Cryptology - Study Scaffolds

Generated: 2026-01-03 22:24

Exam Format

Oral exam with no preparation (max 30 minutes). Students randomly select 1 of 6 subjects and present for up to 18 minutes, followed by questions. Students may bring notes.

Learning Objectives

You must be able to:

- Provide comprehensive overviews of cryptographic concepts and systems.
- Present and prove relevant theorems and security results from course material.
- Explain cryptographic definitions, constructions, and their security properties.
- Demonstrate understanding of both theoretical foundations and practical cryptographic schemes.
- Apply concepts from exercises to explain cryptographic principles.

Subtopic Scaffolds

☑ Information Theory and Cryptography (28 pages)
☑ Symmetric (secret-key) Crypto (38 pages)
☑ Public-key Crypto based on Factoring (27 pages)
☑ Public-key Crypto based on Discrete Log and LWE (21 pages)
☑ Symmetric Authentication and Hash Functions (16 pages)
☑ Digital Signature Schemes (14 pages)

Oral Exam Notes

☑ Information Theory (12:30)
☑ Symmetric Cryptography (14:30)
☑ Public-key Crypto from Factoring (16:00)
☑ Public-key Crypto from Discrete Log and LWE (15:30)
☑ Symmetric Authentication and Hash Functions (15:30)
☑ Digital Signatures (Schnorr Scheme) (15:00)

Statistics

- **Total pages processed:** 162
- **Sources used:** 1

- **Subtopics covered:** 6/6

Source Breakdown

- **CryptographyV6.pdf**: 162 pages