電気通信大学　平成20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	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	太田　和夫		
居室	総合研究棟928		

公開E-Mail	授業関連Webページ
ota@ice.uec.ac.jp	http://www.oslab.ice.uec.ac.jp/class/cryptography_and_information_security/

【主題および達成目標】

暗号理論の代表的なトピックスについて，年毎に１つ話題を選んで，基礎から時代の先端までの話題を講義する．
過去には，証明可能安全な方式，マルチパーティプロトコル，ハッシュ関数の安全性，鍵交換プロトコルの安全性概念について代表的な定義から最新の結果までを紹介した．
本年は「一般化された識別不可能性 (Indifferentiability)とハッシュ関数の設計論」を扱う．
いずれのテーマであっても，定式化の理念，証明方法などを理解することを目的とする．

【前もって履修しておくべき科目】

離散数学第一／第二，アルゴリズム・データ構造，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】

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】

Maurer, Renner, and Holenstein: Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle methodology (TCC2004)

Coron, Dodis, Malinaud, and Puniya: Merkle-Damgard Revisited: how to Construct a Hash Function (CRYPTO2006)

Bertoni, Daemen, Peeters, Assche: On the Indifferentiability of the Sponge Construction (EUROCRYPT 2008)

いくつかの関連する論文

参考書：
「現代暗号」
　岡本,山本
　産業図書
　ISBN4-7828-5353-X
Foundations of Cryptography
　Oded Goldreich
　Cambridge University Press
　ISBN0-521-79172-3

【授業内容とその進め方】

取り上げるテーマの，代表的な論文を精読したのち，時代の最先端の結果の意義を理解できるように解説する．論文の精読は，受講生に分担して報告してもらったり，論文中の証明の論理ギャップを補足説明してもらう予定.

【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．）と
課題に対するレポートの成績による.

【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．RSA法などの公開鍵暗号の知識を前提とします.

【その他】