6.3 実践情報セキュリティとアルゴリズム

[開講科目名]

実践情報セキュリティとアルゴリズム

[開講科目名(英)]

Practical Information Security and Algorithms

[単位数] 2 単位

[開講日]

大阪大学吹田キャンパス E1-115 又は E1-217 水曜 5,6 限

第 1 回 10/2(水)

第 2 回 10/9(水)

第 3 回 10/16(水)

第 4 回 10/23(水)

第 5 回 10/30(水)

第 6 回 11/6(水)

第 7 回 11/13(水)

第 8 回 11/20(水)

第 9 回 11/27(水)

第 10 回 12/4(水)

第 11 回 12/11(水)

第 12 回 12/18(水)

補講日 12/25(水)

第 13 回 1/8(水)

第 14 回 1/15(水)

第 15 回 1/22(水)

第 16 回 1/29(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) RFID タグや携帯端末等, IoT 機器におけるデータ秘匿やデータの偽造を防ぐ技術として脚光を浴びている楕円曲線暗号について解説するとともに, その実装も行う. 応用編では, セキュリティが利用・導入されているシステム, 製品の課題等を学び, セキュアシステム設計に必要な脅威分析, 運用や実装について概観する. 具体的には, システム管理保護技術, サイバーセキュリティ, OS アクセス制御, PKI の仕組みについて理解する.

(2) 現代のアルゴリズムにおいて必要不可欠となった計算に乱数を活用する乱択アルゴリズムについて学習する. 特にその基本的な設計技術および確率的な解析手法を学ぶ.

［授業の目標］

(1) 暗号理論と情報セキュリティの基盤技術およびその構成要素を理解し，暗号理論と情報セキュリティを応用するアプリケーションと適切な実装や応用ができるようになる.

(2) 確率的な振る舞いを効果的に利用したアルゴリズムの設計手法を修得する. またアルゴリズムを確率的解析によって効率性・正当性を分析する手法を修得する.

［講義計画］

【第 1 回 公開鍵暗号の基礎知識】

公開鍵暗号の基礎知識である離散数学及び初等整数論について理解する. ユークリッドの互除法，拡張ユークリッドの互除法，中国人の剰余定理，べき演算など.

知識単位：ユークリッドの互除法，拡張ユークリッドの互除法，中国人の剰余定理，べき演算

【第 2 回 python の利用方法】

数式処理ソフト python の利用方法，及び python を用いた離散数学，暗号処理，暗号解析の実装のために必要な方法を習得する.

【第 3 回 公開鍵暗号】

情報セキュリティの理論で最も重要な技術の一つである公開鍵暗号は現代暗号理論の基本概念であるとともに，秘匿・完全性・可用性を実現する情報セキュリティの基本概念である. 公開鍵暗号の基本原理及び TLS などで利用される具体的な公開鍵暗号について紹介するとともに，その安全性の概念及び効率などの指標について紹介する.

知識単位：公開鍵暗号，安全性

【第 4 回代数アルゴリズムと暗号実装】

離散数学の演習，実装方法について理解する. さらに，公開鍵暗号の演習，実装方法について解説する. さらに，数論などの理論の応用方法及びとその改良可能性について紹介する. 実装アルゴリズムは，ユークリッドの互除法，拡張ユークリッドの互除法，中国人の剰余定理，べき演算など，ElGamal 暗号他.

【第 5 回 楕円曲線暗号】

情報セキュリティの理論で最も重要な技術の一つである公開鍵暗号の中で最も脚光を浴びているのが楕円曲線暗号である. 本講義では，楕円曲線暗号の安全性，特徴，他の公開鍵暗号との違いを含めて解説する.

知識単位：公開鍵暗号，安全性，楕円曲線暗号

【第 6 回 ディジタル署名】

情報セキュリティの理論で最も重要な技術の一つであるディジタル署名は電子署名法を支える技術であるとともにディジタル認証に利用される基本技術である. 本講義ではディジタル署名の基本原理の基本原理及び TLS などで利用される具体的なディジタル署名について紹介するとともに，その安全性の概念及び効率などの指標について紹介する.

知識単位：ディジタル署名，安全性

【第 7 回 ハイブリッド暗号】

これまで講義した公開鍵暗号・ディジタル署名を用いて，実際にデータ秘匿・完全性を実現する方法について紹介するとともに，その安全性の概念及び効率などの指標について紹介する.

知識単位：ハイブリッド暗号，ディジタル署名，公開鍵暗号，安全性，楕円曲線暗号

【第 8 回 ハイブリッド暗号の実装】

公開鍵暗号とディジタル署名，共通鍵暗号を組み合わせたハイブリッド暗号を実際に実装することでその仕組みについて理解する． さらに実装を通して，公開鍵暗号の運用時の問題点について，理解する.

【第 9 回 確率論の基本とアルゴリズム応用】

確率論の基本を復習し，それをアルゴリズムにどのように応用するのかを，多項式等価性判定や行列積検証などの確率解析の具体的例を通じて学ぶ.

知識単位：確率，事象，分布，和集合上界，多項式等価性判定，行列積検証

【第 10 回 離散事象と期待値】

期待値や条件付き期待値，幾何分布や二項分布といったアルゴリズムの確率解析で頻繁に利用する確率論の概念について乱択ソートアルゴリズムの例などを用いて学ぶ.

知識単位：期待値，幾何分布，二項分布，クイックソート

【第 11 回 モーメントと偏差】

Markov の不等式や Chebyshev の不等式といった確率変数のモーメントから得られる不等式を学び，それらをどのようにアルゴリズムの確率的解析に応用するかを乱択アルゴリズムにおける典型的な問題であるクーポン集め問題を通じて修得する.

知識単位：Markov の不等式，Chebyshev の不等式，モーメント，クーポン集め問題

【第 12 回 Chernoff 限界】

乱択アルゴリズムの確率解析で最も重要な不等式である Chernoff 限界について学び，乱択アルゴリズムの成功確率を増幅する技法である多数決法の効率を Chernoff 限界によって解析する.

知識単位：Chernoff 限界，成功確率増幅，多数決法

【第 13 回 ボールとビンのモデル】

情報セキュリティでも確率解析の基本として現れる誕生日のパラドクスをボールとビンのモデルと呼ばれる乱択アルゴリズムの確率解析のための単純なモデルで解析する方法を修得する.

知識単位：誕生日のパラドクス，ボールとビンのモデル

【第 14 回 確率的論法】

アルゴリズムの基本的解析手法である数え上げ法を確率的に一般化した確率的論法について学び，アルゴリズムから乱択性を取り除く応用例について学ぶ.

知識単位：数え上げ法，確率論法，期待値法，脱乱択化

【第 15 回 Markov 連鎖とランダムウォーク】

Markov 連鎖と呼ばれる基本的な確率過程を学び，充足可能性問題と呼ばれる重要な問題に対して Markov 連鎖に基づくランダムウォークアルゴリズムの設計とその解析を行う.

知識単位：Markov 連鎖，ランダムウォーク，2SAT，3SAT

［履修条件・受講条件］

情報セキュリティ演習の課題は行っておくこと.

教育システムで提供される反復課題を行うことで，理解を深めること.

［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. 宮地充子，菊池浩明編「IT Text 情報セキュリティ」，オーム社
3. Michael Mitzenmacher ・Eli Upfal 著・小柴 健史・河内 亮周訳，「確率と計算—乱択アルゴリズムと確率的解析—」，共立出版

［参考文献］

Michael Mitzenmaher and Eli Upfal, Probability and Computing: Randomization and Probabilistic Techniques in Algorithms and Data Analysis, Cambridge University Press

［成績評価］

【評価の観点】応用数理の理解度および応用力による

【評価方法】課題・レポート提出の結果による

【評価基準】暗号応用の評価(40%)，暗号理論の評価(60%)