4.2. 试述DSA数字签名算法，包括密钥产生、签名算法和验证算法，并给出验证过程正确性证明

参考ppt

4.4. 已知schnorr签名的密钥产生和签名算法，试给出验证方程，并证明其正确性。

参考ppt

5.1.试证DSA签名中两次使用相同的会话密钥k，是不安全的

分别给出对m1和对m2的签名表达式,然后将两个关于s的方程联立,这时如果会话密钥k相同则可直接解出k和秘密钥x，证明过程可根据此思路进行