ใบงานที่ 2

การเข้ารหัส ด้วย AES หรือ Advanced Encryption Standard เป็น การเข้ารหัสที่มีความนิยมเป็นอย่างมาก การเข้ารหัสด้วย AES คือต้องใช้ข้อมูลที่ต้องการเข้ารหัส (plaintext) และคีย์ลับ (secret key) ในกระบวนการเข้ารหัส หากถูกเจาะข้อมูล แต่ Hacker ไม่มี คีย์ลับ (secret key) ก็จะไม่สามารถถอดข้อมูลได้

โดยวิธีการนี้ หากเราสามารถเก็บ คีย์ลับ (secret key) ไว้ไม่ให้หลุดหรือรู้จากบุคคลภายนอกก็แถบจะไม่มีวันถูกเจาะข้อมูลได้เลย

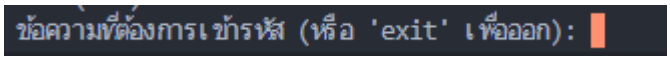
ข้อเสียคือ คีย์ลับ (secret key) หาย ข้อมูลในนั้นก็จะสูญหายหรือกู้คืนไม่ได้เช่นกัน

เสนอ โปรแกรม Code :

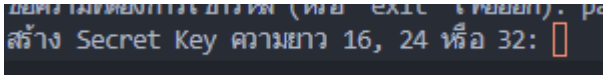
```python
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad
import binascii

def get_valid_key():
    while True:
        key = input("สร้าง Secret Key ความยาว 16, 24 หรือ 32: ")
        if len(key) in [16, 24, 32]:
            return key.encode()
        else:
            print("Secret Key ความยาว 16, 24 หรือ 32")

while True:
    # รับข้อความที่ผู้ใช้ต้องการเข้ารหัส
    plaintext = input("ข้อความที่ต้องการเข้ารหัส (หรือ 'exit' เพื่อออก): ")

    # ตรวจสอบว่าผู้ใช้ต้องการออกจากวงรอบหรือไม่
    if plaintext.lower() == 'exit':
        break

    # รับกุญแจเพื่อเข้ารหัส
    key = get_valid_key()
    cipher = AES.new(key, AES.MODE_ECB)

    # เข้ารหัสข้อความ
    plaintext = plaintext.encode()
    ciphertext = cipher.encrypt(pad(plaintext, AES.block_size))

    hex_output = binascii.hexlify(ciphertext).decode()

    # พิมพ์ผลลัพธ์ที่เข้ารหัส
    print("Secret Key :" ,plaintext)
    print("ข้อความที่ต้องการเข้ารหัส :" ,plaintext)
    print("AES (Hex) หรือ ผลลัพธ์การเข้ารหัสด้วย:", hex_output)
```

เมื่อรันโปรแกรมนะครับ

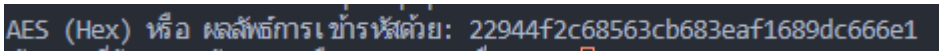
จะมีให้ใส่ข้อความที่เราต้องการเข้ารหัส



จากนั้นจะมีให้สร้าง Secret Key ที่เราเป็นคนกำหนดเอง



จากนั้นจะได้ข้อมูลการเข้ารหัสมา เป็นAES แบบ hex เลขฐาน16



แค่นี้ข้อมูลก็จะถูกเข้ารหัสแล้ว