HW8

P8

P8. 考虑具有 $p=5$ 和 $q=11$ 的 RSA。

a. n 和 z 是什么?

b. 令 e 为 3。为什么这是一个对 e 的可接受的选择?

c. 求 d 使得 $de=1 \pmod{z}$ 和 $d<160$。

d. 使用密钥 (n, e) 加密报文 $m=8$。令 c 表示对应的密文。显示所有工作。提示：为了简化使用如下事实。

$$[(a \bmod n) \cdot (b \bmod n)] \bmod n = (a \cdot b) \bmod n$$

a

n=pq=55

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

b

$e = 3 < n$，并且和z互质

c

d=27，满足27*3 mod 40=1

d

加密：m=8，$m^e = 512$，密文$c = m^e mod n = 17$

解密：$c^d mod n = 17^{27} mod 55 = 8$

P12

P12. 假定 Alice 和 Bob 共享两个秘密密钥：一个鉴别密钥 S_1 和一个对称加密密钥 S_2。扩充图 8-9，使之提供完整性和机密性。

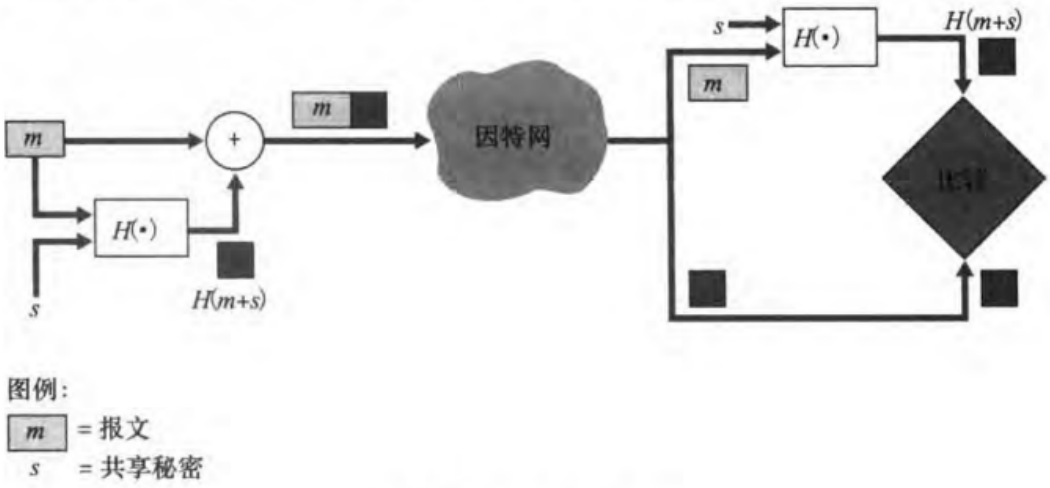
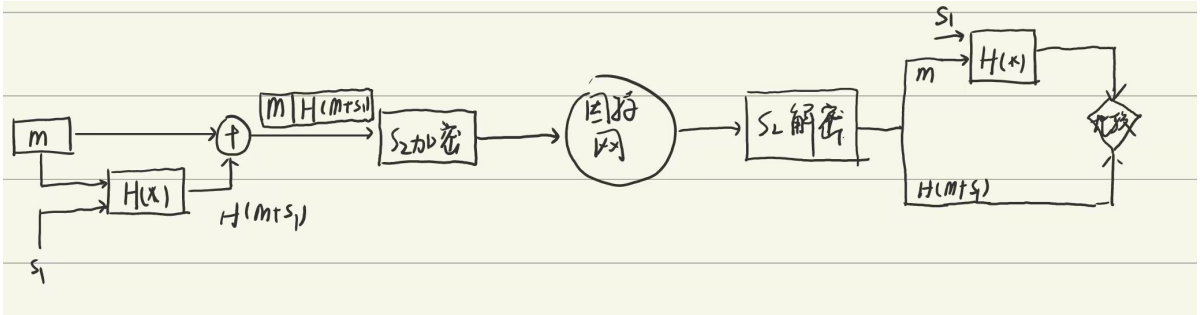


图 8-9　报文鉴别码

扩充后：



P18

P18. 假定 Alice 要向 Bob 发送电子邮件。Bob 具有一个公共－私有密钥对（K_B^+，K_B^-），并且 Alice 具有 Bob 的证书。但 Alice 不具有公钥私钥对。Alice 和 Bob（以及全世界）共享相同的散列函数$H(\cdot)$。

a. 在这种情况下，能设计一种方案使得 Bob 能够验证 Alice 创建的报文吗？如果能，用方框图显示 Alice 和 Bob 是如何做的。

b. 能设计一个对从 Alice 向 Bob 发送的报文提供机密性的方案吗？如果能，用方块图显示 Alice 和 Bob 是如何做的。

a

Alice没有公钥私钥对，Bob无法验证Alice创建了消息

b

可以，因为Bob存在公钥私钥对

Alice可以通过Bob的公钥对消息进行加密，并发送对Bob的加密消息，Bob再用自己的私钥解密

如下图：