



Required Resources

Textbook: *Introduction to Cryptography With Coding Theory*

Read the following chapters from the textbook:

- Chapter 13
- Chapter 14

This module investigates the topic of digital signatures and issues that may arise in their implementation. Digital signatures are cryptographic techniques used to verify the authenticity and integrity of electronic documents or messages. Some of the more popular digital signature schemes that will be studied here include the RSA and ElGamal signature schemes.

RSA relies on the mathematical properties of large prime numbers to create a pair of keys (public and private). The private key is used to create the signature, and the public key is used to verify it. The security of RSA is based on the difficulty of factoring large composite numbers, making it widely used for secure communication. The ElGamal signature scheme is based on the Diffie-Hellman key exchange protocol. It also involves a public key and a private key. The ElGamal algorithm is based on several mathematical concepts in number theory such as modular exponentiation and the discrete logarithm problem.


A variety of issues may arise in the implementation of digital signatures schemes that compromised their security. These areas of concern include key management, weak random number generation, replay attacks, and hash function vulnerabilities.

Video: Bitcoin: Digital Signatures  (<https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-digital-signatures>) (9:46)


This video provides a high-level explanation of digital signature schemes, which are a fundamental building block in many cryptographic protocols.

Video: Breaking RSA  (<https://www.youtube.com/watch?v=-ShwJqAalOk>) (14:49)

This video discusses the vulnerabilities in RSA encryption, specifically the potential for breaking RSA keys when the values for "p" and "q" are weak due to being too close to each other.

A captioned version of this video is available: Breaking RSA (CC) 

([https://urldefense.com/v3/__https://youtu.be/qsKJzxu7olw__;!!BelmMA!7oEVIJrIYNNmlSUVYIKx_WMqfchhG0IKa9GjepszgaLJLhqRtfVIEi9lwoX6uERDkJMHdu5AJAh93GIKIOza87WbyotzBToCtQ\\$](https://urldefense.com/v3/__https://youtu.be/qsKJzxu7olw__;!!BelmMA!7oEVIJrIYNNmlSUVYIKx_WMqfchhG0IKa9GjepszgaLJLhqRtfVIEi9lwoX6uERDkJMHdu5AJAh93GIKIOza87WbyotzBToCtQ$))

A video transcript is available: Transcript for Breaking RSA 

([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=%7B9919C153-35B6-40EB-B291-3FC155F5D4FB%7D&file=MAT%20260%20Transcript%20for%20Breaking%20RSA%20Computerp)

[sourcedoc=%7B9919C153-35B6-40EB-B291-](https://snhu.sharepoint.com/:w:/r/sites/LearningScienceAssessment/_layouts/15/Doc.aspx?sourcedoc=%7B9919C153-35B6-40EB-B291-3FC155F5D4FB%7D&file=MAT%20260%20Transcript%20for%20Breaking%20RSA%20Computerp)

[3FC155F5D4FB%7D&file=MAT%20260%20Transcript%20for%20Breaking%20RSA%20Computerp](https://snhu.sharepoint.com/:w:/r/sites/LearningScienceAssessment/_layouts/15/Doc.aspx?sourcedoc=%7B9919C153-35B6-40EB-B291-3FC155F5D4FB%7D&file=MAT%20260%20Transcript%20for%20Breaking%20RSA%20Computerp)
[hile.docx&action=default&mobileredirect=true](https://snhu.sharepoint.com/:w:/r/sites/LearningScienceAssessment/_layouts/15/Doc.aspx?sourcedoc=%7B9919C153-35B6-40EB-B291-3FC155F5D4FB%7D&file=MAT%20260%20Transcript%20for%20Breaking%20RSA%20Computerp))