情報数学特論

2 単位 (選択) 1 年 (前期)

Mathematics for Information Science

中山 慎一 · 准教授 / 地域科学専攻 (博士前期課程) 基盤科学，片山 真一 · 教授 / 地域科学専攻 (博士前期課程) 基盤科学

【授業目的】近年，ネットワーク社会における情報漏洩，情報改ざんを防ぎ，さらに本人認証 を行う基盤技術として暗号理論が存在する．本講義では，暗号理論で用いられる 代数・整数論・計算量理論のそれぞれの基本概念について講義する．代数・整数 論では，群論，合同式と剰余計算などの基本理論と，計算量理論に基づいた素数 判定法，素因数分解法などの数論アルゴリズムについて講義する．また計算量理 論では，計算モデル，計算可能性，計算量クラスなどの説明を行い，これらの理 論がどのように公開鍵暗号方式に用いられているか解説する．

【授業概要】計算量の理論と非対称鍵暗号系の暗号理論の基礎を理解する．

【キーワード】計算量理論，暗号

【先行科目】[先行科目]

【関連科目】[関連科目]

【履修上の注意】学部レベルの代数学，離散数学を習得していること

【到達目標】[目標]

【授業計画】

1. 計算可能性の理論
2. 判定可能性
3. 帰着可能性
4. 複雑さの理論
5. クラス P，クラス NP
6. NP 完全性
7. 領域の複雑さ
8. 四則演算の複雑さ
9. 剰余環
10. 剰余環の演算に関する計算量
11. 暗号化方式
12. RAS 暗号化方式
13. 離散対数
14. デジタル著名

【成績評価】授業への取り組み状況により総合的に評価する．

【教科書】[教科書]

【参考書】[参考資料]

【授業コンテンツ】http://cms.db.tokushima-u.ac.jp/cgi-bin/toURL?EID=220078

【連絡先】

⇒ 中山 (1204, 088-656-7223, shin@ias.tokushima-u.ac.jp) Mail

⇒ 片山 (1304, 656-7228, katayama@ias.tokushima-u.ac.jp) Mail

Mathematics for Information Science

2 units (selection) 1st-year(1st semester)

Shin-ichi Nakayama · Associate Professor / Fundamental Studies, Regional Sciences, Shin-ichi Katayama · Professor / Fundamental Studies, Regional Sciences

Target〉近年，ネットワーク社会における情報漏洩，情報改ざんを防ぎ，さらに本人認証 を行う基盤技術として暗号理論が存在する．本講義では，暗号理論で用いられる 代数・整数論・計算量理論のそれぞれの基本概念について講義する．代数・整数 論では，群論，合同式と剰余計算などの基本理論と，計算量理論に基づいた素数 判定法，素因数分解法などの数論アルゴリズムについて講義する．また計算量理 論では，計算モデル，計算可能性，計算量クラスなどの説明を行い，これらの理 論がどのように公開鍵暗号方式に用いられているか解説する．

Outline〉計算量の理論と非対称鍵暗号系の暗号理論の基礎を理解する．

Keyword〉*computational complexity, cipher*

Fundamental Lecture〉[先行科目]

Relational Lecture〉[関連科目]

Notice〉学部レベルの代数学，離散数学を習得していること

Goal〉[目標]

Schedule〉

1. 計算可能性の理論
2. 判定可能性
3. 帰着可能性
4. 複雑さの理論
5. クラス P，クラス NP
6. NP 完全性
7. 領域の複雑さ
8. 四則演算の複雑さ
9. 剰余環
10. 剰余環の演算に関する計算量
11. 暗号化方式
12. RAS 暗号化方式
13. 離散対数
14. デジタル著名

Evaluation Criteria〉授業への取り組み状況により総合的に評価する．

Textbook〉[教科書]

Reference〉[参考資料]

Contents〉http://cms.db.tokushima-u.ac.jp/cgi-bin/toURL?EID=220078

Contact〉

⇒ Nakayama (1204, +81-88-656-7223, shin@ias.tokushima-u.ac.jp) Mail

⇒ Katayama (1304, 656-7228, katayama@ias.tokushima-u.ac.jp) Mail