EC-Council Certified Encryption Specialist (ECES)

Course Details

Course Outline

1. Introduction and History of Cryptography
    - What is Cryptography?
    - History
    - Mono-Alphabet Substitution
    - Caesar Cipher
    - Atbash Cipher
    - ROT 13
    - Scytale
    - Single Substitution Weaknesses
    - Multi-Alphabet Substitution
    - Cipher Disk
    - Vigenère Cipher
    - Vigenère Cipher: Example
    - Breaking the Vigenère Cipher
    - Playfair
    - The ADFGVX cipher
    - The Enigma Machine
    - CrypTool
2. Symmetric Cryptography & Hashes
    - Symmetric Cryptography
    - Information Theory
    - Information Theory Cryptography Concepts
    - Kerckhoffs’s Principle
    - Substitution
    - Transposition
    - Substitution and Transposition
    - Binary M

- ath
- Binary AND
- Binary OR
- Binary 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
- Whitening
- AES
- AES General Overview
- AES Specifics
- Blowfish
- Serpent
- Twofish
- Skipjack
- IDEA
- 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
- Hash – Salt
- MD5
- The MD5 Algorithm
- MD6
- Secure Hash Algorithm (SHA)
- Fork 256
- RIPEMD – 160
- GOST
- Tiger
- CryptoBench

3. Number Theory and Asymmetric Cryptography
    - Asymmetric Encryption
    - Basic Number Facts
    - Prime Numbers
    - Co-Prime
    - Eulers Totient
    - Modulus Operator
    - Fibonacci Numbers
    - Birthday Problem
    - Birthday Theorem
    - Birthday Attack
    - Random Number Generators
    - Classification of Random Number Generators
    - Naor-Reingold and Mersenne Twister Pseudorandom Function
    - Linear Congruential Generator
    - Lehmer Random Number Generator
    - Lagged Fibonacci Generator
    - 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

4. Applications of Cryptographyong
    - 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)
    - 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
- 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)
- PPTP VPN
- Layer 2 Tunneling Protocol VPN
- Internet Protocol Security VPN
- SSL/VPN
- Encrypting Files
- Backing up the EFS key
- Restoring the EFS Key
- Bitlocker
- Bitlocker: Screenshot
- Disk Encryption Software: Truecrypt
- Steganography
- Steganography Terms
- Historical Steganography
- Steganography Details
- Other Forms of Steganography
- 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

5. Introduction and History of Cryptography
    - What is Cryptography?
    - History
    - Mono-Alphabet Substitution
    - Caesar Cipher
    - Atbash Cipher
    - ROT 13
    - Scytale
    - Single Substitution Weaknesses
    - Multi-Alphabet Substitution
    - Cipher Disk
    - Vigenère Cipher
    - Vigenère Cipher: Example
    - Breaking the Vigenère Cipher
    - Playfair
    - The ADFGVX cipher
    - The Enigma Machine
    - CrypTool