科目コード／科目名 (Course Code / Course Title)	CA180／情報科学諸論 2 (Special Topics in Information Science 2)		
テーマ／サブタイトル等 (Theme / Subtitle)	楕円曲線法による素因数分解		
担当者名 (Instructor)	篠原 直行(SHINOHARA NAOYUKI)		
学期 (Semester)	秋学期(Fall Semester)	単位 (Credit)	2単位(2 Credits)
科目ナンバリング (Course Number)	MAT3430	言語 (Language)	日本語 (Japanese)
備考 (Notes)	LC196 情報科学特論6、RC196 情報科学特論6と合同授業		

授業の目標(Course Objectives)

楕円曲線を用いた整数の素因数分解法の理解を深めることで，公開鍵暗号の安全性評価について学ぶ.

The aim of this course is for students to cultivate a better understanding of integer factorization by the Elliptic Curve Method to learn about the security evaluations of public key cryptosystems.

授業の内容(Course Contents)

有限体上の楕円曲線の有理点の成す群は，楕円曲線暗号や，整数の素因数分解，素数証明に利用されるなど，暗号や計算機整数論の分野において重要な研究対象となっている．整数の素因数分解を効率よく行う代表的なアルゴリズムに数体篩法と楕円曲線法がある．この講義では主に楕円曲線法について学習することで，数体篩法と楕円曲線法の違いを理解する．さらに，楕円曲線法をフリーソフトである数式処理システム Risa/Asir を用いて実装して数値実験を行うか，アルゴリズムにそった手計算によって，楕円曲線法の効率性について学習する．

The group of rational points of an elliptic curve over a finite field is an important research theme in cryptography and computational number theory because that group is used for Elliptic Curve Cryptography, integer factorization algorithms, and primality test algorithms. There exist two well-known algorithms to factorize integers: the Number Field Sieve and the Elliptic Curve Method (ECM). In this course, students are mainly expected to learn the ECM to understand the difference between those two algorithms. Students learn the efficiency of the ECM by either implementing it on the free software Risa/Asir and performing numerical experiments or hand calculation based on the ECM.

授業計画(Course Schedule)

1. RSA 暗号と素因数分解
2. 計算量
3. ユークリッドの互除法
4. 数式処理ソフト ASIR の使い方
5. 楕円曲線と加法群
6. 群演算の高速化
7. 整数倍算の高速化
8. プログラミング演習
9. p-1 法
10. 楕円曲線法
11. 楕円曲線法
12. プログラミング演習
13. 楕円曲線法の改良
14. プログラミング演習

授業時間外(予習・復習等)の学習(Study Required Outside of Class)

授業時間外の学習に関する指示は，必要に応じて別途指示する。

成績評価方法・基準(Evaluation)

出席態度(49%)/数回の小レポート(51%)

テキスト(Textbooks)

特になし。

参考文献(Readings)

その他（HP 等）（Others(e.g.HP)）

注意事項（Notice）