

集中講義のお知らせ

講師

九州大学
マス・フォア・インダストリ研究所
教授 高木 剛 先生

タイトル

「公開鍵暗号入門」

*** 講義内容 ***

本講義では公開鍵暗号の動作原理およびその数理的側面を解説する。
初等整数論の復習からスタートして、RSA暗号の動作原理、
素数判定法、RSA暗号の鍵長を決定する素因数分解アルゴリズム
などを説明する。

1. 初等整数論アルゴリズムとRSA暗号の動作原理
2. 素数判定法(疑似素数、Miller-Rabin法など)
3. 素因数分解アルゴリズム(ρ 法、2次篩法など)

科目名

(科目番号)

対象年次

3年次： 特別講義Ⅹ(数理308)
4年次： 情報数理学特論Ⅲ数理475)
院 生： 情報数理学特別講義Ⅲ

期 間

平成24年11月19日(月)～11月22日(木)

時 間 割

日時 (時限)	11. 19 月	11. 20 火	11. 21 水	11. 22 木
2		408	複412	407
3		408		予備
4	408	408	408※	

※ 11/21(水)16:00～17:00理408にて談話会があります。

担当教員

… 橋本康史

登録方法

… 数理科学科事務室の名簿へ直接記入して下さい。

登録期間

… 平成24年11月1日(木)～平成24年11月14日(水)