



## Required Resources

---

**Textbook:** *Introduction to Cryptography With Coding Theory*

Read the following chapters and sections from the textbook:


- Chapter 5 through section 5.3: RC4
- Chapter 6

The reading assignment this week covers stream ciphers and block ciphers, two fundamental encryption techniques frequently used in cryptography. Stream ciphers encrypt data by generating a continuous stream of pseudorandom bits, called a keystream, which is then combined (usually via XOR) with the plaintext to produce the ciphertext. In contrast, block ciphers divide data into fixed-size blocks and encrypt each block independently. Block ciphers are often used with feedback and chaining mechanisms to improve security. Both the stream and block cipher techniques have their strengths and weaknesses, and the choice between them will typically depend on application-specific requirements.

**Video:** Linear Algebra Application: The Hill Cipher  ([https://www.youtube.com/watch?v=8SF18\\_tS8xs](https://www.youtube.com/watch?v=8SF18_tS8xs))

This video explains encryption and decryption using the Hill cipher.

Students may experience varying amounts of time for this resource to load, depending on the speed of their internet connection. This video is 12 minutes and 28 seconds in length.

**Website:** Probability and Combinatorics 

(<https://www.khanacademy.org/math/probability/probability-and-combinatorics-topic>)

The Khan Academy site provides video tutorials on permutations, combinations, and how to use combinatorics to solve probability questions. It goes through several examples and has a simple test to provide immediate feedback on your understanding.

**Article:** An Introduction to Stream Ciphers vs. Block Ciphers 

(<https://www.jscape.com/blog/stream-cipher-vs-block-cipher>)

This article discusses the basics of stream ciphers and block ciphers.

**Video:** Linear Feedback Shift Registers  (<https://www.youtube.com/watch?v=vuEmsXWgKkk>) (13:01)

This video discusses how linear feedback shift registers generate a stream of pseudo-random numbers.

A captioned version of this video is available: Linear Feedback Shift Registers (CC). 

([https://urldefense.com/v3/\\_\\_https://youtu.be/uuk9pJBec\\_o\\_\\_;!!BelmMA!6NM70EppqFC4M0YQE6tXH2BfFqPKy8ENRMLn2qAQahtHv8n\\_s5\\_QjkceK5ZPMNAH01ARN89mEloahYq4h6b1hsAN9xZs9\\$](https://urldefense.com/v3/__https://youtu.be/uuk9pJBec_o__;!!BelmMA!6NM70EppqFC4M0YQE6tXH2BfFqPKy8ENRMLn2qAQahtHv8n_s5_QjkceK5ZPMNAH01ARN89mEloahYq4h6b1hsAN9xZs9$))

A video transcript is available: Transcript for Linear Feedback Shift Registers 

([https://snhu.sharepoint.com/:w:/r/sites/LearningScienceAssessment/\\_layouts/15/Doc.aspx?sourcedoc=%7B10AC8D2F-FD07-4769-9576-](https://snhu.sharepoint.com/:w:/r/sites/LearningScienceAssessment/_layouts/15/Doc.aspx?sourcedoc=%7B10AC8D2F-FD07-4769-9576-1AF83B03DC20%7D&file=MAT%20260%20Transcript%20for%20Linear%20Feedback%20Shift%20Registers%20-%20How%20to%20Do%20Them%20by%20Hand.docx&action=default&mobileredirect=true)

[1AF83B03DC20%7D&file=MAT%20260%20Transcript%20for%20Linear%20Feedback%20Shift%20Registers%20-](https://snhu.sharepoint.com/:w:/r/sites/LearningScienceAssessment/_layouts/15/Doc.aspx?sourcedoc=%7B10AC8D2F-FD07-4769-9576-1AF83B03DC20%7D&file=MAT%20260%20Transcript%20for%20Linear%20Feedback%20Shift%20Registers%20-%20How%20to%20Do%20Them%20by%20Hand.docx&action=default&mobileredirect=true)

[1AF83B03DC20%7D&file=MAT%20260%20Transcript%20for%20Linear%20Feedback%20Shift%20Registers%20-](https://snhu.sharepoint.com/:w:/r/sites/LearningScienceAssessment/_layouts/15/Doc.aspx?sourcedoc=%7B10AC8D2F-FD07-4769-9576-1AF83B03DC20%7D&file=MAT%20260%20Transcript%20for%20Linear%20Feedback%20Shift%20Registers%20-%20How%20to%20Do%20Them%20by%20Hand.docx&action=default&mobileredirect=true)

[%20How%20to%20Do%20Them%20by%20Hand.docx&action=default&mobileredirect=true\)](https://snhu.sharepoint.com/:w:/r/sites/LearningScienceAssessment/_layouts/15/Doc.aspx?sourcedoc=%7B10AC8D2F-FD07-4769-9576-1AF83B03DC20%7D&file=MAT%20260%20Transcript%20for%20Linear%20Feedback%20Shift%20Registers%20-%20How%20to%20Do%20Them%20by%20Hand.docx&action=default&mobileredirect=true)