電気通信大学　平成21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	2009年度	開講年次	
開講学期	前学期	開講コース・課程	博士前期課程
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	崎山　一男		
居室	総合研究棟927		

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

【主題および達成目標】

暗号理論の応用として，セキュアシステムを，概論，理論，応用の観点から概説する。
まず，概論として暗号実装に必要となるアルゴリズムとそのハードウェア・ソフトウェアへの応用について解説する。
公開鍵暗号または共通鍵暗号の実装とその安全性評価について，サイドチャネル解析を中心に講義する。

【前もって履修しておくべき科目】

離散数学第一，暗号理論

【前もって履修しておくことが望ましい科目】

論理回路学

【教科書等】

- Handbook of Applied Cryptography, A.J. Menezes, P.C. van Oorschot, S.A. Vanstone (1996)
- ハンドアウトを用意する.

【授業内容とその進め方】

この授業では，まず，暗号実装において要素となる各種演算についての説明から始めます.
次に，公開鍵暗号・秘密鍵暗号のために必要となるアルゴリズムについて説明します.
最後に，実装における安全性評価手法であるサイドチャネル解析について説明し，暗号実装における，コスト・パフォーマンス・耐タンパ性のトレードオフについて講義を行います.

【成績評価方法及び評価基準(最低達成基準を含む)】
レポート（２～３回）により評価する． 公開鍵暗号ならびに秘密鍵暗号の実装において，コスト・パフォーマンス・耐タンパ性のトレードオフを理解していることが合格の基準である．

【オフィスアワー：授業相談】
特に設けない．メールにてアポイントを取ってください．

【学生へのメッセージ】
暗号理論を実装面からの切り口で学んでいく．

【その他】
特になし．