No.44 (2017)

りことパス

理工学図書館パスファインダー

暗号理論

関連授業：電気電子情報工学科
「離散数学と暗号理論」
「セキュリティ基礎論」

りことパスは、主に理工学分野の授業に関連するトピックについて、学習の初めの一歩となる資料やWebサイトを紹介するテーマ別調べ方ガイドです。理工学図書館のラーニング・サポーター (LS) が作成しています。
学習やレポート作成に活用してください。

2018教員監修済

1. イントロダクション

1-1.「暗号理論とは？」

私たちは現在至るところでインターネットを利用しています。暗号理論から生じる暗号技術はそういった通信が安全に行なわれるよう私たちを日々支えています。
ここでは暗号技術の概要から代数学（群・環・体や数論）、さらには近年の暗号理論の研究分野を学習するのに役に立つ書籍を紹介します。
3、4年生向けの講義である「離散数学と暗号理論」や「セキュリティ基礎論」を学習するにあたって、より深く理解をするための手助けとしてください。

1-2.一般向けに書かれた資料・読み物

■ トコトンやさしい暗号の本 / 伊豆哲也 他4名著
【ISBN=978-4526064524】
暗号化の歴史から、現在使われている共通鍵、公開鍵暗号、応用技術である認証コードや電子署名などを分かりやすく紹介、解説しています。各トピックが図を用いて1ページでまとめられていて非常に見やすくなっています。暗号技術を学ぶ学生だけでなく、一般の人にも理解しやすい本です。

■ 暗号技術入門 ： 秘密の国のアリス （第3版） / 結城浩 著
【書誌ID=12400435488】
暗号技術に興味を持っている人にまず読んでほしい一冊です。
秘密鍵暗号、公開鍵暗号、ハッシュ関数、デジタル署名、PKI、SSL/TLSなどといった暗号技術の構成要素について非常に分かりやすく書かれています。
第3版（2015年刊行）では、楕円曲線暗号や、ビットコインにまつわる暗号技術など、最新の内容が盛り込まれています。本書を読むことで、この分野の全体像を把握できるだけでなく、暗号技術への興味がより高まります。

2. 学習用資料

2-1.授業において購入が勧められている本

■ 代数学から学ぶ暗号理論 / 宮地充子著

2017 シラバス

【書誌ID=2004420592 】

数学的背景から暗号理論を学ぶことができる本です。

電子情報工学科の3、4回生向けの講義「離散対数と暗号理論」の教科書にもなっていて、講義は基本的にこの本に沿って行なわれます。また、授業で出される課題を解く上でも参考になります。

2-2.最初に読むべき本

■ 代数学1　群論入門　/ 雪江明彦 著

【書誌ID=2004185546】

代数学の基礎を学ぶ人向けの本で、数学を専門とする研究員も薦めている一冊。群、環、体などのはじめは抽象的で分かりにくい概念も丁寧に解説しています。具体例だけでなく、よくある間違いにも触れていて、非常に親切な内容です。とはいえ、代数学は簡単な内容ではないので、この本を使って、1つ1つ根気よく確実に積み上げていくような学習法をおすすめします。

2-3.理解をさらに深める

■ 暗号理論と楕円曲線　数学的土壌の上に花開く暗号技術 /
辻井重男 他6名著

【書誌ID=2004340121】

第一線の研究者たちが、暗号理論の最新動向を、その背後を支える数学を軸に解説しています。特に近年注目を浴びている楕円曲線暗号については、攻撃手法まで学ぶことができます。また、超楕円曲線暗号やヴェイユペアリング、符号理論に基づく暗号技術などについても詳しく記述されていて、非常に内容の濃い本です。

3. 先行研究、調査・雑誌記事を探す：文献データベース

■ CiNii Articles

http://ci.nii.ac.jp/

日本の学会誌・紀要等に発表された論文を検索できます。

■ MathSciNet

https://mathscinet.ams.org/mathscinet/index.html

アメリカ数学会（American Mathematical Society）が提供する数学の文献や論文が検索できるデータベース。

●図書名・雑誌名の後に【書誌 ID】（10桁の数字）があるものは、大阪大学で所蔵しています。この書誌IDで、大阪大学OPAC（蔵書検索システム）を検索することができます。
https://opac.library.osaka-u.ac.jp/

●パスファインダーは、図書館サイトでも見ることができます。
https://www.library.osaka-u.ac.jp/pathfinder/

※このパスファインダーは、理工学図書館LSが作成しています。

■理工学図書館LS（ラーニング・サポーター）とは…？

工学研究科の院生が皆さんの先輩として、理工学図書館東館１階LSデスクで、学習、就職、進路など学生からの様々な相談に対し、サポートやアドバイスをしています。

●他にも…
- 各LSの経験や専門を生かした講習会を図書館で開催
- 図書館の利用案内ツアー/留学生への英語案内
- 学部生に役立つ本の選書、おすすめ本リスト作成/本の展示

■LSの活動はFacebookでも、随時紹介しています。
https://www.facebook.com/tarikou.osakaunivlib

発行者：理工学図書館
発行：2018年3月　電気電子情報工学専攻LS作成（指導教員監修済）