シラバス参照

科目名	暗号理論Ⅰ
配当年次	3年次
開講期間	春学期
単位数	2
担当教員	池田　暁志(イケダ　アキシ)
期間・曜日・時限・教室	春学期 火曜日 2時限 23－302

※	
授業の目的・目標	①授業の概要：暗号理論の基礎事項に関して、特に数学的側面に重きを置いて学ぶ授業です。 ②授業の目的：ICT社会における情報の安全性（情報セキュリティ）は現代暗号に支えられています。暗号理論における基礎的な概念や具体的な方式や安全性証明などについて学び、理解し修得することを目指します。特に、暗号理論における数学的な側面(計算量、アルゴリズム)について学ぶことを目的とします。 ③修得できる力： 2023年度以前の入学生：DP1○　DP2◎ 2024年度以降の入学生：DP3◎ ④授業の到達目標：様々な暗号化方式について、特にRSA暗号における暗号化や復号化のアルゴリズムの計算を実行できるようになることが到達目標です。
準備学習等の指示	1回の授業について、 ・復習（1時間45分）：授業で取り上げた重要なポイントを中心に、ノートを見直し論点を整理すること。ノートを参考に授業中に配布する演習問題を解いて提出をすること。
講義スケジュール	■1回目 【テーマ】イントロダクション, 暗号とは 【到達目標】暗号とは何か説明できるようになる。 【準備学習】なし 【特記事項】 ■2回目 【テーマ】整数に関する復習 【到達目標】初等整数論について基礎事項を確認・復習をし、基本的な計算が出来るようになる。 【準備学習】前回のノート見直し復習することで、前回の内容を理解しておく。 【特記事項】 ■3回目 【テーマ】計算量(多項式時間、指数関数時間) 【到達目標】アルゴリズムの計算量について、特に多項式時間と指数関数時間について説明が出来るようになる。 【準備学習】前回のノート見直し復習することで、前回の内容を理解しておく。 【特記事項】 ■4回目 【テーマ】ユークリッドのアルゴリズム 【到達目標】ユークリッドの互除法、特に拡張ユークリッド互除法により、modulo計算における逆数の計算が出来るようになる。 【準備学習】前回のノート見直し復習することで、前回の内容を理解しておく。 【特記事項】 ■5回目 【テーマ】整数の剰余, 合同 【到達目標】Modulo計算についての基本的なことが出来るようになる。 【準備学習】前回のノート見直し復習することで、前回の内容を理解しておく。 【特記事項】 ■6回目 【テーマ】有限体 【到達目標】有限体における四則演算が出来るようになる。 【準備学習】前回のノート見直し復習することで、前回の内容を理解しておく。 【特記事項】 ■7回目 【テーマ】暗号化方式 【到達目標】様々な暗号化方式について説明が出来るようになる。 【準備学習】前回のノート見直し復習することで、前回の内容を理解しておく。 【特記事項】 ■8回目 【テーマ】ブロック暗号 【到達目標】ブロック暗号の基礎理論を理解し、暗号化と復号化の計算が出来るようになる。

【準備学習】前回のノート見直し復習することで、前回の内容を理解しておく。
【特記事項】

■9回目
【テーマ】安全性
【到達目標】暗号の安全性について説明が出来るようになる。
【準備学習】前回のノート見直し復習することで、前回の内容を理解しておく。
【特記事項】

■10回目
【テーマ】乱数, 疑似乱数
【到達目標】乱数と疑似乱数とは何かを理解し、乱数生成のアルゴリズムに基づいて乱数生成が出来るようになる。
【準備学習】前回のノート見直し復習することで、前回の内容を理解しておく。
【特記事項】

■11回目
【テーマ】公開鍵暗号
【到達目標】公開鍵暗号の方式について説明が出来るようになる。
【準備学習】前回のノート見直し復習することで、前回の内容を理解しておく。
【特記事項】

■12回目
【テーマ】RSA暗号1
【到達目標】RSA暗号の方式に基づいて暗号化と復号化の計算が出来るようになる。
【準備学習】前回のノート見直し復習することで、前回の内容を理解しておく。
【特記事項】

■13回目
【テーマ】RSA暗号2
【到達目標】RSA暗号の理論について理解し、計算量に基づく安全性について説明が出来るようになる。
【準備学習】前回のノート見直し復習することで、前回の内容を理解しておく。
【特記事項】

教科書	
参考文献	・暗号理論入門, 丸善出版, J.A.ブーフマン 著, 林芳樹 訳 ・代数学と符号暗号理論 −Pythonによる実装−, 寺杣友秀 著
授業の方法	この講義は主として、 ・講義+演習 形式で行う。 授業方法として下記のアクティブラーニングの手法を実践する。 ・演習課題の出来を参考に、難しかったと思われる場所は重点的に復習をしながら講義を進めていく。 ・講義中になるべく細かい頻度で全体に質問をし、回答を参考に理解度を確認しながら進めていく。
成績評価方法	【評価方法】講義中の演習課題と期末レポートによる総合評価 【評価割合】期末レポート90%、講義中の演習課題10% 【評価基準】講義内容の理解度が確認出来る演習問題やレポート問題の点数を基準として評価する
オフィスアワー	火、水、木の講義を担当していない時間帯
居室	坂戸キャンパス23号館517号室
ホームページ	
その他特記事項	私語は厳禁とします。
添付ファイル	