電気通信大学　平成16年度シラバス

授業科目名	暗号理論		
英文授業科目名	Ｃｒｙｐｔｏｇｒａｐｈｙ		
開講年度	2004年度	開講年次	３年次
開講学期	６学期	開講コース・課程	昼間コース
授業の方法		単位数	2
科目区分	専門科目-専門共通科目-選択必修科目		
開講学科・専攻	人間コミュニケーション学科		
担当教官名	佐山　弘樹		
居室	西６-３０７		

公開E-Mail	授業関連Webページ
sayama@hc.uec.ac.jp	http://complex.hc.uec.ac.jp/

【主題および達成目標】

科目名は「暗号理論」となっていますが，この授業ではいわゆる情報理論を含めた情報通信に関する符号化理論全般について，俯瞰的に講義します．現代の情報通信技術の基盤となっている各種の理論に対する最低限の理解を得ることを目指します．

【前もって履修しておくべき科目】

線形代数学，微分積分学など数学の基礎科目

【前もって履修しておくことが望ましい科目】

情報理論

【教科書等】

特に指定しません．授業の進行にあわせて随時参考書を挙げていきます．

【授業内容とその進め方】

理解を深めるため，毎回授業中に２，３問の課題を出し，そこから最低１問を選択して翌週までに小レポートとして提出してもらいます．大まかな流れは以下の通りです．
第１回：イントロダクション
第２回：情報量と情報エントロピー
第３回：相互情報量
第４回：情報源符号化とデータ圧縮
第５回：ハフマン符号とデータ圧縮
第６回：情報源符号化定理
第７回：マルコフ情報源モデル
第８回：通信路のモデル化
第９回：誤り検出・誤り訂正符号
第１０回：線形符号，ハミング符号
第１１回：通信路符号化定理
第１２回：暗号の基礎，秘密鍵暗号系
第１３回：公開鍵暗号系とＲＳＡ暗号
第１４回：量子計算と量子暗号

【成績評価方法及び評価基準(最低達成基準を含む)】

出席１０%，小レポート５０%，期末試験４０%を成績評価におけるウエイトの目安とし，総合的に評価します．この評価方法で最低でも６割以上の評点を得ることを，単位認定の基準とします．個別の最低達成基準は特に設けませんが，過去の経験から，６割以上の評点を得るには以下の条件を満たす必要があるものと思われます．
(a) 確率論の諸概念を理解し，それに基づいた具体的な計算ができる．
(b) 情報量やエントロピーの概念を理解し，具体的な計算がある程度できる．
(c) 授業で紹介する各種符号の原理を理解し，簡単なものなら自分で設計できる．
(d) 暗号の基礎を理解し，簡単な暗号化・復号化ができる．
(e) 小レポートをすべて提出している．

【オフィスアワー：授業相談】

月曜４限
上記以外でも時間が許せば適宜相談に応じます．
メール等で事前に連絡してください．

【学生へのメッセージ】
形式的な厳密性よりも直観的理解の方に重点を置きますが，各種定理の数学的証明も簡単なものはなるべく授業で紹介し，理解を深めるように努めます．内容的にはかなり盛り沢山ですが，どれも現代の情報通信技術を支える基本中の基本と言うべき重要なことばかりですので，頑張って理解に努めてください． 不明な点はどんどん質問してください．

【その他】