<<应用密码学>>

图书基本信息

书名：<<应用密码学>>

13位ISBN编号：9787111075882

10位ISBN编号：7111075889

出版时间：2000-1

出版时间：机械工业出版社

作者：Bruce Schneier

页数：545

译者：吴世忠/等

<<应用密码学>>

内容概要

本书真实系统地介绍了密码学及该领域全面的参考文献。

全书共分四个部分，首先定义了密码学的多个术语，介绍了密码学的发展及背景，描述了密码学从简单到复杂的各种协议，详细讨论了密码技术，并在此基础上列举了如DES、IDEA、RSA、DSA等10多个算法以及多个应用实例，并提供了算法的源代码清单。

作者简介

作者：(美国)Bruce Schneier 译者：吴世忠 等

<<应用密码学>>

书籍目录

译者序
第一部分 密码协议
第二部分 密码技术
第三部分 密码算法
第四部分 真实世界

章节摘录

当她试图第二次使用同一张数字汇票时，商人（同一个商人或另一商人）将在第（7）步中给她一个不同的随机选择字符串。
Alice必须在第（8）步中同意，如果不这样做势必立即提醒商人有些事值得怀疑。
现在，当这个商人在第（10）步中将汇票带到银行时，银行会立即发现带相同唯一字符串的汇票已经存过。
银行接着比较鉴别字符串中所有公开的部分。
两个随机选择字符串相同的机会是2n分之一，在下一个冰期前是不可能发生的。
现在，银行找出这样一对，其中一半第一次被公开，另一半第二次被公开。
它把这两半一起异或，马上得到Alice的名字，于是银行知道谁试图两次花这一张汇票。
应当指出，这个协议不能让Alice不进行欺骗，但它能几乎肯定地检测她的欺骗。
如果Alice进行欺骗，她不可能不暴露身份。
她不可能改变唯一字符串或识别字符串，否则银行的签名将不再有效。
这个商人将在第（6）步中马上意识到这点。
Alice可能试图偷一张空头汇票骗过银行，这张汇票上的识别字符串不会泄露她的名字，或最好是一张其识别字符串泄露其他人名字的汇票。
她在第（3）步中进行这种欺诈骗过银行的机会是n分之一。
这并非不可能，但如果惩罚足够严厉的话，Alice不敢以身试法。
或者，你可以增加Alice在第（1）步中制作的多余汇票的数目。
这个商人能进行欺骗吗？
他的机会甚至更小。
他不能将这张汇票存两次，银行将会发现选择字符串被重复使用。
他不能捏造以陷害Alice，只有Alice才能打开任意的识别字符串。
甚至Alice和商人合谋也不能欺骗银行。
一旦银行在带唯一字符串的汇票上签名，银行就确信只能使用这张汇票一次。
银行又怎样呢？
它能不能知道它从商人那儿收到的汇票是它为Alice签的那张呢？
在第（2）至第（5）中的盲签名协议保护了Alice。
银行无法作出判断，即使它保留了每次交易的完整记录。
说得更重些，银行和商人在一起也无法知道Alice是谁。
Alice可以走进商店并且完全匿名地购买东西。
Eve可以进行欺骗。
如果她能窃听Alice和商人之间的通讯，并能在商人到达银行之前先到达银行，她就能第一个把这笔数字现金存入她的帐户。
银行将会接受，甚至更糟的是，当商人试图去存入数字现金时他会被认为是一个欺骗者。
如果Eve偷到数字现金并在Alice之前花掉它，那么Alice会被认为是一个欺骗者。
没有办法防止这种情况，它是现金匿名的直接后果。
这个协议是介于被仲裁协议和自我执行协议之间的协议。
Alice和商人都相信银行能兑现汇票，但Alice不必信任知道她购物的银行。
6.4.5 数字现金和高明的犯罪　　数字现金也有它不利的一面。
有时人们并不需要那么多的隐私。
看看Alice进行的高明的犯罪[1575]：　　（1）Alice绑架了一个婴儿。
（2）Alice准备了10000张每张1000美元的匿名汇票（或多到她想要的那么多）。
……

版权说明