TEKNOLOGISK INSTITUT

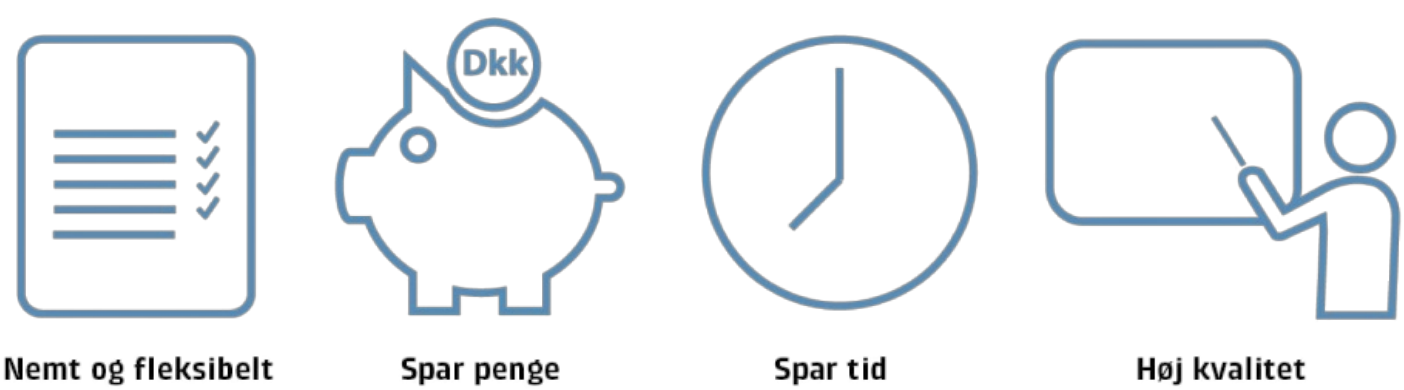
E|CES™

EC-COUNCIL CERTIFIED ENCRYPTION SPECIALIST

Online kursus
365 dage **DKK 7.999**
Nr. 90224 P ekskl. moms

Certified Encryption Specialist (ECES)

Denne kursuspakke indeholder EC-Councils Certified Encryption Specialist (ECES) program, som introducerer dig til området kryptografi. Du har mulighed for at blive certificeret og eksamenen er inkluderet i prisen. Kurset er på engelsk og foregår online, når det passer dig. Du har adgang til onlinekurset i 365 dage.



Bliv introduceret til kryptografi

Du vil få den grundlæggende viden om moderne symmetrisk og key kryptografi, inklusive algoritmer såsom Feistel

Teknologisk Institut
kurser@teknologisk.dk
+45 72 20 30 00

netværker, DES og AES m.fl. Derudover vil du lære at opsætte en VPN, kryptere et drev, og du får praktisk erfaring med steganografi og erfaring med kryptografiske algoritmer lige fra klassisk ciphers og Caesar cipher til mere moderne algoritmer som AES og RSA.

Deltagerprofil

Kurserne er relevante for IT-ansatte som er involveret i opsætning af VPN eller digitale certifikater, etiske hackere og pen-testere og alle som ønsker at få en dybere forståelse for kryptografi.

Udbytte

- Lær om forskellige krypteringsstandarder
- Lær, hvordan du vælger den bedste krypteringsstandard til din organisation
- Lær, hvordan kryptering kan forbedre din viden om pen-testing
- Lær om korrekt og ukorrekt implementering af krypteringsteknologier
- Lær om de mest almindelige fejl ved implementering af krypteringsteknologier
- Lær om best practice ved implementering af krypteringsteknologier

Det får du på arrangementet

- Certificering/eksamen
- Kursusbevis
- Materiale på engelsk
- Undervisning på engelsk

Indhold

Module 1: Introduction and History of Cryptography

- What is Cryptography?
- History of Cryptography
- Mono-Alphabet SubstitutionCaesar 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

Modul 2: Symmetric Cryptography & Hashes

- Symmetric Cryptography
- Information Theory
- Information Theory Cryptography Concepts

Teknologisk Institut
kurser@teknologisk.dk
+45 72 20 30 00

- 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

Modul 3: Number Theory and Asymmetric Cryptography

- Asymmetric Encryption
- Basic Number Facts

Teknologisk Institut
kurser@teknologisk.dk
+45 72 20 30 00

- 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

Modul4: 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

Modul 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

Teknologisk Institut
kurser@teknologisk.dk
+45 72 20 30 00

- Linear Cryptanalysis
- Differential Cryptanalysis
- Integral Cryptanalysis
- Cryptanalysis Resources
- Cryptanalysis Success
- Rainbow Tables
- Password Cracking
- Tools

Læs mere om vores online kurser og se svar på dine spørgsmål (FAQ).

Tidsforbrug

Kursuspakken indeholder 5 moduler og kan gennemføres på ca. 20 timer.

Inkluderet i onlinekurset

- 1 års adgang til instruktørledede videotræningsmoduler
- 1 års adgang til officielt kursusmateriale fra EC-Council
- 6 måneders adgang til den virtuelle lab platform iLabs
- Eksamensvoucher
- Kursusbevis "Course of Completion"

Certificering

Eksamen ECES er inkluderet i prisen. Du skal have 70% rigtige svar for at bestå.

- **Antal spørgsmål:** 50
- **Tid:** 2 timer
- **Format:** Multiple Choice

ECE-Point (EC-Council Continuation Education)

Ved at gennemføre kurset kan du optjene 40 ECE-point og 120 ECE-point, når du har bestået din eksamen. Vær opmærksom på, at første eksamen ikke giver ECE-point, og først ved anden eksamen optjener du 120 ECE-point.

Teknologisk Institut tilbyder denne certificering som akkrediteret træningscenter (ATC) for iLearn Solution under EC-Council.

Søgte du et andet onlinekursus?

Vi tilbyder over 7.000 forskellige onlinekurser inden for mange forskellige områder. Kontakt os på tlf. 72203000 eller kurser@teknologisk.dk, så vi kan hjælpe med at imødekomme dit behov.

Se desuden listen over vores udvalgte online kurser.

Har du faglige spørgsmål så kontakt

Malene Kjærsgaard
+45 72202523
mch@teknologisk.dk