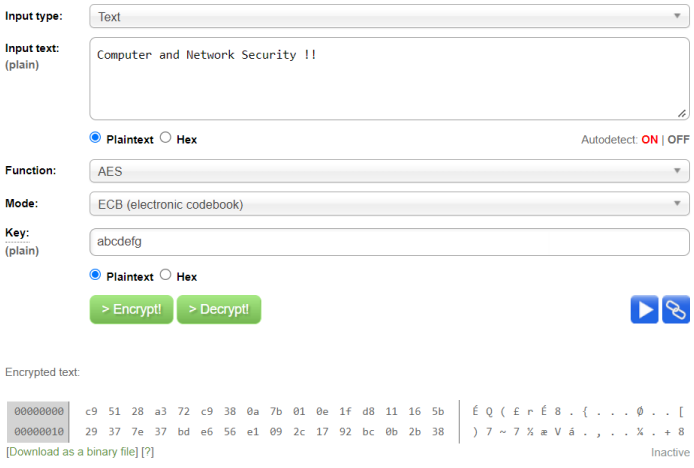
การทำงานของ AES

- SubBytes เป็น Non-linear substitution แต่ละไบต์จะถูกแทนที่ด้วยไบต์ที่ได้จาก LUT

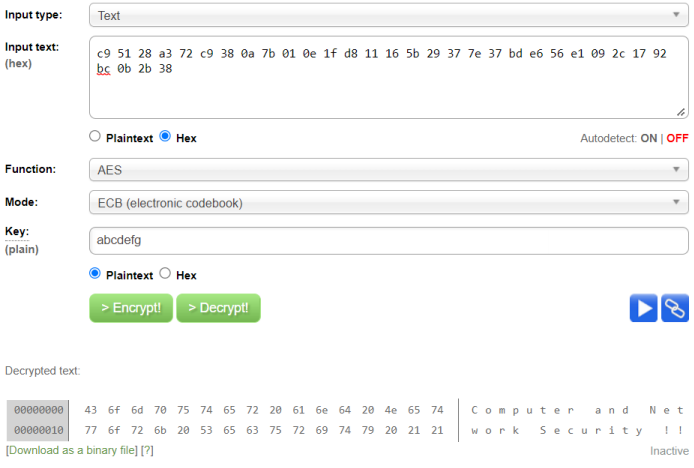
- ShiftRows เป็นการเลื่อนไบต์ในแต่ละแถว ซึ่งจะทำเฉพาะแถวที่ 2 , 3 และ 4

- MixColumn เป็นการผสมรวม 4 ไบต์ภายในคอลัมน์

- AddRoundKey เป็นการนำ Ciper text และ Key ผสมกันจนเป็น Ciper text ใหม่



การเข้ารหัสแบบ 3DES



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*d mod 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 $C = \mathrm{M}^{\mathrm{e}} mod\ n$

(9) สูตรคำนวณการถอดรหัส (Decryption) คือ $M = \mathrm{C}^{\mathrm{d}} mod\ n$

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) mod 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 $C = \mathrm{M}^{\mathrm{e}} mod\ n$ นั่นคือ $C = 13^5 mod\ 15$ ดังนั้น C = 13

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

2.2 Diffle Hellman

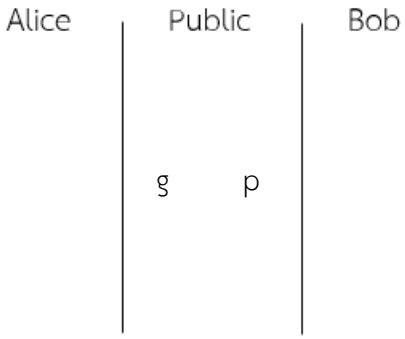
หลักการทำงานของ Diffle Hellman คือ การใช้คุณสมบัติของการ Modulo ดังนี้

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

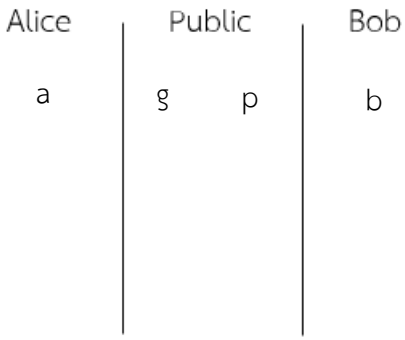
$$(g^b \bmod p)^a \bmod p = g^{ba} \bmod p$$

วิธีการทำงานของ Diffle Hellman

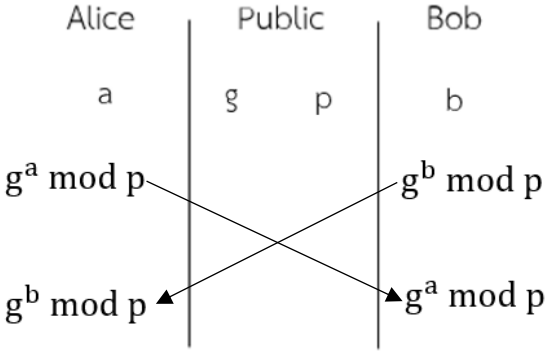
1. Alice และ Bob เลือกเลขจำนวนเฉพาะ g และ p โดยจะใช้ g และ p เป็นค่าเดียวกัน โดยค่าทั้งสองจะสามารถส่งผ่าน Public ได้ โดยปกติแล้ว p จะใหญ่ g มาก เพื่อความปลอดภัย



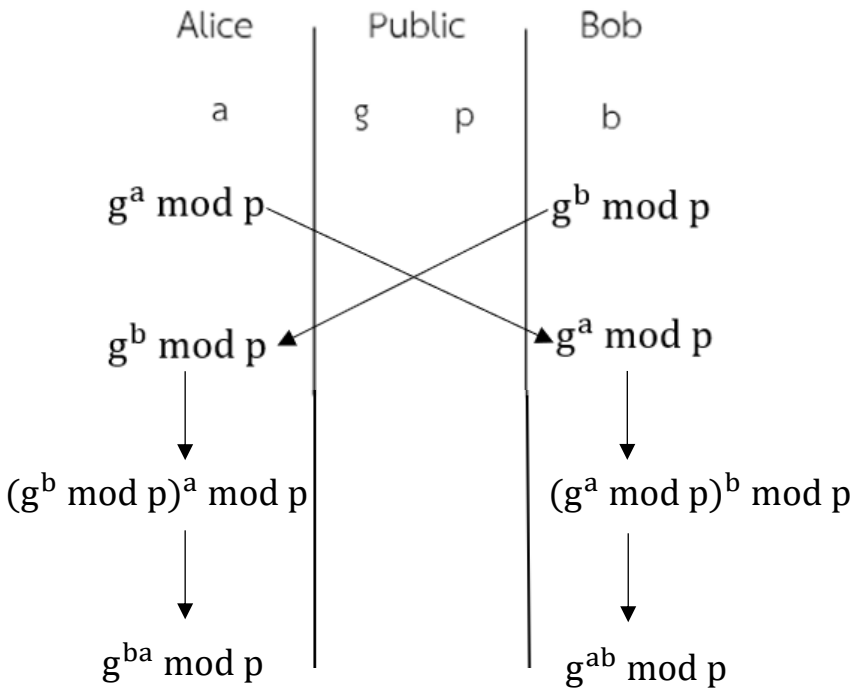
2. Alice และ Bob เลือกเลขขึ้นมา คน ละ 1 เลข โดยเก็บไว้เป็นความลับ



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 หรือกุญแจในการเข้ารหัสและถอดรหัสในการสื่อสารต่อไป 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 ที่ทั้งสองถือนั้นเป็นความลับต่อกัน

- 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

- หลักจากนั้น 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