北陸先端科学技術大学院大学サマースクール 2013

2013.08.2（金）～08.05（月）

～情報セキュリティ～

情報科学研究科　教授　宮地 充子（みやじ あつこ）

高度情報通信ネットワーク社会において，情報セキュリティ技術は私達の生活に不可欠な技術となりました。情報セキュリティ技術はデータの秘匿やデータの信頼性確保からユーザのプライバシー保護を実現する基盤技術であるだけでなく，現在，様々なアプリケーションで利用されています。セキュアなインターネット通信を実現する TLS（Transport Layer Security），キャッシュレス社会を実現する Edy や Suica などの電子現金や ICカード乗車券，高速道路の自動料金システム ETC，ペーパレスを実現する飛行機の e-チケット等のアプリケーションも情報セキュリティ技術が実現するアプリケーションです。

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。

理論を学ぶだけでなく自分で実装することで，より理解を深めるとともに，数学がどのようにセキュリティに応用されているかを体験することができます。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

2007年～現在：北陸先端科学技術大学院大学情報科学研究科　教授
2008年～現在：北陸先端科学技術大学院大学　附属図書館長
2012年～現在：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２日（金）～８月５日（月）の４日間！！
２日（金） 13：30～17：00，３日（土）9：30～17：00
４日（日）　9：30～19：00，５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（定員になり次第，募集を締め切らせていただきます）

■ 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：氏名（ふりがな），学校（勤務先）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）ＦＡＸ又はメールにてお申込ください。

■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）

8/2(金)	13:00-17:00
	自己紹介(講師 及びインストラクタ)
講義1	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
演習0	mathematica の基本的な使い方

8/3(土)	09:30-17:00
演習1	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
講義2	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
	昼休み
演習2	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
講義3	楕円曲線のアルゴリズム

8/4(日)	09:30-19:00
演習3	楕円曲線のアルゴリズム
講義4	楕円曲線暗号
	昼休み
演習4	楕円曲線暗号
講義，演習5	ハイブリッド暗号
講義，演習6	楕円曲線構築
打ち上げ	宮地研究室の皆と夕食を食べて，大学院大学の研究環境を実感！

8/5(月)	09:30-12:00
演習5	ハイブリッド暗号の構築
演習6	楕円曲線構築
	まとめ

サマースクールホームページ

https://grampus.jaist.ac.jp/miyaji-lab/activity/summerschool/index-jp.html