**（1）Elgama算法中，如果公用素取19，本原根选取10，若Alice选择私钥5，并生成公钥发给Bob，Bob想发送M=17给Alice，并随机选取k=6，问：bob生成的密文是什么？Alice如何解密？**

公用素：q = 19；本原根：a = 10；私钥：XA = 5；

公钥：YA = aXa mod q = 105 mod 19 = 3；

加密：M = 17;k = 6；

K = (YA)k mod q = 36 mod 19 = 7

C1 = ak mod q = 106 mod 19 = 11

C2 = KM mod q = 7 \* 17 mod 19 = 5

则生成的密文是（11，5）

解密：K = C1Xa mod q = 115 mod 19 = 7

M = (C2K-1) mod q = (5\*7-1) mod 19 = (5\*11) mod 19 = 17

**（2）DH算法中，如果公用素数选择353，本原根选取3，若alice和bob分别选取私钥97和233，并互相交换公钥，则二人计算出来的秘钥是什么？**

公用素：q = 353；本原根：a = 3；

Alice选择私钥Xa = 97，计算Ya = aXa mod q = 397 mod 353 = 40

Bob选择私钥Xb = 233，计算Y­b = aXb mod q = 3233 mod 353 = 248

双方保留X值，将Y值交换给对方

Alice计算出K = YbXa mod q = 24897 mod 353 = 160

Bob计算出K = YaXb mod q = 40233 mod 353 = 160

则二人计算出的密钥是160

**（3）RSA算法中，如果截获发给用户的密文c=10，该用户的公钥e=5，n=35，那么明文M是多少？**

n = 35 = 5 \* 7

则p = 5，q = 7

φ(n) = (p-1)(q-1) = 4\*6 = 24

ed = 1 mod φo(n)

由e = 5 得d = 5

则公钥（5，35）私钥（5，35）

M = cd mod n = 105 mod 35 = 5

则明文M为5