授業科目名	暗号と情報セキュリティ						
英語名	Cryptography and Information Security						
担当教員名	宮地 充子						
配当学年	1・2 年	単位数	2	開講期	前期	曜時限	
授業種別・ 授業形態	専攻専門科目 講義，演習			授業言語	日本語		

【授業の概要・目的】

情報セキュリティの種々の方式について、その理論的概念を理解するとともに，ISO などで国際規格化されている具体的なアルゴリズムについて紹介すると，それらアルゴリズムに対する最先端の安全性解析・性能などの研究成果について講義する．

具体的には，公開鍵暗号，ディジタル署名の理論的概念とともに，具体的な方式として，ISO で規格化されている DSA 署名，楕円曲線暗号などのアルゴリズムについて紹介する．

【授業計画と内容】

1. 群・環・体
2. 剰余環と有限体
3. ユークリッドの互除法
4. 安全性の定義（頑強性，識別不可能性，強秘匿性）
5. エルガマル暗号
6. エルガマル暗号の解読
7. RSA 暗号
8. RSA 暗号の解読
9. より安全な暗号へ -RSA-OAEP-
10. ディジタル署名の安全性のモデル
11. DSA 署名
12. 楕円曲線
13. 楕円曲線上の暗号と有限体上の暗号の関係
14. ECDH 鍵共有法，計算 DDH 問題
15. 演習

【履修要件】

離散数学に関する基礎知識

【成績評価の方法・基準】

レポート，出席点で評価

【教科書】
宮地充子，菊池浩明編「IT Text 情報セキュリティ」，オーム社
【参考書等】
特になし
【その他（授業外学習の指示・オフィスアワー等）】
TA-miyaji10@aqua.jaist.ac.jp

Course Title	Cryptography and Information Security						
Instructor(s)	Atsuko Miyaji						
Assigned Grade	1･2	Units	2	Semester	Spring semester	Time	
Course Category & Course Type	専攻専門科目 Lecture			Language	Japanese		

Course Description (overview, purpose)

The main objective of this course is to introduce information security and cryptology. In particular, the course focuses on mathematical principles and methodologies to construct concrete cryptosystems, and presents the newest theoretical and implemental analysis of these cryptosystems.

The following issues are emphasized: public key cryptosystem, digital signature, and elliptic curve cryptosystems. Concrete schemes dealt with in this course include schemes standardized in ISO/IEC.

Course Schedule

1. Group, Ring, Field
2. Residue Ring, Finite Field
3. Euclidean Algorithm
4. Security Definition of Encryption
5. ElGamal Encryption
6. Security Analysis on ElGamal Encryption
7. RSA
8. Security Analysis on RSA
9. Security Enhanced Encryption
10. Security Definition of Signature
11. DSA Signature
12. Elliptic Curve
13. Relation Between DLP and ECDLP
14. ECDH-Key Agreement.
15. Exercise

Prerequisites and Course Requirements

Basic knowledge on Discrete Mathematics

Grading Methods and Evaluation Criteria

Report, attendance
Textbooks
宮地充子，菊池浩明編「IT Text 情報セキュリティ」，オーム社
References
N/A
Miscellaneous (homework assignment, office hours etc.)
TA-miyaji10@aqua.jaist.ac.jp