この1冊で暗号理論と符号理論の基礎から最先端まで学習できる！

PARI/GPで計算しながら学ぶ

整数論・暗号理論・符号理論

著者： 鈴木 英男
仕様：B5 ・並製・モノクロ・本文 382 頁
印刷版・電子版価格：4,200円（税抜）
ISBN（カバー付単行本）：978-4-7649-0757-7　C3041
ISBN（POD）：978-4-7649-6115-9　C3041
発行：近代科学社 Digital
発売：近代科学社

内容紹介

本書は「整数論」「暗号理論」「符号理論」の三科目を統合的に解説する教科書であり、特に暗号理論および符号理論の理解に不可欠な整数論を網羅しています。

整数論の章では、現代暗号の基礎となる数の集合論、群・環・体といった代数的な概念から、割り算の原理、ユークリッドの互除法、合同式、フェルマーの小定理、中国剰余定理といった基本定理群を解説します。とくに、楕円曲線上の演算とガロア体（有限体）の解説を丁寧に詳述。付録にあるプログラムでは、ガロア体を生成できる原始多項式をすべてリストアップできます。

暗号理論の章では、現代暗号の構築原理と、その安全性の根拠となる数学的な難問に焦点を当てています。公開鍵暗号の安全性レベル、素因数分解問題や離散対数問題といった暗号の根幹をなす課題を掘り下げ、鍵交換プロトコル、ディジタル署名、一方向性ハッシュ関数、メッセージ認証符号（MAC）、ブロックチェーンと暗号通貨といった主要技術を詳細に解説しています。

符号理論の章では、情報伝送における誤り訂正技術について解説を展開し、符号理論の基礎概念から、情報源符号化および通信路符号化の基本定理、LZ77符号、線形符号、巡回符号、ハミング符号、リード・ソロモン（RS）符号、BCH符号、畳み込み符号、ターボ符号、LDPC符号、QRコードのメカニズムに至るまで、多岐にわたる符号化技術を包括的に紹介しています。

また本書ではPARI/GPおよびSageMathを用いた多数のプログラミング例を提示しており、実際に計算プロセスを追体験することで、各アルゴリズムの動作原理や数学的性質に対する深い洞察を得ることが可能となっています。実践的な応用力まで身につけることができる本格的な教科書です。

全国の書店・ネット書店にてお求めいただけます。お取り扱い店は以下のウェブページをご覧ください。
https://www.kindaikagaku.co.jp/book_list/detail/9784764961159/

近代科学社Digital
https://www.kindaikagaku.co.jp/kdd/ 近代科学社Digitalは、株式会社近代科学社が推進する21世紀型の理工系出版レーベルです。デジタルパワーを積極活用することで、オンデマンド型のスピーディで持続可能な出版モデルを提案します。

お問い合わせ先
株式会社近代科学社
〒101-0051 東京都千代田区神田神保町1-105
神保町三井ビルディング
電子メール: contact@kindaikagaku.co.jp

著者紹介

鈴木 英男（すずき ひでお）
三重県生まれ.
東北大学大学院博士課程修了、博士（工学）
東北大学助手、Stanford大学客員研究員を経て、現在東京情報大学教授

目次