

Introduction to Cryptography

89-656

Yehuda Lindell¹

October 19, 2006

¹This is an *outdated draft* of lecture notes written for an undergraduate course in cryptography at Bar-Ilan University, Israel. The notes are replaced by the textbook *Introduction to Cryptography* by Jonathan Katz and myself. There is a significant difference between the presentation in these notes and in the textbook (and thus how we will teach in class).

© Copyright 2005 by Yehuda Lindell.

Permission to make copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that new copies bear this notice and the full citation on the first page. Abstracting with credit is permitted.

Abstract and Course Syllabus

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 constructions meet these definitions. However, these definitions and arguments will be rather informal. (A rigorous treatment of the theory of cryptography will be given in course 89-856 next semester.) There is no one text book that covers all of the material in the course (nor one that presents the material in the same way as we do). However, much of the material can be found in the textbooks of [36] and [37] in the library.

Course Syllabus

1. (a) **Introduction:** what is modern cryptography (what problems does it attempt to solve and how); the heuristic versus the rigorous approach; adversarial models and principles of defining security.
(b) **Historical ciphers and their cryptanalysis**
2. **Perfectly secret encryption:** definitions, the one-time pad and its proof of security; proven limitations, Shannon's theorem.
3. (a) **Pseudorandomness:** definition, pseudorandom generators and functions.
(b) **Private-key (symmetric) encryption schemes:** Definition of security for eavesdropping adversary, stream ciphers (construction from pseudorandom generators).
4. **Private-key encryption schemes:**
 - (a) **Block ciphers:** CPA-secure encryption from pseudorandom permutations/functions.
 - (b) **The Data Encryption Standard (DES).**
5. **Private-key encryption (continued):**
 - (a) **DES (continued):** Attacks on reduced-round DES; double DES and triple DES.
 - (b) **Modes of operation:** how to encrypt many blocks.
6. **Collision-resistant hash functions:** definition, properties and constructions; the random oracle model
7. **Message authentication:** definition, constructions, CBC-MAC, HMAC
8. (a) **Combining encryption and authentication:** how and how not to combine the two.

- (b) **CCA-secure encryption:** definition and construction.
 - (c) **Key management:** the problem, key distribution centers (KDCs), key exchange protocols
9. **Public-key (asymmetric) cryptography:** introduction and motivation, public-key problems and mathematical background (Discrete Log, Computational and Decisional Diffie-Hellman, Factoring, RSA), Diffie-Hellman key agreement
 10. **Public-key (asymmetric) encryption schemes:** the model and definitions, the El-Gamal encryption scheme, the RSA trapdoor one-way permutations, RSA in practice
 11. **Attacks on RSA:** common modulus, broadcast, timing attacks
 12. **Digital signatures and applications:** definitions and constructions (in the random oracle model), certificates, certificate authorities and public-key infrastructures.
 13. **Secure protocols:** SSL, secret sharing

Much of the material in the course (but far from all of it) can be found in [36] and [37]. Other texts of relevance are [17] and [28].

A note regarding references: Some references are presented throughout the lecture notes. These references are not supposed to be citations in the classic sense, but rather are pointers to further reading that may be of interest to those who wish to understand a topic in greater depth. As such, the references are not complete (in fact, there are many glaring omissions).

Contents

1	Introduction and Historical Ciphers	5
1.1	Introduction	5
1.2	Historical Ciphers and Their Cryptanalysis	7
2	Information Theoretic Security	11
2.1	Preliminaries	11
2.2	Perfect Secrecy	12
2.3	The One-Time Pad (Vernam's Cipher)	13
2.4	Limitations of Perfect Secrecy	14
2.5	Shannon's Theorem	14
3	Pseudorandomness and Private-Key Encryption Schemes	17
3.1	Pseudorandomness	17
3.2	Symmetric (Private-Key) Encryption	18
3.2.1	Defining Security	18
3.2.2	Constructing Secure Encryption Schemes	19
4	Private-Key Encryption Schemes and Block Ciphers	21
4.1	Pseudorandom Functions and Permutations	21
4.2	Private-Key Encryption Schemes from Pseudorandom Functions	22
4.3	DES – The Data Encryption Standard	24
5	Block Ciphers (continued)	27
5.1	Attacks on DES	27
5.1.1	Single-Round DES	27
5.1.2	Two-Round DES	28
5.1.3	Three-Round DES	28
5.1.4	Brute Force Search	29
5.1.5	The Best Known Attacks on Full DES	29
5.1.6	Further Reading	29
5.2	Increasing the Key-Size for DES	29
5.2.1	First Attempt – Alternating Keys	29
5.2.2	Second Attempt – Double DES	30
5.2.3	Triple DES (3DES)	31
5.3	Modes of Operation	31

[Click here to download full PDF material](#)