科 目 名	応用数学特論 Topics in Applied Mathematics			担当教員	橋本竜太		
学　　年	1 年	学　　期	前期	履修条件	選択	単位数	2
分　　野	工学基礎	授業形式	講義	科目番号	13272002	単位区別	学修
学習目標	古典的な公開鍵暗号系を題材として，電子情報通信工学の理論的な裏付けとなっている数理科学の素養を身につけるための学習技術について学修する。						
進 め 方	準備した教材プリントに基づき，出来るだけ多くの時間を演習に振り向けて，問題を解く手続きの中で，理解を深めながら進む。また適宜課題も与える。						

学習内容	学習項目（時間数）	学習到達目標
	１．公開鍵暗号系の概略(2)	
	２．合同式(6) (1) 剰余系と合同式 (2) ユークリッドの互除法	 合同式の扱いに慣れる。 D1:2 ユークリッドの互除法の計算ができる。 D1:2
	３．素数と離散対数(6) (1) エラトステネスの篩 (2) 素因数分解と素数判定 (3) べき乗の計算と離散対数	
	４．公開鍵暗号系の構成(6) (1) 素因数分解と RSA 暗号 (2) 離散対数問題と ElGamal 暗号	公開鍵暗号の概略を理解する。 D1:1
	５．素数判定と素因数分解(10) (1) フェルマーテスト (2) ρ 法 (3) p－１法 (4) その他の方法	いろいろな素数判定や素因数分解を理解する。 D1:1
	期末試験	
	６．試験問題の解答(1)	

評価方法	定期試験 50%，演習およびレポート 50%で総合評価する。
履修要件	特になし
関連科目	本科の数学関連科目（基礎数学，応用数学など）→　応用数学特論
教　　材	教員作成のプリント。
備　　考	オフィスアワー：火曜日放課後