Introduction to Cryptography (89-656)

Yehuda Lindell
Bar-Ilan University

Abstract

The aim of this course is to teach the basic principles and concepts of modern cryptography. The focus of the course will be on cryptographic problems and their solutions, and will contain a mix of both theoretical and applied material. We will present definitions of security and argue why certain construction meet these definitions. We will use the textbook *Introduction to Modern Cryptography* by Jonathan Katz and myself. Copies of the book are available in the library. The textbook contains the exact material that we will study (we will be using the second edition, although most of the material appears in the first edition as well). The course consists of twelve lectures of four hours each (3 hours of actual lecturing). See `http://www.cs.biu.ac.il/~lindell/89-656/main-89-656.html` for more information.

Detailed Course Syllabus

1. **Introduction**
   (a) What is modern cryptography (Section 1.1)
   (b) Historical ciphers and their cryptanalysis (Sections 1.2 and 1.3)
   (c) The heuristic versus the rigorous approach; adversarial models and principles of defining security (Section 1.4)
2. **Perfectly-Secret Encryption**
   (a) Definitions, the one-time pad; proven limitations (Sections 2.1–2.3)
3. **Private-Key (Symmetric) Encryption**
   (a) Computational security (Section 3.1)
   (b) Defining secure encryption (Section 3.2.1)
   (c) Constructing secure encryption; pseudorandomness (Section 3.3)
   (d) Stronger security notions (Section 3.4)
   (e) Constructing CPA-secure encryption (Section 3.5)
   (f) Modes of operation; CBC vs CTR (Section 3.6)
   (g) Security of CTR with $n-k$ bit counter for messages to size 2^k blocks with proof directly to the LR definition
   (h) CCA attacks (Section 3.7)
4. **Message Authentication Codes**
   (a) Message integrity (Section 4.1)
   (b) Definition of security (Section 4.2)
   (c) Constructions from pseudorandom functions (Section 4.3.1)
   (d) CBC-MAC (Section 4.4.1)

   (e) Authenticated encryption (Section 4.5)

5. **Collision-Resistant Hash Functions**
   (a) Definitions (Section 5.1)
   (b) The Merkle-Damgard transform (Section 5.2)
   (c) HMAC in brief (Section 5.3)
   (d) Birthday attacks (Section 5.4.1)
   (e) The Random oracle model (Section 5.5)
   (f) Password hashing (Section 5.6.3)

6. **Constructions of Pseudorandom Permutations (Block Ciphers) in Practice**
   (a) Substitution-permutation and Feistel networks (Sections 6.2.1 and 6.2.2)
   (b) DES and attacks on reduced-round versions, double-DES and triple-DES (Sections 6.2.3 and 6.2.4)
   (c) AES in brief (Section 6.2.5)
   (d) Hash functions from block ciphers (Section 6.3.1)

7. **Number Theory**
   (a) Preliminaries and basic group theory (self review by students; Section 8.1)
   (b) Primes, factoring and RSA (Sections 8.2.1, 8.2.3, 8.2.4, 8.2.5)
   (c) Cryptographic assumptions in cyclic groups (Section 8.3.1, 8.3.2, 8.3.3)
   (d) Collision resistant hash functions from discrete log (Section 8.4.2)

8. **Public-Key (Asymmetric) Cryptography**
   (a) Introduction and motivation
   (b) Diffie-Hellman key exchange (Section 10.3)

9. **Public-Key (Asymmetric) Encryption**
   (a) The model and definitions (Sections 11.1 and 11.2)
   (b) Hybrid encryption and KEM/DEM (Section 11.3)
   (c) El Gamal (Sections 11.4.1 and 11.4.2)
   (d) RSA: textbook encryption, attacks on textbook RSA, padded RSA; CCA-secure RSA KEM (Sections 11.5.1, 11.5.2, 11.5.5)

10. **Digital Signatures**
   (a) Definition and applications (Sections 12.1 and 12.2)
   (b) Hash and sign (Section 12.3)
   (c) RSA signatures: textbook RSA, hashed RSA, security with ROM (Sections 12.4.1 and 12.4.2)
   (d) Certificates and public-key infrastructures (Section 12.7)
   (e) SSL/TLS (Section 12.8)

11. **Advanced Cryptography – A Taste**
   (a) Shamir secret sharing and VSS
   (b) Oblivious transfer
   (c) Secure computation

Prerequisites: Algorithms 1 (89-220), Probability (89-262 or an equivalent), Computability (89-224)

Evaluation: Theoretical exercises and an exam