E|CES
EC-Council Certified Encryption Specialist

EC-Council
Building A Culture Of Security

EC-COUNCIL CERTIFIED ENCRYPTION SPECIALIST

Elevate Your Data Security with Cryptographic and Quantum Practices

INTRODUCING THE E|CESv3:

World's Most Comprehensive and Vendor Neutral Encryption Certification Program

Data is crucial for both businesses and individuals. Encryption is a powerful technique to keep it safe. Encryption transforms data into a secure format, making it unreadable for unauthorized access. This technique ensures privacy, integrity, and authenticity of the data. As cyber threats grow, encryption becomes crucial to keep your information safe.

Who is an encryption specialist?

Encryption specialists are cyber experts who safeguard data in a secure and unreadable format to prevent unauthorized access, skillfully choosing and implementing encryption algorithms into various systems. They specialize in implementing cryptographic methods to protect sensitive data, essential in securing information and preventing cyberattacks.

What is the job role of an encryption specialist?

Encryption specialists integrate encryption methods into systems, ensuring data stays hidden from attackers. Responsible for managing cryptographic keys, these cyber specialists conduct regular audits, respond to security incidents, and develop and enforce encryption policies. They also collaborate with teams and ensure safety compliance.

Why is an encryption specialist important for any organization?

An encryption specialist is essential for organizations as they safeguard sensitive data through encryption methods and choose the required algorithms. An organization's data, if leaked, can have serious repercussions. An encryption specialist's role also protects an organization's critical information (like customer data, credentials, or financial records) from unauthorized access and potential cyber threats.

E|CESv3 Program Overview

What is E|CES?

EC-Council Certified Encryption Specialist (E|CES) program is designed to introduce professionals and students to the intricate field of cryptography. Covering a broad spectrum of topics, the E|CES course delves into modern symmetric key cryptography, offering detailed insights into algorithms like Feistel Functions, DES, and AES. Additionally, students gain familiarity with various other algorithms, including Blowfish, Twofish, Skipjack, CAST, TEA, and more. The curriculum extends to information theory basics as applied to cryptography, covering essential concepts such as hashing algorithms (MD5, MD6, SHA, GOST, RIPMD 256) and asymmetric cryptography with in-depth discussions on RSA, Elgamal, Elliptic Curve, and Digital Signature Algorithm (DSA).

Throughout the program, students delve into crucial cryptographic principles like diffusion, confusion, and Kerckhoff's principle. Practical application is emphasized, enabling students to work with cryptographic algorithms from classical ciphers like the Caesar cipher to contemporary methods such as AES and RSA. Beyond theory, the course equips students with hands-on experience setting up a VPN, encrypting a drive, and exploring steganography. Furthermore, E|CES provides practical cryptanalysis and quantum computing knowledge, ensuring a comprehensive understanding of traditional and cutting-edge cryptographic concepts.

Completing the E|CES program empowers individuals to make informed decisions in selecting suitable encryption standards for their organizations. Candidates learn the theoretical aspects of cryptography and possess the practical skills necessary for effective technology deployment. This includes the ability to implement encryption techniques, secure data with VPNs, and navigate the complexities of emerging technologies like quantum computing, making them valuable assets in cybersecurity.

Why Do We Need E|CES?

As cyber threats evolve, understanding cryptographic principles becomes essential for professionals in various roles, from network administrators to cybersecurity analysts.

The E|CES program goes beyond surface-level information, offering in-depth knowledge of various cryptographic algorithms, both symmetric and asymmetric.

Gain hands-on experience with cryptographic algorithms, learn how to set up secure communication channels through VPNs, encrypt data, and explore steganography.

With coverage of topics like quantum computing, the program ensures that participants are prepared for the challenges posed by emerging technologies.

Graduates of the program have the knowledge and skills needed to make informed decisions concerning encryption standards for their organizations.

The E|CES program contributes to creating a better-prepared workforce to address the increasing complexity of cybersecurity challenges.

Cryptoanalysis knowledge is incredibly useful for ethical hackers and penetration testing specialists, as most courses skip it.

E|CES Course Modules:

Module 01: Introduction and History of Cryptography

- Gaps in Crypto Knowledge
- What is Cryptography?
- History of Cryptography
- Mono-Alphabet Substitution
  - Caesar Cipher
  - Atbash Cipher
  - Affine Cipher
  - ROT13 Cipher
  - Scytale
  - Single Substitution Weaknesses
- Multi-Alphabet Substitution
  - Cipher Disk
  - Vigenère Cipher
    - Vig q enère Cipher: Example
    - Breaking the Vigenère Cipher
  - Gronsfeld Cipher
  - Playfair Cipher
  - Polybius Cipher
  - ADFGVX Cipher
- Homophonic Substitution
- Null Ciphers
- Book Ciphers
- Rail Fence Ciphers
- Vernam Cipher
- The Enigma Machine
- CrypTool

Module 02: Symmetric Cryptography and Hashes

- Symmetric Cryptography
- Information Theory
  - Information Theory Cryptography Concepts
- Kerckhoffs's Principle
- Substitution
- Transposition
- Binary Math
  - Binary AND
  - Binary OR
  - Binary XOR
- Block Cipher vs. Stream Cipher
- Symmetric Block Cipher Algorithms
  - Basic Facts of the Feistel Function
  - S-Box
    - S-Box Design
  - The Feistel Function
  - Unbalanced Feistel Cipher
  - Data Encryption Standard (DES)
  - 3DES
    - DESx
    - Whitening
  - Advanced Encryption Standard (AES)
    - AES General Overview
    - AES Specifics
  - Blowfish
  - Serpent
  - Twofish
  - Skipjack
  - International Data Encryption Algorithm (IDEA)
  - CAST
  - Tiny Encryption Algorithm (TEA)
  - SHARK
  - GOST
  - McGuffin
- Symmetric Algorithm Methods
  - Electronic Codebook (ECB)
  - Cipher-Block Chaining (CBC)
  - Propagating Cipher-Block

- Chaining (PCBC)
  - Cipher Feedback (CFB)
  - Output Feedback (OFB)
  - Counter (CTR)
  - Initialization Vector (IV)
- Symmetric Stream Ciphers
  - Example of Symmetric Stream Ciphers: RC4
  - Example of Symmetric Stream Ciphers: FISH
  - Example of Symmetric Stream Ciphers: PIKE
- Hash Function
  - Hash – Salt
  - MD5
    - The MD5 Algorithm
  - MD6
  - Secure Hash Algorithm (SHA)
  - FORK-256
  - RIPEMD-160
  - Tiger
  - Blake
  - Haval
  - Whirlpool
  - Skein
  - NTLM – Windows Hashing
    - NTLM
  - MAC & HMAC
  - Key Stretching
- CryptoBench

Module 03: Number Theory and Asymmetric Cryptography

- Asymmetric Encryption
- Basic Number Facts
  - Prime Numbers
  - Mersenne Primes
  - Fermat Prime
  - Co-Prime Numbers
  - Euler's Totient
  - Summation
  - Modulus Operator
  - Congruence Numbers
  - Solving Congruence
  - Fibonacci Numbers
  - Algebraic Groups
  - Rings
  - Field
  - Galois Field
  - Logarithms
  - Natural Logarithms
  - Discrete Logarithms
- Birthday Theorem
  - Birthday Paradox
    - Birthday Paradox: Probability
  - Birthday Attack
- Random Number Generator
  - Classification of Random Number Generator
  - Traits of a Good PRNG
  - Middle Square Method
  - Naor-Reingold and Mersenne Twister Pseudorandom Function
  - Linear Congruential Generator
  - Lehmer Random Number Generator
  - Lagged Fibonacci Generator (LFG)
  - Blum Blum Shub
  - Yarrow
  - Fortuna
- Diffie-Hellman
- Rivest Shamir Adleman (RSA)
  - RSA – How it Works
  - RSA Example
- Menezes–Qu–Vanstone
- MQV

- Digital Signature Algorithm
  - Signing with DSA
- Elliptic Curve
  - Elliptic Curve Variations
  - Elliptic Curve
- Elgamal
- Cramer – Shoup
- YAK
- Forward Secrecy
- CrypTool

Module 04: Applications of Cryptography

- FIPS Standards
- Digital Signatures
- What is a Digital Certificate?
  - Digital Certificates
    - X.509
    - X.509 Certificates
    - X.509 Certificate Content
    - X.509 Certificate File Extensions
- Certificate Authority (CA)
- Registration Authority (RA)
- Certificate Authority – Verisign
- Certificate Types
- Public Key Infrastructure (PKI)
- Digital Certificate Terminology
- Server-based Certificate Validation Protocol
- Digital Certificate Management
- Trust Models
- Certificates and Web Servers
- Microsoft Certificate Services
- Windows Certificates: certmgr.msc
- Authentication
  - Password Authentication Protocol (PAP)
  - Shiva Password Authentication Protocol (S-PAP)
  - Challenge-Handshake Authentication Protocol (CHAP)
  - Extensible Authentication Protocol (EAP)
  - Kerberos
    - Components of Kerberos System
    - Kerberos Authentication Process
- PGP Certificates
- Wi-Fi Encryption
  - Wired Equivalent Privacy (WEP)
  - WPA - Wi-Fi Protected Access
  - WPA2
  - WPA3
- SSL
- TLS
  - TLS v 1.3
- Diagram
- Protocols
- Common SSL/TLS Libraries
- Virtual Private Network (VPN)
  - Point-to-Point Tunneling Protocol (PPTP)
    - PPTP VPN
  - Layer 2 Tunneling Protocol VPN
  - Internet Protocol Security (IPSec) VPN
    - IPsec
    - IPSec – Terms
    - IPSec – Protocol Suite
  - SSL/TLS VPN
- Split Tunneling
- VPN Modes
- Encrypting Files
  - Backing up the EFS key
  - Restoring the EFS Key

- BitLocker
  - BitLocker: Screenshot
- Common Cryptography: Mistakes
- Steganography
  - Steganography Terms
  - Historical Steganography
  - Steganography Details
  - Other Forms of Steganography
  - How to Embed?
  - Steganographic File Systems
  - Steganographic Software
  - Demonstration
- Steganalysis
  - Steganalysis – Raw Quick Pair
  - Steganalysis – Chi-Square Analysis
  - Steganalysis – Audio Steganalysis
- Steganography Detection Tools
- National Security Agency and Cryptography
  - NSA Suite A Encryption Algorithms
  - NSA Suite B Encryption Algorithms
  - National Security Agency: Type 1 Algorithms
  - National Security Agency: Type 2 Algorithms
  - National Security Agency: Type 3 Algorithms
  - National Security Agency: Type 4 Algorithms
- Unbreakable Encryption
- Blockchain

Module 05: Cryptanalysis

- Breaking Ciphers
- Cryptanalysis
- Frequency Analysis
- Kasiski
- Cracking Modern Cryptography
  - Cracking Modern Cryptography: Known Plaintext/ Chosen Plaintext Attack
  - Cracking Modern Cryptography: Ciphertext-only and Related-key Attack
- Linear Cryptanalysis
- Differential Cryptanalysis
- Integral Cryptanalysis
- Cryptanalysis Resources
- Cryptanalysis Success
- Rainbow Tables
  - Rainbow Table
- Password Cracking
- Tools

Module 06: Quantum Computing and Cryptography

- Quantum Computing and Cryptography
- Timeline
- Issues for QC
- Two Branches
  - Quantum Key Distribution (QKD)
    - QKD
    - What do we need?
    - Qubits
    - Trends
  - Quantum Key Distribution (QKD)
    - The Problem
    - Why?
- NIST
- Major Approaches
- Lattice-Based Crypto
- Learning with Errors
- GGH
- NTRU
- Overview
- Module Overview

What Do You Learn from E|CES?

01 Types of encryption standards and their differences

02 How to select the best standard for your organization

03 How to enhance your pen-testing knowledge in encryption

04 Correct and incorrect deployment of encryption technologies

05 Common mistakes made in implementing encryption technologies

06 Best practices when implementing encryption technologies

07 Quantum computing and cryptography

Training Prerequisites

No prior knowledge of cryptography is assumed, and no mathematical skills beyond basic algebra are required.

Who Can Apply for E|CES?

- Penetration Testers and Computer Forensics Specialists
- Cloud security architects, designers, and developers
- Anyone involved in selecting and implementing VPNs or digital certificates, or information security operations.
- Anyone involved in developing operating systems, cryptography systems, blockchain based solutions, etc.

Training Information

Title of the Course: **EC-Council Certified Encryption Specialist**

Version:	Training Duration:	Training Timing:
3	3 Days / 20 Hours	9:00 AM to 4:00 PM

E|CES Exam Information

Exam Title: **EC-Council Certified Encryption Specialist**

Exam Code:	Number of Questions:	Duration:	Exam Availability Locations:
212-81	50	2 Hours	EC-Council ExamPortal

Test Formats:	Passing Score:
Multiple Choice	70%

About EC-Council

EC-Council invented the Certified Ethical Hacker (C|EH) Program. Founded in 2001 in response to 9/11, the EC-Council's mission is to provide the training and certifications that apprentice and experienced cybersecurity professionals need to keep corporations, government agencies, and others who employ them safe from cyber-attacks.

Best known for its Certified Ethical Hacker program, EC-Council today offers 200 different training programs, certifications, and degrees in everything from Computer Forensic Investigation and Security Analysis to Threat Intelligence and Information Security. An ISO/IEC 17024 Accredited organization recognized under the US Defense Department Directive 8140/8570 and many other authoritative cybersecurity bodies worldwide, the company has certified over 350,000 professionals across the globe. EC-Council is the gold standard in cybersecurity education and certification, trusted by seven of the Fortune 10, half of the Fortune 100, and various agencies, public and private, across 140 nations.

A truly global organization with a driving belief in bringing diversity, equity, and inclusion to the modern cybersecurity workforce, EC-Council maintains 11 offices in the US, the UK, India, Malaysia, Singapore, and Indonesia.

For more details, visit: www.eccouncil.org