EC-Council Certified Encryption Specialist (ECES) + Voucher d'examen

Durée: 3 Jours **Réf de cours: ECES** **Méthodes d'apprentissage: Classe à distance**

Résumé:

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 Networks, DES, and AES. 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: How to set up a VPNEncrypt a driveHands-on experience with steganographyHands on experience in cryptographic algorithms ranging from classic ciphers like Caesar cipher to modern day algorithms such as AES and RSA.

Classe à Distance - site Client

Cette formation peut être suivie à distance en synchrone depuis n'importe quel site pourvu d'une connexion internet (2 Mb/s en symétrique recommandés). Le programme (théorie et pratique) suit le même déroulé pédagogique qu'en présentiel. La solution technologique adoptée permet aux apprenants à distance de suivre les présentations faites au tableau, de voir et d'entendre l'instructeur et les participants en temps réel, mais également d'échanger avec eux.

Public visé:

Anyone involved in selecting, implementing VPN's or digital certificates should attend this course first. Without understanding the cryptography at some depth, people are limited to following marketing hype. Understanding the actual cryptography allows you to know which one to select. 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.

This course is excellent for ethical hackers and penetration testing professionals as most penetration testing courses skip cryptanalysis completely. Many penetration testing professionals testing usually don't attempt to crack cryptography. A basic knowledge of cryptanalysis is very beneficial to any penetration testing.

Objectifs pédagogiques:

- Introduction and History of Cryptoraphy
- Symmetric Cryptography and Hashes
- Number theory and Asymmetric Cryptography
- Applications of Cryptography part 1
- Applications of Cryptography part 2

Contenu:

Introduction and History of Cryptoraphy

- 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

Symmetric Cryptography and 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:

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

Applications of Cryptography part 1

- 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

Applications of Cryptography part 2

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

- 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
- 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

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement