

Study Guide to Midterm Exam

Exam Topics

You are responsible for the topics covered in lecture notes 1–11, as well as the concepts used in homework assignments 1–4. Not everything in the lecture notes was covered in class, but you should read any slides that were skipped to make sure you understand them.

Supplementary Textbook

Most of these same topics are covered in the Paar and Pelzl online textbook, *Understanding Cryptography*, often to greater depth. Roughly speaking, we've covered the following chapters and sections:

- Chapter 1 [Introduction], sections 1.1–1.3, 1.4.1, 1.4.3, 1.4.4.
- Chapter 2 [Stream Ciphers], sections 2.1, 2.2
- Chapter 3 [DES], sections 3.1–3.5.
- Chapter 4 [AES], sections 4.1, 4.2, 4.4, 4.5.
- Chapter 5 [Block Ciphers], sections 5.1.1–5.1.4, 5.2, 5.3.1.
- Chapter 6 [Public Key Cryptography], sections 6.1, 6.2.1, 6.2.2, 6.3.1, 6.3.3.
- Chapter 7 [RSA], sections 7.1, 7.2, 7.4.
- Chapter 8 [Discrete Log Cryptosystems], section 8.1, 8.3.1, 8.4, 8.5.1, 8.5.2.
- Chapter 10 [Digital Signatures], section 10.1, 10.2.
- Chapter 12 [Message Authentication Codes], sections 12.1, 12.3.

While the exam will not cover material from the textbook that was not covered in class and in the lecture notes, the textbook gives additional perspective and context for understanding the course material.

Index to the Lecture Notes

Below is a list of all sections and subsections from the lecture notes 1–11. You can use this as an index to the lecture notes and as a high-level overview of the course so far.

- | | | |
|---|---------------------------|-------------|
| 1 | Highlights from Syllabus | [lecture 1] |
| 2 | Data Breaches | [lecture 1] |
| 3 | Defending Against Attacks | [lecture 1] |

4	Course Overview	[lecture 2]
5	Security Principles	[lecture 2]
5.1	Confidentiality	[lecture 2]
5.2	Integrity	[lecture 2]
5.3	Availability	[lecture 2]
5.4	Crypto as a security tool	[lecture 2]
6	Threats	[lecture 2]
7	Who are the Attackers?	[lecture 2]
8	Secret Message Transmission	[lecture 3]
9	Symmetric Cryptography	[lecture 3]
10	Caesar cipher	[lecture 3]
11	Some other classical ciphers	[lecture 3]
11.1	Generalized shift ciphers	[lecture 3]
11.2	Polyalphabetic ciphers	[lecture 3]
11.3	Polygraphic Ciphers	[lecture 3]
12	Analyzing Confidentiality of Cryptosystems	[lecture 4]
12.1	Secret ballot elections	[lecture 4]
12.2	Information protection	[lecture 4]
12.3	Adversaries with unlimited power	[lecture 4]
12.4	Computationally limited adversaries	[lecture 4]
12.5	Kinds of attacks	[lecture 4]
13	Modification Attack	[lecture 5]
14	Computational Security	[lecture 5]
15	Information-Theoretic Security	[lecture 5]
15.1	Some probability theory	[lecture 5]
15.2	Information-theoretic security	[lecture 5]
15.3	Loss of perfection	[lecture 5]
16	Symmetric Cryptosystem Families	[lecture 5]
16.1	Stream ciphers	[lecture 5]
16.2	Block ciphers	[lecture 5]
17	Symmetric Cryptosystem Components	[lecture 6]
18	Padding	[lecture 6]
18.1	Bit padding	[lecture 6]
18.2	Byte padding	[lecture 6]
19	Data Encryption Standard (DES)	[lecture 6]
20	Multiple Encryption	[lecture 7]
20.1	Composition	[lecture 7]
20.2	Group property	[lecture 7]
21	Birthday Attack	[lecture 7]
22	Advanced Encryption Standard	[lecture 7]

23	Advanced Encryption Standard (cont.)	[lecture 8]
24	AES Alternatives	[lecture 8]
25	Chaining Modes	[lecture 8]
25.1	Block chaining modes	[lecture 8]
25.2	Extending chaining modes to bytes	[lecture 8]
26	Public-key Cryptography	[lecture 8]
27	RSA	[lecture 8]
28	Tools Needed for RSA	[lecture 9]
29	Algorithms	[lecture 9]
29.1	Computing with Big Numbers	[lecture 9]
29.2	Fast Exponentiation Algorithms	[lecture 9]
30	Number Theory	[lecture 9]
30.1	Factoring Assumption	[lecture 9]
30.2	Number Theory for RSA	[lecture 9]
30.3	Division of Integers	[lecture 9]
31	Integers Modulo n	[lecture 10]
32	Multiplicative Subgroup of \mathbf{Z}_n	[lecture 10]
32.1	Greatest common divisor	[lecture 10]
32.2	Multiplicative subgroup of \mathbf{Z}_n	[lecture 10]
33	Discrete Logarithm	[lecture 10]
34	Diffie-Hellman Key Exchange	[lecture 10]
35	ElGamal Cryptosystem	[lecture 11]
36	Message Integrity and Authenticity	[lecture 11]
36.1	Message authentication codes	[lecture 11]
36.2	Asymmetric digital signatures	[lecture 11]
36.3	Implications of Digital Signatures	[lecture 11]
37	Digital Signature Algorithms	[lecture 11]
37.1	Signatures from commutative cryptosystems	[lecture 11]
37.2	Signatures from non-commutative cryptosystems	[lecture 11]
38	Security of Digital Signatures	[lecture 11]
38.1	Forgery	[lecture 11]