科目基礎科目番号授業形態開設学科開設期		専門学校	│ 開講年度 │ 令和05	年度 (2023年	F(++)	授業科目 🕆	情報セキュリ	ティ論
科目番号 授業形態 開設学科	I I FIX			牛皮 (2023-			IH TK ピイエフ	/ ノ ヿ pm
授業形態 開設学科		0026		和中区	7.4	専門 / 選択		
開設学科		授業						
開設期		生産環境シ			生年 生	専1	学修単位: 2 専1	
נאַ אַנוּתוּ			連携教育プログラム) 前期		 引数	2	2	
					19A		<u></u>	
担当教員	, ,	藤澤 義範						
<u></u>	į	13.77 13.71 0						
					≠ IDEV時日1	ませか原理 PG	SA暗号方式の頂	
できる. こ	れらの内容	学を満足するこ	ことで、学習・教育目標の(D.	-1)の達成とする).	71(0 <i>7)</i> 永珪,代	カス・日 つりエルシルホ	生で配列することが
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			ネットワーク上の脅威を理 セキュリティの重要性を理 る.	ぬった ユー・コーツー	ネットワーク上の脅威についてる る程度理解できる.		ネットワーク_ 解できない.	上の脅威について理
公開鍵暗号	方式の理解	 4	公開鍵暗号方式の仕組みを ,プログラムにより実装で		理暗号方式の仕続 できる.	組みについて	公開鍵暗号方式	式の仕組みが理解で
共通鍵暗号	方式の理解	7 4	共通鍵暗号方式の仕組みを , プログラムにより実装で	理解し 共通級	通鍵暗号方式の仕組みについて 解できる.		 :	式の仕組みが理解で
学科の到	達目標項	目との関係		'				
教育方法			-					
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、現代							
授業の進み方・方法 講義形式で			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. m 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		<偏考>星 グラミンク	画> 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。 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。 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 プの知識が不足する場合は各自が事前に補っておくこと。 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。					
哲業の屋	一. 屋.		日は子形半位行日にのり,12	又未吋间30吋间	に加えて, 日子	日日时间20时	回が必安である	•
<u>1又未り)</u> □ アクティ		<u>を上の区分</u>	☑ ICT 利用	口造	 隔授業対応		□ 宇致奴除在)ある教員による授業
	1 /	- <i>D</i> -D			附及未刈心			のの対対による技法
授業計画	i							
<u> </u>		週)EI -	**トク到を日播		
	1stQ		業内谷 ットワークセキュリティの概要			週ごとの到達目標 ネットワークセキュリティの重要性について理解でき ス		
		2週 問	号技術の歴史と概要			る・ 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 2	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	翌数論の基礎(1)			ットワークセ	ナユリナイの夫ュ	
		十四				シットワークセ	ィュリティの夫! ついて理解でき [;]	の諸問題ついて学び 現方法を理解できる
			整数論の基礎(2)		初步	シトワークセ:		の諸問題ついて学び 現方法を理解できる る.
		5週	隆数論の基礎(2) 隆数論の基礎(3)		初步	シトワークセ:	ついて理解でき [、] ついて理解でき [、]	の諸問題ついて学び 現方法を理解できる る.
		5週 虫 6週 虫			初步 初步 Feri	マットワークセ 的な整数論に 的な整数論に matの小定理を	ついて理解でき [、] ついて理解でき [、]	の諸問題ついて学び 現方法を理解できる る. る.
前期		5週 素 6週 素 7週 N 8週 N	整数論の基礎(3)		初歩 初歩 Feri ナッ MHI	マットワークセットのな整数論に でのな整数論に matの小定理を プザック問題 暗号方式ついて	ついて理解できっ ついて理解できる. を証明できる. について説明で について記明できる.	の諸問題ついて学び 現方法を理解できる る. る.
		5週 惠 6週 惠 7週 N 8週 N 9週 R	を数論の基礎() MH暗号方式(1) HH暗号方式(2) SA暗号の論文を読み理解を	深める	初歩 初歩 Feri ナッ MHI RSA	ベットワークセ のな整数論に のな整数論に matの小定理を パプザック問題 暗号方式ついて 暗号について	ついて理解できっついて理解できる. 証明できる. について説明で に理解できる. 理解できる.	の諸問題ついて学び 現方法を理解できる る. る. きる.
		5週 惠 6週 惠 7週 N 8週 N 9週 R	を数論の基礎(3) IH暗号方式(1) IH暗号方式(2)	深める	初歩 初歩 Feri ナッ MHI RSA RSA	w トワークセ のな整数論に のな整数論に matの小定理を プザック問題 暗号方式ついて い暗号について 、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、	ついて理解できって理解できる。 ご明できる。 について説明できる。 理解できる。 理解できる。 号方式についても	の諸問題ついて学び 現方法を理解できる る. る. きる. 世解できる.
		5週 整 6週 整 7週 N 8週 N 9週 R 10週 R 11週 力	整数論の基礎(3) IH暗号方式(1) IH暗号方式(2) SA暗号の論文を読み理解を SA, Elgamal暗号方式 共通鍵暗号方式の概要と分類	深める	初歩 初歩 Feri ナッ MHI RSA RSA 共通	w トワークセ 的な整数論に matの小定理を プザック問題 暗号方式ついて 暗号について は、Elgamal暗 鍵暗号方式の の仕組みを理	ついて理解できって理解できる。 について説明できる。 について説明できる。 理解できる。 理解できる。 号方式について現 基本となる仕組織 解できる。	の諸問題ついて学び 現方法を理解できる る. る. きる. 世解できる. みや問題点を学び
前期	2ndQ	5週 整 6週 整 7週 N 8週 N 9週 F 10週 F 11週 井 12週 C	整数論の基礎(3) IH暗号方式(1) IH暗号方式(2) SA暗号の論文を読み理解を SA, Elgamal暗号方式 性通鍵暗号方式の概要と分類		初歩 初歩 Feri ナッ MHI RSA RSA 共通 , そ	w トワークセ 的な整数論に 的な整数論に matの小定理を プザック問題 暗号方式ついて M暗号について A、Elgamal暗 鍵暗号方式の の仕組みを理 い暗号方式について	ついて理解できる. について説明できる. について説明で: 理解できる. 理解できる. 号方式について! 基本となる仕組。 解できる. いて理解できる.	の諸問題ついて学び 現方法を理解できる る. る. きる. 単解できる. みや問題点を学び
前期	2ndQ	5週 整 6週 整 7週 N 8週 N 9週 F 10週 F 11週 力 12週 C 13週 I	整数論の基礎(3) IH暗号方式(1) IH暗号方式(2) SA暗号の論文を読み理解を SA, Elgamal暗号方式 共通鍵暗号方式の概要と分類 DES暗号方式の論文を読み理		初歩 初歩 Feri ナッ MHI RSA RSA 共通 、そ DES	wyトワークセ のな整数論に のな整数論に matの小定理を プザック問題 暗号方式ついて N Elgamal暗 は鍵暗号方式の の仕組みを理 の暗号方式につ A暗号方式につ	ついて理解できる。 について説明できる。 について説明でにはなる。 理解できる。 理解できる。 号方式については 基本となる仕組を解できる。 いて理解できる。 いて理解できる。	の諸問題ついて学び 現方法を理解できる る. る. きる. 世解できる. みや問題点を学び
前期	2ndQ	5週 整 6週 整 7週 N 8週 N 9週 F 10週 F 11週 ⇒ 12週 C 13週 I 14週 I	整数論の基礎(3) IH暗号方式(1) IH暗号方式(2) SA暗号の論文を読み理解を決らA、Elgamal暗号方式 共通鍵暗号方式の概要と分類 DES暗号方式 DEA暗号方式の論文を読み理 DEA暗号方式		初歩 初歩 Feri ナッ MHI RSA RSA 共通 、そ DES	wyトワークセ のな整数論に のな整数論に matの小定理を プザック問題 暗号方式ついて N Elgamal暗 は鍵暗号方式の の仕組みを理 の暗号方式につ A暗号方式につ	ついて理解できる. について説明できる. について説明で: 理解できる. 理解できる. 号方式について! 基本となる仕組。 解できる. いて理解できる.	の諸問題ついて学び 現方法を理解できる る. る. きる. 世解できる. みや問題点を学び
前期	2ndQ	5週 整 6週 整 7週 N 8週 N 9週 F 10週 F 11週 ⇒ 12週 C 13週 I 14週 I	整数論の基礎(3) IH暗号方式(1) IH暗号方式(2) SA暗号の論文を読み理解を SA, Elgamal暗号方式 共通鍵暗号方式の概要と分類 DES暗号方式の論文を読み理		初步 初歩 Fern ナッ MHI RSA RSA 共通 、で DES IDE	wトワークセミ 的な整数論に matの小定理を プザック問題 暗号方式ついて 、、Elgamal暗号 の仕組みを理 の借号方式につ A暗号方式につ A暗号方式にこ	ついて理解できる。 について説明できる。 について説明できる。 理解できる。 理解できる。 号方式について 基本となる仕組み 解できる。 いて理解できる。 いて理解できる。 いて理解できる。	の諸問題ついて学び 現方法を理解できる る. る. きる. 世解できる. みや問題点を学び
前期	2ndQ	5週 整 6週 整 7週 N 8週 N 9週 R 10週 R 11週 ‡ 12週 C 13週 I 14週 I 15週 前	整数論の基礎(3) IH暗号方式(1) IH暗号方式(2) SA暗号の論文を読み理解を決らA、Elgamal暗号方式 共通鍵暗号方式の概要と分類 DES暗号方式 DEA暗号方式の論文を読み理 DEA暗号方式		初歩 初歩 Feri ナッ MHI RSA RSA 共通子 DES IDE	wトワークセミ 的な整数論に matの小定理を プザック問題 暗号方式ついて 、、Elgamal暗号 の仕組みを理 の借号方式につ A暗号方式につ A暗号方式にこ	ついて理解できる。 について説明できる。 について説明できる。 理解できる。 理解できる。 号方式について! 基本となる仕組。 解できる。 いて理解できる。 いて理解できる。 いて理解できる。	の諸問題ついて学び 現方法を理解できる る. る. きる. 世解できる. みや問題点を学び
前期		5週 整 6週 整 7週 N 8週 N 9週 R 10週 R 11週 ‡ 12週 C 13週 I 14週 I 15週 前	整数論の基礎(3) IH暗号方式(1) IH暗号方式(2) SA暗号の論文を読み理解をSA、Elgamal暗号方式 性通鍵暗号方式の概要と分類 DES暗号方式 DEA暗号方式の論文を読み理 DEA暗号方式 前期期末試験		初歩 初歩 Feri ナッ MHI RSA RSA 共通子 DES IDE	マットワークセージのな整数論にでいる整数論にでいる整数論にでいる。 でいるを数論にでいる。 では、アザック問題では、アザック問題では、 では、自身では、では、 は、自身では、では、 は、自身では、 は、 は、 は、 は、 は、 は、 は、 は、 は、	ついて理解できる。 について説明できる。 について説明できる。 理解できる。 理解できる。 号方式について! 基本となる仕組。 解できる。 いて理解できる。 いて理解できる。 いて理解できる。	の諸問題ついて学び 現方法を理解できる る. る. きる. 世解できる. みや問題点を学び
前期		5週 生 6週 生 7週 N 8週 N 9週 R 10週 F 11週 上 12週 C 13週 I 14週 I 15週 f 16週 ā	整数論の基礎(3) IH暗号方式(1) IH暗号方式(2) SA暗号の論文を読み理解を決 SA, Elgamal暗号方式 共通鍵暗号方式の概要と分類 DES暗号方式 DEA暗号方式の論文を読み理 DEA暗号方式の論文を読み理 DEA暗号方式 DEA暗号方式 DEA暗号方式	解を深める	初歩 初歩 Feri ナッ MHI RSA RSA 共通 , で DES IDE IDE	メットワークセミのな整数論に のな整数論に のな整数論に のな整数論に のはである。 のはである。 のはでは、のは、 のは、	ついて理解できる. について説明できる. について説明できる. 理解できる. 理解できる. 号方式について理解できる. いて理解できる. いて理解できる. いて理解できる. いて理解できる. いて理解できる.	の諸問題ついて学び現方法を理解できる。 る。 きる。 理解できる。 みや問題点を学び 5.
前期	, III	5週 整 6週 整 7週 N 8週 N 9週 R 10週 R 11週 ‡ 12週 C 13週 I 14週 I 15週 前	整数論の基礎(3) IHH暗号方式(1) IHH暗号方式(2) SA暗号の論文を読み理解を決 SA, Elgamal暗号方式 共通鍵暗号方式の概要と分類 DES暗号方式 DEA暗号方式の論文を読み理 DEA暗号方式の論文を読み理 DEA暗号方式 DIEA暗号方式の論文を読み理 DEA暗号方式	解を深める	初歩 初歩 Feri ナッ MHI RSA RSA 共通子 DES IDE	マットワークセージのな整数論にでいる整数論にでいる整数論にでいる。 でいるを数論にでいる。 では、アザック問題では、アザック問題では、 では、自身では、では、 は、自身では、では、 は、自身では、 は、 は、 は、 は、 は、 は、 は、 は、 は、	ついて理解できる. について説明できる. について説明できる. 理解できる. 理解できる. 号方式について理解できる. いて理解できる. いて理解できる. いて理解できる. いて理解できる. いて理解できる.	の諸問題ついて学び 現方法を理解できる る. る. きる. 世解できる. みや問題点を学び