陳奕嘉 E94115011 資訊 115

資訊安全 HW3

案例 1：不同金鑰(相差 1bit)加密相同明文

步驟:
使用 DES 加密算法加密明文，分別使用金鑰 1 和金鑰 2 進行加密。計算兩個密文的 XOR 差異，然後統計有多少位不同。將兩個密文進行 XOR 運算，這樣每個不同的位將會變成 1，相同的位保持為 0。密文總共有 64 位，因此可以用以下公式計算差異比例:
差異比例 =(差異位數/64) × 100%

我們使用 python 來協助我們運算。

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

def hex_to_bytes(hex_str):
    return binascii.unhexlify(hex_str)

def count_bit_differences(byte_str1, byte_str2):
    diff = int.from_bytes(byte_str1, byteorder='big') ^ int.from_bytes(byte_str2, byteorder='big')
    return bin(diff).count('1')

plaintext_hex = '0123456789ABCDEF'
plaintext_bytes = hex_to_bytes(plaintext_hex)

key1_hex = '133457799BBCDFF1'
key2_hex = '133457799BBCDFE2'
key1_bytes = hex_to_bytes(key1_hex)
key2_bytes = hex_to_bytes(key2_hex)

des1 = DES.new(key1_bytes, DES.MODE_ECB)
des2 = DES.new(key2_bytes, DES.MODE_ECB)

ciphertext1 = des1.encrypt(pad(plaintext_bytes, DES.block_size))
ciphertext2 = des2.encrypt(pad(plaintext_bytes, DES.block_size))

bit_difference = count_bit_differences(ciphertext1, ciphertext2)

ciphertext1_hex = binascii.hexlify(ciphertext1).decode()
ciphertext2_hex = binascii.hexlify(ciphertext2).decode()

print(f"密文 1: {ciphertext1_hex}")
print(f"密文 2: {ciphertext2_hex}")
print(f"密文之間的位元差異數: {bit_difference} 位")
print(f"密文差異比例: {(bit_difference / 64) * 100:.2f}%")
```

明文 = 0123456789ABCDEF
金鑰 1 = 133457799BBCDFF1
金鑰 2 = 133457799BBCDFE2

以下是輸出:

```
密文 1: 85e813540f0ab405fdf2e174492922f8
密文 2: c6725a94b8ad501d66ce8a70fdda6a25
密文之間的位元差異數: 62 位
密文差異比例: 96.88%
```

案例 2：相同金鑰加密不 同明文(相差 1bit)

步驟:

和案例 1 大同小異，只不過我們用同一個金鑰，加密明文 1 和明文 2。

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

def hex_to_bytes(hex_str):
    return binascii.unhexlify(hex_str)

def count_bit_differences(byte_str1, byte_str2):
    diff = int.from_bytes(byte_str1, byteorder='big') ^ int.from_bytes(byte_str2, byteorder='big')
    return bin(diff).count('1')

plaintext1_hex = '0123456789ABCDEF'
plaintext2_hex = '0123456789ABCDEE'
plaintext1_bytes = hex_to_bytes(plaintext1_hex)
plaintext2_bytes = hex_to_bytes(plaintext2_hex)

key1_hex = '133457799BBCDFF1'
key1_bytes = hex_to_bytes(key1_hex)

des = DES.new(key1_bytes, DES.MODE_ECB)

ciphertext1 = des.encrypt(pad(plaintext1_bytes, DES.block_size))
ciphertext2 = des.encrypt(pad(plaintext2_bytes, DES.block_size))

bit_difference = count_bit_differences(ciphertext1, ciphertext2)

ciphertext1_hex = binascii.hexlify(ciphertext1).decode()
ciphertext2_hex = binascii.hexlify(ciphertext2).decode()

print(f"密文 1: {ciphertext1_hex}")
print(f"密文 2: {ciphertext2_hex}")
print(f"密文之間的位元差異數: {bit_difference} 位")
print(f"密文差異比例: {(bit_difference / 64) * 100:.2f}%")
```

明文 1 = 0123456789ABCDEF

明文 2 = 0123456789ABCDEE

金鑰 2 = 133457799BBCDFE1

輸出:

```
密文 1: 85e813540f0ab405fdf2e174492922f8
密文 2: 28378e295be22a84fdf2e174492922f8
密文之間的位元差異數: 37 位
密文差異比例: 57.81%
```

結論:

案例 1 的密文差異比例是 96.88%，案例 2 的則是 57.81%，案例 1 的密文差異比較多。可以得出用不同的金鑰加密同一個明文出來的密文差異比例會比較大，即使兩個金鑰只相差 1bit。