YALE UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE



# 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.