JAIST
JAPAN ADVANCED INSTITUTE OF SCIENCE AND TECHNOLOGY 1990

北陸先端科学技術大学院大学サマースクール 2012

2012.08.03（金）～08.06（月）

～情報セキュリティ～

情報科学研究科　教授　宮地（みやじ） 充子（あつこ）

スマートフォンやソーシャルネットワークの普及に伴い、誰もが容易に情報を発信・入手できるという、新しいコミュニケーション手段が広がっています。誰もが対等に情報発信できることはとても便利なことです。しかしその一方で、自分が望まないデータが第三者に渡るという事件も起こっています。つまり、新しいコミュニケーション手段の普及には、自分のデータを主体的に保護あるいは活用することが必要です。データの保護、活用に必要不可欠な技術が情報セキュリティ技術です。情報セキュリティ技術はEdyなどの電子現金、SuicaなどのIC切符、高速道路の自動料金システム等を支える先端技術です。

本コースでは情報セキュリティ技術を紹介するとともに，その基盤となる数学の知識である初等整数論、暗号方式の仕組みを解説し，計算機を用いて実際に利用される暗号ソフトを実装します。暗号実装を用いて，基礎科学である数学がどのようにアプリケーションである暗号に利用されるのかを体験的に習得します。なお，プログラム初心者でも安心して受講できるように，研究室の学生がサポートします。

■講師略歴

1998年　北陸先端科学技術大学院大学情報科学研究科　准教授
2007年～北陸先端科学技術大学院大学情報科学研究科　教授
2008年～北陸先端科学技術大学院大学　附属図書館長
2012年～北陸先端科学技術大学院大学　特別学長補佐
著書「代数学から学ぶ暗号理論」（日本評論社）

■開催日程：８月３日（日）～８月６日（火）の４日間！！
３日（金）１３：３０～１７：００，４日（土）９：３０～１７：００
５日（日）　９：３０～１７：００，６日（月）９：３０～１２：００

■開催場所：北陸先端科学技術大学院大学　情報科学研究科

■対 象 者：大学院生（修士課程），学部４年生、社会人

■定　　員：７名（募集締切：７月１０日（火）１７：００）

■参 加 費：無料（ただし，旅費及び宿泊費は本人負担）

■宿泊施設：サマースクール開催に際して，本学に隣接の石川ハイテク交流センターを斡旋しています。宿泊を希望される方は，部屋タイプの第１，第２希望及び宿泊日を明記の上，お申込みください。なお，部屋数に限りがありますので，ご希望に添えない場合がありますことをあらかじめご了承ください。
【１泊料金（お一人様朝食付[税込]】シングル：4,330円
ツイン：5,250円（１名利用），4,060円（２名利用）

■申込方法：参加希望の方は、氏名（ふりがな）、生年月日、学校（勤務先）名，学生の方は指導教員名、参加動機，書類送付先住所，電話番号，メールアドレス，宿泊希望の有無（部屋タイプ，宿泊日数）を明記の上，郵送，ＦＡＸ又はメールにてお申込みください。

■交通手段：本学へは，金沢駅からＪＲ，北陸鉄道，大学シャトルバスを乗り継ぐ方法が便利です。（所要時間：約１時間）詳細は，下記ホームページでご確認ください。
http://www.jaist.ac.jp/~kouhou/General_info/access/access.html

■本件に関する問合せ／申込み先：923-1292　石川県能美市旭台1-1
北陸先端科学技術大学院大学　学術協力課　学術助成係
TEL:0761-51-1894　FAX:0761-51-1919　E-mail:josei@jaist.ac.jp

～プログラム（予定）～

２０１２．８．３ (金) １３：３０～２０１２．８．６ (月) １２：００

8/3　１３：３０～１７：００

１３：３０～１４：３０　講義１．暗号の原理：暗号の実用例，共通鍵暗号，公開鍵暗号
１５：００～１７：００　演習０．Pythonの基本的な使い方

8/4　９：３０～１７：００

９：３０～１１：００　演習１．Pythonの関数・プログラミング
１１：３０～１２：３０　講義２．暗号の基礎となる整数論及び必要なアルゴリズムの紹介I
---昼休み---
１３：３０～１５：３０　演習２．有限体の基本アルゴリズムの構築
１６：００～１７：００　講義３．ElGamal暗号の紹介・暗号の基礎となる整数論及び必要なアルゴリズムの紹介II

8/5　９：３０～１７：００

９：３０～１０：３０　演習３．ElGamal暗号の構成
１１：００～１２：００　講義４．楕円曲線
講義５．楕円曲線暗号
---昼休み---
１３：００～１５：３０　演習４．楕円曲線のアルゴリズムの構築
演習５．楕円曲線暗号の構築
１６：００～１７：００　講義６．楕円曲線の加法公式
１８：００～　打ち上げ：受講生の皆様と宮地研究室のメンバで打ち上げ！大学院大学の研究環境を実感！

8/6　９：３０～１２：００

９：３０～１０：３０　演習６．楕円曲線の加法公式
１１：００～１２：００　まとめ及びClosing Ceremony

サマースクールホームページ
https://grampus.jaist.ac.jp/miyaji-lab/index-jp.html