3. 電気電子情報工学系　Electrical, Electronics and Computer Engineering Field			**EEC-F2**
授業科目名 Course Title	暗号学入門 Introduction to Cryptology	単位数 Credit	**2**
担当教員 Instructor	廣瀬　勝一 HIROSE Shoichi	開講学期 Semester	秋学期 Fall
キーワード Keywords	暗号，ディジタル署名，ハッシュ関数，認証 encryption, digital signature, hash function, authentication		

授業概要　Course summary

この授業は，現代暗号の入門であり，その数学的基礎に重点を置く．まず初めに，現代暗号の理解に必要な代数，整数論，確率論，計算理論に関する結果や定義について講義する．その後に，秘匿に関する暗号アルゴリズムである共通鍵暗号と公開鍵暗号について講義する．また，完全性に関する暗号アルゴリズムであるディジタル署名，ハッシュ関数，認証について講義する．

This is an introductory course of modern cryptology with some emphasis on its mathematical foundation. This course first gives necessary mathematical materials from algebra, number theory, probability theory, and computation theory. Then, it gives cryptographic algorithms for confidentiality such as symmetric encryption and asymmetric encryption. It also gives cryptographic algorithms for integrity such as digital signature, cryptographic hash function and authentication.

到達目標　Course goal

共通鍵暗号，公開鍵暗号，ディジタル署名，ハッシュ関数，認証の主な方式とその数学的基礎を理解する．
The goal of this course is to understand the schemes for symmetric key encryption, public key encryption, digital signature, hashing, and authentication, and their introductory mathematical foundations.

授業内容　Course description

整数論と代数学の初歩 (Elementary number theory and algebra): Euclidean algorithm, Euler's theorem, Group, Ring, Field
共通鍵暗号 (Symmetric key encryption): DES, AES, Modes of operation
公開鍵暗号 (Public key encryption): RSA, ElGamal, Diffie-Hellman key exchange
ディジタル署名 (Digital signature): RSA, ElGamal
ハッシュ関数 (Cryptographic hash function)
メッセージ認証 (Message authentication)

準備学習（予習・復習）等　Preparation / Review

予習および復習として，教科書を読み，章末の問題を解くこと．
Students are required to read the textbook and solve exercises in the textbook.

授業形式　Class style

講義
Lectures

成績評価の方法・基準　Method of evaluation

レポート
Reports

教科書・参考書等　Textbook and material
J. A. Buchmann, Introduction to Cryptography, 2nd ed., 2004, Springer.
受講要件・予備知識　Prerequisite
特になし None
その他の注意事項　Note
特になし None