EC-Council

Ferro Technics Inc.

# SECURING CRITICAL DATA WITH ENCRYPTION

## EC-Council Certified Encryption Specialist v2

ECES™

EC-Council Certified Encryption Specialist

PROGRAM BROCHURE

# Introducing the ECESv2:

## World's most comprehensive and vendor neutral Encryption certification program

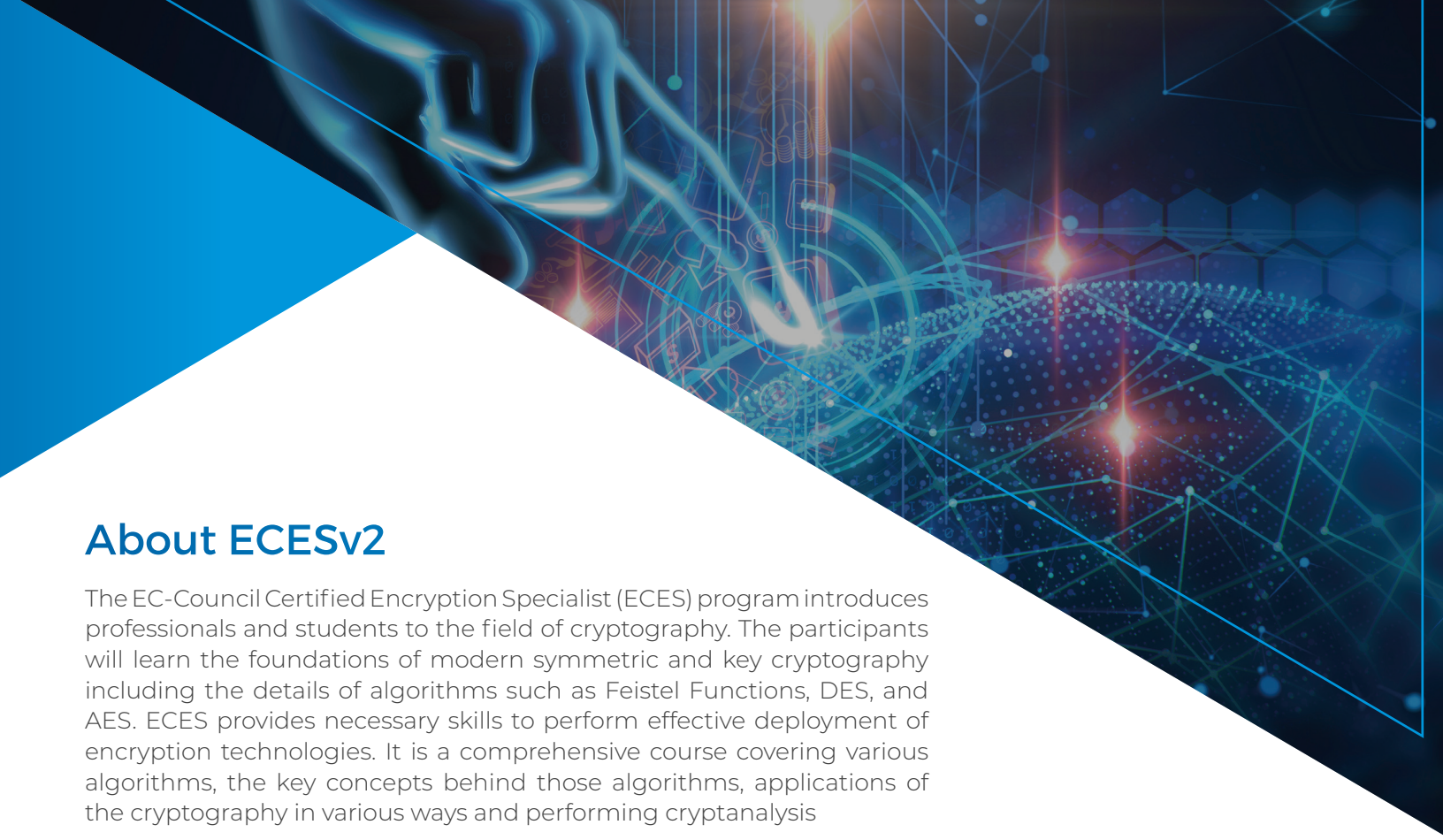

## About Encryption

As the size and frequency of data breaches increasing over time, more and more organizations are rapidly recognizing that encryption is no longer an option. They are busy formulating comprehensive strategy and shifting their stance towards encryption technologies and rapidly deploying a range of technologies to defend and protect their sensitive data from internal and external threats. Increasingly, business users are influencing the adoption of encryption technologies more than IT operations teams.

Adoption of encryption in organizations are increasing at a rapid pace as are the urgency in the encryption implementation plans. The increasing rate of adoption is due to fast evolving regulations and necessity to protect sensitive data across enterprise networks, multiple devices and especially the increasing move to storing data on a cloud.

If you think that there is only one type of encryption – think again!

Encryption considerations differ for technologies namely – database encryption, VoIP encryption, portable storage encryption, mobile devices encryption, Wi-Fi encryption, e-mail encryption, file encryption, network link encryption, web server encryption, tape backup encryption and many more.



## About ECESv2

The EC-Council Certified Encryption Specialist (ECES) program introduces professionals and students to the field of cryptography. The participants will learn the foundations of modern symmetric and key cryptography including the details of algorithms such as Feistel Functions, DES, and AES. ECES provides necessary skills to perform effective deployment of encryption technologies. It is a comprehensive course covering various algorithms, the key concepts behind those algorithms, applications of the cryptography in various ways and performing cryptanalysis

**Other topics introduced:**

- Overview of other algorithms such as Blowfish, Twofish, and Skipjack
- Hashing algorithms including MD5, MD6, SHA, GOST, RIPMD 256 and others
- Asymmetric cryptography including thorough descriptions of RSA, Elgamal, Elliptic Curve, and DSA
- Significant concepts such as diffusion, confusion, and Kerkchoff's principle

**Participants will also be provided a practical application of the following:**

- Hands on experience in cryptographic algorithms ranging from classic ciphers like Caesar cipher to modern day algorithms such as AES and RSA
- How to set up a VPN and encrypt a drive
- Hands-on experience with steganography

> **I work with decryption tools in my current position. This class gives a better understanding of different algorithms and how to attack the weaknesses.**
>
> **- John Minotti**
>
> *Manager of Professional Services, AccessData, USA*

# Why Do We Need ECES?

Understanding the cryptography allows you to make informed choices

Without understanding the cryptography at some depth, people are limited to only marketing hype of information security solutions

A person successfully completing this course will be able to select the encryption standard that is most beneficial to their organization and understand how to effectively deploy that technology

Knowledge of cryptanalysis is very beneficial for ethical hackers and penetration testing professionals as most penetration testing courses skip cryptanalysis completely.

> **The course gave me a basic and at times advance understanding of cryptography. I really enjoyed the class. It gave a much better understanding of what cryptography entails. The course helps me to evaluate if an organization's security in these areas are up to standard.**
>
> **- Huey Nguyen**
>
> *Detective, Arlington Police Department, USA*

# Who Is It For?

## Prerequisites

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

## Target Audience

- **Penetration Testers and Computer Forensics Specialists**
- **Cloud Security architects, designers, and developers**
- **Anyone involved in selecting and implementing VPNs or digital certificates, Information Security Operations**
- **Anyone involved in developing Operating Systems, Cryptography Systems, Blockchain based solutions, etc.**

## Duration

3 days / 20 hours
(9:00 AM to 4:00 PM)

## Certification

The EC-Council Certified Encryption Specialist (ECES) may be taken on the last day of training (optional). Students need to pass the online exam to receive ECES certification.

> **The course provides a good insight of encryption. As a forensic examiner, it is not a matter of "If", but "When" you encounter situations where knowledge of encryption becomes useful.**
>
> **- Mike Weaver**
> *Detective, Arlington Police Department, USA*

# Exam Details

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

**Exam Code:**
212-81

**Number of Questions:**
50

**Duration:**
2 Hours

**Exam Availability:**
EC-Council Exam Portal

**Test Format:**
Multiple Choice

**Passing Score:**
70%

## What will you Learn?

- Types of encryption standards and their differences
- How to select the best standard for your organization?
- How to enhance your pen-testing knowledge in encryption?
- Correct and incorrect deployment of encryption technologies
- Common mistakes made in implementing encryption technologies
- Best practices when implementing encryption technologies

## Benefits/Takeaways

### The student will

- Develop skills to protect critical data in organizations with encryption
- Develop a deep understanding of essential cryptography algorithms and their applications
- Make informed decisions about applying encryption technologies
- Save time and cost by avoiding common mistakes in implementing encryption technologies effectively
- Develop working knowledge of cryptanalysis

# Course Outline

## Module 01: Introduction and History of Cryptography

- What is Cryptography?
- History of Cryptography
- Mono-Alphabet Substitution (Caesar Cipher, Atbash Cipher, Affine Cipher, ROT13 Cipher)
- Multi-Alphabet Substitution (Cipher Disk, Vigenère Cipher, Playfair Cipher, ADFGVX Cipher)
- Homophonic Substitution
- Null and Book Ciphers
- Rail Fence Ciphers
- The Enigma Machine
- CrypTool

## Module 02: Symmetric Cryptography and Hashes

- Symmetric Cryptography
- Information Theory
- Kerckhoffs's Principle
- Substitution and Transposition
- Binary Math
- Block Cipher vs. Stream Cipher
- Symmetric Block Cipher Algorithms (Feistel Function, DES, 3DES, AES, Blowfish, Serpent, Twofish, Skipjack, IDEA, CAST, TEA, SHARK)
- Symmetric Algorithm Methods
- Symmetric Stream Ciphers (RC4, FISH, PIKE)
- Hash Function (Hash – Salt, MD5, MD6, SHA, FORK-256, RIPEMD-160, GOST, Tiger)
- CryptoBench

## Module 03: Number Theory and Asymmetric Cryptography

- Asymmetric Encryption
- Basic Number Facts
- Birthday Theorem
- Random Number Generator
- Diffie-Hellman
- Rivest Shamir Adleman (RSA)
- Menezes–Qu–Vanstone
- Digital Signature Algorithm
- Elliptic Curve
- Elgamal
- CrypTool

## Module 04: Applications of Cryptography

- FIPS Standards
- Digital Signatures
- Digital Certificate
- Public Key Infrastructure (PKI)
- Digital Certificate Management
- Trust Models
- Certificates and Web Servers
- Authentication (PAP, S-PAP, CHAP, Kerberos)
- Pretty Good Privacy (PGP)
- Wi-Fi Encryption
- SSL and TLS
- Virtual Private Network (VPN)
- Encrypting Files
- BitLocker
- Disk Encryption Software: VeraCrypt
- Common Cryptography Mistakes
- Steganography
- Steganalysis
- Steganography Detection Tools
- National Security Agency and Cryptography
- Unbreakable Encryption

## Module 05: Cryptanalysis

- Breaking Ciphers
- Cryptanalysis
- Frequency Analysis
- Kasiski
- Cracking Modern Cryptography
- Linear Cryptanalysis
- Differential Cryptanalysis
- Integral Cryptanalysis
- Cryptanalysis Resources
- Cryptanalysis Success
- Rainbow Tables
- Password Cracking


EC-Council

www.eccouncil.org

Ferro Technics Inc.

www.ferrotechnics.com