《密码学》课程习题

执笔 张焕国

第六章习题

1. 为什么数字签名能够确保数据真实性？
2. 说明对于RSA的数字签名，为什么先加密后签名不安全？
3. 说明HASH函数在数字签名中的作用。
4. 编程实现RSA数字签名方案。
5. 说明在ELGamal密码签名中，参数k为什么必须是一次性的。
6. 编程实现ELGamal数字签名方案。
7. 说明在椭圆曲线密码签名中，参数k有无一次性的要求？
8. 编程实现椭圆曲线密码数字签名方案。
9. 说明DSS的签名方案与ELGamal密码签名方案有何不同？
10. 编程实现DSS数字签名方案。
11. 说明不可否认签名与普通签名有何不同？它在软件知识产权保护方面有何作用？
12. 盲签名与普通签名有何不同？举出一个盲签名的实例。
13. 阅读中国数字签名标准（GB15851-1995）。