# EC-Council Certified Encryption Specialist

## 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
  - 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

## 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
    - 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

## Module 03: 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

## 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)
  - 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

## Module 05: 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