ECES
EC-Council Certified Encryption Specialist

TGK
DIGITAL BUSINESS

EC-Council

ASEGURANDO DATOS CRÍTICOS CON CIFRADO

Certificado por el EC-Council

Especialista en cifrado v2

PROGRAM BROCHURE

PRESENTACIÓN DEL ECESV2:

El programa de certificación de cifrado más completo e independiente del proveedor del mundo

ACERCA DEL CIFRADO

A medida que el tamaño y la frecuencia de las violaciones de datos aumentan con el tiempo, cada vez más organizaciones reconocen rápidamente que el cifrado ya no es una opción. Están ocupados formulando una estrategia integral y cambiando su postura hacia las tecnologías de encriptación e implementando rápidamente una variedad de tecnologías para defender y proteger sus datos confidenciales de amenazas internas y externas. Cada vez más, los usuarios empresariales influyen en la adopción de tecnologías de cifrado más que los equipos de operaciones de TI.

La adopción del cifrado en las organizaciones está aumentando a un ritmo acelerado, al igual que la urgencia en los planes de implementación del cifrado. La creciente tasa de adopción se debe a la rápida evolución de las regulaciones y la necesidad de proteger los datos confidenciales en las redes empresariales, múltiples dispositivos especialmente el movimiento cada vez mayor hacia el almacenamiento de datos en una nube.

Si cree que solo hay un tipo de encriptación, ¡piénselo de nuevo!

Las consideraciones de cifrado difieren para las tecnologías, a saber: cifrado de base de datos, cifrado de VoIP, cifrado de almacenamiento portátil, cifrado de dispositivos móviles, cifrado de Wi-Fi, cifrado de correo electrónico, cifrado de archivos, cifrado de enlace de red, cifrado de servidor web, cifrado de copia de seguridad en cinta y muchos más.

SOBRE ECESV2

El programa EC-Council Certified Encryption Specialist (ECES) introduce a profesionales y estudiantes al campo de la criptografía. Los participantes aprenderán los fundamentos de la criptografía simétrica y clave moderna, incluidos losdetalles de algoritmos como las funciones de Feistel, DES y AES. ECES proporciona las habilidades necesarias para realizar un despliegue efectivo de tecnologías de encriptación. Es un curso integral que cubre varios algoritmos, los conceptos clave detrás de esos algoritmos, aplica:

OTROS TEMAS INTRODUCIDOS:

- Descripción general de otros algoritmos como Blowfish, Twofish y Skipjack
- Algoritmos hash que incluyen MD5, MD6, SHA, GOST, RIPMD 256 y otros
- Criptografía asimétrica que incluye descripciones detalladas de RSA, Elgamal, Elliptic Curve, y DSA
- Conceptos significativos como difusión, confusión y principio de Kerkchoff

LOS PARTICIPANTES TAMBIÉN SE PROPORCIONARÁ UNA APLICACIÓN PRÁCTICA DE LO SIGUIENTE:

- Experiencia práctica en algoritmos criptográficos que van desde cifrados clásicos como el cifrado César hasta algoritmos modernos como AES y RSA
- Cómo configurar una VPN y cifrar una unidad
- Experiencia práctica con esteganografía

Trabajo con herramientas de descifrado en mi posición actual. Esta clase brinda una mejor comprensión de los diferentes algoritmos y cómo atacar las debilidades.

- Juan Minotti
Gerente de Servicios Profesionales,
AccessData, EE. UU.

¿POR QUÉ NECESITAMOS ECES?

El programa EC-Council Certified Encryption Specialist (ECES) introduce a profesionales y estudiantes al campo de la criptografía. Los participantes aprenderán los fundamentos de la criptografía simétrica y clave moderna, incluidos losdetalles de algoritmos como las funciones de Feistel, DES y AES. ECES proporciona habilidades necesarias para realizar un despliegue efectivo de tecnologías de encriptación. Es un curso integral quecubre varios algoritmos, los conceptos clave detrás de esos algoritmos, la aplicación

1. Entendiendo la criptografía le permite tomar decisiones informadas

2. Sin entender la criptografía en cierta profundidad, las personas se limitan solo a la publicidad exagerada de la información soluciones de seguridad

3. Una persona que complete con éxito este curso podrá seleccionar el estándar de encriptación que sea más beneficioso para su organización y entender cómo implementar efectivamente ese tecnología

4. Conocimiento de El criptoanálisis es muy beneficioso para la ética los piratas informáticos y los profesionales de las pruebas de penetración, ya que la mayoría de los cursos de pruebas de penetración omiten el criptoanálisis por completo

El curso me dio una comprensión básica y a veces
avanzada de la criptografía. Realmentedisfruté la clase. Dio una mejor comprensiónde lo que implica la criptografía. El curso me ayuda a evaluar si la seguridad de una organización en estas áreas está a la altura.

-Huey Nguyen
Detective, Policía de Arlington
Departamento, Estados Unidos

¿PARA QUIÉN?

requisitos previos

Sin conocimiento previo Se asume el conocimiento de la criptografía y no hay habilidadesmatemáticas más allá de los conocimientos básicos de Algebra.

PÚBLICO OBJETIVO

- Probadores de penetración y especialistas en informática forense
- Arquitectos, diseñadores y desarrolladores de Cloud Security
- Cualquier persona involucrada en la selección e implementación de VPN o certificados digitales, Operaciones de Seguridad de la Información
- Cualquier persona involucrada en el desarrollo de Sistemas Operativos, Sistemas de Criptografía, soluciones basadas en Blockchain, etc.

DURACIÓN

3 días / 20 horas (9:00 AM a 4:00 PM)

CERTIFICACIÓN

El especialista en cifrado certificado por el EC-Council (ECES) se puede tomar el último día de capacitación (opcional). Los estudiantes deben aprobar el examen en línea para recibir la certificación ECES

> El curso proporciona una buena perspectiva del cifrado. Como examinador forense, no se trata de "si", sino de "cuándo" se encuentra con situaciones en las que el conocimiento del cifrado se vuelve útil.
>
> **-mike tejedor**
> Detective, Departamento de Policía de Arlington, EE. UU.

DETALLES DEL EXAMEN

Título del examen:

Certificado por el Consejo de la CE
Especialista en cifrado

Código xam

212-81

Duración:

2 horas

examen disponible

Consejo CE E
Portal

Formato de prueba:

Opción multiple

Puntaje de aprobación:

70%

¿QUE APRENDERÁS?

• Tipos de estándares de encriptación y sus diferencias

• ¿Cómo seleccionar el mejor estándar para su organización?

• ¿Cómo mejorar su conocimiento de pruebas de penetración en encriptación?

• Implementación correcta e incorrecta de tecnologías de encriptación

• Errores comunes que se cometen al implementar tecnologías de encriptación

• Mejores prácticas al implementar tecnologías de encriptación

BENEFICIOS/PUNTOS PARA LLEVAR

el estudiante

• Desarrollar habilidades para proteger datos críticos en organizaciones con encriptación

• Desarrollar una comprensión profunda de los algoritmos criptográficos esenciales y sus aplicaciones

• Tomar decisiones informadas sobre la aplicación de tecnologías de encriptación

• Ahorre tiempo y dinero al evitar errores comunes en la implementación efectiva de tecnologías de encriptación

• Desarrollar conocimientos prácticos de criptoanálisis.

ESQUEMA DEL CURSO

Módulo 01: Introducción e Historia de la Criptografía

- ¿Qué es la Criptografía?
- Historia de la Criptografía
- Sustitución de monoalfabeto (Cifrado César, Cifrado Atbash, Cifrado afín, Cifrado ROT13)
- Sustitución de varios alfabetos (disco de cifrado,cifrado Vigenère, cifrado Playfair, cifrado ADFGVX)
- Sustitución homofónica
- Cifrado nulo y de libro
- Cifrados de vallas ferroviarias
- La Máquina Enigma
- Herramienta criptográfica

Módulo 02: Criptografía simétrica y hashes

- Criptografía simétrica
- Teoría de la información
- Principio de Kerckhoff
- Sustitución y Transposición
- Matemáticas binarias
- Cifrado de bloque vs. Cifrado de flujo
- Algoritmos de cifrado de bloques simétricos (función Feistel, DES, 3DES, AES, Blowfish, Serpent, Twofish, Skipjack, IDEA, CAST, TEA, SHARK)
- Métodos de algoritmos simétricos
- Cifrados de flujo simétrico (RC4, FISH, PIKE)
- Función Hash (Hash – Salt, MD5, MD6, SHA,FORK-256, RIPEMD-160, GOST, Tiger)
- Criptobanco

Módulo 03: Teoría de Números y Criptografía Asimétrica

- Cifrado asimétrico
- Datos numéricos básicos
- Teorema del cumpleaños
- Generador de números aleatorios
- Diffie-Hellman
- Rivest Shamir Adleman (RSA)
- Menezes-Qu-Vanstone
- Algoritmo de firma digital
- Curva elíptica
- Elgamal
- Herramienta criptográfica

Módulo 04: Aplicaciones de la Criptografía

- Normas FIPS
- Firmas digitales
- Certificado digital
- Infraestructura de clave pública (PKI)
- Gestión de Certificados Digitales
- Modelos de confianza
- Certificados y Servidores Web
- Autenticación (PAP, S-PAP, CHAP, Kerberos)
- Privacidad bastante buena (PGP)
- Cifrado Wi-Fi
- SSL y TLS
- Red privada virtual (VPN)
- Cifrado de archivos
- BitLocker
- Software de cifrado de disco: VeraCrypt
- Errores criptográficos comunes
- Esteganografía
- Estegoanálisis
- Herramientas de detección de esteganografía
- Agencia Nacional de Seguridad y Criptografía
- Cifrado indescifrable

Módulo 05: Criptoanálisis

- Romper cifrados
- Criptoanálisis
- Análisis de frecuencia
- Kasiski
- Descifrando la criptografía moderna
- Criptoanálisis lineal
- Criptoanálisis diferencial
- Criptoanálisis Integral
- Recursos de criptoanálisis
- Éxito del criptoanálisis
- Gráfica Arcoiris
- Descifrado de contraseñas

DIGITAL BUSINESS

EC-Council

Envia un Correo a:
academiaciber@tgk.com.mx
Siguenos en nuestras redes