现代密码学作业——第八讲

1、签名值为（10，29）

2、

（1）随机数 k 的泄露：

如果签名过程中使用的随机数 k 被泄露，攻击者可以利用已知的 k 重新计算签名私钥 d。这种情况下，签名系统就被破解了，攻击者可以轻易地伪造合法签名，从而破坏了数字签名的可信性和完整性。

（2）随机数 k 的重用：

如果同一个 k 被多次重用来生成不同的签名，攻击者可以通过观察相同 k 值生成的签名，利用数学方法推导出私钥 d。一旦攻击者获得了私钥 d，他们就可以生成有效的签名，从而破坏了签名系统的安全性。