Cryptology Syllabus for graduate and advanced undergraduate Students in Math. & CS Majors

"Cryptography and Security are two of the best examples of the interaction between theory and practice." *Aviel Rubin*

This course is an introduction to the basic theory and practice of cryptographic techniques used in computer security.

This is a 4-credit course, consisting of two weekly 2-hour meetings. It is intended for graduate and advanced year undergraduate students.

Prerequisites: Elementary Number Theory, Elementary Course in Abstract Algebra, Linear Algebra, Elementary Course in Statistics and Probability theory.

Introduction (3 sessions)

- History, Overview of cryptography.
- Classical encryptions and their cryptanalysis:

  Permutation Ciphers

  - The Spartan Scytale
  - The Transposition Cipher

  Monoalphabetic Substitution Ciphers

  - The Shift Cipher
  - The Affine Cipher
  - Introduction to modular arithmetic
  - Solving linear congruences
  - Euclidean Algorithm

  Polyalphabetic Substitution Ciphers

  - The Vigenère Cipher
  - The Hill Cipher
  - The One-Time Pad
  - Pseudorandom Sequences

Basic Secret Key Encryption (security against eavesdropping) (7 sessions)

- Information theoretic security: Entropy, Perfect Secrecy, unicity distance, One time pad.
- Boolean Functions.
- Cryptanalysis of classical ciphers; Stream ciphers; RC4, LFSRs.
- Product cryptosystems: block ciphers; Feistel Type Cryptosystems, Substitution-permutation networks (SPNs).
- Mathematical preliminaries: probability distributions, random variables.
- Feistel networks: Data Encryption Standard (DES), Using block ciphers (basic modes of operation).
- Strengthening DES: Triple-DES.
- Cryptanalysis of block ciphers: Time-Space Trade-off, Differential & Linear cryptanalysis, Meet-in-the-Middle, Algebraic cryptanalysis.
- The Advanced Encryption Standard (AES) cipher.
- Semantic security, Pseudorandom Permutations, Statistical Tests for Pseudo-random Number Generators for Cryptographic Applications.

Message Integrity (Hashing) (2 sessions)

- Cryptographic hash functions: Properties of hashing, Birthday paradox, Security requirements, Collisions, Birthday attack, Security uses: Passwords, Message and Data Integrity, Message Digest; MD5, SHA, Keyed hashing; Message authentication codes (MACs).

Public Key Encryption (12 sessions)

- Mathematical preliminaries: primes, Factorization,GCDs and the Extended Euclidean Algorithm, modular exponentiation and inverses.
- Introduction to public-key cryptography.
- Mathematical preliminaries: Chinese Remainder Theorem, primality testing, modular square roots; Rabin's cryptosystem, Factoring algorithms: Pollard's rho method, p-1 method,Number Field Sieve, Quadratic S ieve method.

The RSA Algorithm

- Mathematical preliminaries: Fermat's little theorem, Euler's Phi-function, Euler's theorem, arithmetic modulo composites.

- The Asymmetric Key Concept and RSA Implementation, Trapdoor one-way function.
- RSA and Rabin encryption, Performance of RSA, How to use RSA? Hybrid encryption.
- Vulnerabilities: Unpadded RSA is insecure. Small private key.

  Random message padding.

- Miller-Rabin primality testing; Protecting against attacks on RSA: Strong primes.

Diffie-Hellman Key Agreement

- Mathematical preliminaries: Abelian groups and finite fields, some more modular arithmetic: Arithmetic modulo primes, big number arithmetic; repeated squaring.
- The Discrete Logarithm Problem.
- The Key Agreement Scheme.

ElGamal encryption

Digital Signatures (2 sessions)

- Definition of secure signature schemes. Lamport and Merkle schemes.
- How to sign using RSA, vulnerabilities.
- Brief overview of the Digital Signature Standard (DSS).
- Digital signature schemes: ElGamal, DSA; undeniable signatures.

Authentication and Key Exchange (2 sessions)

- One time password, Key Exchange , Challenge-Response authentication.
- Zero-knowledge proofs, Bit commitment, Pseudorandom Number Generation.

Course Books

1. Douglas R. Stinson; *Cryptography: Theory and Practice*, 2nd. ed., CRC Press, 2002.

2. D. R. Stinson; *Cryptography: Theory and Practice*, 1st ed., CRC Press, 1995.

3. Johannes A. Buchmann, *Introduction to Cryptography*, Springer-Verlag, 2001.

4. Hans Delfs, Helmut Knebl, *Introduction to Cryptography, Principles and Applications,* Springer Verlag, 2002.

5. Josef Pieprzyk, Thomas Hardjono, Jennifer Sebbery, *Fundamentals of Computer Security,* Springer Verlag, 2003.

6. Albrecht Beutelspacher; *Cryptology*, The Mathematical Association of America, 1994.

Other Books (Publications)

1. Oded Goldreich, *The Foundations of Cryptography,* A two-volume book Vol.1(Basic Tools): published June 2001, Vol. 2 (Basic Applications): published May 2004, both Volumes by Cambridge University Press.

2. Neal Koblitz; *A Course in Number Theory and Cryptography,* 2nd. ed., Springer-Verlag, 1994.

3. A. J. Menezes, P. C. van Oorschot and S. A. Vanstone; *Handbook of Applied Cryptography*, CRC Press, 1997. Available online.

4. Bruce Schneier; *Applied Cryptography:Protocols, Algorithms, and Source Code in C*, 2 nd. ed., John Wiley & Sons, 1996.

5. Rukhin A. et al.; *A Statistical Test Suite for Random and Pseudo Random Number Generators for Cryptographic Applications,* NIST Special Publication 800-22, 2001, http://www.csrc.nist.gov/publications/nistpubs/800-22/sp-800-22-051501.pdf

References for the Syllabus:

http://crypto.stanford.edu/~dabo/cs255/syllabus.html

http://www.cse.sc.edu/research/isl/csce557Syllabus.shtml

http://www.cs.bgu.ac.il/~beimel/Courses/crypto/crypto.html

http://www.math.temple.edu/~renault/cryptology/syllabus.html