计算机网络作业 7

傅申 PB20000051

P8.

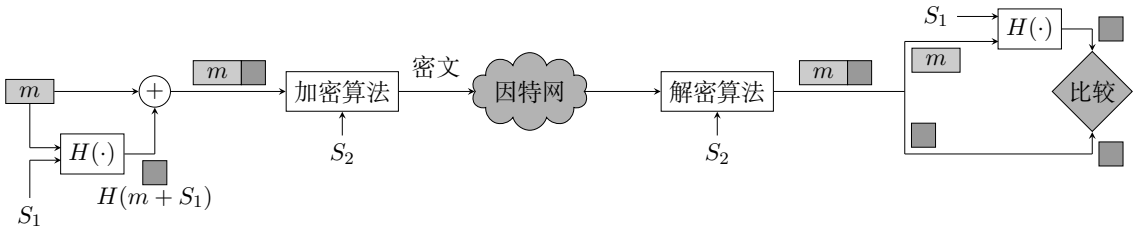
a. $n = pq = 55$, $z = (p-1)(q-1) = 40$.

b. 因为 $z = 3 < n$, 且 e 和 n 没有非 1 的公因数.

c. $d = 27 (\mathrm{mod}\, 40)$, 因此可选的 d 有 27, 67, 107.

d. 密文 $c = m^e \bmod n = 512 \bmod 55 = 17$.

P12.



P18.

a. 因为 Alice 不具有公钥私钥对, 所以 Bob 无法验证 Alice 创建的报文.

b. 可以, 如下