

平成23年度 シラバス	学年・期間・区分	5年次・後期・B群	
	対象学科・専攻	情報工学科	
システム工学特論Ⅱ (System Engineering TopicsⅡ)	担当教員	幸田 晃 (Kouda, Akira)	
	教員室	情報工学科棟4階 (tel 42-9094)	
	E-Mail	kouda@kagoshima-ct.ac.jp	
教育形態 / 単位の種別 / 単位数	講義 / 学修単位[講義Ⅰ] / 1単位		
週あたりの学習時間と回数	[授業 (100分) + 自学自習 (80分)] × 15回		
[本科目の目標] 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理解する。			
[本科目の位置付け] 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。			
[学習上の留意点] 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。			
[授業の内容]			
授 業 項 目	時限数	授 業 項 目 に 対 す る 達 成 目 標	予習の内容
1. 秘匿概説	7	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把握する事ができる。	暗号の歴史を調べておく。
2. シーザ秘匿系 —後期中間試験—	8	組立、翻訳、解読できる。	
3. ビジネル秘匿系	7	組立、翻訳、解読できる。	
4. 単文字鍵語秘匿系	4	組立、翻訳、解読できる。	
5. その他の秘匿系 —後期期末試験— 試験答案の返却・解説	4	ランダム秘匿系、鍵語秘匿系、公開鍵系について概要を理解できる。 授業項目1～5について達成度を確認する。 各試験において間違った部分を理解できる。	現代の暗号について調べておく。

