電気通信大学　平成17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	2005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-学科専門科目-選択科目		
開講学科・専攻	情報通信工学科		
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.oklab.ice.uec.ac.jp/class/cryptology/

【主題および達成目標】

情報セキュリティ技術を，概論，理論，応用の観点から概説する。

まず，概論として暗号，認証の基本的な概念を解説する。

続いて，公開鍵暗号または共通鍵暗号の安全性について

理論的な解析方法を中心に講義する。

【前もって履修しておくべき科目】

離散数学第一

【前もって履修しておくことが望ましい科目】

アルゴリズム基礎論，情報理論

【教科書等】

授業のWebページに掲載する予定

参考書

１．「情報セキュリティの科学」太田,黒澤,渡辺,

講談社ブルーバックス, ISBN4-06-257055-6

２．「現代暗号」岡本,山本, 産業図書，ISBN4-7828-5353-X

３．「暗号理論」太田，國廣，岩波書店，ISBN4-00-026871-6

【授業内容とその進め方】

１．情報セキュリティ概論

（1） 暗号技術

・共通鍵暗号　・公開鍵暗号　・鍵配送

（2） 認証技術

・本人確認　　・デジタル署名等

（3） 技術動向

・応用例　　・標準化等

２．安全性証明理論

２．１ 公開鍵暗号

・原理　　・署名への応用　・ゼロ知識証明

２．２ 秘密鍵暗号

・原理　　・差分解読法　　・線形解読法等

３．暗号・署名の安全性

・安全性の定義　　・証明技法

４．セキュリティ技術の応用

年ごとにテーマを選んで紹介する予定

（例：電子マネー，電子投票/オークション等）

【成績評価方法及び評価基準(最低達成基準を含む)】

(a) 評価方法：

原則として期末試験の成績に基づいて評価を行う．

レポートなどの評点を成績評価の付加的な判断材料とすることもあるが，

その場合は授業の初めに説明する．

(b) 評価基準：

基本的な公開鍵暗号の概念を理解して，簡単な計算ができること，および

安全性証明の論理を理解していることをもって合格基準とする．

【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】

安全性証明理論については，計算可能性の理論に慣れていることが望ましい。

この講義を100%理解できれば，あとは努力次第で論文を書けるようになります.

安全性証明で扱う話題については，年ごとに選択します．その年の内容は,

9月末ころに授業関連Web ページに掲載しますので，必ず参照すること.

（例）

「もの作り」にたずさわる人にとっては勿論のこと、たとえハ-ドウェアを扱わなくてもシステムの動作原理を理解し、発展させるためには、電子回路の

基本を十分理解している必要がある。授業中に一つずつしっかり理解していけば、難しい内容ではない。

【その他】