3 Days

ECES- [EC-Council Certified Encryption Specialist]

The EC-Council Certified Encryption Specialist (ECES) Training sets the foundation base for the professionals in the field of cryptography. The training will provide hands-on lab experience with steganography to fundamentals of symmetric and modern key cryptographic algorithms such as Feistel Networks, DES, and AES.

Moreover, the course will also introduce the deployment of asymmetric cryptographic algorithms such as DSA, RSA, ElGamal and Elliptic Curve.

A professional who successfully completes the certification will be able to select the right encryption standards that are most beneficial to the organization. This course will provide essential knowledge to cryptanalysis that is also useful to any penetration testing. The ECES Certification will qualify you to carry out the best practices to implement encryption technologies in an organization.

Course Details

Course Outline

1. Introduction and History of Cryptography

- What is Cryptography?
- History
- Monoalphabetic Substitution
- Caesar Cipher
- Atbash Cipher
- Scytale
- ROT 13
- Single Substitution Weaknesses
- Cipher Disk
- Multi-Alphabet Substitution
- Vigenère Cipher
- Breaking the Vigenère Cipher
- The ADFGVX cipher
- The Enigma Machine
- CrypTool
- Playfair

2. Symmetric Cryptography & Hashes

- Symmetric Cryptography
- Information Theory Cryptography Concepts
- Kerckhoffs's Principle
- Substitution and Transposition
- Binary M, AND, OR, XOR

- Block Cipher vs. Stream Cipher
- Symmetric Block Cipher Algorithms
- Basic Facts of the Feistel Function
- The Feistel Function
- A Simple View of a Single Round
- Unbalanced Feistel Cipher
- DES, 3DES, DESx
- AES
- AES Specifics
- AES General Overview
- Whitening
- Blowfish, Twofish, Serpent, Skipjack
- IDEA
- Symmetric Algorithm Methods
- Electronic Codebook (ECB)
- Propagating Cipher-Block Chaining (PCBC)
- Cipher-Block Chaining (CBC)
- Cipher Feedback (CFB)
- Output Feedback (OFB)
- Counter (CTR)
- Initialization Vector (IV)
- Symmetric Stream Ciphers
- Hash – Salt
- MD5, MD6 & MD5 Algorithm
- Secure Hash Algorithm (SHA)
- RIPEMD – 160
- GOST
- Tiger
- Fork 256
- Crypto Bench

3. Number Theory and Asymmetric Cryptography

- Asymmetric Encryption
- Basic Number Facts
- Euler's Totient
- Modulus Operator
- Birthday Theorem
- Birthday Problem
- Birthday Attack
- Fibonacci Numbers
- Random Number Generators
- Classification of Random Number Generators
- Naor-Reingold and Mersenne Twister Pseudorandom Function
- Lehmer Random Number Generator
- Linear Congruential Generator
- Lagged Fibonacci Generator
- Diffie-Hellman
- Rivest Shamir Adleman (RSA)
- RSA – How it Works
- Menezes–Qu–Vanstone
- Digital Signature Algorithm
- Signing with DSA
- Elliptic Curve
- Elgamal
- CrypTool

4. Applications of Cryptography Kong

- Digital Signatures & Digital Certificates
- X.509 Certificates, Content & File Extensions

- Certificate Authority (CA), Registration Authority (RA) & Public Key Infrastructure (PKI)
- Server-based Certificate Validation Protocol
- Digital Certificate Management
- Trust Models
- Certificates and Web Servers
- Microsoft Certificate Services
- Windows Certificates: certmgr.msc
- Password Authentication Protocol (PAP)
- Shiva Password Authentication Protocol (S-PAP)
- Challenge-Handshake Authentication Protocol (CHAP)
- Kerberos & its Components
- Pretty Good Privacy (PGP)
- PGP Certificates
- Wifi Encryption
- Wired Equivalent Privacy (WEP)
- WPA – Wi-Fi Protected Access
- WPA2, SSL, TLS
- Virtual Private Network (VPN)
- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol VPN
- Internet Protocol Security VPN
- SSL/VPN
- Encrypting Files
- Backing up the EFS key
- Restoring the EFS Key
- Bitlocker
- Disk Encryption Software: Truecrypt
- Steganography – Terms, History, Details & Forms
- Steganography Implementations
- Demonstration & Steganalysis
- National Security Agency and Cryptography
- Steganography Detection Tools
- 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

Who Should Attend

The EC-Council Certified Encryption Specialist (ECES) Training course is intended for:

- People involved in the selection of implementation of VPNs or Digital Certificates
- Suitable for ethical hackers and penetration testing professionals

Pre Requisite

The eligibility for EC-Council ECES certification course is:

- The participant should have basic knowledge of information security and network security.

Exams

EC-Council Certified Encryption Specialist (E|CES) [ECES 212-81 exam]

464, Udyog Vihar Phase V,Gurgaon (Delhi NCR)-122016,India	+91 8882 233 777	training@mercury.co.in	www.mercurysolutions.co

Date - Jun 18, 2025