1、1234-1 mod 4321

(1234, 4321)=>

4321 = 1234\*3 + 619

1234 = 619\*1 + 615

619 = 615\*1 + 4

615 = 4\*153 + 3

4 = 3\*1 + 1 =>

1 = 4 – 3\*1

= 4 – 615 + 4\*153 = 4\*154 – 615

= (619 – 615)\*154 -615 = 619\*154 – 615\*155

= 619\*154 – (1234 – 619)\*155 = 619\*309 – 1234\*155

= (4321 – 1234\*3)\*309 – 1234\*155 = 4321\*309 – 1234\*(927+155) = 4321\*309 – 1234\*1082 =>

1234\*(-1082) = 1 mod 4321 =>

1234\*3239 = 1 mod 4321

所以1234-1 mod 4321 == 3239

2、下式是仿射密码的加密变换

c= (3m+5) mod 26，试求：

1. 该密码的密钥空间是多少

26\*φ(26)=26\*12=312

1. 求出消息“hello”对应的密文

h: 7, e: 4, l: 11, o: 14

3\*7+5 mod 26 = 0 => a

3\*4+5 mod 26 = 17 => r

3\*11+5 mod 26 = 12 => m

3\*14+5 mod 26 = 21 => v

密文：armmv

1. 写出它的解密变换

(26, 3) => 26 = 3\*8+2

3 = 2\*1 + 1 =>

1 = 3 - 2\*1

= 3 – (26-3\*8) = 3\*9 -26

3\*9 = 1 mod 26

D=9(y-5) mod 26

1. 试对密文进行解密

9\*-5 mod 26 = 7 => h

9\*12 mod 26 = 4 => e

9\*7 mod 26 = 11 => l

9\*16 mod 26 = 14 => o