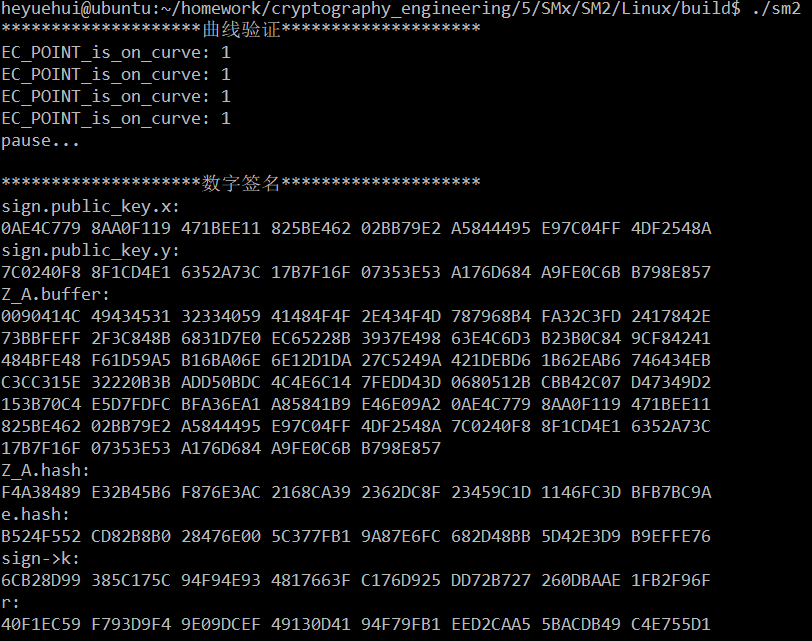
密码工程-课后作业5

# 实现并调试SM2代码



# 使用SM2，SM3，SM4实现一个简易的密钥协商协议

思路如下：

预先假设alice和bob共享SM4密钥share\_key,

alice 拥有公钥alice\_pk, 私钥alice\_sk,

bob 拥有公钥bob\_pk, 私钥bob\_sk,

协商流程如下：

1.alice 向 bob 发送 Enc.bob\_sk[a], a为随机数

2. bob 接受到a, 产生随机数b, c = a\*b， 使用SM4算法与share\_key加密c生成共享密钥， 然后将Enc.alice\_sk[b]， 与c的消息摘要(SM3)发送给alice

3. alice接受消息，先解密得到b，然后c = a\*b，验证c与alice的c一致，使用SM4算法与share\_key加密c生成共享密钥