釧路工業高等専門学校	開講年度	令和02年度 (2020年度)	授業科目	情報数学特論

科目基礎情報

科目番号	0014	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: 2
開設学科	建設・生産システム工学専攻	対象学年	専1
開設期	前期	週時間数	2
教科書/教材	教科書：暗号とセキュリティ（新保雅一、オーム社）、参考書：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）、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）		
担当教員	大槻 典行		

到達目標

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、暗号 の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。公開鍵暗号の理論を解説でき簡単な例題を解くことができる。共通鍵暗号の理論を解説でき簡単な例題を解くことができる。

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	暗号で用いる基礎数理を理解し活用することができる。	暗号で用いる基礎数理を理解し基本的な計算をすることができる。	暗号で用いる基礎数理が理解できず、基本的な計算をすることができない。
評価項目2	公開鍵暗号の理論を理解し、秘密鍵の生成、暗号化、複合が自由にできる。	公開鍵暗号の理論を理解し、与えられた問題に対し秘密鍵の生成、暗号化、複合ができる。	公開鍵暗号の理論を理解できず、与えられた問題で秘密鍵の生成、暗号化、複合ができない。
評価項目3	共通鍵暗号の理論を理解し、秘密鍵の生成、暗号化、複合が自由にできる。	共通鍵暗号の理論を理解し、与えられた問題に対し秘密鍵の生成、暗号化、複合ができる。	共通鍵暗号の理論を理解できず、与えられた問題で秘密鍵の生成、暗号化、複合ができない。

学科の到達目標項目との関係

学習・教育到達度目標 C
JABEE d-1

教育方法等

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、暗号の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。
授業の進め方・方法	講義毎にテキストの代わりにプリントを配布する。スライドを使った講義を聴きながら配布されたプリントに書き込みを入れテキストとして完成する。 公開鍵暗号および共通鍵暗号の理論とアルゴリズムを解説するので、手計算で暗号の実際を理解する。講義の中に演習問題をいくつか解くので電卓は必須。 合否判定：期末試験の点数が60点以上を合格とする。 最終評価：合格した者に対して、期末試験の点数および演習問題の評価最大 1割の加点で評価点を算出する。 合否判定で不合格の者は、全範囲を対象とした再試験を行い、その点数が60点 以上を合格とする。ただし、最終評価は60点とする。
注意点	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。講義毎に演習問題集を配布する。演習問題集は、自己学習の教材として利用できるようにしているので授業時間外に解答すること。解答した演習問題集は、期限までに必ず提出し自己学習の実施の確認を受けること。

授業計画

		週	授業内容	週ごとの到達目標
前期	1stQ	1週	暗号の基礎知識	暗号とは何か、公開鍵暗号および共通鍵暗号について解説できる。
		2週	暗号の基礎数理１	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。
		3週	暗号の基礎数理２	素数の性質、合同式について理解し使うことができる。
		4週	暗号の基礎数理３	オイラーの定理、フェルマーの定理を理解し使うことができる。
		5週	公開鍵暗号１	公開鍵の原理を理解し、公開鍵暗号に使う定理について解説できる。
		6週	公開鍵暗号２	RSA暗号の理論を理解し、平文の暗号化、暗号文の復号ができる。
		7週	公開鍵暗号３	RSA暗号の欠点に対するエルガマル暗号の優位点を解説できる。エルガマル暗号を使って平文の暗号化、暗号文の復号ができる。
		8週	素数１	公開鍵方式の暗号で重要な要素となる素数に関する問題を理解し解説できる。素数判定ができる。
	2ndQ	9週	素数２	素因数分解に関する問題を理解し解説できる。効率の良い素因数分解ができる。
		10週	ディジタル署名	公開鍵の原理を応用した電子書名について解説できる。
		11週	共通鍵暗号１	共通鍵暗号の原理とその重要性を理解し解説できる。安全な共通鍵の生成方法を解説できる。
		12週	共通鍵暗号２	共通鍵暗号の一つであるDES暗号についてアルゴリズムを理解し解説できる。
		13週	共通鍵暗号３	教育用DES暗号を利用して、暗号化および復号ができる。
		14週	セキュリティ（１回）	ネットワークを含むセキュリティ問題について理解し解説できる。

		15週	暗号の歴史	暗号の歴史に触れ、エニグマ暗号機の簡易モデルを操作し暗号化および復号ができる。
		16週	期末試験	

モデルコアカリキュラムの学習内容と到達目標

分類	分野	学習内容	学習内容の到達目標	到達レベル	授業週

評価割合

	試験	発表	相互評価	態度	ポートフォリオ	その他	合計
総合評価割合	100	0	0	0	0	0	100
基礎的能力	0	0	0	0	0	0	0
専門的能力	100	0	0	0	0	0	100
分野横断的能力	0	0	0	0	0	0	0