長野工業高等専門学校	開講年度	令和05年度 (2023年度)	授業科目	情報セキュリティ論

科目基礎情報

科目番号	0026	科目区分	専門 / 選択
授業形態	授業	単位の種別と単位数	学修単位: 2
開設学科	生産環境システム専攻（先端融合テクノロジー連携教育プログラム）	対象学年	専1
開設期	前期	週時間数	2
教科書/教材	教科書：必要に応じてプリントを配布する		
担当教員	藤澤 義範		

到達目標

共通鍵暗号方式と公開鍵暗号方式の違いを仕組みと用途から説明することができ，IDEA暗号方式の原理，RSA暗号方式の原理を説明することができる．これらの内容を満足することで，学習・教育目標の(D-1)の達成とする．

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
情報セキュリティについての理解	ネットワーク上の脅威を理解してセキュリティの重要性を理解できる．	ネットワーク上の脅威についてある程度理解できる．	ネットワーク上の脅威について理解できない．
公開鍵暗号方式の理解	公開鍵暗号方式の仕組みを理解し，プログラムにより実装できる．	公開鍵暗号方式の仕組みについて理解できる．	公開鍵暗号方式の仕組みが理解できない．
共通鍵暗号方式の理解	共通鍵暗号方式の仕組みを理解し，プログラムにより実装できる．	共通鍵暗号方式の仕組みについて理解できる．	共通鍵暗号方式の仕組みが理解できない．

学科の到達目標項目との関係

教育方法等

概要	授業の目的と概要 情報セキュリティの中でも特に重要な技術である暗号技術について主に学習する．暗号技術は，現在のインターネットセキュリティのために開発された技術ではなく，通信全般で利用可能な技術である．暗号方式には，共通鍵暗号方式と公開鍵暗号方式の2種類があり，それぞれについて学習し理解を深める．
授業の進め方・方法	講義形式で授業を進め，プログラムによる暗号アルゴリズムの実装の課題を課す． Classroom English として毎回 Dictation を実施するとともに，授業内で英語の論文等を積極的に利用する．
注意点	＜成績評価＞ 前期期末試験（40%），レポート（60%）の合計100点満点で(D-1)を評価する． ＜オフィスアワー＞毎週水曜日16:00.17:00，電子情報工学科1F第二教員室． ＜備考＞基礎的な整数論について理解していることが望ましい．また，プログラムによる暗号の実装も行うので，プログラミングの知識が不足する場合は各自が事前に補っておくこと． なお、本科目は学修単位科目であり，授業時間30時間に加えて，自学自習時間30時間が必要である．

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
前期	1stQ	1週	ネットワークセキュリティの概要	ネットワークセキュリティの重要性について理解できる．
		2週	暗号技術の歴史と概要	暗号技術のこれまでの発展の歴史と古典暗号と近代暗号の違いが説明できる．
		3週	公開鍵暗号方式の概要と分類	公開鍵暗号方式の基本となる数学の諸問題ついて学び，ネットワークセキュリティの実現方法を理解できる
		4週	整数論の基礎(1)	初歩的な整数論について理解できる．
		5週	整数論の基礎(2)	初歩的な整数論について理解できる．
		6週	整数論の基礎(3)	Fermatの小定理を証明できる．
		7週	MH暗号方式(1)	ナップザック問題について説明できる．
		8週	MH暗号方式(2)	MH暗号方式ついて理解できる．
	2ndQ	9週	RSA暗号の論文を読み理解を深める	RSA暗号について理解できる．
		10週	RSA，Elgamal暗号方式	RSA，Elgamal暗号方式について理解できる．
		11週	共通鍵暗号方式の概要と分類	共通鍵暗号方式の基本となる仕組みや問題点を学び，その仕組みを理解できる．
		12週	DES暗号方式	DES暗号方式について理解できる．
		13週	IDEA暗号方式の論文を読み理解を深める	IDEA暗号方式について理解できる．
		14週	IDEA暗号方式	IDEA暗号方式について説明できる．
		15週	前期期末試験	
		16週	まとめ	暗号技術が世の中でどのように利用されているのかを理解することができる．

評価割合

	試験	小テスト	平常点	レポート	その他	合計
総合評価割合	40	0	0	60	0	100
配点	40	0	0	60	0	100