塩田研究室

２０１９年１０月

◇ **指導教員の専門分野**

塩田は学生時代は整数論を専攻し、５０年間解けていなかった問題を解決したりして博士号を取りました。プログラミング能力を買われて 1990 年に情報科学科に職を得てからは、数学に基づく情報技術

公開鍵暗号　誤り訂正符号　数値計算　アルゴリズム　離散数学

等の研究に進出しています。

◇ **ゼミの研究分野**

ゼミでは公開鍵暗号の理論からテーマを選ぶことが多いです。最先端の理論は相当難しいので、学部段階では、RSA 暗号や楕円曲線暗号などの基本的な暗号に関わるプログラムを実際に組んで

仕組みを理解して、本当に使えるものを、自信をもって作る

体験をしてもらっています。

修士課程では楕円曲線暗号の発展形であるペアリング暗号などの研究を行っています。

◇ **ゼミで勉強すること**（塩田研究室に限らず）

学生の間に身につけた知識だけで一生生きて行ける人はいません。たとえば塩田研究室の卒業生で暗号分野に就職した人はほとんどいません。就職先ではそれぞれに新しい分野の勉強をしているはずです。ゼミの勉強で大事なことは、

勉強のやり方を覚える

ことです。勉強のやり方を覚えるために、まずは興味の持てる分野を選ぶこと、それが研究室配属です。

◇ ホームページ

研究室のページの「卒業生・論文題目」、「修士論文の概要」、「ゼミの履歴」、教員のページの「研究分野」などが参考になると思います。教員のページには研究室訪問可能な時間帯も掲載しておきます。

http://lupus.is.kochi-u.ac.jp/shiota/

◇ **教員研究室**：512 号室 / **学生研究室**：504・404 号室