電気通信大学　平成20年度シラバス

授業科目名	暗号理論特論		
英文授業科目名	Advanced Topics on Cryptography		
開講年度	2008年度	開講年次	
開講学期	前学期	開講コース・課程	博士前期・後期課程
授業の方法	講義	単位数	2
科目区分	電気通信学研究科-情報通信工学専攻-専門科目		
開講学科・専攻	情報通信工学専攻		
担当教官名	國廣　昇		
居室	非常勤講師		

公開E-Mail	授業関連Webページ
kunihiro@ice.uec.ac.jp	

【主題および達成目標】

いくつかの公開鍵暗号に対して格子理論に基づく安全性解析を講述する．

【前もって履修しておくべき科目】

学部科目：離散数学第一，暗号理論，情報セキュリティシステム

【前もって履修しておくことが望ましい科目】

【教科書等】

参考書：ほんとうに安全？現代の暗号（岩波書店）（太田，國廣）
技術的な参考書：暗号理論のための格子の数学
適宜，必要な資料は配付します．

【授業内容とその進め方】

本年度は，以下の順に夏期集中講義の形式で行う予定である．
1. 格子理論の基礎および暗号解読への応用の導入
2. RSA暗号の解読（その１）-1変数方程式に帰着でき時-
3. RSA暗号の解読（その２）-2変数以上の方程式に帰着できる時-
4. ナップザック暗号に対する解読
5. まとめ

【成績評価方法及び評価基準(最低達成基準を含む)】
講義の内容をベースにしたレポート課題を出題し，その内容と提出状況により，成績を評価する.

【オフィスアワー：授業相談】

【学生へのメッセージ】
暗号理論の基本的な知識（RSA暗号の暗号化など）は前提とします.

【その他】