计网hw8

Question 8、12、18

8、考虑具有 $p=5$ 和 $q=11$ 的RSA

a、 n和z

$n = 5\times 11 = 55$

$z = 4\times 10 = 40$

b、 令 $e=3$ 为什么可接受

$3 < z$ 且 z 与 e 互质

当 $d=27$ 时 $27\times 3 \bmod 20 \equiv 1$ $e=3$ 合理

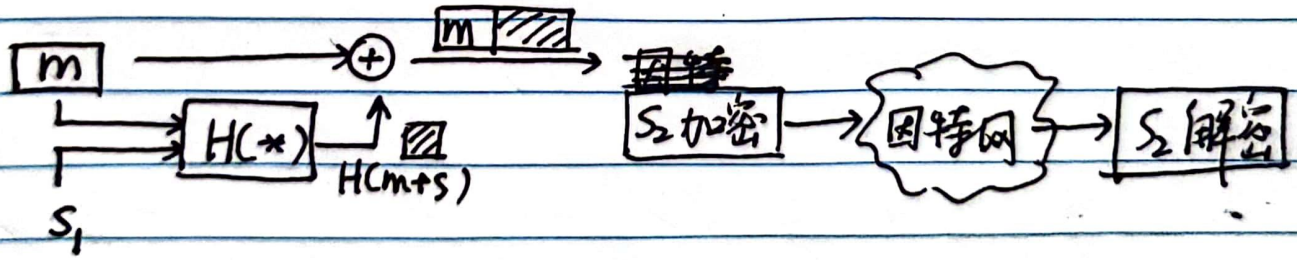
c、 $d=27$

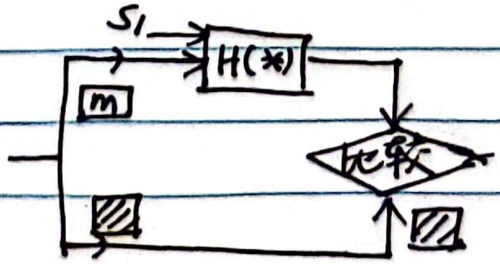
d、 使用 (n, e) 加密报文 $m=8$

加密 $c = m^e \bmod n = 8^3 \bmod 55 = 17$

解密 $m' = c^d \bmod n = 17^{27} \bmod 55 = 8$

12、 Alice 和 Bob 共享鉴别密钥 S_1，对称加密密钥 S_2





18. Alice ⟶ Bob

Bob有公共-私有密钥对 (K_B^+, K_B^-)

Alice有Bob证书但没有公钥私钥对，

会把另共享散列函数 $H(*)$

a. 不能，因为Alice没有 (K_B^+, K_B^-)

b. 能，从Alice出发