1.

取金鑰2、3位元 => 11 (二進位)

32=01001

加密: C = P ⊕ f(K) = 10110 ⊕ 01001 = 11111

解密: P = C ⊕ f(K) = 11111 ⊕ 01001 = 10110

2.

要證: 若𝑝是質數且k為正整數，則𝜙 (𝑝k) =𝑝k−𝑝k−1

對於所有𝑥≤𝑝k使得gcd(𝑥,𝑝k)≠1的皆為𝑝之倍數，也就是𝑥= {1𝑝,2𝑝,3𝑝,…,𝑝k-1 ,𝑝}，總共𝑝k-1個數字與𝑝k不互質，得證

3.

(1).

ϕ(12)=ϕ(22⋅3)=12(1−1/2​)(1−1/3​)=12⋅1/2​⋅2/3​=4

x=1:

14≡1(mod 12) => True

x=5:

54=625

1. d 12=625−52⋅12=625−624=1

54≡1(mod12) => True

x=7:

74=2401

2401 mod 12=2401−200⋅12=2401−2400=1

74≡1(mod12) => True

x=11:

114=14641

14641 mod 12=14641−1220⋅12=14641−14640=1

114≡1(mod12) => True

(2).

Prove (xd)e≡ x(mod n)

de=1+kϕ(n)

(xd)e=xde=x1+kϕ(n)= x1⋅xkϕ(n)=x⋅(xϕ(n))k

Euler's theorem:

xϕ(n)≡1(mod n)

(xϕ(n))k≡1k≡1(mod n)

x⋅(xϕ(n))k≡x⋅1≡x(mod n)

* 得證(xd)e≡x(mod 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],

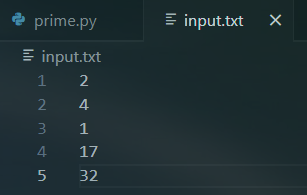
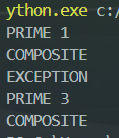
[3E, 2E, B8, 8C],

[10, 15, 58, 0A] ]

5.

執行方式為讀取input.txt -> RUN code

輸入: 輸出:

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。