

電気通信大学 平成17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	2005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		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	総合研究棟 9 2 7		

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

【主題および達成目標】

安全に情報通信を行なうために、暗号および電子署名が用いられている。本講義では、これらの基礎理論、特に、情報理論的に安全な暗号系、IDに基づく暗号系などに焦点を絞って講述する。

【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：暗号理論（岩波書店）（太田，國廣訳）

【授業内容とその進め方】

年度により、いくつかのトピックスを絞り、取り上げる予定である。

本年度は、以下の順に講義をする予定である。

1. 楕円曲線暗号
2. 楕円曲線暗号の攻撃（特に，pairingを用いた攻撃）

3. pairingに基づくID baseの暗号系

4. Public Key Infrastructure (PKI)

に関して、講述する。講義の予定は以下の通りである。

1-2: RSA暗号, ElGamal暗号

3-4: 楕円曲線の基礎, 楕円曲線暗号

5-6: 楕円曲線暗号に対する攻撃

9-11: IDに基づく暗号系

12-13 PKIについて

14: まとめ

年度により、

- ・情報理論に安全な暗号に関する話題
- ・秘密分散法に関する話題
- ・量子暗号に関して

などをテーマにすえる予定である。

【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。

電気通信大学 平成17年度シラバス

【その他】