《密码学》课程习题

执笔 张焕国

第八章习题

1. 什么是协议？协议的安全设计原则主要有哪些？
2. 什么是认证？认证与数字签名的区别是什么？
3. 身份认证的途径有哪些？各有什么优缺点？
4. 使用对称密码设计一个安全的双向认证协议。
5. 使用公钥密码设计一个安全的双向认证协议。
6. 根据式（8-4），消息认证码 MAC=C（M，K）。说明密钥 K 在其中起什么作用？
7. 构造消息认证码（MAC）的方法有哪些？
8. 在报文认证中加入序号的作用是什么？
9. 给出一个完整的报文认证方案。
10. Kerberos 系统中的票据有什么作用？
11. 分析 Kerberos 系统的优缺点。
12. 在下述站点认证协议中函数 f 起什么作用？去掉 f 行不行？为什么？

设 A，B 是两个站点，A 是发方，B 是收方。它们共享会话密钥 K_s，f 是公开的简单函数。A 认证 B 是否是他的意定通信站点的协议如下：

1 A 产生一个随机数 RN，并用 K_s 对其进行加密：C＝E（RN，K_s），并发 C 给 B。同时 A 对 RN 进行 f 变换，得到

f(RN)。

2 B 收到 C 后，解密得到 RN＝D（C，K_s）。B 也对 RN 进行 f 变换，得到 f（RN），并将其加密成 C’＝E（f（RN），K_s），然后发 C’给 A 。

A对收到的C’解密得到f（RN），并将其与自己在第①步得到的f（RN）比较。若两者相等，则A认为B是自己的意定通信站点。否则A认为B不是自己的意定通信站点。