6.4 セキュリティ基盤技術

[開講科目名]

(授業科目)離散数学と計算の理論／(enPiT-Pro)セキュリティ基盤技術

[開講科目名(英)]

Discrete Mathematics and Theory of Computation

[単位数] 2 単位

[開講日]

大阪大学吹田キャンパス E1-115, E1-217 水曜 5,6 限

第 1 回 4/10(水)

第 2 回 4/17(水)

第 3 回 4/24(水)

第 4 回 5/8(水)

第 5 回 5/15(水)

第 6 回 5/22(水)

第 7 回 5/29(水)

第 8 回 6/5(水)

第 9 回 6/12(水)

第 10 回 6/19(水)

第 11 回 6/26(水)

第 12 回 7/3(水)

第 13 回 7/10(水)

第 14 回 7/17(水)

第 15 回 7/24(水)

第 16 回 7/31(水) 試験

[担当教員]

宮地 充子(大阪大学), 河内 亮周(大阪大学)

[授業の目的・概要]

(1)情報セキュリティにおいて必要となる離散的な構造に対する数学的諸概念や考え方に習熟し, 数学の各種定理を応用する方法について理解すること, 及び

(2)情報セキュリティ技術の数理的基盤である計算の理論における重要概念を修得し, その理論を情報セキュリティ技術へ応用する方法を学ぶことを目的とする.

［授業の目標］

(1)離散的な構造に対する数学的諸概念として，群，環，体，初等整数論の概念を理解するとともに，各種数論的アルゴリズムを習熟し，それらの情報セキュリティへの応用方法を習得すること，及び

(2)計算を数理科学的に議論するための計算モデル(Turing 機械，論理回路)の概要を理解し，計算モデルに基づいて情報セキュリティ技術の基盤概念(一方向性関数，疑似乱数生成器等)の定式化に応用することを目標とする.

［講義計画］

【第 1 回 群(1)】

知識単位：群の公理，部分群

【第 2 回 群(2)】

知識単位：剰余類（Lagrange の定理），正規部分群，剰余群

【第 3 回 環】

知識単位：環の公理，準同形写像（準同形定理），環の公理，イデアル

【第 4 回 環・体】

知識単位：Euclid 環，体，有限体

【第 5 回 整数論(1)】

知識単位：素数，除法の原理，Euclid の互除法

【第 6 回 整数論(2)】

知識単位：不定方程式，合同式，中国人の剰余定理，平方剰余記号

【第 7 回 総合課題】

知識単位：代数学，初等整数論，数論アルゴリズム

【第 8 回 中間試験】

【第 9 回 コンピュータの数理モデル】

知識単位：Turing 機械，論理回路，計算不能性

【第 10 回 P 対 NP 予想と計算量クラス】

知識単位：クラス P，クラス NP, NP 完全問題

【第 11 回 乱択計算】

知識単位：クラス RP，クラス BPP，クラス ZPP

【第 12 回 いかに問題の困難さを比較するか】

知識単位：帰着アルゴリズム，計算量仮定

【第 13 回 平均な計算困難さと暗号構成要素】

知識単位：Impagliazzo の五つの世界，一方向性関数，一方向性置換，落とし戸一方向性置換

【第 14 回 暗号理論における疑似乱数】

知識単位：疑似乱数生成器，識別不可能性

【第 15 回 対話型証明システム・ゼロ知識証明システム】

知識単位：クラス MA，クラス AM，対話型証明システム，ゼロ知識証明システム，模倣可能性

【第 16 回 まとめ】

［教科書・教材］

1. 宮地充子著，「代数学から学ぶ暗号理論」，日本評論社
2. Sanjeev Arora and Boaz Barak, ″Computational Complexity: A Modern Approach, Cambridge University Press

［成績評価］

【評価の観点】情報セキュリティに必要な基礎知識及びセキュリティの理解度による.

【評価方法】 中間試験(40%)及びレポート成績(60%)