PB21000224

P8

a. n 等于 51，z 等于 40

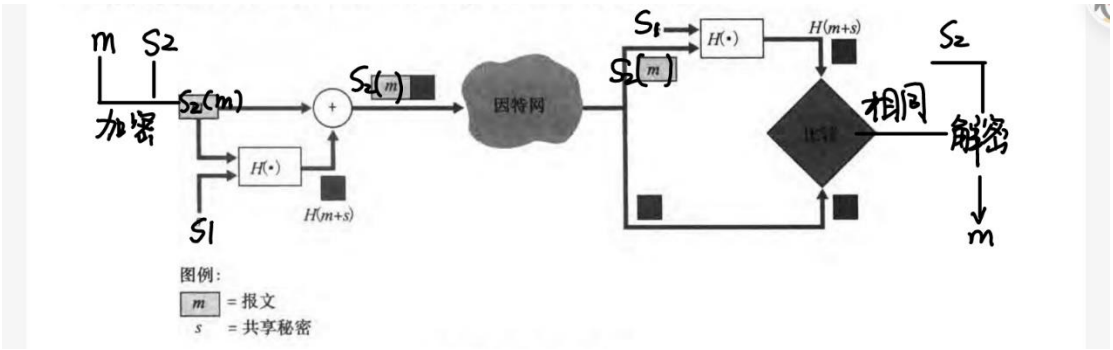
b. 可以发现 e=3 和 40 是互素，所以是可接受的

c. 可以发现 d = 27 时，27*3 = 1 (mod 40)，所以是 27，67，107，147 都可以

d. 8^27 (mod 40) = (512 mod 40)^9 mod 40 = -8^9 (mod 40) = -(512 mod 40)^3 = 39 (mod 40)
所以密文是 39.

P12

如下图所示



P18

a. 不能，Alice 只持有 bob 的公钥，没有自己和 bob 所独有的一段报文认证密钥 s1，也没有公钥私钥对，无法证明自己是 Alice

b. 可以支持 Alice 向 Bob 发送机密性邮件，只需要 Alice 的报文用 Bob 的公钥加密进行机密传输即可。