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:为了简化计算,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. $e=3 < n$,且与 z 互质.

c. $3d \equiv 1 \pmod{40}$, $d<160$

$d = 27$

d. 公钥为 $(3, 55)$,私钥为 $(27, 55)$

加密:

明文 $m=8$,则密文 $c = m^e \pmod n = 8^3 \pmod{55} = 17$

解密:

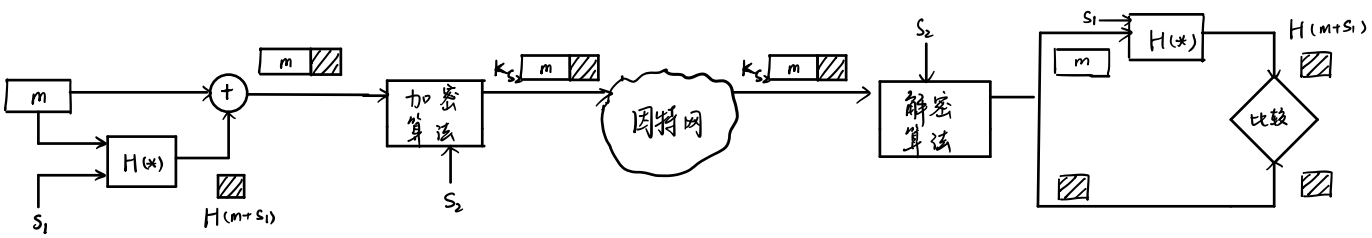
计算 $m = c^d \pmod n = 17^{27} \pmod{55} = 14^{13} \cdot 17 \bmod 55 = 31^6 \cdot 14 \cdot 17 \bmod 55$

$= 26^3 \cdot 14 \cdot 17 \bmod 55 = 16 \cdot 26 \cdot 14 \cdot 17 \bmod 55 = 8$

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。

8-9 中 报文鉴别码提供了完整性,但不关心机密性.

使用对称加密密钥 S_2 对报文进行加密和解密,提供机密性.



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. 不能. Alice 不具有表明自己身份的信息. Alice 不具有公钥私钥对或其他提前共享的秘密, Bob 不能验证 Alice 创建的报文.

b. Alice 使用 Bob 的公钥加密报文并发送，Bob 使用私钥解密.