Schedule of Topics
CSC 214P, "Cryptography"
Department of Computer Science
Grinnell College
August 29, 2019

Reading: Katz and Lindell, *Introduction to Modern Cryptography*, chapter 1 (pages 3–24)

**August 29:** Modern Cryptography in a Historical Setting

Reading: Katz and Lindell, from the beginning of chapter 2 through section 2.2 (pages 25–34)

**September 5:** The One-Time Pad

Reading: Katz and Lindell, from section 2.3 to the end of chapter 2 (pages 35–40)

**September 12:** Perfect Security

Reading: Katz and Lindell, from the beginning of chapter 3 through section 3.2 (pages 43–60)

**September 19:** Computationally Secure Encryption

Reading: Katz and Lindell, section 3.3 (pages 60–70)

**September 26:** Pseudo-Random Generators and Stream Ciphers

Reading: Katz and Lindell, sections 3.4 and 3.5 (pages 70–86)

**October 3:** Security against Chosen-Plaintext Attacks

Reading: Katz and Lindell, from sections 3.6 to the end of chapter 3 (pages 86–106)

**October 10:** Block Ciphers; Modes of Operation; Security against Chosen-Ciphertext Attacks

Reading: Katz and Lindell, sections 4.1 through section 4.4 (pages 107–130)

**October 17:** Message Authentication Codes

Reading: Katz and Lindell, section 4.5 (pages 131–141)

**October 31:** Authenticated Encryption

Reading: Katz and Lindell, from section 4.6 to the end of chapter 4 (pages 142–151)

**November 7:** Information-Theoretic MACs

Reading: Katz and Lindell, from the beginning of chapter 5 through section 5.4 (pages 153–173)

**November 14:** Cryptographic Hash Functions

Reading: Katz and Lindell, from section 5.5 to the end of chapter 5 (pages 174–191)

**November 21:** Merkle Trees

Reading: Katz and Lindell, chapter 10 (pages 359–373)

**December 5:** Key Exchange and Distribution; the Diffie–Hellman Protocol

Reading: Katz and Lindell, sections 12.7 through 12.9 (pages 473–483)

**December 12:** Digital Signatures

Copyright © 2019 John David Stone

This work is licensed under the Creative Commons Attribution-ShareAlike 4.0 International License. To view a copy of this license, visit

http://creativecommons.org/licenses/by-sa/4.0/deed.en

or send a letter to Creative Commons, 543 Howard Street, 5th Floor, San Francisco, California, 94105, USA.