计网第十四次作业

彭程 2020011075

**第一题：**

n = pq = 5×11 = 55

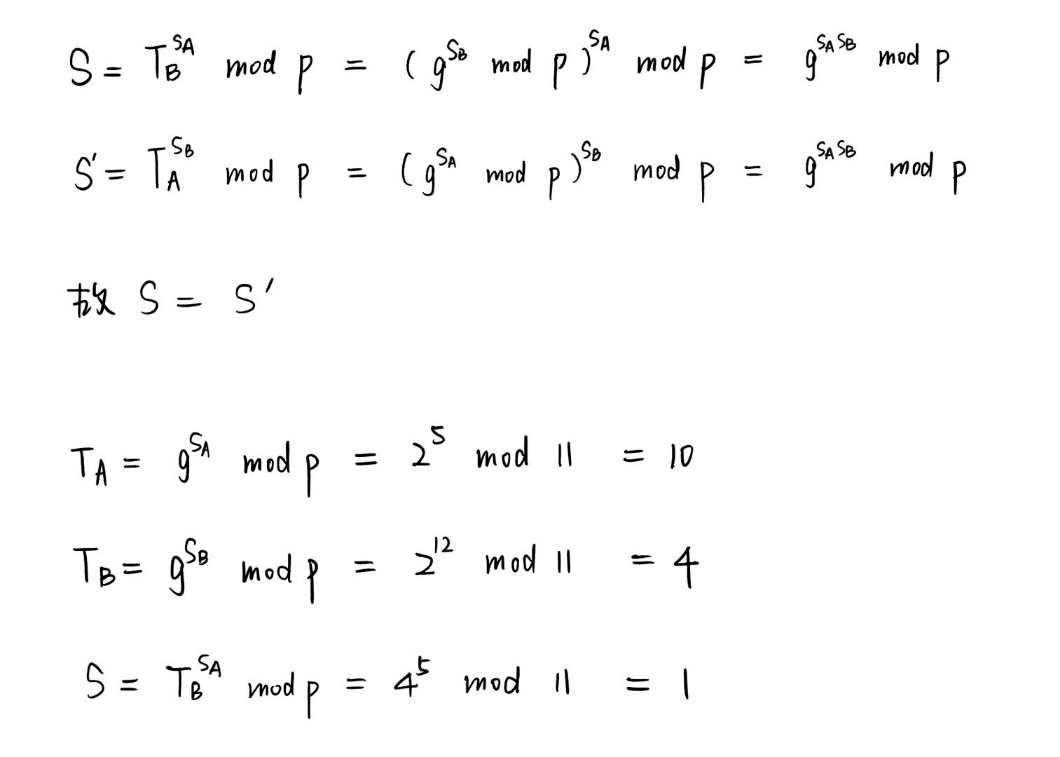
z = (p-1)(q-1) = 40

则(de-1)可以被z整除： (3𝑑-1) = 𝑘 × 𝑧 = 40𝑘  
因此𝑑 = (40𝑘 + 1)/3 其中 k = 0,1,2,3……，且要求d也为整数；  
可以求得： 𝑑 = 27, 67,107,147 均符合条件；  
**1.3**

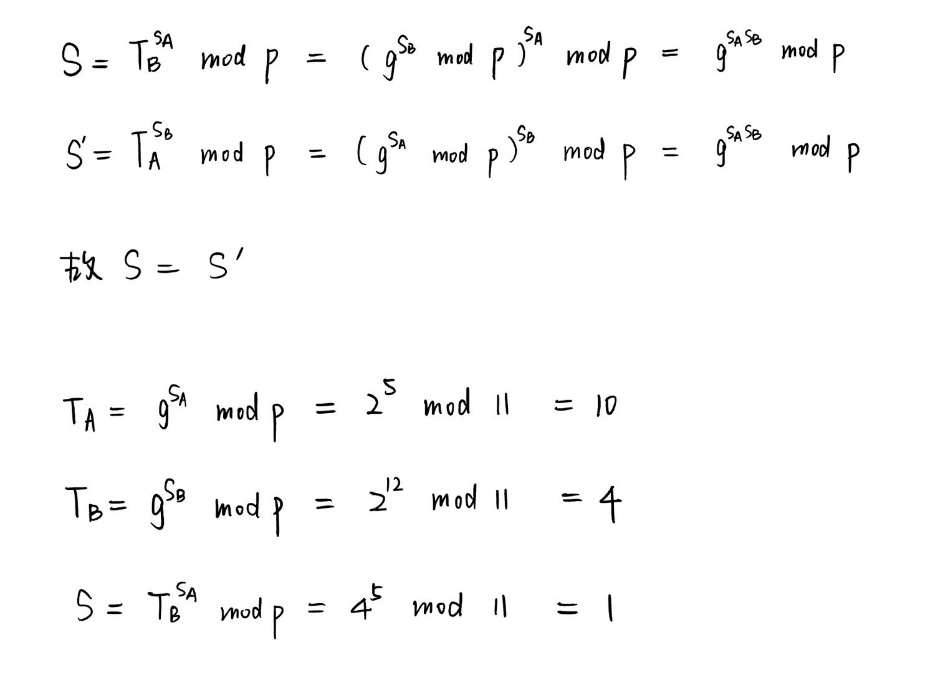
𝑐 = 𝑚𝑒 𝑚𝑜𝑑 𝑛 = 83 𝑚𝑜𝑑 55 = 17

**第二题：**

**2.1**

****

**2.2**

****

**2.3**

1. 中间人截获Alice的公钥 (TA)，将自己的公钥 (TC)发送给Bob。

2. 中间人截获Bob的公钥 (TB)，将自己的公钥 (TC)发送给Bob。

3. 中间人和Alice使用一个共享密钥(S)，中间人和Bob使用另一个共享密钥(S’)。

4. 中间人便可以解密Alice或Bob通过公钥发出的任何消息。