高知工業高等専門学校	開講年度	令和04年度 (2022年度)	授業科目	暗号理論

科目基礎情報

科目番号	I4003	科目区分	専門 / 必修
授業形態	講義	単位の種別と単位数	学修単位: 2
開設学科	SD 情報セキュリティコース	対象学年	4
開設期	後期	週時間数	2
教科書/教材	教材はオリジナルのものを作成し配布する		
担当教員	立川 崇之		

到達目標

1. 暗号の基本概念を理解し，古典的な暗号を解くことができる.
2. 共通鍵暗号，公開鍵暗号の原理を説明できる.
3. ハッシュ関数の性質を説明できる.
4. デジタル署名，証明書の仕組みを説明できる.

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	古典的な暗号の仕組みを理解し，解読方法を説明できる.	古典的な暗号の仕組みを説明できる.	古典的な暗号の仕組みを説明できない.
評価項目2	共通鍵暗号，公開鍵暗号の原理を理解し，具体的な運用方法を説明できる.	共通鍵暗号，公開鍵暗号の原理を説明できる.	共通鍵暗号，公開鍵暗号の原理を説明できない.
評価項目3	ハッシュ関数の性質を理解し，脆弱性について説明できる.	ハッシュ関数の性質を説明できる.	ハッシュ関数の性質を説明できない.
評価項目4	デジタル署名，証明書の仕組みを理解し，セキュリティのどの部分を担保するのかを説明できる.	デジタル署名，証明書の仕組みを説明できる.	デジタル署名，証明書の仕組みを説明できない.

学科の到達目標項目との関係

学習・教育到達度目標 (C)

教育方法等

概要	現代の情報通信において，特に機密性，完全性を担保する暗号理論を理解し，どのような局面でいかに運用すべきかを考えられるようにする．現代暗号の強度がいかにして保証されるか，数学的側面から理解する．また，不適切な運用がセキュリティ上の深刻な問題を引き起こす可能性についても理解する.
授業の進め方・方法	教材は市販の教科書を使用せず，独自に作成したものを印刷し配布する．授業では教材に沿ってポイントを説明する．学生はノートを取り，わからないことがあれば，時間中あるいは授業時間外に質問する．進度によっては各トピックを扱う週を短縮したり増やしたりすることもある.
注意点	【成績評価の基準・方法】 試験の成績を80%，課題を20%の割合で総合的に評価する．成績評価は中間と期末の各期間の評価の平均とする．学年の評価は後学期末の評価とする．技術者が身に着けるべき専門科目として，上記の到達目標に対する達成度を試験等において評価する. 【事前・事後学習】 事前学習として配布した教材を読んだ上で，理解が難しかった部分を整理して授業に臨むこと．また，事後学習として授業内で取り扱った項目について練習問題を複数回解き理解を深めること. 【学修単位科目（授業時間外の学習時間等）】 本科目は学修単位のため，以下の標準学習時間を設定した自主学習を累計45時間分以上実施して課題等を提出しなければ，成績が60点を超えた場合でも59点として扱い単位を認定しない. ・全15回の授業に対して，0.5時間の事前学習と1.5時間の事後学習．計30時間分. ・中間試験および期末試験に対してそれぞれ試験勉強のための課題学習4時間．計8時間分. ・授業期間中に出題する課題を学習する時間7時間分. 【履修上の注意】 本科目は情報セキュリティコース3年で学んだ「情報代数」「論理回路」「ディジタル信号処理」を理解している前提で進める．特に「情報代数」について十分に理解していない者は，受講前に復習しておくことを強く勧める．場合によっては運用の実例を兼ねた課題を課すこともあるので，Linux のコマンド操作に慣れておくこと.

授業の属性・履修上の区分

□ アクティブラーニング	□ ICT 利用	□ 遠隔授業対応	□ 実務経験のある教員による授業

授業計画

		週	授業内容	週ごとの到達目標
後期	3rdQ	1週	ガイダンス 既習事項の確認	授業の進め方，評価法などについて理解する. 3年生までで既習の事項を確認する.
		2週	古典的な暗号	シーザー暗号，単一換字暗号，エニグマなど古典的な暗号について理解する
		3週	論理演算	共通鍵暗号で必要な論理演算について振り返る.
		4週	共通鍵暗号I	共通鍵暗号の基本原理，論理演算との関係を理解する
		5週	共通鍵暗号II	DES，3DES，AESなどの共通鍵暗号の仕組みを理解する.
		6週	情報代数	公開鍵暗号で必要な情報代数について振り返る.
		7週	公開鍵暗号I	共通鍵暗号の問題点と，それを解決する公開鍵暗号として，RSA暗号の特徴と利点を理解する.
		8週	公開鍵暗号II	RSA暗号以外の公開鍵暗号について学び，公開鍵暗号の利点，欠点を理解する.
	4thQ	9週	鍵配送問題	共通鍵暗号を安全に配送するための方法として，ハイブリッド暗号などを理解する.
		10週	ハッシュ関数	ハッシュ関数の特徴と危殆化について理解する.
		11週	暗号論的疑似乱数	暗号技術に適した疑似乱数の生成方法について理解する.

		12週	デジタル署名	暗号技術の応用としてのデジタル署名を理解する.
		13週	証明書	サーバや個人の正当性を証明する，証明書の仕組みを理解する.
		14週	SSL/TLS	Webブラウザとサーバ間での通信に用いられる，SSL/TLSについて理解する.
		15週	暗号技術の現状と将来I	暗号技術を高度に応用した現状について理解する.
		16週	暗号技術の現状と将来II	暗号技術を高度に応用した現状について理解する.

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
基礎的能力	工学基礎	情報リテラシー	情報リテラシー	情報を適切に収集・処理・発信するための基礎的な知識を活用できる。	4	
				論理演算と進数変換の仕組みを用いて基本的な演算ができる。	4	
				コンピュータのハードウェアに関する基礎的な知識を活用できる。	3	
				情報伝達システムやインターネットの基本的な仕組みを把握している。	4	
				同一の問題に対し、それを解決できる複数のアルゴリズムが存在しうることを知っている。	4	
				与えられた基本的な問題を解くための適切なアルゴリズムを構築することができる。	4	
				任意のプログラミング言語を用いて、構築したアルゴリズムを実装できる。	3	
				情報セキュリティの必要性および守るべき情報を認識している。	4	
				個人情報とプライバシー保護の考え方についての基本的な配慮ができる。	3	
				インターネット(SNSを含む)やコンピュータの利用における様々な脅威を認識している	3	
				インターネット(SNSを含む)やコンピュータの利用における様々な脅威に対して実践すべき対策を説明できる。	3	
専門的能力	分野別の専門工学	情報系分野	情報数学・情報理論	集合に関する基本的な概念を理解し、集合演算を実行できる。	4	
				集合の間の関係(関数)に関する基本的な概念を説明できる。	4	
				ブール代数に関する基本的な概念を説明できる。	4	
				論理代数と述語論理に関する基本的な概念を説明できる。	4	
				離散数学に関する知識をアルゴリズムの設計、解析に利用することができる。	4	
				コンピュータ上での数値の表現方法が誤差に関係することを説明できる。	3	
				コンピュータ上で数値計算を行う際に発生する誤差の影響を説明できる。	3	
				コンピュータ向けの主要な数値計算アルゴリズムの概要や特徴を説明できる。	3	

評価割合

	試験	発表	相互評価	態度	ポートフォリオ	課題	合計
総合評価割合	80	0	0	0	0	20	100
基礎的能力	40	0	0	0	0	10	50
専門的能力	30	0	0	0	0	5	35
分野横断的能力	10	0	0	0	0	5	15