<<程序员密码学>>

图书基本信息

书名：<<程序员密码学>>

13位ISBN编号：9787111216605

10位ISBN编号：7111216601

出版时间：2007-7

出版时间：机械工业

作者：丹尼斯

页数：328

译者：沈晓斌

<<程序员密码学>>

内容概要

是目前市面上惟一一本把密码学算法的理论和实现结合在一起的书，也是惟一一本能够如此深入浅出地把这两个方面融合到一起的书，没有深厚的程序设计功力和广博的密码学理论知识是不可能撰写出这样一书的。
无论对于需要开发安全产品的开发者，还是密码学相关研究人员来说，《程序员密码学》均值得一读，它能对安全产品开发工作以及密码学理论研究工作起到辅助作用，并可以达到事半功倍的效果。

<<程序员密码学>>

书籍目录

<<程序员密码学>>

编辑推荐

信息安全越来越受到人们的重视，对信息安全的基石：密码学的研究也是如火如荼。
但是，许多信息安全软硬件产品的开发者并不是专业的密码学研究人员。
虽然他们擅长程序设计，而且现在也有许多各种各样的密码学算法库，如LibTomCrypt、Crypto++，但是，由于缺少一定的密码学理论知识以及对密码学算法的准确理解，因此在实现各种复杂的密码学算法时，经常会对算法进行不当的使用，而这又往往会导致在其开发的产品中存在各种潜在的漏洞及安全风险。
另一方面，许多密码学理论工作者在实现密码学算法时，由于缺少程序设计方面的知识，在算法实现的易用性和高效性上遇到了不少障碍，从而也会导致其实现上存在不少的安全缺陷。
《程序员密码学》的出版恰好可以解决上述问题，它在程序员和密码学研究人员之间架起了一座桥梁，使他们能够轻松地在理论和实践之间进行角色转换，并且将会缓解信息安全业界的种种尴尬。
书中涉及密码学的各个研究方向，分组密码、散列函数、公钥密码以及相关的攻击，同时也讲解了密码学算法实现上常用的ASN.编码、大整数算术相关内容。

版权说明