第8次作业答案

作业答案

1. **Consider RSA with $p = 5$ and $q = 11$.**
   a. **What are n and z?**
   b. **Let e be 3. Why is this an acceptable choice for e?**
   c. **Find d such that $de \equiv 1(\mod z)$ and $d < 160$**
   d. **Encrypt the message m = 8 using the key (n, e). Let c denote the corresponding ciphertext. Show all work. Hint: To simplify the calculations, use the fact**:

$$[(a \mod n) \cdot (b \mod n)] \mod n = (a \cdot b) \mod n$$

a.

$$n = pq = 55$$
$$z = (p-1) \cdot (q-1) = 40$$

b. 因为 $e = 3 < z$，且 e 与 z 互质
c. 可以求得 $d = 27$
d. 加密过程：

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

解密过程：

$$m^{'} = c^d \mod n = 17^{25} \mod 55 = 8$$

$m^{'} = m$, 结果正确
（注：d的选取不唯一）

---

2. **Suppose Alice and Bob share two secret keys: an authentication key S1 and a symmetric encryption key S2. Augment Figure 8.9 so that both integrity and confidentiality are provided**

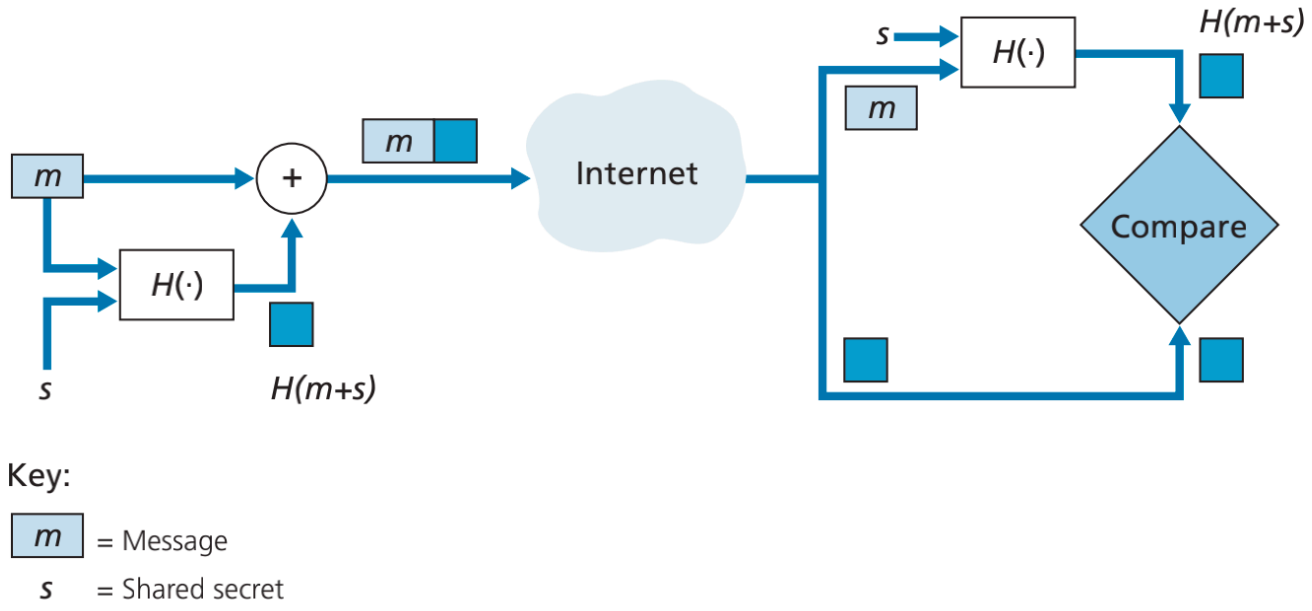
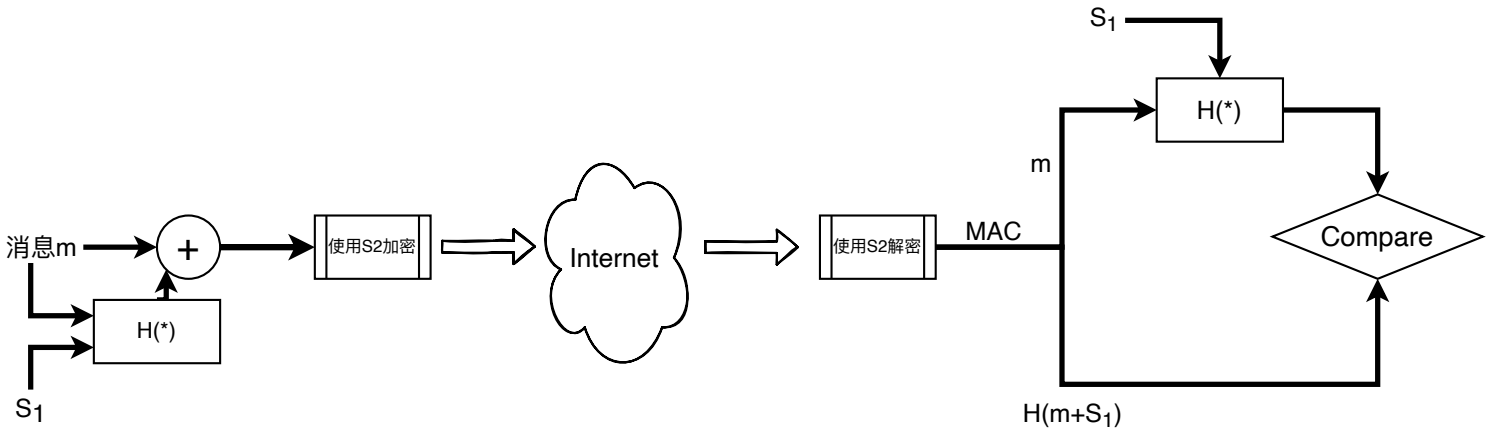


Figure 8.9 ♦ Message authentication code (MAC)

这是课本上的图8.9，已经指出了它仅满足而不满足机密性。
现在我们用S_1 和S_2实现机密性即可

其中，S_1 需要作为图8.9中的Shared Secret，之后我们在用S_2对MAC进行加解密即可。流程图如下



---

3. **Suppose Alice wants to send an e-mail to Bob. Bob has a public-private key pair (K_B^+, K_B^-), and Alice has Bob's certificate. But Alice does not have a public, private key pair. Alice and Bob (and the entire world) share the same hash function $H(\cdot)$**

   a. In this situation, is it possible to design a scheme so that Bob can verify that Alice created the message? If so, show how with a block diagram for Alice and Bob.

   b. Is it possible to design a scheme that provides confidentiality for sending the message from Alice to Bob? If so, show how with a block diagram for Alice and

> **Bob.**

a. 不可能的。`Alice`没有任何可以表明自己身份的信息。她没有任何密钥（对称/非对称的都没有）。同时即便有这样的密钥，也必须让`Bob`知道后才能实现端点认证。比如`Alice`生成一对公私钥，然后拿公钥去申请一个CA并且让`Bob`了解到这个CA

b. 这道题只要求我们实现从`Alice`到`Bob`的通信机密性，因此`Alice`发消息时直接用`Bob`的公钥加密即可。