2011年度春期

情報数学特論[理工学専攻情報学領域]

担当：角皆 (つのがい)

授業に関する連絡

主に Loyola 掲示板、情報学領域掲示板 (3 号館 2 階・電気電子工学科／情報理工学科事務室前)、及び web page

http://pweb.cc.sophia.ac.jp/tsunogai/kougi/11/johosuugaku.html

で行なう。また、角皆への連絡は研究室 (4 号館 5 階 574A 室奥) に直接来てもよいが、電子メイル tsuno-h@cc.sophia.ac.jp が確実である。

授業の進め方

情報化社会の安全を支える数理技術である公開鍵暗号・鍵共有などの暗号理論について概説を行ない、その基礎数理について、入門的に紹介する。有限体・代数幾何・整数論などの必要な予備知識についても適宜補いつつ講義を進める。

授業内容の詳細は未定だが、

- 概説: 情報通信と暗号
- 暗号でできること (秘密通信・認証・署名・鍵共有・秘密分散など)
- 公開鍵暗号方式の概念と原理
- 安全な暗号の実現とそれを支える数理現象 (RSA 暗号・離散対数問題)
- 数学的な準備または復習
  - ⋆ 有限体とその上の線型代数・多項式環・Galois 理論
  - ⋆ 初等整数論・中国式剰余定理・平方剰余の相互律
  - ⋆ 楕円曲線論の初歩

などから、受講生の予備知識を鑑みて決める予定。詳しくは上の web page を参照のこと。

評価方法・課題の提出

評価は適宜出題する授業時演習および課題レポートにより行なう予定。授業時演習以外のレポートは、紙媒体または電子メイルで提出のこと。電子メイルで提出の場合は、**メディアセンターの自分のアカウント**から上記の宛先に提出すること。質問などのメイルも歓迎する。但し、添付ファイルのみのメイルは読まずに消すことがあるので注意。

主な参考書

- S. C. Coutinho, “The Mathematics of Ciphers: Number Theory and RSA Cryptography” (A K Peters)
- N. Koblitz, “A Course in Number Theory and Cryptography (2nd ed.)” (Springer-Verlag, GTM 114)
- J.A. Buchmann “Introduction to Cryptography (2nd ed.)” (Springer-Verlag)

など。他にも暗号理論などと名の付いた本は多数あるので、適宜参照されたい。基礎数理に関しては、線型代数・有限体・Galois 理論・初等整数論・楕円曲線などをキーワードとして探されたい。

— よろづの事どもをたづねて末をみればこそ、事は故あれ。
堤中納言物語「虫愛づる姫君」より