

《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）。