1、使得a^m ≡ 1 mod n成立的最小正幂m，称为a所属的模n的指数。因此可计算，7所属的模19的指数为多少？

a^(p-1) ≡ 1 (mod p)。因此，7^3 ≡ 1 (mod 19)，所以7在模19下的指数为3。

2、计算7^120 mod 143

7^120 mod 143 = 1 \* 128 \* 36 \* 71 \* 49 \* 49 \* 7 mod 143 = 62。

3、计算3^201 mod 11

3^10 ≡ 1 (mod 11)，因此3^201 ≡ 3^(10\*20+1) ≡ (3^10)^20 \* 3^1 ≡ 1^20 \* 3^1 ≡ 3 (mod 11)。

4、给出在RSA密码系统中，使用公钥(e, n)=(7, 77)加密M=4的结果及解密C=2的计算过程。

加密：M=4，e=7，n=77，C=M^e mod n = 4^7 mod 77 = 66。

解密：C=2，d=e^(-1) mod (p-1)(q-1)，根据扩展欧几里得算法可得d=43。

M=C^d mod n = 2^43 mod 77 = 4。

1. 给出对称加密（如AES）与公钥密码系统（如RSA）的强度和弱点的比较。

对称加密的优点是加解密速度快，适合大量数据的加密和传输；缺点是需要事先共享密钥，并且一旦密钥被泄漏，所有传输的数据都将面临泄露风险。公钥密码系统的优点是不需要事先共享密钥，可以安全地传输密钥以及其他信息；缺点是加解密速度慢，适合少量数据的加密和传输。因此，在实际应用中，对称加密和公钥密码系统常常结合使用，以充分发挥各自的优势并弥补缺点。

6、在对称密码体制下，A想验证一下B是否拥有和自己一样的密钥K。有人提出了如下方法：

A产生一个与K等长的随机二进制数R，用R与K异或得到W，然后将W发给B。

如果B确实知道K，用W与K异或可得到R，将R发给A

A收到B发来的R，和之前自己发出的R相同，说明B确实拥有和自己一样的密钥K。

这个方法有个漏洞，你发现了吗？

这个方法存在一个中间人攻击的漏洞。假设有Eve在A和B之间进行监听和欺骗，当A产生随机数R并将W = R ⊕ K发送给B时，Eve可以截获W并将其替换为另一个随机数W'，然后将W'发送给B。此时，B计算出K' = W' ⊕ R，并将其发送给A，A收到K'后计算出R' = W' ⊕ K'，如果R'等于A之前产生的随机数R，则A会认为B拥有正确的密钥K。但实际上，Eve通过截获和替换W成功欺骗了A，从而得到了与A和B一样的密钥K'。因此，这种方法并不能很好地验证B是否拥有正确的密钥K。