電子情報システム工学専攻		情報数学特論					
学年	専攻科1年	担当教員名	大槻　典行				
単位数・期間		2単位	前期	週当りの開講回数	1回	専門共通･選択	学修単位1
授業の目標と概要		情報通信分野で利用される基礎数学を理解する．情報倫理と情報セキュリティに関する問題の中で，特に暗号に焦点を当て，暗号と数学の密接な関連性を理解し，情報数学の知識を修得する．暗号に用いられる数学的なものの考え方や証明を行うことによって，原理を理解すると共に，基礎知識を修得し，それらを実践で有効に活用できる能力を身につける．					
		釧路高専目標	C:100%	JABEE目標	d-1-2		
履修上の注意 (準備する用具･前提となる知識等)		高専1学年から3学年までの数学の基礎を理解していることが必要．演習問題を解くときに電卓が必要．演習問題集が2回の講義に対して1つ与えられるので，解答した演習問題集は，提出期限内に提出すること．					
到達目標		情報技術で使う数学が情報処理分野，通信分野などの現場で実用的に利用できる．					
成績評価方法		合否判定:期末試験の点数が60点以上． 最終評価:期末試験の点数9割，演習問題の評価1割					
テキスト･参考書		教科書:暗号 -ネットワーク社会の安全を守る鍵-，笠原正雄，共立出版社 参考書:現代暗号の基礎知識，黒澤馨，コロナ社，暗号理論，伊藤正史，ナツメ社，やり直しのための工業数学，三谷政昭，CQ出版社，					
メッセージ		専門的な基礎知識を必要としないので，本科3年生までの数学の知識で十分履修が可能です．(微分･積分は使いません)					

授 業 内 容	
授業項目	授業項目ごとの達成目標
･暗号の役割 (1回) ･基礎数学 (4回) ･公開鍵暗号 (2回) ･ディジタル署名 (1回)	･情報社会における暗号の重要性および必要性について解説できる． ･暗号理論に必要な整数論を理解し，効率の良い算法を利用することができる． ･公開鍵の原理を理解し，平文の暗号化，暗号文の平文化ができる． ･公開鍵の原理を応用した電子書名について解説できる．
前期中間試験	実施しない
･素因数分解問題 (2回) ･ID情報に基づく暗号技法 (3回) ･秘密鍵暗号 (2回)	･公開鍵方式の暗号で重要な要素となる素因数および素因数分解に関する問題を理解し，解説できる． ･近年，重要視されている暗号技法の一つであるID情報に基づく技法について理解し，解説できる． ･秘密鍵暗号の原理とその重要性について理解し，実際に応用できる．
前期期末試験	実施する
後期中間試験	
後期期末試験	