ナンバリング 科目名	暗号数理特論	担当者職 氏名	准教授 福光　正幸	単位数 2単位

授業概要とテーマ	暗号技術とこれを支える情報数理及び計算機科学を暗号数理という．本授業では，共通鍵暗号，公開鍵暗号，デジタル署名，ゼロ知識証明といった要素暗号技術を暗号数理の言葉で厳密に記述できるよう，また，正しく取り扱えるよう，教員が指導し，学生が自ら訓練する．
到達目標	要素暗号技術を暗号数理の言葉で厳密に記述できるようになる．また，正しく取り扱えるようになる．

授業計画 （主題/内容）		
1	ガイダンス／1.1 Introduction	履修上の留意点の説明／1.1 序論
2	1.1 Introduction	1.1 序論
3	1.2 Central Paradigm	1.2 主要な考え方
4	1.2 Central Paradigm	1.2 主要な考え方
5	1.3 Pseudorandomness	1.3 疑似ランダム
6	1.3 Pseudorandomness	1.3 疑似ランダム
7	1.4 Zero-Knowledge	1.4 ゼロ知識
8	1.4 Zero-Knowledge	1.4 ゼロ知識
9	1.5 Encryption	1.5 暗号
10	1.5 Encryption	1.5 暗号
11	1.6 Signatures	1.6 署名
12	1.6 Signatures	1.6 署名
13	1.7 Cryptographic Protocols	1.7 暗号プロトコル
14	1.7 Cryptographic Protocols	1.7 暗号プロトコル
15	補足・まとめ	補足・まとめ
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･･･80～100点 B･･･70～79点 C･･･60～69点 D･･･59点以下	成績評価の方法	提出したレポートの内容により評価を決める．

テキスト	Oded Goldreich: "Modern Cryptography, Probabilistic Proofs and Pseudorandomness," Springer, 1998.
参考文献	黒沢 馨, 尾形 わかは: 現代暗号の基礎数理 (電子情報通信レクチャーシリーズ), コロナ社, 2004. 中西 透: 現代暗号のしくみ ―共通鍵暗号,公開鍵暗号から高機能暗号まで― (共立スマートセレクション 12), 共立出版, 2017. （その他，授業中に必要に応じ提示）
科目のキーワード	チューリング機械，NP，対話証明，疑似ランダム性，確率的アルゴリズム，多項式時間，証明可能安全
授業の特徴	テキストに沿い，かつ，対話形式で講義を行う．
関連科目	学部授業『統計学』『情報理論』『暗号技術』『暗号応用技術』
履修上の注意等 （履修条件等）	学部授業『統計学』『情報理論』『暗号技術』『暗号応用技術』を履修合格済みあるいは同等の内容を勉強済みであることが望ましい．