暗号の数理シラバス

河野

授業の概要・達成目標

暗号の基礎と公開鍵暗号について学ぶ。そのために最初に整数の基礎について学習する。その後公開鍵暗号・非対称暗号およびその代表である RSA 暗号について学ぶ。楕円暗号に関しても簡単にふれる。

授業内容

0. イントロ
1. 郡と演算
2. 整数と剰余類
3. 公開鍵暗号
4. RSA 暗号
5. 楕円暗号

参考文献

「暗号の数学的基礎」(S.C. コウチーニョ),
「数論アルゴリズムと楕円暗号理論入門」(N. コブリッツ),
「群論の基礎」(永尾 汎),「暗号技術大全」(ブルース・シュナイアー),
「暗号解読 -ロゼッタストーンから量子暗号まで-」(サイモン・シン)

成績評価

試験およびレポートにより評価する。

連絡先

研究室または kouno@math.cs.kitami-it.ac.jp まで。質問にはいつ来てもかまいませんが, 2011 年度後期は月曜日 15 時から 16 時 30 分までがオフィスアワーなので, その時間帯は研究室または情報システム 2 号棟 5 階のどこかの部屋にいます。

その他留意事項

教室への出入りは自由ではない。途中入室・途中退室は自由だが, 再度入室する意思をもって退室する場合は私の許可をとってから退室する事。ただし,「タバコを吸いたい」「電話をかけたい」等の理由は原則不許可。

私語禁止。数学的質問は勿論私語ではないので, 随時 (私の話している途中でも) してかまわない。

食事禁止。

講義等で配布するプリントは http://math.cs.kitami-it.ac.jp/~kouno/kougi.html (Renandi から辿れます) で閲覧できる。成績・試験の点数は Renandi に載せる。試験等の連絡は掲示と同時に Renandi に載せる。