

鹿児島工業高等専門学校		開講年度	平成30年度 (2018年度)		授業科目	システム工学特論Ⅱ	
科目基礎情報							
科目番号	0049			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: 1		
開設学科	情報工学科			対象学年	5		
開設期	前期			週時間数	前期:2		
教科書/教材	〔教科書〕 なし〔参考書・補助教材〕 コンピュータによる暗号解読入門 松井甲子 森						
担当教員	幸田 晃						
到達目標							
秘匿方式の歴史的流れに沿って、暗号理論概要及び各方式とその強度を説明できるようにする。							
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		未到達レベルの目安	
評価項目1	秘匿の種類・歴史・特徴を説明できる。			秘匿の種類を説明でき、生文の特徴を説明できる。		秘匿の種類を説明できず、生文の特徴を説明できない。	
評価項目2	各種暗号方式を組み立て、解読できる。			特定の暗号方式のみを組み立て、解読できる。		特定の暗号方式のみを組み立て、解読できない。	
評価項目3							
学科の到達目標項目との関係							
教育方法等							
概要	数学的基礎知識が必要。本科目を修得した場合、システムセキュリティの秘匿部分の基礎となる。						
授業の進め方・方法	毎回の授業内容をよく理解し、次回内容との関連性について把握しておくこと。このためには講義終了後のレポート、演習問題、宿題等80分以上取組むこと。また疑問点があれば、その都度質問すること。						
注意点	疑問点があれば、その都度質問すること。						
授業計画							
		週	授業内容		週ごとの到達目標		
前期	1stQ	1週	1. 秘匿概説 (1) 概論		□ 秘匿体系形式を理解できる。 □ スペクトラム拡散通信、数学的表現、や用語の定義を理解でき、事前準備として文字の出現特徴を評価する事ができる。		
		2週	継続 (2) 英文調査		継続 □ 英文における単文字、連接文字の出現度数を調査し、その結果を報告する。		
		3週	継続 2. 各種暗号方式 (1) シーザ秘匿系		継続 □ 組立、翻訳、解読できる。		
		4週	継続		継続		
		5週	継続		継続		
		6週	(2) ビジネル秘匿系		□ 組立、翻訳、解読できる。		
		7週	継続		継続		
		8週	(3) 単文字鍵語秘匿系		□ 組立、翻訳、解読できる。		
	2ndQ	9週	継続		継続		
		10週	(4) ランダム秘匿系		□ 組立、翻訳、解読できる。		
		11週	継続		継続		
		12週	(5) ストリーム秘匿系		□ 組立、翻訳、解読できる。		
		13週	継続		継続		
		14週	(6) その他の秘匿系		□ 組立、翻訳、解読できる。		
		15週	継続		継続		
		16週	試験答案の返却・解説		各試験において間違った部分を自分の課題として把握する		
評価割合							
	定期試験			小テスト・レポート等		合計	
総合評価割合	0			0		0	
	75±10			25±10		0	
	0			0		0	