1) 试对 good job 进行加密

先求 19 在模 73 时的逆元

$$1 = 6 \cdot 73 - 23 \cdot 19$$

故 19 在模 73 时的逆元为 50

使用逆元对 A_i 进行操作

A=(3, 4, 9, 17, 35)

$$B_i = A_i \cdot 50 \pmod{73}$$

B=(4, 54, 12, 47, 71)

编程求 `goodjob` 对应的 ASCII 码以及二进制串

```
s = "goodjob"
for c in s:
    print(c, ord(c) - ord("a"), bin(ord(c) - ord("a")))
```

```
g 6 0b110
o 14 0b1110
o 14 0b1110
d 3 0b11
j 9 0b1001
o 14 0b1110
b 1 0b1
```

编程对二进制串进行加密

```
B=(4, 54, 12, 47, 71)
S=["00110", "01110", "01110", "00011", "01001", "01110", "00001"]
for s in S:
    sum = 0
    for i in range(5):
        if s[i] == "1":
            sum += B[i]
    print(s, sum % 73)
```

```
00110 59
01110 40
01110 40
00011 45
01001 52
01110 40
00001 71
```

2) 求明文 M

由 $n = 35$ **易得** $p = 5, q = 7$

$\varphi(n) = (p-1)(q-1) = 24$

求 5 **在模 24 时的逆元** 5^{-1}

易得 $5 \cdot 5 \equiv 1 \pmod{24}$

故明文 $m = 10^5 \pmod{35} = 5$

3) 计算公钥与私钥，计算明文 m = 19 对应的密文

$p = 7, q = 17, e = 13$

$n = pq, ed \equiv 1 \pmod{\varphi(n)}$

故公钥(13, 119) 私钥(37, 119)

$c = m^e \pmod{n}$

即密文 $c = 19^{13} \pmod{119}$

$(13)_{10} = (1101)_2$

$19^{13} = 19^{1+4+8} = 19 \cdot (130321 \mod 119) \cdot 19^8 = 19 \cdot 16 \cdot (16^2 \mod 119) =$

$19 \cdot 16 \cdot 18 = 5472$

密文 $c = 117$

4) 求明文 M=10所对应的密文

$c_1 = g^k \pmod p, c_2 = {y_B}^k M \pmod p$

即密文 $(c_1, c_2) = (59, 57)$

4) 试恢复消息 M

由 $7^k \equiv 59 \pmod{71}$ **得** $k = 3$

由 $29 = 3^3 M \pmod{71}$ **得** $M = 30$

5) 求 A 的公钥 P_A

$P_A = n_A G = 7 \cdot (2,7) = 3 \cdot ((2,7) + (2,7)) + (2,7)$

$(2,7) + (2,7) = (5,2)$

$(5,2) + (5,2) + (5,2) + (2,7) = (7,9) + (2,7) = (7,2)$

即 $P_A = (7,2)$

5) 求密文 C_m

$c_1 = kG, c_2 = P_m + kP_A$

$C_m = (3 \cdot (2,7), (10,9) + 3 \cdot (7,2)) = ((8,3), (10,9) + (7,9)) = ((8,3), (5,2))$

即密文 $C_m = ((8,3), (5,2))$

5) 简述接收方 A 从密文 C_m 恢复消息 P_m 的过程

由$P_A = n_A G$

得$P_m = c_2 - n_A c_1 = P_m + kP_A - n_A kG = P_m + kn_A G - n_A kG = P_m$

即接收方收到密文后只需令 c_2 减去私钥 n_A 点乘 c_1 的结果即可得到 P_m

6) 简述 CRT-RSA 的密钥生成、加密及解密运算的过程

密钥生成

1. 随机选取两个大素数 p 和 q
2. 计算 $n = p \times q$ 作为公钥和私钥的一部分
3. 计算 $\varphi(n) = (p-1)(q-1)$
4. 选择一个与 $\varphi(n)$ 互质的小整数 e
5. 找到一个整数 d 使得 $ed \equiv 1 \mod \varphi(n)$
6. 应用中国剩余定理进行优化：
    - 计算 $d_p = d \mod (p-1)$
    - 计算 $d_q = d \mod (q-1)$
    - 计算 $q_{inv} = q^{-1} \mod p$

公钥为 (n, e)，私钥为 $(n, d, p, q, d_p, d_q, q_{inv})$。

加密运算

$C = M^e \mod n$

解密运算

1. 使用 d_p 和 d_q 分别对 C 进行部分解密：
    - $M_1 = C^{d_p} \mod p$
    - $M_2 = C^{d_q} \mod q$
2. 应用中国剩余定理合并结果：
    - $h = q_{inv}(M_1 - M_2) \mod p$
    - $M = M_2 + hq$

7) 简述A、B利用 Diffie-Hellman 密钥交换协议生成公共密钥的过程

A 和 B 共享同一个公钥 g 和 p

A 和 B 各自选择一个私钥 a 和 b

A 计算出 $g^a \mod p$ 后发送给 B

B 计算出 $g^b \mod p$ 后发送给 A

A 接收 g^b 后计算 $(g^b)^a \mod p$

B 接收 g^a 后计算 $(g^a)^b \mod p$

此时 A 和 B 得到了相同的公共密钥 g^{ab}