计算 $2^{1000000} \bmod 77 \equiv ?$ 注：手工计算

计算 $2^{1000000} \bmod 77 \equiv ?$

显然，gcd(2,77)=1，φ(77)=φ(7*11)=6*10=60。

根据欧拉定理，$2^{60} \bmod 77 \equiv 1$。

由于，1000000=16666*60+40

所以，$2^{1000000} \bmod 77 = 2^{16666*60+40} \bmod 77$

$\equiv 2^{40} \bmod 77 \equiv 1024^4 \bmod 77 \equiv 23^4 \bmod 77$

$\equiv 67^2 \bmod 77 \equiv 10^2 \bmod 77 \equiv 23$。

$23^2=529 \bmod 77=67$

$2^{10}=1024$

1. 设 p=11,q=17,取 e=7 作为公钥，求 n, φ(n)及说明为什么私钥 d=23。

2.假如明文 m=111，加密后得到的密文 c 是多少？对密文 c 进行解密，得到明文 m 是多少？

3.假如明文 m=222，如何加密，得到的密文 c 是多少？对密文 c 进行解密，最后如何得到明文 m。

1.n=187, φ(n)=(p-1)(q-1)=160, $7*23 \bmod 160 \equiv 1$

2.$111^7 \bmod 187 \equiv 155$ $155^{23} \bmod 187 \equiv 111$

3.分组为 2 22 加密： $2^7 \bmod 187 \equiv 128$ $22^7 \bmod 187 \equiv 44$

密文 128 044 解密：$128^{23} \bmod 187 \equiv 2$ $44^{23} \bmod 187 \equiv 22$