



## Required Resources

---

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


Read the following chapters and sections from the textbook:


- Chapter 11
- Chapter 12 through section 12.4: Using Hash Functions to Encrypt


Hash functions, such as those in the Merkle-Damgård construction, SHA-2, and SHA-3 families are cryptographic tools that transform variable-length inputs into fixed-size outputs, maintaining properties like preimage resistance, second preimage resistance, and collision resistance.


The Merkle-Damgård construction technique is a widely used algorithm for designing hash functions, breaking down larger inputs into blocks for processing. SHA-2 is a popular hash function family, including SHA-256 and SHA-512, known for their security and resistance to birthday attacks, where an attacker finds two distinct inputs producing the same hash. SHA-3, a newer standard than SHA-2, offers a different design approach for hash functions with the goal of enhancing security.

Birthday attacks on hash functions attempt to exploit the statistical likelihood of finding collisions (two different inputs with the same hash) in hash functions, highlighting the importance of choosing hash functions with sufficient output size to mitigate this risk.

**Video:** Bitcoin: Cryptographic Hash Functions  (<https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-cryptographic-hash-function>) (10:14)  
This video describes cryptographic hash functions.

**Video:** Explanation of Cybersecurity Hashing and MD5 Collisions   
([https://www.youtube.com/watch?v=DqnBTP5p3\\_o](https://www.youtube.com/watch?v=DqnBTP5p3_o)) (12:02)  
This video explains cybersecurity hashing and MD5 collisions.

A captioned version of this video is available: Explanation of Cybersecurity Hashing and MD5 Collisions (CC)   
([https://urldefense.com/v3/\\_\\_https://youtu.be/4pmF092PZpg\\_\\_;!!BelmMA!7oEVIJrIYNNmISUVYIKx\\_WMqfchhG0IKa9GjepszgaLJLhqRtfVIEi9lwoX6uERDkJMHdu5AJAh93GIKIOza87WbyouOUcsXbA\\$](https://urldefense.com/v3/__https://youtu.be/4pmF092PZpg__;!!BelmMA!7oEVIJrIYNNmISUVYIKx_WMqfchhG0IKa9GjepszgaLJLhqRtfVIEi9lwoX6uERDkJMHdu5AJAh93GIKIOza87WbyouOUcsXbA$))

A video transcript is available: Transcript for Explanation of Cybersecurity Hashing and MD5 Collisions   
([https://snhu.sharepoint.com/:w:/r/sites/LearningScienceAssessment/\\_layouts/15/Doc.aspx?](https://snhu.sharepoint.com/:w:/r/sites/LearningScienceAssessment/_layouts/15/Doc.aspx?)

sourcedoc=%7B44736015-D29E-4213-83F7-

CFA97D0DFDB6%7D&file=MAT%20260%20Transcript%20for%20Explanation%20of%20Cybersecu  
rity%20Hashing%20and%20MD5%20Collisions.docx&action=default&mobileredirect=true)