

1.

取金鑰 2、3 位元  $\Rightarrow 11$  (二進位)

$$3^2=01001$$

$$\text{加密: } C = P \oplus f(K) = 10110 \oplus 01001 = 11111$$

$$\text{解密: } P = C \oplus f(K) = 11111 \oplus 01001 = 10110$$

2.

要證: 若  $p$  是質數且  $k$  為正整數, 則  $\phi(p^k) = p^k - p^{k-1}$

對於所有  $x \leq p^k$  使得  $\gcd(x, p^k) \neq 1$  的皆為  $p$  之倍數, 也就是  $x = \{1p, 2p, 3p, \dots, p^{k-1}, p\}$ , 總共  $p^{k-1}$  個數字與  $p^k$  不互質, 得證

3.

(1).

$$\phi(12) = \phi(2^2 \cdot 3) = 12(1 - 1/2)(1 - 1/3) = 12 \cdot 1/2 \cdot 2/3 = 4$$

$x=1$ :

$$1^4 \equiv 1 \pmod{12} \Rightarrow \text{True}$$

$x=5$ :

$$5^4 = 625$$

$$625 \div 12 = 625 - 52 \cdot 12 = 625 - 624 = 1$$

$$5^4 \equiv 1 \pmod{12} \Rightarrow \text{True}$$

$x=7$ :

$$7^4 = 2401$$

$$2401 \bmod 12 = 2401 - 200 \cdot 12 = 2401 - 2400 = 1$$

$$7^4 \equiv 1 \pmod{12} \Rightarrow \text{True}$$

$x=11$ :

$$11^4 = 14641$$

$$14641 \bmod 12 = 14641 - 1220 \cdot 12 = 14641 - 14640 = 1$$

$$11^4 \equiv 1 \pmod{12} \Rightarrow \text{True}$$

(2).

Prove  $(x^d)^e \equiv x \pmod{n}$

$$de = 1 + k\phi(n)$$

$$(x^d)^e = x^{de} = x^{1+k\phi(n)} = x^1 \cdot x^{k\phi(n)} = x \cdot (x^{\phi(n)})^k$$

Euler's theorem:

$$x^{\phi(n)} \equiv 1 \pmod{n}$$

$$(x^{\phi(n)})^k \equiv 1^k \equiv 1 \pmod{n}$$

$$x \cdot (x^{\phi(n)})^k \equiv x \cdot 1 \equiv x \pmod{n}$$

$\Rightarrow$  得證  $(x^d)^e \equiv x \pmod{n}$

4.

(1). 原始狀態

State Matrix: [ [00, 04, 08, 0C],  
                  [01, 05, 09, 0D],  
                  [02, 06, 0A, 0E],  
                  [03, 07, 0B, 0F] ]

(2). AddRoundKey

Key Matrix: [ [01, 01, 01, 01],  
                  [01, 01, 01, 01],  
                  [01, 01, 01, 01],  
                  [01, 01, 01, 01] ]

XOR:

[ [01, 05, 09, 0D],  
[00, 04, 08, 0C],  
[03, 07, 0B, 0F],  
[02, 06, 0A, 0E] ]

(3). SubBytes

[ [7C, 6B, 01, D7],  
[63, F2, 30, FE],  
[7B, C5, 2B, 76],  
[77, 6F, 67, AB] ]

(4). ShiftRows

[ [7C, 6B, 01, D7],  
[F2, 30, FE, 63],  
[2B, 76, 7B, C5],  
[AB, 77, 6F, 67] ]

(5). MixColumns

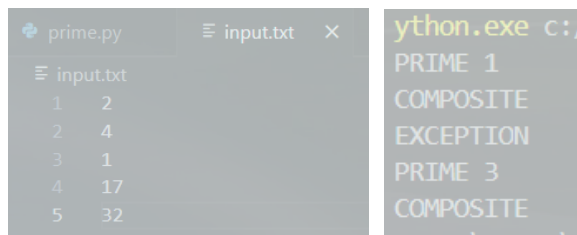
[ [75, 87, 0F, B2],  
[55, E6, 04, 22],  
[3E, 2E, B8, 8C],  
[10, 15, 58, 0A] ]

5.

執行方式為讀取 input.txt -> RUN code

輸入:

輸出:



The screenshot shows a code editor with two tabs: 'prime.py' and 'input.txt'. The 'input.txt' tab is active, displaying a list of numbers: 1, 2, 4, 17, 32. To the right, a terminal window shows the output of the program: 'PRIME 1', 'COMPOSITE', 'EXCEPTION', 'PRIME 3', 'COMPOSITE'.

| Input | Output    |
|-------|-----------|
| 1     | PRIME 1   |
| 2     | COMPOSITE |
| 4     | EXCEPTION |
| 17    | PRIME 3   |
| 32    | COMPOSITE |

分析次數說明:

因為對任何非質數可因數分解成  $n=a*b$ ，ex:17 的分析次數只需要分析 3 次，因為 17 的平方根約莫是 4.~，只需要檢查 2、3、4 是否有人可以整除 17，又例如 32 平方根約莫是 5.~，只需檢查 2、3、4、5，而 32 可以被 2 整除  $32=2*16$ ，16 是可以不用管他的，所以先取平方根可以減少分析次數。