

開講期間	配当年	単位数	科目必選区分
3年後期	3	2	選択（教職「数学」は選択）
担当教員			
大石 和臣			
添付ファイル			
講義概要			
符号・暗号理論はデジタル時代における基礎的で重要な技術である。本講義では、これらの基本となる代数学や確率について復習しながら、主に暗号の具体的方式について学び、その応用についても学習する。この科目は、情報セキュリティ技術分野の実務経験のある教員が担当する科目である。			
授業計画	1	イントロダクション。情報理論、符号理論、暗号理論の背景、歴史、具体例。 カリキュラムにおける本講義の位置づけ（ステップ4、コース、分野科目）を説明する。講義概要をシラバスを使って説明する。情報理論、符号理論、暗号理論の背景、歴史、具体例を学ぶ。 AL①。講義の最後に簡単な演習を行う（iLearnあるいはMicrosoft Formsを活用する場合がある）。 準備：シラバスを読んでくること。 課題：今回の復習および次回の講義内容を予習。	
	2	情報量とエントロピー、確率、暗号の情報理論的な安全性 情報量とエントロピーを学ぶ。確率を復習し、暗号の情報理論的な安全性を学ぶ。講義の最後に簡単な演習を行う（iLearnあるいはMicrosoft Formsを活用する場合がある）。 準備：今回の講義内容を予習してくる。こと。 課題：今回の復習および次回の講義内容を予習。	
	3	確率変数、情報源符号化定理、暗号のモデル、古代～現代暗号、無条件安全性 第2回の講義の続きおよび現代暗号に至る歴史と無条件安全性の概念を学ぶ。AL①。講義の最後に簡単な演習を行う（iLearnあるいはMicrosoft Formsを活用する場合がある）。 準備：今回の講義内容を予習してくる。こと。 課題：今回の復習および次回の講義内容を予習。	
	4	共通鍵暗号（One-time Pad、ブロック暗号、ストリーム暗号、DES、AES） 共通鍵暗号、無条件安全なOne-time Pad、ブロック暗号とストリーム暗号の違いについて学び、代表的な方式であるDESとAESについて、その内部構造を学ぶ。講義の最後に簡単な演習を行う（iLearnあるいはMicrosoft Formsを活用する場合がある）。 準備：今回の講義内容を予習してくる。こと。 課題：今回の復習および次回の講義内容を予習。	
	5	共通鍵暗号（利用モード） 共通鍵暗号の利用モードECB、CBC、CFB、OFB、CTRについてそれぞれの構造と特徴を学ぶ。講義の最後に簡単な演習を行う（iLearnあるいはMicrosoft Formsを活用する場合がある）。 準備：今回の講義内容を予習してくる。こと。 課題：今回の復習および次回の講義内容を予習。	
	6	メッセージ認証 メッセージの完全性(Integrity)を確認するメッセージ認証の仕組みと具体的な方式としてのMACを学ぶ。AL①。講義の最後に簡単な演習を行う（iLearnあるいはMicrosoft Formsを活用する場合がある）。 準備：今回の講義内容を予習してくる。こと。 課題：今回の復習および次回の講義内容を予習。	
	7	公開鍵暗号 公開鍵暗号について、鍵管理の効率と特徴について学び、木曾となる計算量理論と群について復習する。講義の最後に簡単な演習を行う（iLearnあるいはMicrosoft Formsを活用する場合がある）。 準備：今回の講義内容を予習してくる。こと。 課題：今回の復習および次回の講義内容を予習。	
	8	公開鍵暗号 有限体、公開鍵配送法のDiffie-Hellmann方式、代表的な公開鍵暗号であるRSAについて学ぶ。講義の最後に簡単な演習を行う（iLearnあるいはMicrosoft Formsを活用する場合がある）。 準備：今回の講義内容を予習してくる。こと。 課題：今回の復習および次回の講義内容を予習。	
	9	公開鍵暗号 RSA暗号を具体的な数値で計算して学ぶ。ユークリッド互助法、拡張ユークリッド互助法を学習する。講義の最後に簡単な演習を行う（iLearnあるいはMicrosoft Formsを活用する場合がある）。 AL①。 準備：今回の講義内容を予習してくる。こと。 課題：今回の復習および次回の講義内容を予習。	
	10	ハッシュ関数 ハッシュ関数について詳細を学ぶ。講義の最後に簡単な演習を行う（iLearnあるいはMicrosoft Formsを活用する場合がある）。 準備：今回の講義内容を予習してくる。こと。 課題：今回の復習および次回の講義内容を予習。	
	11	DH公開鍵配送法の具体例、Intruder In The Middle攻撃、ElGamal暗号 DHを具体的な数値で計算し手学ぶ。IITM攻撃の仕組みを学び、ElGamal暗号を学習する。講義の最後に簡単な演習を行う（iLearnあるいはMicrosoft Formsを活用する場合がある）。 準備：今回の講義内容を予習してくる。こと。 課題：今回の復習および次回の講義内容を予習。	

	12	デジタル署名 デジタル文書に対する署名機能を実現するデジタル署名について概念を学び、公開鍵暗号に基づくデジタル署名方式の特徴、RSA、ElGamal、DSAを学習する。安全性について学習する。講義の最後に簡単な演習を行う(iLearnあるいはMicrosoft Formsを活用する場合がある)。 準備：今回の講義内容を予習しておくこと。 課題：今回の復習および次回の講義内容を予習。
	13	ハイブリッド方式、公開鍵証明書、SSL/TLS、IPsec、IKE 共通鍵暗号と公開鍵暗号を組み合わせたハイブリッド方式、公開鍵暗号とその利用者の対応を保証する公開鍵証明書の概念と仕組み、具体的な暗号プロトコルのSSL/TLS、IPsec、IKEを学習する。講義の最後に簡単な演習を行う(iLearnあるいはMicrosoft Formsを活用する場合がある)。 準備：今回の講義内容を予習しておくこと。 課題：今回の復習および次回の講義内容を予習。
	14	IDに基づく暗号他 IDに基づく暗号、確定的暗号と確率的暗号、安全性定義と等価性、ゼロ知識証明について学ぶ。講義の最後に簡単な演習を行う(iLearnあるいはMicrosoft Formsを活用する場合がある)。 準備：今回の講義内容を予習しておくこと。 課題：今回の復習および次回の講義内容を予習。
	15	まとめ、総合演習 まとめ、総合演習を行う。
	16	準備：いままでの講義内容を復習しておくこと。 定期試験
授業形態	講義と演習 アクティブラーニング：①:5回, ②:0回, ③:0回, ④:0回, ⑤:0回, ⑥:0回	
達成目標	1) 暗号の考え方を理解できる 2) 共通鍵暗号の使い方を理解できる 3) 公開鍵暗号の仕組みを理解できる, 小さな数値で計算できる 4) 鍵配送法, デジタル署名の仕組みを理解できる, 小さな数値で計算できる 5) 暗号の応用について理解できる	
評価方法・フィードバック	演習・課題40% 定期試験60%の配点で評価する。講義中の演習については演習直後に回答と解説を行い、各回の最後に行う簡単な演習については次回の講義の最初に回答と解説を行う。課題(宿題)は採点して返却し、結果をフィードバックする。	
評価基準	100～90：秀, 89～80：優, 79～70：良, 69～60：可, 60未満：不可 達成目標の100～90%に到達した場合は秀, 達成目標の89～80%に到達した場合は優, 達成目標の79～70%に到達した場合は良, 達成目標の69～60%に到達した場合は可, 達成目標の59～0%に到達した場合は不可。	
教科書・参考書	教科書：指定しない。 参考書： 1 黒澤馨, 現代暗号への招待, サイエンス社, 2010年。 2 黒澤馨, 現代暗号の基礎数理, コロナ社, 2004年。	
履修条件	符号・暗号理論1の単位を修得していること。	
履修上の注意	演習, 課題(宿題), レポート等は必ず提出すること。	
準備学習と課題の内容	1回の講義につき2時間程度の予習・復習を行って授業にのぞむこと。予習として、授業計画の各内容に関して、参考書の該当する章を読むことあるいはインターネットで調べて準備することが望ましい。復習として、講義のスライドやノートを読み返して講義内容を理解し、参考書の該当する章を読むことあるいはインターネットで調べて理解を深めることが望ましい。演習や課題(宿題)を繰り返し解くことは有効な復習および試験対策になるため、講義内に理解が難しかった内容について複数の参考書などを参照して次回までに理解することを課題とする。	
ディプロマポリシーとの関連割合(必須)	知識・理解:40%, 思考・判断:40%, 関心・意欲:10%, 態度:5%, 技能・表現:5%	
DP1 知識・理解		
DP2 思考判断		
DP3 関心意欲		
DP4 態度		
DP5 技能・表現		