HW8 参考答案

P8

1. $n = pq = 55$, $z = (p-1)(q-1) = 40$
2. 因为 $e < z$，且与 z 没有公因数
3. $3d = 1(mod40), d = 27, 67, 107, 147(d < 160)$

> 只写 27 也没扣分

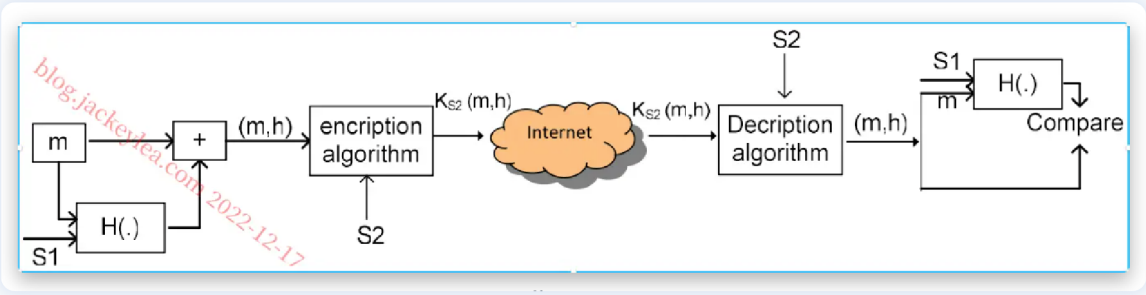
4. $c = m^e mod n = 512 mod 55 = 17$

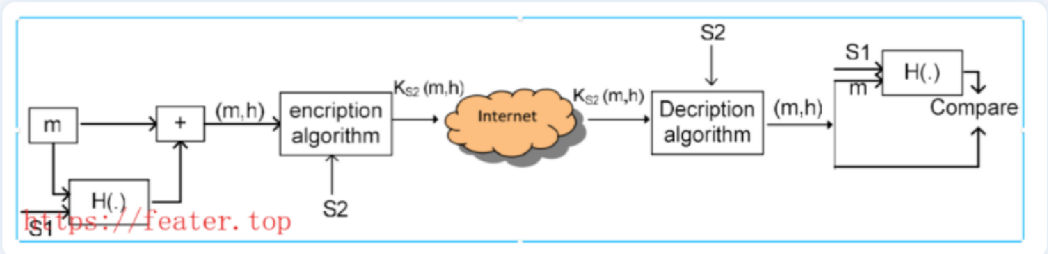
P12

需要增加的内容

->S2加密-> internet -> S2解密->

> 这道题直接截答案图和网图（甚至还有水印）都会被判抄袭





P18

不行，原因是 Bob 没有 Alice 的公私钥对或预先共享密钥，无法验证 Alice 创建的报文。

可以， Alice 直接使用 Bob 的公钥加密