授業科目名(英文名)／Course title	情報代数学B／Introductory Mathematical System B				
担当教員(所属)／Instructor	木村 巌(理学部)				
授業科目区分／Category	専門教育科目　専攻科目				
地域課題解決型人材育成プログラム科目／COC+Course		授業種別／Type of class	講義科目		
開講学期曜限／Period	T2, 火2/T2, Tue 2nd	対象所属／Eligible Faculty	理学部理学科数理情報学プログラム		
時間割コード／Registration Code	140014	対象学年／Eligible grade	3	単位数／Credits	1
ナンバリングコード／Numbering Code					
連絡先（研究室、電話番号、電子メールなど）／Contact	iwao@sci.u-toyama.ac.jp				
オフィスアワー（自由質問時間）／Office hours	水曜5限／Wed, 5th				
Moodleコース統合時間割コード／Moodle course join Registration Code					
Moodleコース登録教員名／Moodle course registered Instructor					
MoodleコースURL／Moodle course URL					
各種教育プログラム1／Various Educational programs1					
各種教育プログラム2／Various Educational programs2					
各種教育プログラム3／Various Educational programs3					
各種教育プログラム4／Various Educational programs4					
各種教育プログラム5／Various Educational programs5					

昨年度からの改善点／Changes from last year

リアルタイム・アドバイス／Real-time advice　更新日 2025/02/11

授業のねらいとカリキュラム上の位置付け（一般学修目標）／Course Objectives

教育目標／Educational Goals

情報の表現，効率のよい記録，計算，安全な通信の原理，基盤となるような代数学の諸概念を習得する．同時に，広く用いられる情報セキュリティの数学的基礎を学び，プログラミングを通して理解することを目標とする．

達成目標／Course Goals

有限環，有限体の乗法群の構造に基づく暗号理論の初歩を学び，それらを実際にプログラムとして実装できるようになり，計算効率の感覚を身につける．

授業計画（授業の形式、スケジュール等）／Class schedule

第1回：整数環の剰
余環の単数群
第2回：暗号理論の
基礎
第3回：共通鍵暗号
第4回：公開鍵暗号
（Elgamal暗号,
RSA暗号）
第5回：公開鍵暗号
（楕円曲線暗号）
第6回：コンピュー
タ演習（公開鍵暗
号）
第7回：線形符号,
公開鍵暗号の実用例
と標準化について
第8回：授業の振り
返りと試験

授業時間外学修（事前・事後学修）／Independent Study Outside of Class

事前に配付資料に基づいて60分程度，事後に講義内容を踏まえて60分程度の自習を目安とする．

キーワード／Keywords	整数環と剰余環，既約剰余類群，共通鍵暗号，公開鍵暗号，Elgamal暗号，RSA暗号，楕円曲線暗号
履修上の注意／Notices	理論面のみならず，コンピュータによる実習も行うので，コンピュータの操作にある程度慣れておくこと．

教科書／Required Text

教科書は指定しない

参考書／Required Materials

代数と数論の基礎 / 中島匠一, 共立出版, 2000(ISBN:9784320015616)

公開鍵暗号の数理 / 森山大輔,西巻陵,岡本竜明著，共立出版, 2011(ISBN:9784320019515)

シルヴァーマン 代数学 : 代数学への統一的入門 / 木村巖訳,ジョセフ　H　シルヴァーマン著,丸善出版, 2025-03-

28(ISBN:9784621311011)

教科書・参考書に関するその他通信欄	
成績評価の方法／Evaluation	講義期間中の小テスト・レポートを3割，期末試験の成績を7割の割合で評価する．
関連科目／Related course	
リンク先URL ／URL of syllabus or other information	
備考／Notes	

授業追加情報／Course add information

使用言語／Language	日本語
アクティブ・ラーニングの実施／Active learning	あり
アクティブラーニングの実施内容／Contents of Active learning	コンピュータでの演習と演習内容の発表
実務経験教員科目／Work Experience teacher's subjects	該当しない
データサイエンス科目／Data Science subjects	該当する
他学部・他研究科等学生の履修可否／	