

# 暗号とインターネットセキュリティ -数学が情報を守る-

単位数	ナンバリングコード	
2	DIF423	
	教員名	福光 正幸
	専門	暗号理論, 情報セキュリティ
	出身校等	東北大学大学院情報科学研究科 博士 (情報科学)
	現職	長崎県立大学 情報システム学部 情報セキュリティ学科 准教授
<b>授業形態</b>		
前期印刷授業・後期印刷授業		
<b>授業範囲</b>	<b>試験範囲</b>	
教科書全ページ	教科書全ページ	
	【試験時参照許可物】 一切自由 ※ただしWebページ (通信教育部POLITEを除く) と生成系AIの参照は不可とする。	
<b>科目の概要</b>		
<p>インターネット上で安全な通信路を構築する1つの道具として、公開鍵暗号系が利用されています。本講義では、その中でも代表的なRSA暗号に着目し、その仕組みを理解するために必要な数論の基礎を習得します。具体的には、合同式、剰余系、オイラーの定理、ユークリッドの互除法などです。また、学習した数論の知識を用いて、RSA暗号の仕組みを理解し、安全性についても議論していきます。</p>		
<b>授業における学修の到達目標</b>		
(1) 合同式, 剰余系, オイラーの定理, ユークリッドの互除法について習得する。 (2) RSA暗号の暗号化・復号の仕組みと安全性の議論について理解する。		
<b>講義の方針・計画</b>		
第1回: 予備知識の整理 第2回: 負の数への拡張 第3回: 割り算 第4回: 合同式の定義と基本性質 第5回: 合同式の応用 第6回: 集合 第7回: 剰余系 第8回: 整域, 写像 第9回: フェルマーの小定理 第10回: 互いに素の性質 第11回: オイラーの定理 第12回: ユークリッド互除法と逆元の計算 第13回: 暗号の定義と公開鍵暗号系 第14回: RSA暗号方式 第15回: 計算量的安全性とRSA暗号の安全性の根拠		

<b>準備学習</b>
印刷授業は、教科書や学習用プリントなどを基に自学自習で学習を進めますが、授業範囲の内容の他に、教科書の内容全体を2単位で90時間かけて学習することを目安としています。 わからない用語や内容は、参考文献等で検索することが準備学習として必要になります。  (予習) 学習用プリントの該当する回の内容を確認して下さい。(1時間) (復習) 学習用プリントに記載されている問題に解答して下さい。(3時間)
<b>課題(試験やレポート等)に対するフィードバック方法</b>
システム上でレポートのフィードバックを行います。
<b>成績評価の方法およびその基準</b>
科目試験による評価100%
<b>教科書</b>
書名：『ゼロからわかる数学-数論とその応用』 (初版) 著者名：戸川美郎 発行所：朝倉書店 ISBN：9784254115611
<b>参考書</b>
書名：『工科系のための初等整数論入門-公開鍵暗号をめざして』 著者名：楫元 発行所：培風館 書名：『暗号の数理』 著者名：一松信 発行所：講談社 書名：『群・環・体入門』 著者名：新妻弘, 木村哲三 発行所：共立出版
<b>その他</b>
特になし
<b>試験期間</b>
シラバス検索画面トップページ ( <a href="https://syllabus-tsushin.do-johodai.ac.jp/">https://syllabus-tsushin.do-johodai.ac.jp/</a> ) 下部の「2024学年暦」を参照
<b>学習プリント</b>
あり
<b>教職科目</b>
<b>関連受講科目</b>
代数学, ネットワークセキュリティ
<b>担当教員の実務経験</b>
実務経験なし