

<<欧洲信息安全算法工程>>

图书基本信息

书名：<<欧洲信息安全算法工程>>

13位ISBN编号：9787030121424

10位ISBN编号：7030121422

出版时间：2003-8

出版时间：科学出版社

作者：冯登国 林东岱 吴文玲

页数：194

字数：252000

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<欧洲信息安全算法工程>>

内容概要

本书主要介绍了NESSIE工程算法套件，该套件包括12个决选算法和5个已经作为标准或即将成为标准的算法。

全书共6章，内容包括分组密码、非对称加密码、MAC算法和Hash函数、数学签名方案、GPS识别方案。

本书可供从事信息安全、密码学、计算机、通信、数学等专业的科技人员和高等院校相关专业的师生参考。

书籍目录

第一章 绪论 1.1 NESSIE工程的背景 1.2 NESSIE工程的主要目标 1.3 NESSIE工程的具体内容和进度安排 1.4 NESSIE工程的预期成果和影响 1.5 对候选密码标准的基本要求和评估标准 1.6 征集情况介绍 1.7 各类候选标准简况 1.8 决选结果第二章 分组密码 2.1 NESSIE中的分组密码概述 2.2 MISTY1 2.3 Camellia 2.4 SHACAL2 2.5 AES 参考文献第三章 非对称加密方案 3.1 NESSIE中的公钥密码概述 3.2 预备知识 3.3 KEM-DEM 3.4 PSEC-KEM 3.5 RSA-KEM 3.6 ACE-KEM 参考文献第四章 MAC算法和Hash函数 4.1 Two-Track-MAC 4.2 UMAC 4.3 CBC-MAC 4.4 HMAC 4.5 Whirlpool 4.6 安全Hash标准 (SHS) (FIPS PUB 180-2) 第五章 数字签名方案 5.1 NESSIE中的数字签名方案概述 5.2 预备知识 5.3 RSA-PSS 5.4 椭圆曲线数字签名算法 5.5 SFLASH 参考文献第六章 GPS识别方案 6.1 概述 6.2 基于离散对数问题的识别方案综述 6.3 GPS识别方案 6.4 GPS识别方案的安全性分析 6.5 实际及应用考虑 参考文献其他相关文献

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>