東京工業高等専門学校	開講年度	令和05年度 (2023年度)	授業科目	応用数理学（2022年度以降入学生用科目）

科目基礎情報

科目番号	0024	科目区分	専門 / 選択
授業形態	講義	単位の種別と単位数	学修単位: 2
開設学科	機械情報システム工学専攻	対象学年	専1
開設期	前期	週時間数	2
教科書/教材	参考図書： ニール コブリッツ (著)，桜井 幸一 (翻訳)『 数論アルゴリズムと楕円暗号理論入門』 シュプリンガー・フェアラーク東京		
担当教員	南出 大樹		

到達目標

暗号理論の基礎となっている数論アルゴリズムを扱う。離散数学の復習をおこなった後に、初等整数論の基礎について概説し、素因数分解に応用する。後半では、公開鍵暗号の具体例を用いて、暗号・複合を解説する。
アルゴリズムの基礎となっている数学について深く理解するとともに、修得した理論を基に暗号化・復号化を実装するためのアルゴリズムを複合的に応用・実現できる技術を身につけることを目標とする。

ルーブリック

	理想的な到達レベルの目安	標準的な到達レベルの目安	最低限の到達レベルの目安(可)	未到達レベルの目安
数論アルゴリズム	数論的命題の証明を理解し，アルゴリズムへ応用することができる.	数論的命題を理解し，アルゴリズムへ応用することができる.	数論的命題を理解し，アルゴリズムで表現することができる.	数論的命題を，アルゴリズムで表現することができない.
計算量	アルゴリズムの計算量を正確に把握・比較することができる.	アルゴリズムの計算量を正確に比較することができる.	アルゴリズムの計算量を大きく分類することができる.	アルゴリズムの計算量を分類することができない.
素因数分解	各種素因数分解法の利点や欠点を理解し，使い分けることができる.	各種素因数分解法を用いて，素因数分解できる.	素因数分解アルゴリズムを組むことができる.	素因数分解アルゴリズムを組むことができない.
暗号理論	暗号理論の仕組みを理解し，各種暗号における暗号化と復号化を行うことができる.	各種暗号理論における暗号化と復号化を行うことができる.	与えられた暗号において，復号することができる.	各種暗号において，暗号化・復号化ができない.

学科の到達目標項目との関係

教育方法等

概要	講義内容は、現在社会において、情報インフラを支えている「暗号」の安全性を担保している数学理論を扱う。講義に加えて、実際に自ら「公開鍵暗号」を実装することで、プログラミング技術も身につけることを要請する。また、講義では歴史的背景を紹介することで、解読を試みる者との攻防において暗号理論がどのような発展を遂げてきたかを学ぶ。最後に、現在開発が進んでいる量子計算機に対して、暗号理論をどう発展させていくべきかを議論することで、持続可能な社会を実現する技術者としての素養を磨いてほしい。 講義形式は、暗号理論における通信の発展と解読の歴史に焦点を当てたPBLにより学習を進める。ＰＢＬによる学習を推進するために多くの演習問題を用意している。本講義で扱う理論では計算量が大きくなるので、プログラミングの素養がある方が望ましい。そのために、講義内容に関するプログラミングを習得できるよう補助教材も用意しているので、受講者は自学自習において、取り組まれたい。
授業の進め方・方法	主に講義形式で行う．必要に応じてプリントを配布する. 配布プリントを用いて予習し，授業中に扱った内容については復習しておくこと。 復習時，余裕のある者はアルゴリズムを実装して，その動作を確認すること。
注意点	この授業では、事前に提示される課題への取り組みが重要となってくる。 課題への取り組みを中心とした自学自習の習慣を身につけること。 数論アルゴリズムの理解について試験を実施する。試験の結果をもって評価する。 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。

授業の属性・履修上の区分

☑ アクティブラーニング	□ ICT 利用	□ 遠隔授業対応	□ 実務経験のある教員による授業

授業計画

		週	授業内容	週ごとの到達目標
前期	1stQ	1週	基数，合同式，計算量	整数に関する基礎事項、除法の定理を理解し，計算量の概念を理解する.
		2週	ユークリッド互除法，中国剰余定理	合同一次方程式を解くことができる
		3週	フェルマーの小定理（オイラーの定理）	フェルマーの小定理を用いて，素数判定ができる.
		4週	有限体，平方剰余相互法則	ルジャンドル記号とヤコビ記号を用いて，剰余判定ができる.
		5週	簡単な素数判定と擬素数	素数判定と擬素数の関係を理解する.
		6週	素因数分解１	モンテカルロ法，フェルマー法を用いて，素因数分解を行うことができる
		7週	素因数分解２	連分数法，２次ふるい法を用いて，素因数分解を行うことができる
		8週	中間試験	
	2ndQ	9週	暗号理論入門	簡単な暗号系を理解し，行列による暗号化と復号化を行うことができる.
		10週	公開鍵暗号，ＲＳＡ暗号	公開鍵暗号の仕組みを理解し，ＲＳＡ暗号による暗号化と復号化を行うことができる.
		11週	離散対数問題	離散対数問題の計算量的難しさを理解し，簡単な計算を行うことができる.
		12週	離散対数暗号	離散対数暗号による暗号化と復号化を行うことができる.

		13週	楕円曲線入門	楕円曲線の初歩を理解し，簡単な計算を行うことができる.
		14週	楕円曲線暗号	楕円曲線暗号による暗号化と復号化を行うことができる.
		15週	耐量子計算機暗号概説	量子計算機実現後に危惧される問題を理解し、現在の取り組みを知る.
		16週	期末試験	

モデルコアカリキュラムの学習内容と到達目標

分類	分野	学習内容	学習内容の到達目標	到達レベル	授業週

評価割合

	試験	発表	相互評価	態度	ポートフォリオ	その他	合計
総合評価割合	50	0	0	0	0	50	100
基礎的能力	50	0	0	0	0	50	100
専門的能力	0	0	0	0	0	0	0
分野横断的能力	0	0	0	0	0	0	0