# 離散数学

科目ナンバー　3C221
専門　　選択　　2単位

盛　拓生

1. 授業の概要（ねらい）

現代の情報社会において、情報セキュリティ技術は必須の技術です。情報セキュリティ技術の基礎として暗号があります。

本講義では、世界初の公開鍵暗号であるRSA暗号系を理解し、それを支える数論、抽象代数学の基礎を学ぶことを目的とします。

また、RSA暗号を支える数学的定理を証明を通して理解することに加えて、最終的にRSA暗号系をプログラムとして理解できるようになるを目指します。そのために、数学的定理をアルゴリズム的な観点で理解することを目指します。

暗号学では巨大な整数を扱うことが必要になるため、メモリが許す範囲内で任意の大きさの整数値を扱うことができるプログラミング言語であるRubyによりプログラムを記述します。

この科目は、学位授与の方針(ディプロマポリシー)DP3、DP4C、DP4Mに関連する科目です。

2. 授業の到達目標

この科目では次のような能力を修得することを目標とします。
学生は、Rubyで記述された簡単なアルゴリズムを読んで、実行することができる。
学生は、簡単なアルゴリズムをRubyで記述することができる。
学生は、Euclidアルゴリズム及び拡張Euclidアルゴリズムについて説明できる。
学生は、素数の定義及びその基本的な性質、擬素数との関係を説明することができる。
学生は、基礎的な素因数分解アルゴリズム、素数性判定アルゴリズムを実装できる。
学生は、合同式の定義を説明し，合同式に関して四則演算の計算ができる。
学生は、中国人の剰余定理について説明ができ、簡単な連立合同式を解くことができる。
学生は、群、部分群及び巡回部分群の定義及び基本的な性質を説明できる。
学生は、RSA暗号の鍵生成、暗号化、復号の手順を説明できる。

3. 成績評価の方法および基準

中間レポート(50%)、期末試験の成績(50%)。
講義内容、レポート、試験への質問，フィードバック等は原則的にLMSまたはオフィスアワーで対応します。

4. 教科書・参考文献

教科書
S. C. コウチーニョ著、林彬訳　暗号の数学的基礎　丸善出版、ISBN-13: 978-4621062869
参考文献
五十嵐邦明、松岡浩平著　ゼロからわかる　Ruby　超入門　(かんたんIT基礎講座)　技術評論社、ISBN-13:　978-4297101237

5. 準備学修の内容

この科目はBYOD端末を利用して、学んだアルゴリズムをRubyにより実装し、動作等を確認します。そのため、Rubyの実行環境をBYOD端末にインストールする必要がります。インストールについては講義ビデオ等で示します。また、予め、各回の講義資料をLMS上で公開します。
講義資料はPC、タブレット、スマートフォン等にダウンロードするか紙に印刷するなどして、講義中いつでも参照、書き込みできるようにしてください。
授業前にこれらの資料に1時間程度目を通した上で、理解できた点、理解できていない点をそれぞれ把握して授業に臨んでください。
授業後には、30分程度かけてLMS上のテストで理解度を確認し、復習してください。

6. その他履修上の注意事項

中間レポートが提出されない場合は単位の取得が著しく困難になります。中間レポートは締切を守って必ず提出するようにしてください。

自主学習支援のためにLMSを利用します。講義資料等はLMS上で公開されているので事前に入手し、講義中はノートをとることよりも、講義を聞いて理解すること、演習問題を解くことに集中してください。

事前に履修すべき科目は、論理数学、プログラミング1、線形代数、プログラミング2、プログラミング演習1です。

同時に履修すべき科目は、情報科学プログラミング1、プログラミング演習2、データ構造とアルゴリズムです。

事後に履修すべき科目は、情報理論、情報セキュリティです。

7. 授業内容

【第1回】　本講義が目指すもの、Ruby
【第2回】　基本アルゴリズム
【第3回】　素因数分解の一意性
【第4回】　素数
【第5回】　法演算
【第6回】　帰納法とFelmat
【第7回】　擬素数
【第8回】　連立合同式
【第9回】　べき再び、秘密分散、平方剰余問題
【第10回】　群/Group1
【第11回】　巡回部分群
【第12回】　MersenneとFelmat
【第13回】　素数判定と原始根
【第14回】　RSA暗号系
【第15回】　テスト、まとめ