ナンバリング 科目名	現代暗号特論	担当者職 氏名	教授 星野　文学	単位数

授業概要とテーマ	暗号技術はICT社会を支える基盤技術であり、情報セキュリティのCIAつまり、機密性、完全性、可用性のうち、機密性と完全性を技術的に実現する。これらの技術は長年評価されても「破れていない」ということにより信頼を得られている「プリミティブ」と、プリミティブが安全だという仮定の上で数学的証明により安全だと証明された「帰着安全性」をもつ技術からなる。本講義では、まずは暗号技術により実現可能なことの概要を理解した後、いくつかの具体的な暗号プリミティブに関して、その設計、応用、安全性解析のエッセンスを解説する。
到達目標	情報通信技術において必要とされる専門的知識とそれらを応用する能力を養う為、具体的な暗号プリミティブの設計、応用、安全性解析について深く理解する事を目標とする。

授業計画 （主題/内容）		
1	ガイダンス、暗号技術の基礎（１）	One Time Pad を例として、暗号・認証の文法と機能、群の概念および暗号の安全性などについて紹介する。
2	暗号技術の基礎（２）	第１回に説明しきれなかった暗号・認証の文法と機能、体の概念および認証の安全性などについて紹介する。
3	離散対数問題	離散対数問題、Diffie-Hellman問題、準同型暗号、ペアリング等の概念を解説する。
4	離散対数問題等の応用	離散対数問題、ペアリング等を用いた暗号方式等を解説する。
5	暗号プロトコルの設計（１）	Schnorr 認証とその応用を解説する。
6	暗号プロトコルの設計（２）	ペアリングを用いた暗号プロトコルの設計を解説する。
7	その他の技法	小レポートの問題の解説、及びさまざまな技法を紹介する。
8	楕円曲線暗号	楕円曲線を用いた離散対数プリミティブの実装を紹介する。
9	楕円曲線上の有理関数	楕円曲線上の有理関数によるペアリングの実装を紹介する。
10	MOVリダクション	ペアリングを用いた楕円曲線暗号の攻撃を紹介する。
11	耐量子計算機暗号	耐量子計算機暗号に関する入門的な内容と最近の動向を紹介する。
12	格子に基づく暗号（１）	格子に基づく暗号の入門的な内容を紹介する。
13	格子に基づく暗号（２）	第１２回に説明しきれなかった格子に基づく暗号の話題について紹介する。
14	他の耐量子計算機暗号（１）	その他の耐量子計算機暗号について簡単に紹介する。
15	他の耐量子計算機暗号（２）	第１４回に説明しきれなかったその他の耐量子計算機暗号の話題について紹介する。
16	定期試験は実施しない	成績評価については「成績評価の方法」欄参照

成績評価の基準	A（秀）　･･･90～100点Ｂ（優）　･･･80～89点Ｃ（良）　･･･70～79点Ｄ（可）　･･･60～69点Ｆ（不可）･･･59点以下	成績評価の方法	平常点（授業への参加態度など）とレポート類（最終レポートまたは小テストなど）を総合的に勘案して評価する。
テキスト	なし		
参考文献	岡本龍明, 現代暗号の誕生と発展, 近代科学社, 2019, ISBN 978-4764905795, 縫田光司, 耐量子計算機暗号, 森北出版, 2020, ISBN 978-4627872110, 高木剛, 暗号と量子コンピュータ, オーム社, 2019, ISBN 978-4274224102		
科目のキーワード	公開鍵暗号、離散対数問題、ペアリングに基づく暗号、耐量子計算機暗号、格子に基づく暗号		
授業の特徴	現代的な公開鍵暗号のプリミティブに関して広く浅い知識が得られる		
関連科目	暗号技術, 暗号応用技術, 暗号数理特論		
履修上の注意等（履修条件等）	講義内容の専門性は比較的高い		