応用数学６

2010 年度, 後期, 木曜日 1 時限 (9:00 – 10:30), 教室 14 – 502

担当教官

安永 憲司 (Kenji Yasunaga), 所属: 東京工業大学 数理・計算科学専攻, email: yasunaga (at) is.titech.ac.jp

概要

通信を行うとき，その内容を他者にわからないように秘匿したいときがある．秘匿通信など，他者に対する安全性を確保するための仕組みを数学的に扱うのが暗号理論である．本講では，秘匿通信問題において，どのような設定でどのような安全性をもつ秘匿通信が可能なのか，また，安全性はどのように定式化すべきなのかについて理解することを目的とする．特に，現代暗号における重要な考え方である，「敵は効率的な計算しか出来ないという仮定のもとで，安全性を証明する」ことを行っていく．

教科書

特になし．

講義資料

講義資料を教科書の代わりとして使用します．講義資料は，こちらで準備して授業中に渡しますが，以下のページにもアップロードするので，必要なときは利用してください．

`http://www.is.titech.ac.jp/~yasunaga/appmath6/index.html`

参考文献

講義資料は以下の資料を参考にしています．

- Rafael Pass の Cornell University での講義ノート (2009 年)
  `http://www.cs.cornell.edu/courses/cs4830/2010fa/` (授業ページ)
  `http://www.cs.cornell.edu/courses/cs4830/2010fa/lecnotes.pdf` (講義ノート)
- Yevgeniy Dodis の New York University での講義ノート (2008 年)
  `http://www.cs.nyu.edu/courses/fall08/G22.3210-001/index.html` (授業ページ)
  `http://cs.nyu.edu/courses/fall08/G22.3210-001/syllabus.html` (講義ノート)
- Salil Vadhan の Harvard University での講義ノート (2006 年)
  `http://people.seas.harvard.edu/~salil/cs120/` (授業ページ)
  `http://people.seas.harvard.edu/~salil/cs120/handouts.html` (講義ノート)

参考となる書籍としては以下をあげます．

- 黒澤 馨, 現代暗号への招待.
- Hans Delfs, Helmut Knebl, 暗号と確率的アルゴリズム入門—数学理論と応用.
- Jonathan Katz, Yehuda Lindell, Introduction to Modern Cryptography.
- Oded Goldreich, Foundations of Cryptography, volume I, (Basic Tools).
- Oded Goldreich, Foundations of Cryptography, volume II, (Basic Applications).

小テスト

授業の中で数回（予定では 4 回），小テストを行います．小テストを行う日は，通常の授業に加え，小テストとその解説を行います．小テストでは，ノートや本を見ても構いません．

小テストの内容も，テスト終了後に，http://www.is.titech.ac.jp/~yasunaga/appmath6/index.html にアップロードする予定です．

期末試験

最終授業の日に期末試験を行います．期末試験でのノートや本の持ち込みについては，試験前に連絡します．

評価

小テストと期末試験で評価します．最終的な評価では，小テスト分が 40%，期末試験分が 60% の割合を占めます．

スケジュール

公開されているシラバスから少し変更しています．内容はほとんど変わっていません．

9/30　第 1 回: ガイダンス，秘匿通信問題の導入，現代暗号の考え方
10/7　第 2 回: Shannon による安全性の定式化，完全秘匿性，使い捨て鍵暗号
10/14　第 3 回: **小テスト**，Shannon の定理
10/21　休講（創立記念日）
10/28　第 4 回: 計算能力に制限のある敵，一方向性関数
11/4　第 5 回: 一方向性関数（続き）
11/11　第 6 回: **小テスト**，計算量的識別不能性
11/18　第 7 回: 擬似ランダム分布
11/25　第 8 回: 擬似乱数生成器，ハードコアビット
12/2　休講（出張）
12/9　第 9 回: **小テスト**，秘密鍵暗号方式，一方向安全性，識別不能安全性
12/16　第 10 回: より強い攻撃（選択平文攻撃，選択暗号文攻撃）
12/23　冬期休業
12/30　冬期休業
1/6　第 11 回: 公開鍵暗号方式
1/13　第 12 回: **小テスト**，零知識安全性
1/20　第 13 回: Diffie-Hellman 鍵交換，ElGamal 暗号
1/27　休講（出張）
2/3　第 14 回: **期末試験**

上記はあくまで予定であり，予定が変更となる場合があります．その際は，随時連絡します．