

Study Guide to the Final Exam

Exam Topics

You are responsible for the topics covered in the whole course. Emphasis will be on the material in lecture notes 12–25 as well as the concepts used in homework assignments 5–9.

Not everything in the lecture notes was covered in class, but you should read any slides that were skipped over to make sure you have a general understanding of what they are about.

You may find handouts [11](#) (number theory), [12](#) (linear congruence equations), and [13](#) (pseudo-random number generations) useful for filling in details that may have been glossed over in class.

Index to the Lecture Notes

Below is a list of all sections and subsections from lecture notes 12–25. You can use this as an index to the lecture notes and as a high-level overview of the course since the midterm study guide.

- | | | |
|------|--|--------------|
| 1 | Using Digital Signatures | [lecture 12] |
| 1.1 | Adding redundancy | [lecture 12] |
| 2 | Signing Message Digests | [lecture 12] |
| 2.1 | Signed encrypted messages | [lecture 12] |
| 3 | Practical Signature Algorithms | [lecture 12] |
| 3.1 | ElGamal digital signature scheme | [lecture 12] |
| 3.2 | Digital signature algorithm (DSA) | [lecture 12] |
| 4 | Elliptic Curves Basics | [lecture 13] |
| 5 | Elliptic Curve Cryptography | [lecture 13] |
| 6 | Computing in \mathbf{Z}_n | [lecture 14] |
| 6.1 | Modular multiplication | [lecture 14] |
| 6.2 | Modular inverses | [lecture 14] |
| 6.3 | Extended Euclidean algorithm | [lecture 14] |
| 7 | Generating RSA Encryption and Decryption Exponents | [lecture 14] |
| 8 | Euler's Theorem | [lecture 14] |
| 9 | Generating RSA Modulus | [lecture 14] |
| 9.1 | Finding primes by guess and check | [lecture 14] |
| 9.2 | Density of primes | [lecture 14] |
| 10 | Primitive Roots | [lecture 15] |
| 10.1 | Properties of primitive roots | [lecture 15] |
| 10.2 | Lucas test | [lecture 15] |
| 10.3 | Special form primes | [lecture 15] |
| 11 | Functions That Look Random | [lecture 15] |

12	Cryptographic Hash Functions	[lecture 15]
12.1	Properties of random functions	[lecture 15]
12.2	Message digest functions	[lecture 15]
13	Properties of Hash Functions	[lecture 16]
13.1	Hash functions do not always look random	[lecture 16]
13.2	Relations among hash function properties	[lecture 16]
14	Constructing New Hash Functions from Old	[lecture 16]
14.1	Extending a hash function	[lecture 16]
14.2	A general chaining method	[lecture 16]
15	Common Hash Functions	[lecture 16]
15.1	SHA-2	[lecture 16]
15.2	SHA-3	[lecture 16]
15.3	MD5	[lecture 16]
16	Appendix: Birthday Attack Revisited	[lecture 16]
17	Hashed Data Structures	[lecture 17]
17.1	Motivation: Peer-to-peer file sharing networks	[lecture 17]
17.2	Hash lists	[lecture 17]
17.3	Hash Trees	[lecture 17]
18	Lamport One-Time Signatures	[lecture 17]
19	Merkle Signatures	[lecture 17]
20	Authentication Using Passwords	[lecture 17]
20.1	Authentication problem	[lecture 17]
20.2	Passwords authentication schemes	[lecture 17]
20.3	Secure password storage	[lecture 17]
20.4	Dictionary attacks	[lecture 17]
21	Authentication While Preventing Impersonation	[lecture 18]
21.1	Challenge-response authentication protocols	[lecture 18]
21.2	Authentication using zero knowledge interactive proofs	[lecture 18]
22	Quadratic Residues, Squares, and Square Roots	[lecture 18]
22.1	Modular square roots	[lecture 18]
22.2	Square roots modulo n	[lecture 18]
22.3	Square roots modulo an odd prime p	[lecture 18]
22.4	Square roots modulo the product of two odd primes	[lecture 18]
23	Zero Knowledge Protocols	[lecture 18]
23.1	Feige-Fiat-Shamir Authentication Protocol	[lecture 18]
23.2	Secret cave protocol	[lecture 18]
24	Chinese Remainder Theorem	[lecture 18]
25	Zero Knowledge Interactive Proofs (ZKIP)	[lecture 19]
25.1	ZKIP for graph isomorphism	[lecture 19]
25.2	Feige-Fiat-Shamir Authentication Protocol	[lecture 19]
25.3	Abstraction from two ZKIP examples	[lecture 19]

26	Information Splitting	[lecture 19]
27	Public Key Infrastructure (PKI) and Trust	[lecture 19]
28	Formalizing Zero Knowledge	[lecture 20]
28.1	Computational Knowledge	[lecture 20]
28.2	Composing Zero-Knowledge Proofs	[lecture 20]
29	Quadratic Residues Revisited	[lecture 20]
29.1	Euler criterion	[lecture 20]
29.2	QR Probabilistic Cryptosystem	[lecture 20]
29.3	Summary	[lecture 20]
30	Appendix: Finding Square Roots	[lecture 20]
30.1	Square roots modulo special primes	[lecture 20]
30.2	Square roots modulo general odd primes	[lecture 20]
31	Secure Random Sequence Generators	[lecture 21]
31.1	Pseudorandom sequence generators	[lecture 21]
31.2	Looking random	[lecture 21]
32	Similarity of Probability Distributions	[lecture 21]
32.1	Cryptographically secure PRSG	[lecture 21]
32.2	Indistinguishability	[lecture 21]
33	The Legendre and Jacobi Symbols	[lecture 21]
33.1	The Legendre symbol	[lecture 21]
33.2	Jacobi symbol	[lecture 21]
33.3	Computing the Jacobi symbol	[lecture 21]
34	BBS Pseudorandom Sequence Generator	[lecture 22]
35	Secret Splitting	[lecture 22]
36	Shamir's Secret Splitting Scheme	[lecture 22]
36.1	Secret Splitting with Dishonest Parties	[lecture 22]
37	Appendix: Security of BBS	[lecture 22]
38	Mutual Privacy-Preserving Protocols	[lecture 23]
39	Bit Commitment Problem	[lecture 23]
39.1	Bit Commitment Using QR Cryptosystem	[lecture 23]
39.2	Bit Commitment Using Symmetric Cryptography	[lecture 23]
39.3	Bit Commitment Using Hash Functions	[lecture 23]
39.4	Bit Commitment Using Pseudorandom Sequence Generators	[lecture 23]
40	Coin-Flipping	[lecture 23]
41	Appendix: Formalization of Bit Commitment Schemes	[lecture 23]
42	Locked Boxes	[lecture 24]
42.1	Locked Box Paradigm	[lecture 24]
42.2	Locked Box Implementation	[lecture 24]
43	Oblivious Transfer	[lecture 24]
44	The Millionaires' Problem	[lecture 24]

45	Privacy-Preserving Boolean Function Evaluation	[lecture 24]
45.1	Boolean circuits	[lecture 24]
45.2	Implementation Using Value Shares	[lecture 24]
45.3	Implementation Using Garbled Circuits	[lecture 24]
46	Appendix: Problems at Least as Hard as Factoring	[lecture 24]
47	Encryption with Special Properties	[lecture 25]
47.1	Homomorphic Encryption	[lecture 25]
47.2	Encryption with Other Properties	[lecture 25]
48	Bitcoins	[lecture 25]