# 第8章-计算机网络中的安全

## 231880038 张国良

## Problem 1

R5. 考虑一个 8 块密码。这个密码有多少种可能的输入块？有多少种可能的映射？如果我们将每种映射视为一个密钥，则该密码具有多少种可能的密钥？

**解：**

8块密码共有$2^8$钟可能的输入块，两两对应映射，共有$2^8!$种可能的映射，所以有$2^8!$种密钥

## Problem 2

R15. 假设 Alice 有一个准备发送给任何请求者的报文。数以千计的人要获得 Alice 的报文，但每个人都要确保该报文的完整性。在这种场景下，你认为是基于 MAC 还是基于数字签名的完整性方案更为适合？为什么？

**解：**

对于基于MAC的方案，Alice必须与每个潜在的接收者建立共享密钥。对于数字签名，她对每个接收者使用相同的数字签名；数字签名是通过用她的私钥签名消息的散列来创建的。数字签名显然是更好的选择

## Problem 3

R23. 假设 Bob 向 Trudy 发起一条 TCP 连接，而 Trudy 正在伪装她是 Alice。在握手期间，Trudy 向 Bob 发送 Alice 的证书。在 SSL 握手算法的哪一步，Bob 将发现他没有与 Alice 通信？

**解：**

客户端将生成预主密钥(PMS)后，它将用Alice对其进行加密公钥，然后将加密的PMS发送到Truddy。Truddy将无法解密PMS，因为她没有Alice的私钥。因此,Truddy将不能够确定共享的认证密钥。她可以猜猜看一个人选择随机密钥。在握手的最后一个步骤中，她向Bob发送所有握手消息的MAC，使用所猜测的验证密钥。当Bob接收MAC，MAC测试将失败，Bob将结束TCP连接。

## Problem 4

P8. 考虑具有 $p=5$ 和 $q=11$ 的 RSA。

a. $n$ 和 $z$ 是什么？

b. 令 $e$ 为 3。为什么这是一个对 $e$ 的可接受的选择？

c. 求 $d$ 使得 $de=1 \pmod z$ 和 $d<160$。

d. 使用密钥 $(n, e)$ 加密报文 $m=8$。令 $c$ 表示对应的密文。显示所有工作。提示：为了简化计算，使用如下事实。

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

**a.**

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

**b.**

因为3小于55并且和40互质

**c.**

```
i := 41
d := 1
while d < 160:
        d := i / 3;
        if i % 3 == 0: 选出一个符合题意的d
        i := i + 40
```

最终得到d为27或67或107或147

**d.**

密钥为$(55, 3)$

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

# Problem 5

P9. 在这个习题中，我们探讨 Diffie-Hellman（DH）公钥加密算法，该算法允许两个实体协商一个共享的密钥。该 DH 算法利用一个大素数 $p$ 和另一个小于 $p$ 的大数 $g$。$p$ 和 $g$ 都是公开的（因此攻击者将知道它们）。在 DH 中，Alice 和 Bob 每人分别独立地选择秘密密钥 $S_A$ 和 $S_B$。Alice 则通过将 $g$ 提高到 $S_A$ 并以 $p$ 为模来计算她的公钥 $T_A$。类似地，Bob 则通过将 $g$ 提高到 $S_B$ 并以 $p$ 为模来计算他的公钥 $T_B$。此后 Alice 和 Bob 经过因特网交换他们的公钥。Alice 则通过将 $T_B$ 提高到 $S_A$ 并以 $p$ 为模来计算出共享密钥 $S$。类似地，Bob 则通过将 $T_A$ 提高到 $S_B$ 并以 $p$ 为模来计算出共享密钥 $S'$。

a. 证明在一般情况下，Alice 和 Bob 得到相同的对称密钥，即证明 $S = S'$。

b. 对于 $p = 11$ 和 $g = 2$，假定 Alice 和 Bob 分别选择私钥 $S_A = 5$ 和 $S_B = 12$，计算 Alice 和 Bob 的公钥 $T_A$ 和 $T_B$。显示所有计算过程。

c. 接着（b），现在计算共享对称密钥 $S$。显示所有计算过程。

d. 提供一个时序图，显示 Diffie-Hellman 是如何能够受到中间人攻击的。该时序图应当具有 3 条垂直线，分别对应 Alice、Bob 和攻击者 Trudy。

**a.**

$$S = T_B^{S_A} \% p = (g^{S_B} \% p)^{S_A} \% p = g^{S_A S_B} \% p$$
$$S' = T_A^{S_B} \% p = (g^{S_A} \% p)^{S_B} \% p = g^{S_B S_A} \% p$$
所以$S = S'$

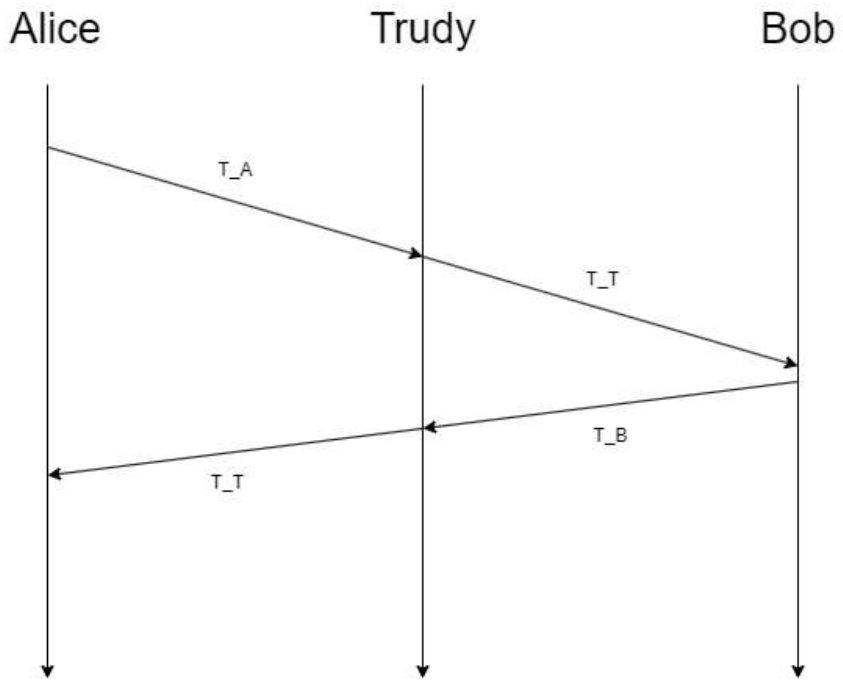
**b.**

$$T_A = g^{S_A} \% p = 10$$
$$T_B = g^{S_B} \% p = 4$$

**c,**

$$S = T_B^{S_A} \% p = 1$$
$$S' = T_A^{S_B} \% p = 1$$

**d.**




Trudy向Alice伪装成Bob并且向Bob伪装成Alice，最终Alice与Trudy之间商量了共享密钥S_AT，Bob与Trudy之间商量了共享密钥S_BT，最终Alice与Bob间的通话受到了Trudy的攻击

# Problem 6

P18. 假定 Alice 要向 Bob 发送电子邮件。Bob 具有一个公共－私有密钥对（$K_B^+$，$K_B^-$），并且 Alice 具有 Bob 的证书。但 Alice 不具有公钥私钥对。Alice 和 Bob（以及全世界）共享相同的散列函数$H(\cdot)$。

a. 在这种情况下，能设计一种方案使得 Bob 能够验证 Alice 创建的报文吗？如果能，用方框图显示 Alice 和 Bob 是如何做的。

b. 能设计一个对从 Alice 向 Bob 发送的报文提供机密性的方案吗？如果能，用方块图显示 Alice 和 Bob 是如何做的。

**a.**

没有有公钥/私钥对或预共享秘密，Bob无法验证Alice创建了消息

**b.**

可以，Alice使用Bob的公钥对消息进行加密，并向Bob发送加密消息