650.470: Basics of Applied Cryptography and Network Security

Sujata Garera

Cryptography is an important tool used to protect information and communication channels. Cryptography is necessary to provide both integrity and confidentiality of data exchanged in a communication network.

This course will cover some key aspects of applied cryptography. The course will provide an overview of some early systems in cryptography such as substitution and permutation ciphers. The course will further provide a thorough understanding of recent topics in applied cryptography. Topics include algorithms for encryption and decryption using symmetric key and public key techniques, design and analysis of block and stream ciphers, pseudo-random number generation, hash functions and their uses, message authentication codes, authentication protocols, key establishment, key management, digital signatures and secret sharing. Students will understand how cryptosystems are designed and analysed along with specific applications of cryptography.

Course Information

This course is for both advanced undergraduate and graduate level students.

Prerequisites

Students are expected to enter this course with basic knowledge on Number Theory, Discrete Math and Algorithms.

Grading

Grades will be determined as follows

- Final: 30%
- Midterm: 25%
- In Class Assignments: 20%
- Take Home Assignments: 20%
- Participation and Suprise Quizzes 5%

Assignments are due at the beginning of class on the stated due date. Late submissions of take home assignments will be penalized 10% points per day. No collaboration is allowed on assignments unless otherwise stated. In class assignments must be submitted within the allocated class time. No collaboration is allowed on exams.

Academic Integrity

Academic Integrity and Ethical behavior are required in this course, as it is in all courses at Johns Hopkins University. Here is the link for academic integrity in the Department of Computer Science http://www.cs.jhu.edu/integrity-code/.

Lecture Timings

Tuesday, Wednesday 3-4:15pm Wyman Park Conference Room

Office Hours

After class on Wednesday from 4:30-5:30pm in Office 420 and you can meet me by appointment. Email me at sgarera@cs.jhu.edu .

Teaching Assistant

TBA

Textbooks

Recommended textbooks for this course are

- Cryptography and Network Security, Principles and Practices by William Stallings
- Handbook of Applied Cryptography by Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, available online at `http://www.cacr.math.uwaterloo.ca/hac/`

Syllabus

These may be subject to change as the course proceeds

Unit 1: Introduction

Computer security definitions and aspects (confidentiality, integrity, authentication, access control, availability, privacy), basic terminology, cryptographic system, classical cryptography, substitution and transposition techniques, statistical attacks, cryptanalysis

Suggested Reading:

- Chapter 2 from Stallings

Unit 2: Block Ciphers and Stream Ciphers

Modes of operation (ECB, CBC, CFB, OFB), multiple encryption, DES, Triple-DES, DES-X, AES, stream ciphers, RC4

Suggested Reading:

- Chapter 3,5,6 from Stallings
- Attacks on RC4 and WEP, Fluhrer, Mantin and Shamir, Cryptobytes 2002, available at `http://www.wisdom.weizmann.ac.il/~itsik/RC4/Papers/rc4_wep.ps`
- The Security of DES-X, Phillip Rogaway, Cryptobytes 1996, available at `http://www.cs.ucdavis.edu/~rogaway/papers/cryptobytes.ps`

Unit 3: Random Number Generation

Random and pseudorandom bit generation, statistical tests of randomness (chi-square statistic, frequency test, runs test, serial test, maurer's universal test),cryptographically secure pseudo-random bit generators

Suggested Reading:

- Chapter 5 from the Handbook
- Cryptanalytic Attacks on Pseudorandom Number Generators, John Kelsey, Bruce Schneier, David Wagner and Chris Hall, available at `http://www.schneier.com/paper-prngs.html`

Unit 4: Hash Functions and MAC

Properties of hash functions, standard hash functions MD5, SHA-1, birthday attack, unkeyed hash functions, keyed hash functions, Message Authentication Code Algorithms, nested MACs, HMAC, CBC-MAC

Suggested Reading:

- Chapter 11 from Stallings

Unit 5: Public Key Cryptography

Diffie Hellman, Attacks on Diffie Hellman, Diffie Hellman problems, Vanilla RSA and OAEP-RSA, Attacks on RSA, ElGamal, Attacks on ElGamal, Semantic Security

Suggested Reading:

- Chapter 8 from the Handbook
- New Directions in Cryptography, Whitefield Diffie and Martin Hellman, IEEE Transactions on Information Theory 1976, available at `http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1055638`

Unit 6: Digital Signatures

Classification of signature schemes, RSA signature, Schnorr signature, Digital Signature Standard, one time signature schemes, attacks on Digital Signatures, Blind Signatures

Suggested Reading:

- Chapter 11 from the Handbook
- Blind signatures for untraceable payments, David Chaum, Crypto 1982, available at `http://web.skku.edu/~gsic/cgi-bin/webboard/data/data/chaum-c82.pdf`

Unit 7: Key Management and Authentication Protocols

Techniques for distributing confidential and public keys, session keys, Needham-Schroeder, Otaway-Rees, Kerberos

- Chapter 13 from the Handbook
- Using Encryption for Authentication in Large Networks of Computers, Roger Needham, Michael Schroeder, CACM 1978, available at `http://portal.acm.org/citation.cfm?id=359659`
- Designing an Authentication System: a Dialogue in Four Scenes, Bill Bryant 1988, available at `http://web.mit.edu/Kerberos/dialogue.html`

Unit 8: Secret Sharing

Shamir's Secret Sharing scheme, Verifiable Secret Sharing, Threshold RSA, Visual Cryptography

Suggested Reading:

- How to Share a Secret, Adi Shamir CACM 1979, available at `http://www.caip.rutgers.edu/~virajb/readinglist/shamirturing.pdf`
- A Simplified Approach to Threshold and Proactive RSA, Tal Rabin Crypto 1998, available at `http://www.research.ibm.com/security/prsa.ps`
- Visual cryptography and threshold schemes, Doug Stinson, available at `http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=747238`