COURSE SYLLABUS

Cryptography Essentials Course

Learn how encryption, hashing, and digital signatures work and where each fits, so you can make sound cryptography decisions.

Group classes in Live Online and onsite training is available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/courses/cryptography-essentials-course

support@graduateschool.edu •
(888) 744-4723

Course Outline

Module 1: Why Cryptography Matters: Goals and Core Concepts

- Lessons:
  - What Problem Cryptography Actually Solves
  - The Four Goals: Confidentiality, Integrity, Authenticity, Non-Repudiation
  - Plaintext, Ciphertext, and the Idea of a Key
- Applied activity: Learners review a short scenario describing a business email exchange and identify which of the four cryptographic goals is at risk if a specific control, encryption, a hash check, or a digital signature, is missing.

Module 2: Symmetric Encryption

- Lessons:
  - How Symmetric Encryption Works
  - Common Symmetric Algorithms and Key Lengths
  - Block Ciphers versus Stream Ciphers
  - The Key Distribution Problem
- Applied activity: Learners review a short scenario in which two remote offices need to exchange encrypted files and identify the practical problem with securely sharing a symmetric key over an untrusted channel, without yet knowing the solution covered in the next module.

Module 3: Asymmetric Encryption and Public Key Cryptography

- Lessons:
  - How Asymmetric Encryption Solves the Key Distribution Problem
  - Public and Private Keys: What Each One Does
  - Common Asymmetric Algorithms
  - Symmetric versus Asymmetric: When Each Is Used
- Applied activity: Learners review a short scenario describing an online purchase and identify which parts of the transaction likely use symmetric encryption and which use asymmetric encryption, and why.

Module 4: Hashing and Data Integrity

- Lessons:

- What a Hash Function Does
- Properties of a Secure Hash Function
- Using Hashes to Verify Integrity
- Hashing Passwords: Why It Is Not Encryption

- Applied activity: Learners are given a described file and its published hash value, then a second, slightly modified version of the file with a different hash value, and explain what the mismatch tells them.

Module 5: Digital Signatures and Non-Repudiation

- Lessons:
  - How a Digital Signature Is Created and Verified
  - Why a Digital Signature Provides Non-Repudiation
  - Digital Signatures versus Encryption: Not the Same Job
- Applied activity: Learners review a short scenario in which a signed document is later disputed by its sender and explain, step by step, how the digital signature settles the dispute.

Module 6: Public Key Infrastructure and Certificates

- Lessons:
  - What Problem PKI Solves: Trusting a Public Key
  - Certificate Authorities and the Chain of Trust
  - What Is Inside a Digital Certificate
  - Certificate Validation and Revocation
- Applied activity: Learners review a short, described certificate chain, root certificate authority, intermediate authority, and website certificate, and explain what breaks if the intermediate certificate is removed from the chain.

Module 7: Cryptography in Practice: Protocols and Everyday Use Cases

- Lessons:
  - Encrypting Data in Transit: TLS and HTTPS
  - Encrypting Data at Rest
  - Virtual Private Networks and Secure Tunnels
  - Where You Already Use Cryptography Every Day
- Applied activity: Learners review a short description of an organization's data flows (files on a laptop, email in transit, a database) and identify whether encryption in transit, encryption at rest, or both, applies to each.

Module 8: Cryptographic Weaknesses and Common Attacks

- Lessons:
  - Weak and Outdated Algorithms
  - Key Management Failures
  - Common Attacks on Cryptographic Systems
- Applied activity: Learners review a short scenario describing an organization that uses strong encryption but stores its keys in an insecure location and explain why the encryption does not actually protect the data in that case.