暗号の数理シラバス

2009–10–5　　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。そのために前半は代数系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。

授業内容

0. イントロ
1. 群と演算
2. 整数と剰余類
3. 公開鍵暗号
4. RSA 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，2009 年度後期は 月曜日の 16:30 から 18:00 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

講義等で配布するプリントは Renandi から閲覧できる。