PB21000224

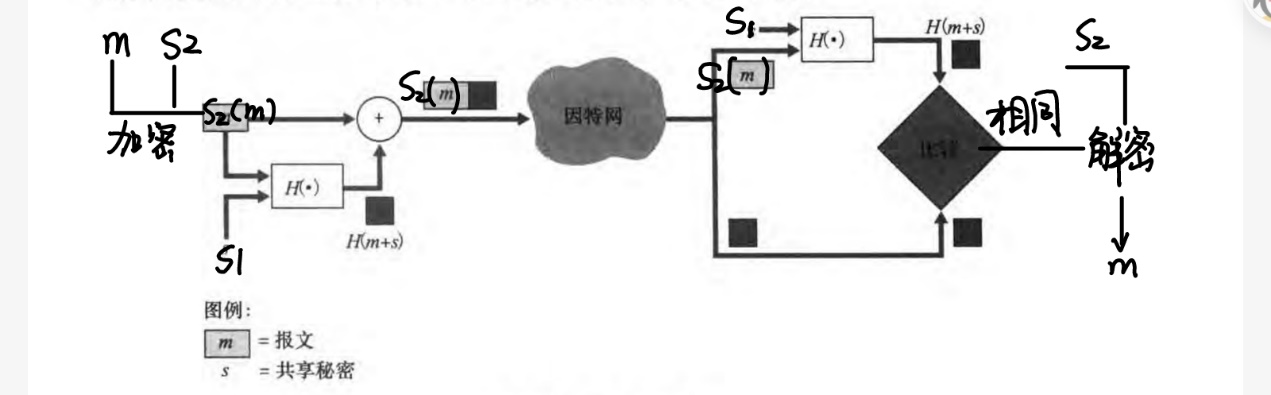
P8

1. n等于51，z等于40
2. 可以发现e=3和40是互素，所以是可接受的
3. 可以发现d = 27时，27\*3 = 1 (mod 40)，所以是27，67，107，147都可以
4. 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

1. 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
2. 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。

