☰   🔊 **Listen**   ▶

Required Resources

Textbook: *Introduction to Cryptography With Coding Theory*

Read the following chapters from the textbook:

- Chapter 8
- Chapter 9

The Advanced Encryption Standard (AES) is a widely used symmetric-key encryption algorithm that was established as a federal standard by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES operates on blocks of data and supports key lengths of 128, 192, or 256 bits. AES is commonly used across a wide range of applications, including securing data in transit over the internet, protecting data at rest on storage devices, and ensuring the confidentiality and integrity of communications.

The RSA algorithm, named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman, is a widely used asymmetric-key encryption and digital signature algorithm. At its core, it relies on the mathematical properties of large prime numbers. In the RSA algorithm, a pair of keys is used: a public key for encryption and a private key for decryption (or signing). The RSA algorithm is primarily used for key exchange and digital signatures, as opposed to bulk data encryption operations.

Video: Prime Factorization 🔗 (https://www.youtube.com/watch?v=ZKKDTfHcsG0) (4:09) This video discusses primes, factoring integers into prime numbers, and exponential notation.

A captioned version of this video is available: Prime Factorization (CC). 🔗 (https://urldefense.com/v3/__https:/youtu.be/3i_-a8q9zng__;!!BeImMA!6NM70EpqFC4M0YQE6tXH2BfFqPKy8ENRMLn2qAQahtHv8n_s5_QjkceK5ZPMNAH01ARN89mEloahYq4h6b1hsIH5s7tW$)

A video transcript is available: Transcript for Prime Factorization 🔗 (https://snhu.sharepoint.com/:w:/r/sites/LearningScienceAssessment/_layouts/15/Doc.aspx?sourcedoc=%7BD9CEFDF5-F52E-46E1-AE1F-45EC0A77CADE%7D&file=MAT%20260%20Transcript%20for%20Prime%20Factorization%20-%20Factors%20and%20Multiples%20-%20Pre-Algebra%20-%20Khan%20Academy.docx&action=default&mobileredirect=true)

Video: Public Key Cryptography: RSA Encryption Algorithm 🔗 (https://www.youtube.com/watch?
v=wXB-V_Keiu8) (16:30)
This video introduces the concepts of public key encryption, trapdoors, and the RSA algorithm.

A captioned version of this video is available: Public Key Cryptography: RSA Encryption Algorithm 🔗
(https://urldefense.com/v3/__https:/youtu.be/G6SJD-D-
3OA__;!!BeImMA!6NM70EpqFC4M0YQE6tXH2BfFqPKy8ENRMLn2qAQahtHv8n_s5_QjkceK5ZPM
NAH01ARN89mEloahYq4h6b1hsNfprnEW$)

A video transcript is available: Transcript for Public Key Cryptography: RSA Encryption Algorithm 🔗
(https://snhu.sharepoint.com/:w:/r/sites/LearningScienceAssessment/_layouts/15/Doc.aspx?
sourcedoc=%7BB7B8969C-E13D-4E92-A18F-
96054F228E70%7D&file=MAT%20260%20Transcript%20for%20Public%20Key%20Cryptography%
20RSA%20Encryption%20Algorithm.docx&action=default&mobileredirect=true)

Video: Diffie-Hellman Key Exchange 🔗 (https://www.youtube.com/watch?v=YEBfamv-_do) (8:37)
This video discusses the revolutionary Diffie-Hellman key-exchange protocol, used by two physically
separate parties to agree on a secret key.

A captioned version of this video is available: Diffie-Hellman Key Exchange (CC). 🔗
(https://urldefense.com/v3/__https:/youtu.be/OzisH4JmhT4__;!!BeImMA!6NM70EpqFC4M0YQE6tX
H2BfFqPKy8ENRMLn2qAQahtHv8n_s5_QjkceK5ZPMNAH01ARN89mEloahYq4h6b1hsFraGvIN$)

A video transcript is available: Transcript for Diffie Hellman Key Exchange 🔗
(https://snhu.sharepoint.com/:w:/r/sites/LearningScienceAssessment/_layouts/15/Doc.aspx?
sourcedoc=%7B4E7D191D-8329-4D91-A7FC-
860959E16538%7D&file=MAT%20260%20Transcript%20for%20Public%20Key%20Cryptography%
20-
%20Diffie%20Hellman%20Key%20Exchange%20(Full%20Version).docx&action=default&mobileredir
ect=true)