



EC-Council Certified Encryption Specialist v3

La criptografía es esencial para las organizaciones, ya que protege los datos confidenciales del acceso no autorizado, garantizando la privacidad y la confidencialidad mediante el cifrado de los mensajes. El cifrado de datos confidenciales mantiene la privacidad en las comunicaciones y se ajusta a las estrictas medidas de seguridad que se suelen observar en las aplicaciones de mensajería segura..

Descripción del curso

El programa de Especialista Certificado en Cifrado (ECES) de EC-Council está diseñado para introducir a profesionales y estudiantes en el complejo campo de la criptografía. Cubriendo un amplio espectro de temas, el programa ECES profundiza en la criptografía moderna de clave simétrica, ofreciendo información detallada sobre los algoritmos Feistel Networks, Data Encryption Standard (DES) y Advanced Encryption Standard (AES).

Además, los estudiantes se familiarizan con otros algoritmos, como Blowfish, Twofish, Skipjack, CAST, TEA y más. El plan de estudios se extiende a los fundamentos de la teoría de la información aplicada a la criptografía, cubriendo conceptos esenciales como algoritmos de hash (MD5, MD6, SHA, GOST, RIPEMD 160) y criptografía asimétrica, con análisis en profundidad de Rivest-Shamir-Adleman (RSA), ElGamal, Elliptic Curve y Digital Signature Algorithm (DSA).

¿Quién debería asistir?

- Ingeniero en Criptografía
- Analista de criptografía
- Consultor de criptografía
- Ingeniero de software para clientes, seguridad y criptografía
- Especialista en investigación
- Consultor en seguridad e investigación criptográfica
- Administrador de seguridad informática
- Auditor de criptografía

Agenda del curso

Duración: 20 horas

Módulo 1 | Introducción e historia de la criptografía

- ¿Qué es la criptografía?
- Historia de la criptografía
- Sustitución de una sola letra del alfabeto
- Sustitución de múltiples letras
- Sustitución homofónica
- Cifrado de Vernam
- Cifrados nulos
- Cifrados de libros
- La máquina Enigma
- Herramienta criptográfica

Módulo 2 | Criptografía simétrica y funciones hash

- Criptografía simétrica
- Teoría de la información
- Teoría de la información, criptografía, conceptos
- Principio de Kerckhoff
- Sustitución
- Transposición
- Matemáticas binarias
- Cifrado por bloques frente a cifrado de flujo
- Algoritmos de cifrado de bloques simétricos
- Métodos de algoritmos simétricos
- Cifrados de flujo simétrico
- Función hash

Módulo 3 | Teoría de números y criptografía asimétrica

- Cifrado asimétrico
- Datos numéricos básicos
- Generador de números aleatorios
- Diffie-Hellman
- Rivest Shamir Adleman (RSA)
- Menezes-Qu-Vanstone
- Algoritmo de firma digital
- Curva elíptica
- Elgamal
- Perfect Forward Secrecy

Módulo 4 | Aplicaciones de la criptografía

- Firmas digitales
- Certificados digitales
- Infraestructura de clave pública (PKI)
- Autenticación
- Certificados PGP
- Tipos de certificados
- Errores comunes en criptografía
- Agencia de Seguridad Nacional y Criptografía
- Cifrado irrompible
- Blockchain

Módulo 5 | Criptoanálisis

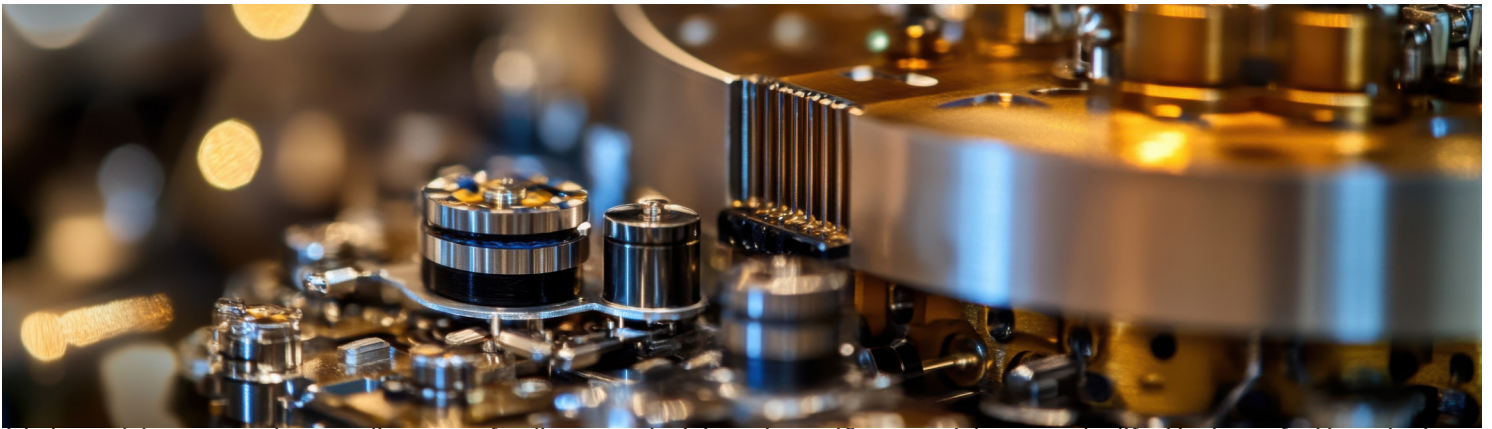
- Descifrando códigos
- Criptoanálisis
- Análisis de frecuencia
- Kasiski
- Descifrando la criptografía moderna
- Criptoanálisis lineal
- Criptoanálisis diferencial
- Criptoanálisis integral
- Recursos de criptoanálisis
- Éxito en el criptoanálisis

Módulo 6 | Computación cuántica y criptografía

- Computación cuántica y criptografía
- Problemas para el control de calidad
- Dos ramas
 - Distribución de claves cuánticas (QKD)
 - Computadoras cuánticas
- NIST
- Enfoques principales
- Criptografía basada en retículos
- Aprender de los errores
- GGH
- NTRU



EC-Council



A lo largo del programa, los estudiantes profundizan en principios criptográficos cruciales como la difusión, la confusión y el principio de Kerckhoff. Se hace hincapié en la aplicación práctica, lo que permite a los estudiantes trabajar con algoritmos criptográficos, desde cifrados clásicos como el cifrado César hasta métodos contemporáneos como el Estándar de Cifrado Avanzado (AES) y el Rivest-Shamir-Adleman (RSA). Más allá de la teoría, el curso proporciona a los estudiantes experiencia práctica en la configuración de una VPN, el cifrado de una unidad y la exploración de la esteganografía. Además, ECES ofrece conocimientos prácticos de criptoanálisis y computación cuántica, lo que garantiza una comprensión integral de los conceptos criptográficos tradicionales y de vanguardia.

Completar el programa ECES capacita a las personas para tomar decisiones informadas al seleccionar los estándares de cifrado adecuados para sus organizaciones. Los candidatos de ECES aprenden los aspectos teóricos de la criptografía y poseen las habilidades prácticas necesarias para una implementación tecnológica eficaz. Esto incluye la capacidad de implementar técnicas de cifrado, proteger datos con VPN y desenvolverse en las complejidades de tecnologías emergentes como la computación cuántica,



¿Qué hay para mí en ECES v3?

Adquiera experiencia práctica con algoritmos criptográficos, aprenda a configurar canales de comunicación seguros mediante VPN, a cifrar datos y a explorar la esteganografía.

Al abarcar temas como la computación cuántica, el programa garantiza que los participantes estén preparados para los desafíos que plantean las tecnologías emergentes.

El conocimiento del criptoanálisis beneficia a los hackers éticos y a los profesionales de las pruebas de penetración, ya que la mayoría de los cursos de pruebas de penetración omiten por completo este tema.

Los graduados del programa poseen los conocimientos y las habilidades necesarias para tomar decisiones informadas sobre los estándares de cifrado para sus organizaciones.

El programa ECES contribuye a crear una fuerza laboral mejor preparada para afrontar la creciente complejidad de los desafíos de la ciberseguridad.



EC-Council



A medida que evolucionan las ciberamenazas, comprender los principios criptográficos se vuelve esencial para los profesionales que desempeñan diversas funciones, desde administradores de red hasta analistas de ciberseguridad.

El programa ECES va más allá de la información superficial, ofreciendo un conocimiento profundo de diversos algoritmos criptográficos, tanto simétricos como asimétricos.

Examen

Duración: 2 horas

Título del examen: Especialista en cifrado certificado por EC-Council

Código del examen: 212-81

Número de preguntas: 50

Puntuación mínima requerida para aprobar: 70%

Duración del examen: 2 horas

Certificación

Los candidatos que aprueben con éxito el examen recibirán su certificado ECES y privilegios comunitarios

Se espera que los miembros se adhieran a la recertificación requisitos a través de los requisitos de Educación Continua de del EC-Council

Información general

- Los honorarios de la certificación se incluyen en el precio del examen
- Acceso por suscripción al material digital durante un año
- Incluye acceso a los laboratorios
- El cupón para tomar el examen en línea es válido durante doce meses



EC-Council