応用数理情報概論 II

担当：内田　幸寛

講義のテーマ・目的・内容

現代暗号理論への入門としてその基礎数理について講義する．

インターネットに代表されるオープンネットワークを用いて安全に通信を行うためには暗号技術が不可欠である．この講義では，暗号技術の中でも，公開鍵暗号と呼ばれるものの中で代表的な方式である RSA 暗号を中心に据え，現代暗号理論の基礎的な数理についての理解を目的とする．

講義計画は以下の通り．ただし，講義の進み具合に応じて変更することがある．

第 1 回　イントロダクション及びガイダンス
第 2 回　現代暗号と情報セキュリティ概要
第 3 回　基本アルゴリズム
第 4 回　素因数分解とその一意性
第 5 回　素数
第 6–7 回　合同と法演算
第 8 回　まとめ及び中間試験
第 9 回　擬素数
第 10–11 回　素数判定法
第 12 回　原始根と既約剰余類群
第 13–14 回　RSA 暗号とその応用
第 15 回　まとめ及び期末試験

テキスト・参考書等

教科書は特に指定しない．参考書として以下を挙げておく．

- S. C. コウチーニョ著（林彬訳）「暗号の数学的基礎」丸善出版
- ヨハネス・A・ブーフマン著（林芳樹訳）「暗号理論入門」（原書第 3 版）丸善出版

成績評価方法

授業参加度（レポート含む）（20%），中間試験（30%）と期末試験（50%）により評価する．

原則として，合計 4 回以上欠席した場合は不合格とする．インターンシップ等で欠席する場合は必ず事前に教員まで申し出ること．

オフィスアワー

8 号館 6 階 667 号室，水曜 5 時限 (16:20–17:50)

ウェブページ

`http://www.comp.tmu.ac.jp/y-uchida/lectures/`

講義に関する情報をここに掲載する．