| 科目名 | 情報数学 | 英文表記 | Information Mathematics | 平成23年度3月 |
|---|---|---|---|---|
| 科目コード | 6304 | | | |
| 教員名：玉城史朗<br>技術職員名： | | | | 作成 |

| 対象学科／専攻コース | 学年 | 必・選 | 履修・学修 | 単位数 | 授業形態 | 授業期間 |
|---|---|---|---|---|---|---|
| 創造システム工学専攻・情報工学コース | 専1 | 選 | 学修 | 2単位 | 講義 | 前期 |

| 目標及び評価方法 | 目標項目 | 評価方法及びその割合 |
|---|---|---|
| | 整数論を修得する。特に有限体を理解する。 | 演習問題を通じて、理解度を図る。10% |
| | 符号理論の基礎を修得する。 | ハミング距離、ハミング符号、シンドロームを理解する。試験で評価する。20% |
| | 公開鍵暗号の基礎を理解する。 | オイラー関数、フェルマーの定理を理解する。試験で評価する。20% |
| | 集合演算の公理を理解する。 | レポートで評価する。10% |
| | 関係データベースを理解する。 | 関係データベースの構造、操作、更新の意味を理解する。演習問題で評価する。10% |
| | 最適化、線形計画法の基礎を修得する。 | 試験問題で評価する。20%。 |
| | | |

| 高専目標 | 1 | 2 | 3 | 4 | JABEEプログラム名称 | メディア情報工学 |
|---|---|---|---|---|---|---|
| | | | | | JABEEプログラム教育目標 | |

| 授業概要、方針、履修上の注意 | |
|---|---|
| | 本講義では、まず、整数論の基礎概念（合同の概念、合同方程式）を学んだ上で、その美しい応用である、符号理論、及び、暗号理論の基礎を講義する。ここでは、特に、ハミング距離、ハミング符号を学んだ上で、シンドロームの概念を導入し、誤り訂正機構の説明を行う。次に、暗号理論では、従来の暗号法を概説した後、公開鍵暗号の数学的構成を明らかにする。すなわち、素因数分解、オイラー関数、オイラーの定理、フェルマーの小定理を導入して、公開鍵暗号における暗号化、符号化法とその数学的構造を明らかにする。また、関係データベースでは、集合演算の公理から始めて、関係代数、関係データベースの構造について説明する。最後に最適化法、線形計画法の概説を行う。毎週、課題を出して、各自、翌週の講義時間に解答を行わせるのでしっかり予習・復習を行うこと。 |

| 教科書・教材 | |
|---|---|
| | 情報数学の基礎、寺田他著、サイエンス社、 |

**授　業　計　画**

| 回次 | 授　業　項　目 | 時間 | 授　業　内　容 | 予　習　項　目 |
|---|---|---|---|---|
| 1 | 本講義の概説 | 2 | 情報数学を鳥瞰する。 | 情報数学の概念を調べる。 |
| 2 | 整数論入門 | 2 | 整数の理論、最大公約数、最小公倍数 | 公約数、公倍数をの求め方。 |
| 3 | ユークリッド互除法 | 2 | ユークリッド互除法の使い方 | ユークリッド互除法演習 |
| 4 | 最大公約数と不定方程式 | 2 | 最大公約数と不定方程式の構造 | 不定方程式演習 |
| 5 | 合同式と合同方程式 | 2 | 合同方程式演習 | 合同方程式の性質 |
| 6 | ハミング距離、ハミング符号 | 2 | ハミング距離、ハミング符号の概念 | 符号理論の性質 |
| 7 | BCH符号概説 | 2 | BCH符号の数学的構造 | BCH符号の性質 |
| 8 | 暗号理論概説 | 2 | 暗号理論の概説とオイラー関数、オイラーの定理 | 暗号とは |
| 9 | 公開鍵暗号の数学的構造 | 2 | 例題による公開鍵暗号アルゴリズムの説明 | 公開鍵暗号の一方向性 |
| 10 | 集合論と集合代数 | 2 | 集合代数と集合演算 | 集合演算問題 |
| 11 | 関係データベース | 2 | 関係データベースの構造 | 関係データベースとは |
| 12 | 最適化法 | 2 | 最適化の概念と目的関数 | 最適化の性質 |
| 13 | 最急降下法 | 2 | 最急降下法の原理とその計算法 | 最急降下法の性質 |
| 14 | 線形計画法 | 2 | 線形計画法概説 | 線形計画法の性質 |
| 15 | シンプレックス法 | 2 | シンプレックス法による問題の解法 | 解法の演算 |
| | 前学期期末試験 | | | |
| | 学習時間合計 | 30 | 実時間 | 25 |

**学修単位における自学自習時間の保証（レポート頻度など）** 10

Alt+Enterで改行

学習時間は、実時間ではなく単位時間で記入する。（５０分＝１、１００分＝２）