计算机网络 · 理论作业8

20337251伍建霖

P8

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。

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

答:

a.

n = p x q = 55

z = (p - 1)(q - 1) = 40

b.

e = 3 is less than n and has no common factors with z

因为e为3的话，e小于n且gcd(e，n) = 1

c.

d = 27

d.

m = 8, m^e = 512

密文即为m^e mod n = 17

P22

P22. 下列是有关图 8-28 的判断题。

a. 当在 172.16.1/24 中的主机向一台 Amazon.com 服务器发送一个数据报时，路由器 R1 将使用 IPsec 加密该数据报。

b. 当在 172.16.1/24 中的主机向在 172.16.2/24 中的主机发送一个数据报时，路由器 R1 将改变该 IP 数据报的源和目的地址。

c. 假定在 172.16.1/24 中的主机向在 172.16.2/24 中的 Web 服务器发起一个 TCP 连接。作为此次连接的一部分，由 R1 发送的所有数据报将在 IPv4 首部字段最左边具有协议号 50。

d. 考虑从在 172.16.1/24 中的主机向在 172.16.2/24 中的主机发送一个 TCP 报文段。假定对该报文段的应答丢失了，因此 TCP 重新发送该报文段。因为 IPsec 使用序号，R1 将不重新发送该 TCP 报文段。

答:

a. F

b. T

c. T

d. F

P24

P24. 考虑下列伪 WEP 协议。其密钥是 4 比特，IV 是 2 比特。当产生密钥流时，IV 被附加到密钥的后面。假定共享的密钥是 1010。密钥流的 4 个可能输入如下：

101000：0010101101010101001011010100100…

101001：1010011011001010110100100101101…

101010：0001101000111100010100101001111…

101011：1111101010000000010101010010111…

假定所有报文都是 8 比特长。假定 ICV（完整性检查）是 4 比特长，并且通过用数据的后 4 比特异或数据的前 4 比特来计算。假定该伪 WEP 分组由 3 个字段组成：首先是 IV 字段，然后是报文字段，最后是 ICV 字段，这些字段中的某些被加密。

a. 我们希望使用 IV = 11 和 WEP 发送报文 m = 10100000。在这 3 个 WEP 字段中将有什么样的值？

b. 说明当接收方解密该 WEP 分组时，它恢复报文和 ICV。

c. 假定 Trudy 截获了一个 WEP 分组（并不必要使用 IV = 11）并要在向接收方转发前修改该分组。假定 Trudy 翻转了第一个 ICV 比特。假定 Trudy 并不知道用于任何 IV 的密钥流，则 Trudy 也必须翻转哪些其他比特，使得接收到的分组通过 ICV 检查？

d. 通过修改（a）中 WEP 分组中的比特，解密所生成的分组，并验证完整性检查来评价你的答案。

答：

a.

IV = 11，报文字段 = 01011010，ICV = 1010

b.

接收方提取 IV (11) 并生成密钥流 111110100000 .....

将加密消息与密钥流进行异或以恢复原始消息：01011010 xor 11111010 = 10100000

将加密的 ICV 与密钥流进行异或以恢复原始 ICV：1010 xor 0000 = 1010

接收方然后将恢复消息的前 4 位与其后 4 位进行异或：1010 xor 0000 = 1010

c.

报文的第一位或者第五位

d.

在part(a)中，加密后的消息为 01011010 翻转第一位后为11011010。

将此消息与密钥流进行异或运算：11011010 xor 11111010 = 00100000

如果翻转了加密 ICV 的第一位，则接收方收到的 ICV 值为 0010

接收方将此值与密钥流进行异或以获得 ICV： 0010 xor 0000 = 0010

接收方现在根据恢复的消息计算 ICV：0010 XOR 0000 = 0010，等于恢复的 ICV，因此接收到的数据包通过了 ICV 检查。