密码学作业002 学号 20131910023 姓名 金洋

1. 什么是离散对数问题？

答：离散对数问题是指以下问题：设g是的一个原根，h是的非零元，寻找一个x，使其满足.

1. 什么是Diffie-Hellman问题？

答：Diffie-Hellman问题是指以下问题：设p为素数，g为整数，已知、的值，以此来计算的值.

1. Diffie-Hellman密钥交换蕴含了安全两方计算，予以解释。

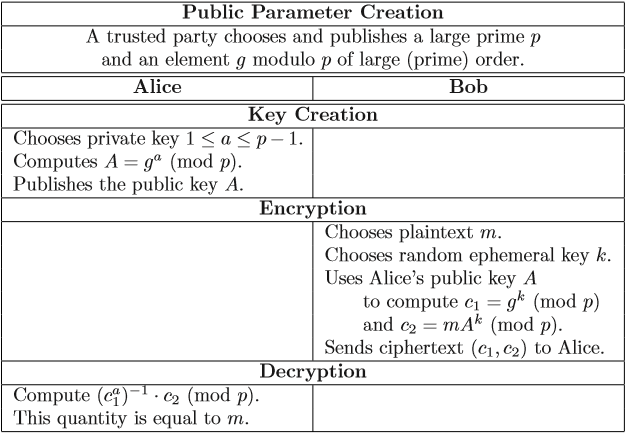
答：安全多方计算（SMC）是解决一组互不信任的参与方之间保护隐私的协同计算问题，SMC要确保输入的独立性，计算的正确性，同时不泄露各输入值给参与计算的其他成员。

特点是特点是：<1>. 两或更多方参与基于他们各自私密输入的计算。<2>. 而且他们都不想其他方知道自己的输入信息。

Diffie-Hellman密钥交换中Alice独立计算出给Bob，Bob独立计算出；g, p公开，Alice得到了B由于DLP难题难以计算出Bob的b，Bob得到了A由于DLP难题难以计算出Alice的a，（对第三方得到A,B也不可能计算出a或b）。交换后，Alice和Bob又能各自结合收到的值和自己的私钥独立计算出共享秘密,（而第三方不能计算出）。综上Diffie-Hellman密钥交换蕴含了安全两方计算。

1. 证明ElGamal密码体制的解密正确性。

答：ElGamal密码体制如下：







∴Alice最终计算时：

1. ElGamal密码体制蕴含了一个完整的Diffie-Hellman密钥交换协议，予以解释。

答：A蕴含B的定义为：当A事件发生，则必导致B事件发生。

1. ElGamal密码体制和Diffie-Hellman密钥交换协议的第三方发布公开参数g、p做法相同；
2. ElGamal密码体制中Alice 计算后发送给Bob，这一步和Diffie-Hellman密钥交换协议中Alice做法相同；
3. ElGamal密码体制中，Bob收到了A，并计算，之后作为密文之一发送给Alice，这一步和Diffie-Hellman密钥交换协议中Bob计算做法同；
4. ElGamal密码体制中，Bob在完成计算后，计算了，（并计算出发送给Alice），这一步和Diffie-Hellman密钥交换协议中最后计算共享密钥做法相同。

综上，密码体制蕴含了一个完整的Diffie-Hellman密钥交换协议。

1. 查阅文档，了解离散对数问题用于密码设计时对于参数规模的要求。

答：基于解离散对数问题密码体制主要是Diffie-Hellman密钥交换和ElGamal密码体制，两者都首先需要由公信方公布大素数p和g。

针对离散对数问题的攻击有以下：

①**蛮力攻击**：实际中为了避免针对基于离散对数密码体制的蛮力攻击，底层群G的基必须足够大。在群为了抵抗使用目前计算机技术发起的蛮力攻击攻击，**|G|=p-1至少应该在280左右**。

②**Shanks’ Baby-step Giant-step方法**：Baby-step Giant-step方法需要次计算步骤和相同大小的内存。对阶为280的群而言，攻击者大概只需要=240次计算和240个存储单元就能破解；这个数目在目前的PC机和硬盘上是非常容易实现的。为了获得280的攻击复杂度，群的解至少为**|G|≥**2160，因此在**群G=中素数p的长度应该至少为160位。**

③**Pollard’s Rho方法**：Pollard’s Rho方法期望的时间和与Baby-step Giant-step方法相同，都是，但是Pollard’s Rho方法对空间的需求却微不足道。因此**p的长度应该至少为160位。**

④**Pohlig-Hellman算法：**为了防止攻击，群的阶的最大质因子必须在2160范围内。

⑤**Index-Calculus算法**：为了防止攻击，内DLP的素数p长度至少为1024位。

而对于g的选择，要求g在中有一个大的素数阶，约.