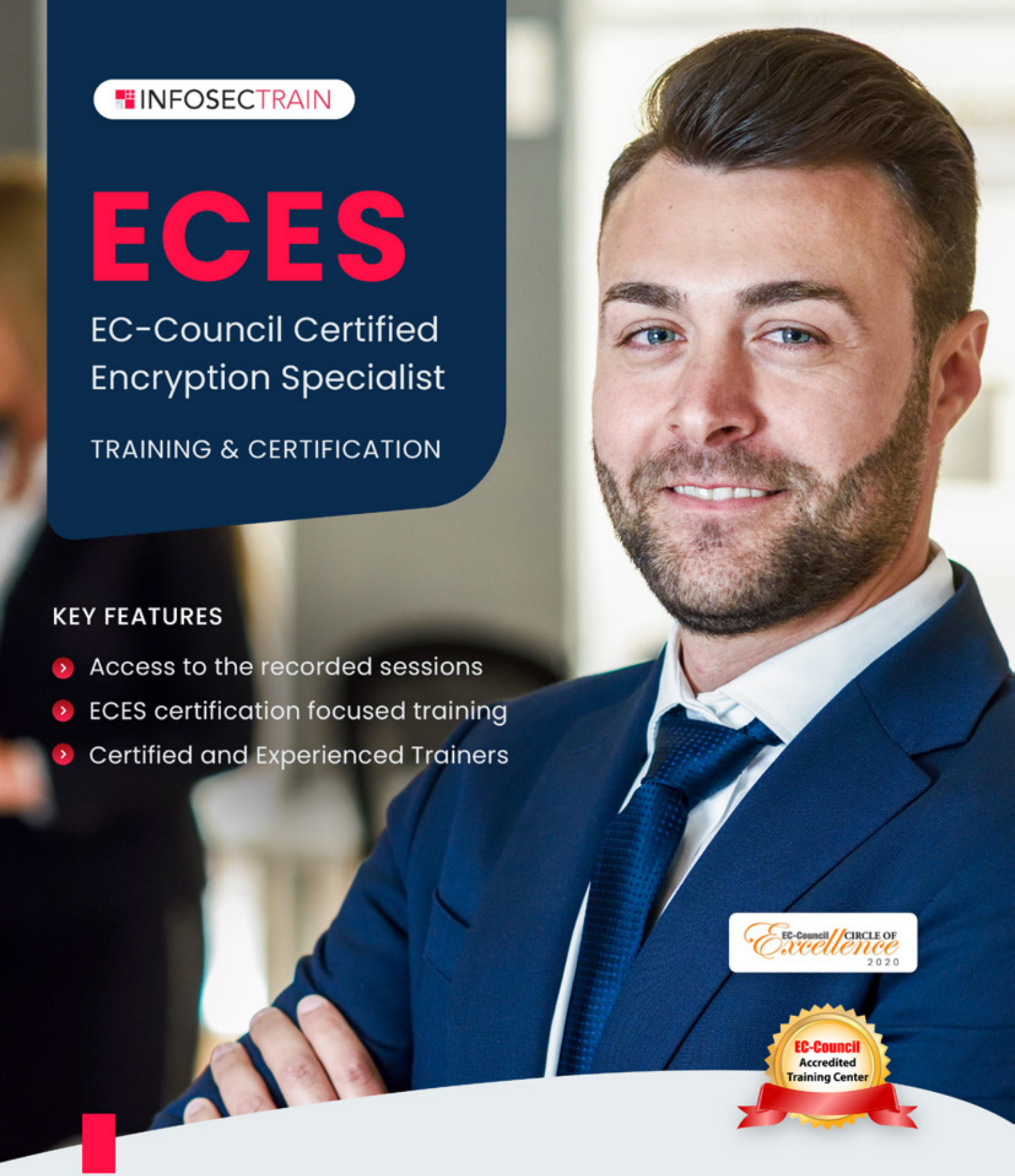
INFOSECTRAIN

ECES

EC-Council Certified Encryption Specialist

TRAINING & CERTIFICATION



KEY FEATURES

- Access to the recorded sessions
- ECES certification focused training
- Certified and Experienced Trainers

EC-Council CIRCLE OF Excellence 2020

EC-Council Accredited Training Center

EC-Council Certified Encryption Specialist, ECES certification and training helps information security professionals to gain far-reaching understanding of cryptography. The training provides understanding of the core concepts of futuristic key and symmetric cryptography along with a detailed understanding of algorithms including DES, AES and...

Overview

EC-Council Certified Encryption Specialist, ECES certification and training helps information security professionals to gain far-reaching understanding of cryptography. The training provides understanding of the core concepts of futuristic key and symmetric cryptography along with a detailed understanding of algorithms including DES, AES and Feistel Networks. Candidates also learn about algorithms such as Twofish, Blowfish, and Skipjack, hashing algorithms such as SHA, MD5, MD6, RIPMD 256, Gost, etc. The program also covers the fundamentals of asymmetric cryptography that consists of ElGamal, RSA, DSA, and Elliptic Curve. Eminent concepts like confusion, diffusion, and Kerkchoff's principle, setting up a VPN, encrypting a drive, implementing steganography and cryptographic algorithms including ciphers such as Caesar cipher, AES and RSA are also explained during this certification training.

Why Certified Encryption Specialist?

This encryption specialist training and certification course helps you acquire extensive understanding of:

- History of cryptography
- Fundamentals of symmetric cryptography and hashes
- Implementing number theory and asymmetric cryptography
- Applying cryptography
- Performing cryptanalysis

Target Audience

- Ethical hackers
- Penetration testing professionals
- Cryptanalysts

Pre-Requisite

Work experience of at least one year in the Information Security domain

Exam Information

To become the ECES certified, you have passed the following exam:

Certification Name	EC-Council Certified Encryption Specialist (ECES)
Test Format	Multiple choice questions
Number of Questions	50
Test Duration	2 hours
Passing Score	70%

Why Infosec Train?

Certified & Experienced Instructor

Flexible Schedule

Access to the recorded sessions

Post Training Support

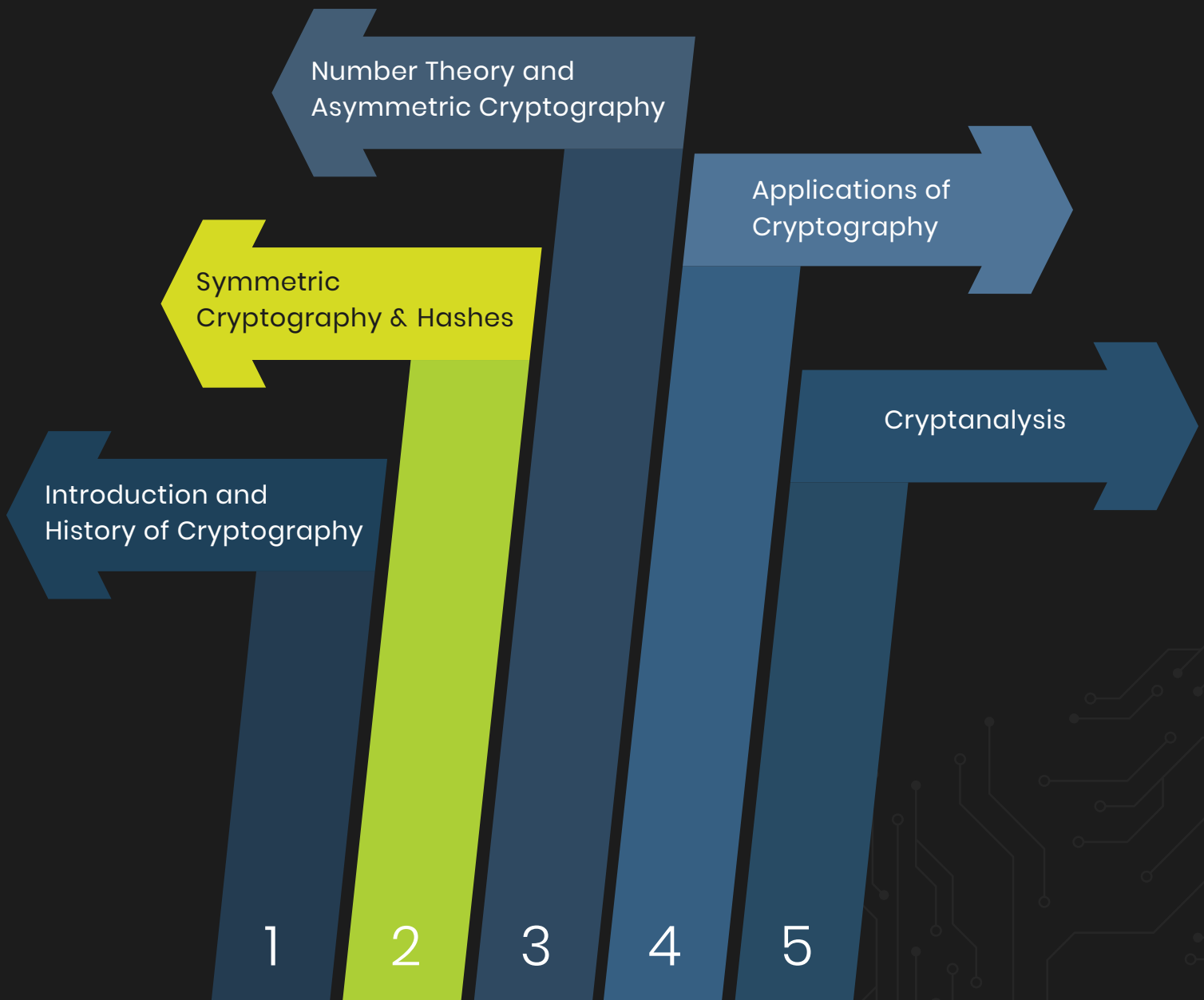
Tailor Made Training

EC-Council Authorized Partner

INFOSECTRAIN

ECES Course Outline

The five domains in ECES include



Domain 1: Introduction and History of Cryptography

- 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
    - Vigenère Cipher: Example
    - Breaking the Vigenère Cipher
  - Playfair Cipher
  - ADFGVX Cipher
- Homophonic Substitution
- Null Ciphers
- Book Ciphers
- Rail Fence Ciphers
- The Enigma Machine
- CrypTool

Domain 2: Symmetric Cryptography & 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
    - 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
- 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
  - GOST
  - Tiger
  - MAC and HMAC
- CryptoBench

Domain 3: Number Theory and Asymmetric Cryptography

- Asymmetric Encryption
- Basic Number Facts
  - Prime Numbers
  - Co-Prime Numbers
  - Euler's Totient
  - Modulus Operator
  - Fibonacci Numbers
- Birthday Theorem
  - Birthday Paradox
    - Birthday Paradox: Probability
  - Birthday Attack
- Random Number Generator
  - Classification of Random Number Generator
  - Traits of a Good PRNG
  - 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
- Digital Signature Algorithm
  - Signing with DSA
- Elliptic Curve
  - Elliptic Curve Variations
- Elgamal
- CrypTool

Domain 4: 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)
  - Certificate Authority – Verisign
- Registration Authority (RA)
- 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)
  - Kerberos
    - Components of Kerberos System
    - Kerberos Authentication Process
- Pretty Good Privacy (PGP)
  - PGP Certificates

- Wi-Fi Encryption
  - Wired Equivalent Privacy (WEP)
  - WPA – Wi-Fi Protected Access
  - WPA2
- SSL
- TLS
- Virtual Private Network (VPN)
  - Point-to-Point Tunneling Protocol (PPTP)
    - PPTP VPN
  - Layer 2 Tunneling Protocol VPN
  - Internet Protocol Security VPN
  - SSL/TLS VPN
- Encrypting Files
  - Backing up the EFS key
  - Restoring the EFS Key
- BitLocker
  - BitLocker: Screenshot
- Disk Encryption Software: VeraCrypt
- Common Cryptography Mistakes
- Steganography
  - Steganography Terms
  - Historical Steganography
  - Steganography Details
  - Other Forms of Steganography
  - How to Embed?
  - Steganographic File Systems
  - Steganography Implementations
  - 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

Domain 5: Cryptanalysis

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

www.infosectrain.com | sales@infosectrain.com