Document Generated: 11/22/2026

Learning Style: Virtual Classroom

Technology: EC-Council

Difficulty: Intermediate

Course Duration: 3 Days

EC-Council Certified Encryption Specialist (ECES)



About This Course:

Encryption protects nearly every system an organization runs, yet many security professionals use it without fully understanding how it works or where it fails. The EC-Council Certified Encryption Specialist (ECES) course gives you a solid grounding in modern cryptography.

Course Objectives:

- Explain the history and foundational concepts of cryptography, from classic ciphers to modern algorithms
- Describe how symmetric algorithms work, including Feistel networks, DES, AES, Blowfish, Twofish, and Skipjack
- Understand hashing algorithms such as MD5, MD6, SHA, and RIPEMD, and their role in data integrity
- Apply the number theory concepts behind asymmetric cryptography, including RSA, ElGamal, DSA, and elliptic curve cryptography
- Identify the different types of encryption standards and how they differ
- Recognize correct and incorrect deployments of encryption technologies
- Avoid common mistakes made when implementing encryption
- Apply best practices for implementing encryption in VPNs, disk encryption, digital certificates, and wireless networks
- Use cryptanalysis techniques to strengthen your penetration testing skills
- Prepare for the EC-Council Certified Encryption Specialist (ECES) exam

Audience:

- Penetration testers and ethical hackers
- Computer forensics specialists
- Information security analysts and security operations staff
- Cloud security architects, designers, and developers
- IT professionals who select or implement VPNs, PKI, or digital certificates
- Developers who build operating systems, cryptographic systems, or blockchain-based solutions
- Students and professionals who want a strong foundation in cryptography

Prerequisites:

There are no formal prerequisites for this course. However, we recommend that you have:

- A basic understanding of networking concepts (TCP/IP, network protocols)

- General familiarity with information security principles
- Comfort with basic math, since the course introduces the number theory used in asymmetric cryptography

Course Outline:

- Module 01: Introduction and History of Cryptography
- Module 02: Symmetric Cryptography & Hashes
- Module 03: Number Theory and Asymmetric Cryptography
- Module 04: Applications of Cryptography
- Module 05: Cryptanalysis
- Module 06: Quantum Computing and Cryptography