EC-COUNCIL



EC-COUNCIL · PROGRAMA DE CRIPTOGRAFÍA

EC-Council Certified Encryption Specialist (E|CES) v3

Domine la criptografía, de los cifrados clásicos a la criptografía poscuántica, y elija los estándares de cifrado correctos para su organización

¿Por qué debería asistir?

El programa EC-Council Certified Encryption Specialist (E|CES) introduce a profesionales y estudiantes en el campo de la criptografía. Cubre la criptografía simétrica moderna con algoritmos como las funciones Feistel, DES y AES, además de Blowfish, Twofish y otros; las funciones hash (MD5, SHA, GOST) y la criptografía asimétrica con RSA, Elgamal, curva elíptica y DSA.

Más allá de la teoría, los participantes configuran una VPN, cifran una unidad y exploran la esteganografía, y adquieren conocimientos prácticos de criptoanálisis y computación cuántica. Al finalizar, podrán tomar decisiones informadas sobre los estándares de cifrado adecuados para su organización y desplegarlos correctamente.

3 días	20 h	6	Fundamentos	Poscuántica
DURACIÓN	FORMACIÓN	MÓDULOS	NIVEL	COBERTURA



¿Quién debería participar?

Pruebas de penetración y forense
Pentesters y especialistas en informática forense que necesitan dominar el criptoanálisis.

Seguridad en la nube
Arquitectos, diseñadores y desarrolladores de seguridad en la nube.

Operaciones de seguridad
Responsables de seleccionar e implementar VPN y certificados digitales, y equipos de operaciones de seguridad de la información.

Desarrollo de sistemas
Desarrolladores de sistemas operativos, sistemas criptográficos y soluciones basadas en blockchain.

Objetivos de aprendizaje

- Conocer los tipos de estándares de cifrado y sus diferencias
- Seleccionar el estándar de cifrado más adecuado para su organización
- Fortalecer sus conocimientos de pruebas de penetración aplicados al cifrado
- Distinguir el despliegue correcto e incorrecto de las tecnologías de cifrado
- Reconocer los errores comunes al implementar tecnologías de cifrado
- Aplicar las mejores prácticas al implementar tecnologías de cifrado
- Comprender la computación cuántica y su impacto en la criptografía
- Configurar una VPN, cifrar una unidad y trabajar con esteganografía en la práctica

Áreas de habilidad del programa

Criptografía simétrica | Funciones hash | Criptografía asimétrica | PKI y certificados digitales | VPN y cifrado de discos | Esteganografía | Criptoanálisis | Criptografía poscuántica

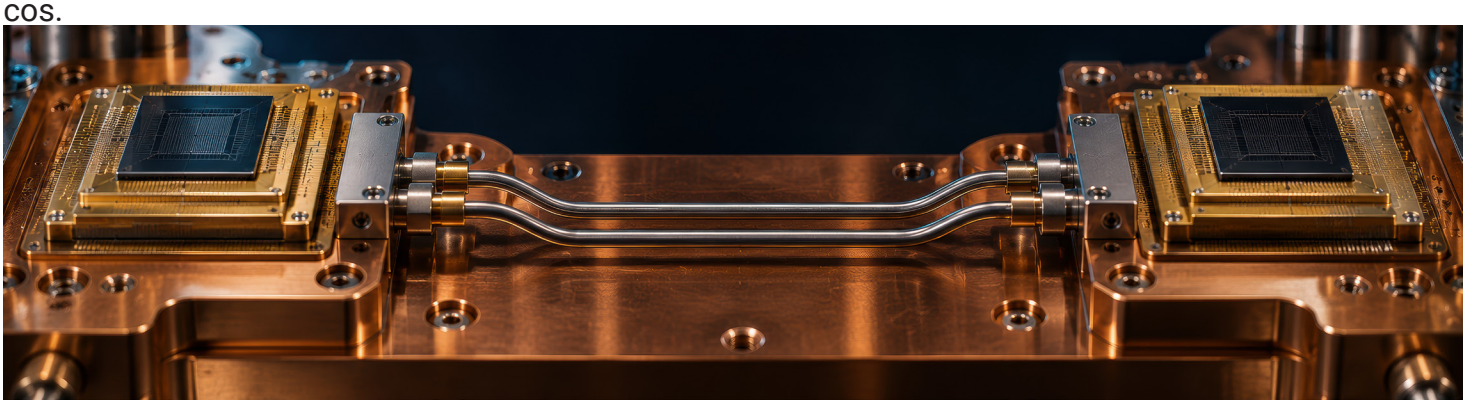
Programa del curso

Duración: 3 días (20 horas)

Módulo	Contenido
Módulos 1–2 Día 1	**01 Introducción e historia de la criptografía:** qué es la criptografía; sustitución monoalfabética (César, Atbash, Afín, ROT13, escítala) y polialfabética (disco de cifrado, Vigenère, Playfair, ADFGVX); cifrados homofónicos, nulos, de libro, rail fence y Vernam; la máquina Enigma y CrypTool. **02 Criptografía simétrica y hashes:** teoría de la información, principio de Kerckhoffs, sustitución, transposición y matemática binaria; cifrado por bloques y de flujo; función Feistel y S-Box; DES, 3DES, AES, Blowfish, Serpent, Twofish, Skipjack, IDEA, CAST, TEA y GOST; modos ECB, CBC, CFB, OFB y CTR; RC4; funciones hash (MD5, MD6, SHA, RIPEMD-160, Whirlpool, NTLM), MAC/HMAC y key stretching.
Módulos 3–4 Día 2	**03 Teoría de números y criptografía asimétrica:** números primos, totiente de Euler, aritmética modular, campos de Galois y logaritmos discretos; paradoja y ataque del cumpleaños; generadores de números aleatorios (Blum Blum Shub, Yarrow, Fortuna); Diffie-Hellman, RSA, MQV, DSA, curva elíptica, Elgamal, Cramer-Shoup, YAK y forward secrecy. **04 Aplicaciones de la criptografía:** estándares FIPS; firmas y certificados digitales X.509, CA, RA y PKI; autenticación (PAP, CHAP, EAP, Kerberos) y PGP; cifrado Wi-Fi (WEP, WPA2, WPA3) y SSL/TLS 1.3; VPN (PPTP, L2TP, IPsec, SSL/TLS); EFS y BitLocker; errores comunes; esteganografía y estegoanálisis; algoritmos de la NSA y blockchain.
Módulos 5–6 Día 3	**05 Criptoanálisis:** ruptura de cifrados, análisis de frecuencia y método Kasiski; ataques de texto plano conocido o elegido, solo texto cifrado y clave relacionada; criptoanálisis lineal, diferencial e integral; tablas arcoíris, cracking de contraseñas y herramientas. **06 Computación cuántica y criptografía:** línea de tiempo y desafíos de la computación cuántica; distribución cuántica de claves (QKD) y qubits; enfoque del NIST para la criptografía poscuántica; criptografía basada en retículos, Learning with Errors, GGH y NTRU.

El módulo de computación cuántica y criptografía prepara a los participantes para uno de los mayores desafíos de la seguridad de la información: la llegada de computadoras cuánticas capaces de romper los algoritmos de clave pública que hoy protegen las comunicaciones, como RSA y la criptografía de curva elíptica.

El curso repasa la evolución de la computación cuántica, sus limitaciones actuales y sus dos grandes vertientes: la distribución cuántica de claves (QKD), basada en qubits, y la criptografía poscuántica. En esta última se estudian los enfoques que impulsa el NIST, en especial la criptografía basada en retículos, el aprendizaje con errores (LWE) y algoritmos como GGH y NTRU, para que el profesional pueda planificar con criterio la migración de su organización hacia estándares resistentes a ataques cuánticos.



Examen

Duración: 2 horas

Título	EC-Council Certified Encryption Specialist (E|CES) – Versión 3		
Código	212-81	**N.º de preguntas**	50
Formato	Opción múltiple	**Duración**	2 horas
Aprobación	70 %	**Plataforma**	EC-Council Exam Portal

Requisitos

- **Conocimientos previos:** no se requiere experiencia en criptografía ni conocimientos matemáticos más allá del álgebra básica.
- **Con capacitación oficial de EC-Council:** puede presentar el examen sin proceso de elegibilidad. **Sin capacitación oficial:** al menos dos años de experiencia en seguridad de la información, solicitud de elegibilidad aprobada y una cuota de US$100.

Formación de 3 días

El programa se imparte en **3 días (20 horas)**, de **9:00 a. m. a 4:00 p. m.**, combinando teoría y práctica: configuración de una VPN, cifrado de una unidad, esteganografía y ejercicios de criptoanálisis con herramientas como CrypTool y CryptoBench.

Información general

- Material oficial de EC-Council
- EC-Council es una organización acreditada bajo la norma ISO/IEC 17024 y reconocida por la Directiva 8140/8570 del DoD
- Cobertura de la criptografía clásica a la poscuántica, con criptoanálisis práctico