1、在 DSS 数字签名标准中，参数选取 p=83，q=41，g=4 mod 83，若 Alice 的私钥 x 为 16。

（1）计算出 Alice 的公钥 y；

（2）Alice 对消息 h(m)=56 签名时，选择 k=23，然后发送给 Bob。写出 Alice 签名及 Bob 验证的过程。

2、（1）叙述基于 hash 的 RSA 签名算法的过程（包括参数设置、密钥生成、签名及验签过程）。

（2）阐述 hash 函数的三个基本性质（抗原像、抗第二原像及抗碰撞）的定义，并以 MD5 为例分别说明对这三种性质进行攻击的复杂度。

（3）结合 hash 函数的三个基本性质，分别说明基于 hash 的 RSA 签名算法如何（1）抵抗唯密钥攻击（2）抗已知消息攻击及（3）抗选择消息攻击的？

3、（1）简述 DSA 签名体制的过程（包括参数设置、密钥生成、签名及验签过程）。

（2）说明签名者随机选取的 k 被泄露，或者 k 值重复使用的危害性。

4、简述密钥管理采用层次化的结构的好处。