HW8

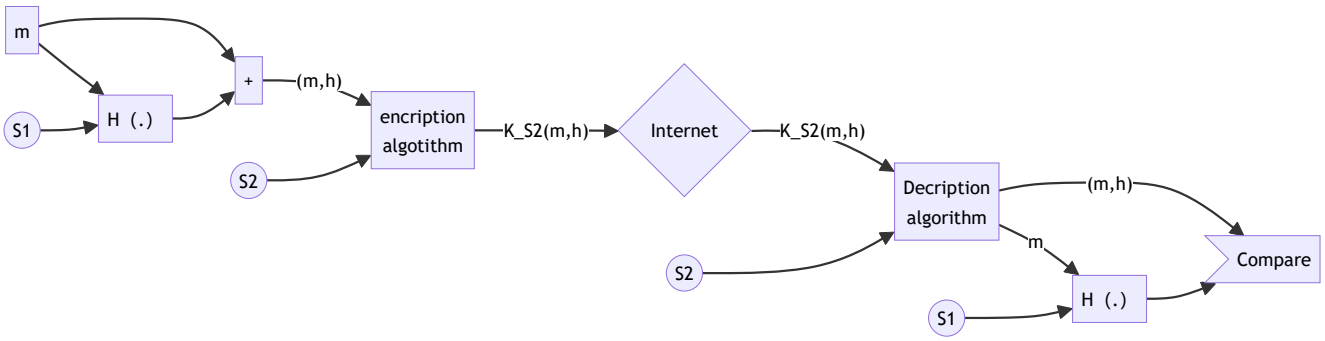
PB21111686_赵卓

8

- $(a).$
  $n = p * q = 55$
  $z = (p-1) * (q-1) = 40$
- $(b).$
  $e = 3$时，e比n小并且和z没有相同的因子
- $(c).$
  $d = 27$时，$de = 1(mod\ \ z)$，且$d = 27$满足$d \leq 160$
- $(d).$
  $m = 8$，$me = 512$
  则$c = me\ \ mod\ \ n = 17$

12

- 如图：



18

- $(a).$
  不具有公钥/私钥对或预共享秘密，所以Bob无法验证$Alice$创建了消息。
- $(b).$
  是的，$Alice$简单地使用Bob的公钥对消息进行加密，并发送对Bob的加密消息。