计网 HW8

林宸昊 PB20000034

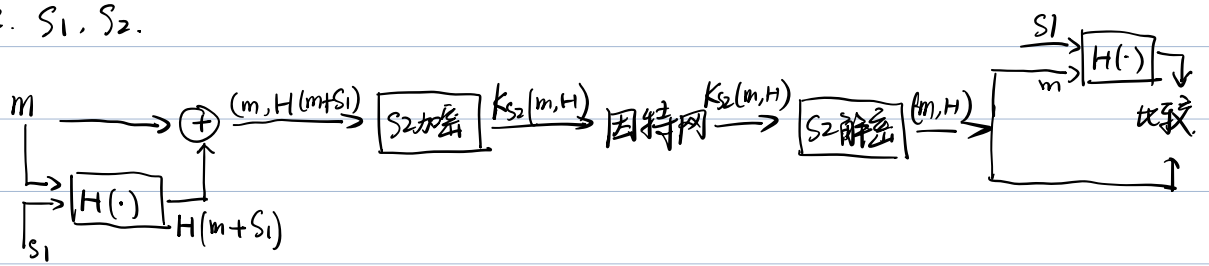
P8. a. $n = pq = 55$, $z = (p-1)(q-1) = 40$

b. $1 < e < z$, $\gcd(e, z) = 1$.

c. $de = 81 = 1 \bmod (40)$, $d = 27 < 160$.

d. $8^3 \bmod 55 = 17$.

P12. S_1, S_2.



P18. a. 不行. 如果受到中间人攻击, 由于Alice不具有公钥-私钥对, Bob无法验证报文的确由Alice创建;

b. Alice用Bob的公钥加密报文即可.