電気通信大学　平成18年度シラバス

授業科目名	暗号・情報セキュリティ特論		
英文授業科目名	Cryptography and Information Security		
開講年度	2006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		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	太田　和夫		
居室	総合研究棟９２８		

公開E-Mail	授業関連Webページ
	http://www.oklab.ice.uec.ac.jp/class/advanced-cryptology/

【主題および達成目標】

暗号・認証は，古来より，提案と攻撃が繰り返されてきた．80年代の半ばより，これらの安全性を証明する技術が，計算量理論の枠組みのもとで徐々に確立されてきた．

本講義では，公開鍵の暗号法と署名法の安全性証明技法を教材として，現代暗号の最先端の話題に対する審美眼を養い，技術の本質を理解することを目標とする．

【前もって履修しておくべき科目】

暗号理論 (C科第6学期)，情報セキュリティシステム (C科第7学期)

【前もって履修しておくことが望ましい科目】

学部科目離散数学第一／第二，アルゴリズム・データ構造．大学院の科目では，計算科学特論，理論計算機科学特論，情報数理特論などを合わせて聴講すると，さらに理解が深まります．

【教科書等】

教科書は用いない．教材は講義中にURL等を指定する予定．

参考書として次の2冊を推薦する．

岡本龍明，山本博資：現代暗号，産業図書　ISBN-7828-5353-X

Oded Goldreich: Foundations of Cryptography,
Cambridge University Press ISBN0-521-79172-3

【授業内容とその進め方】

前半の講義では，暗号，署名方式のモデル化，安全性の概念等の基本的な定義を導入しつつ，最近20年間の公開鍵暗号研究の流れを紹介する．講義の後半では，いくつかの代表的な「エポックメーキングな」論文を選んで，論文の読み方の訓練もねらいとして，受講者にも報告してもらう．

年度ごとに新しいテーマを取り上げる予定です．
（今年度は未定．8月に
http://www.oklab.ice.uec.ac.jp/class/index.html
に掲載の予定）

【成績評価方法及び評価基準(最低達成基準を含む)】

平常点（報告を聞きながら議論するので，積極的に議論に参加してもらいたい．）

【オフィスアワー：授業相談】

特に設けない．質問等があるときは事前にメールでアポイントメントを取ってから研究室を訪問すること．

【学生へのメッセージ】

論理的な思考ができていること．キッチリと論文を読む習慣が身につくように指導したいと考えています．RSA法などの公開鍵暗号の知識を前提とします．

読み替え科目：
この講義は旧J専攻の「暗号理論特論」の読み替え科目です．C専攻の科目として，「暗号理論特論」（國廣講師）がありますが，旧Jの読み替え科目ではないので注意して下さい．

【その他】

9月の中旬に5日間の集中講義形式で開講の予定．