计网第十四次作业

彭程 2020011075

第一题：

1.1

n = pq = 5×11 = 55

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

1.2

则(de-1)可以被 z 整除： $(3d\text{-}1) = k \times z = 40k$

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

$c = m^e \bmod n = 8^3 \bmod 55 = 17$

第二题：

2.1

$$S = T_B^{S_A} \bmod p = (g^{S_B} \bmod p)^{S_A} \bmod p = g^{S_A S_B} \bmod p$$

$$S' = T_A^{S_B} \bmod p = (g^{S_A} \bmod p)^{S_B} \bmod p = g^{S_A S_B} \bmod p$$

故 $S = S'$

2.2

$$T_A = g^{S_A} \bmod p = 2^5 \bmod 11 = 10$$

$$T_B = g^{S_B} \bmod p = 2^{12} \bmod 11 = 4$$

$$S = T_B^{S_A} \bmod p = 4^5 \bmod 11 = 1$$

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。