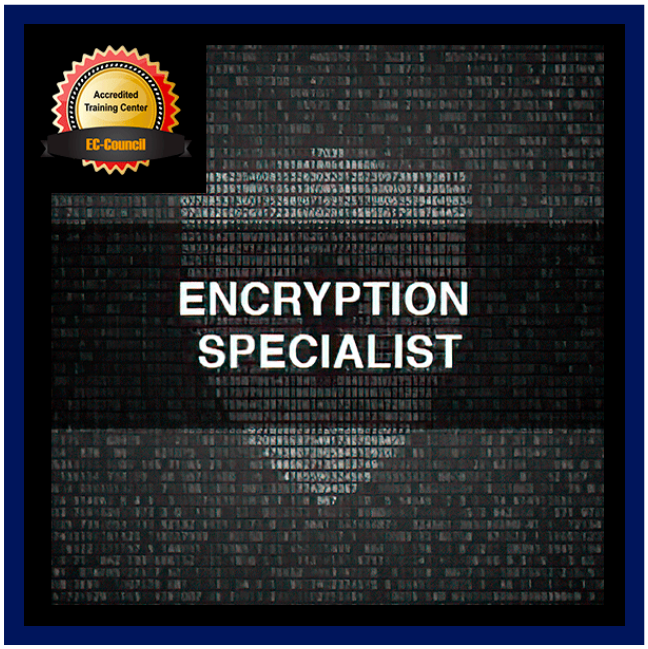
EC-Council Certified Encryption Specialist (ECES)

Código: ECES-001

Propuesta de Valor: EC-COUNCIL

Duración: 24 Horas



El especialista (E|CES) de EC-Council es un programa que introduce a profesionales y estudiantes en el campo de la criptografía.
Los participantes aprenderán fundamentos de la simetría moderna y la clave de criptografía incluyendo detalles de algoritmos como Feistel Networks, DES y AES.

Otros temas introducidos son:

- Panorámica de algoritmos como Blowfish, Twofish, y Skipjack.
- Algoritmos hashing incluyendo MD5, MD6, SHA, Gost, RIPMD 256 y otros.
- La criptografía asimétrica incluye descripciones de RSA, Elgamal, Elliptic Curve, y DSA.
- Conceptos importantes como difusión, confusión y el principio de Kerkchoff.

En el presente curso, el participante conocerá los diversos algoritmos criptográficos existentes, sus características, ventajas y desventajas; así como la forma de implementarlos en situaciones reales y las aplicaciones de criptografía existentes. Todo esto bajo un esquema totalmente práctico y utilizando diversos lenguajes de programación.
Este curso lo prepara para la certificación: EC-Council Certified Encryption Specialist.

AUDIENCIA

- Dirigido a profesionales técnicos, tanto del área de la seguridad en TI, como del área de desarrollo de aplicaciones.

PRE REQUISITOS

- El curso está dirigido a profesionales técnicos, tanto del área de la seguridad en TI (evaluadores de la seguridad en sistemas, pentesters y peritos informáticos) como del área de desarrollo de aplicaciones que tengan que ver con la protección de datos sensibles.

OBJETIVOS

- Comprender los diferentes esquemas de cifrado existentes, así como la evolución de los sistemas criptográficos.
- Aprender los fundamentos de los algoritmos criptográficos y la forma de aplicarlos.
- Implementar los diversos algoritmos criptográficos en situaciones reales.

CERTIFICACIÓN DISPONIBLE

Especialista certificado en cifrado del EC-Council (ECES):

- Número de preguntas: 50.
- Calificación de aprobación: 70%.
- Duración de la prueba: 2 horas.
- Formato de la prueba: Prueba de opción múltiple.
- Entrega: Centro de exámenes del EC-Council (EXAMEN ECC).

CONTENIDO

1. INTRODUCCIÓN E HISTORIA DE LA CRIPTOGRAFÍA

1.1. ¿QUÉ ES LA CRIPTOGRAFÍA?
1.2. HISTORIA DE LA CRIPTOGRAFÍA
1.3. SUSTITUCIÓN MONO-ALFABETO
1.4. SUSTITUCIÓN DE VARIOS ALFABETOS
1.5. SUSTITUCIÓN HOMOFÓNICA
1.6. CIFRADOS NULOS
1.7. CIFRADOS DE LIBROS
1.8. CIFRADOS DE VALLAS FERROVIARIAS
1.9. LA MÁQUINA ENIGMA
1.10. CRIPTOHERRAMIENTA

2. CRIPTOGRAFÍA SIMÉTRICA Y HASHES

2.1. CRIPTOGRAFÍA SIMÉTRICA
2.2. TEORÍA DE LA INFORMACIÓN
2.3. EL PRINCIPIO DE KERCKHOFF
2.4. SUSTITUCIÓN
2.5. TRANSPOSICIÓN
2.6. MATEMÁTICAS BINARIAS
2.7. CIFRADO DE BLOQUE FRENTE A CIFRADO DE FLUJO
2.8. ALGORITMOS DE CIFRADO DE BLOQUES SIMÉTRICOS
2.9. MÉTODOS DE ALGORITMOS SIMÉTRICOS
2.10. CIFRADOS DE FLUJO SIMÉTRICO
2.11. FUNCIÓN HASH
2.12. CRIPTOBANCO

3. TEORÍA DE NÚMEROS Y CRIPTOGRAFÍA ASIMÉTRICA

3.1. CIFRADO ASIMÉTRICO
3.2. DATOS NUMÉRICOS BÁSICOS
3.3. TEOREMA DEL CUMPLEAÑOS
3.4. GENERADOR DE NÚMEROS ALEATORIOS
3.5. DIFFIE-HELLMAN
3.6. RIVEST SHAMIR ADLEMAN (RSA)
3.7. MENEZES–QU–VANSTONE
3.8. ALGORITMO DE FIRMA DIGITAL
3.9. CURVA ELÍPTICA
3.10. ELGAMAL
3.11. CRIPTOHERRAMIENTA

4. APLICACIONES DE LA CRIPTOGRAFÍA

4.1. ESTÁNDARES FIPS
4.2. FIRMAS DIGITALES
4.3. ¿QUÉ ES UN CERTIFICADO DIGITAL?
4.4. AUTORIDAD DE CERTIFICACIÓN (CA)
4.5. AUTORIDAD DE REGISTRO (RA)
4.6. INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)
4.7. TERMINOLOGÍA DE CERTIFICADOS DIGITALES
4.8. PROTOCOLO DE VALIDACIÓN DE CERTIFICADOS BASADO EN SERVIDOR
4.9. GESTIÓN DE CERTIFICADOS DIGITALES
4.10. MODELOS DE CONFIANZA
4.11. CERTIFICADOS Y SERVIDORES WEB
4.12. SERVICIOS DE CERTIFICADOS DE MICROSOFT
4.13. CERTIFICADOS DE WINDOWS: CERTMGR.MSC
4.14. AUTENTICACIÓN
4.15. PRIVACIDAD BASTANTE BUENA (PGP)
4.16. CIFRADO DE WI-FI
4.17. SSL
4.18. TLS
4.19. RED PRIVADA VIRTUAL (VPN)
4.20. CIFRAR ARCHIVOS
4.21. BITLOCKER
4.22. SOFTWARE DE CIFRADO DE DISCO: VERACRYPT
4.23. ERRORES COMUNES DE CRIPTOGRAFÍA
4.24. ESTEGANOGRAFÍA
4.25. ESTEGANÁLISIS
4.26. HERRAMIENTAS DE DETECCIÓN DE ESTEGANOGRAFÍA
4.27. AGENCIA DE SEGURIDAD NACIONAL Y CRIPTOGRAFÍA
4.28. CIFRADO INQUEBRANTABLE

5. CRIPTOANÁLISIS

5.1. ROMPIENDO CIFRADOS
5.2. CRIPTOANÁLISIS
5.3. ANÁLISIS DE FRECUENCIA
5.4. KASISKI
5.5. DESCIFRANDO LA CRIPTOGRAFÍA MODERNA
5.6. DESCIFRANDO LA CRIPTOGRAFÍA MODERNA: ELEGIDO
5.7. ATAQUE DE TEXTO PLANO
5.8. DESCIFRANDO LA CRIPTOGRAFÍA MODERNA:
5.9. ATAQUE DE SOLO TEXTO CIFRADO Y DE CLAVE RELACIONADA
5.10. CRIPTOANÁLISIS LINEAL
5.11. CRIPTOANÁLISIS DIFERENCIAL
5.12. CRIPTOANÁLISIS INTEGRAL
5.13. RECURSOS DE CRIPTOANÁLISIS
5.14. ÉXITO DEL CRIPTOANÁLISIS
5.15. MESAS ARCOIRIS

5.16. DESCIFRANDO CONTRASEÑAS
5.17. HERRAMIENTAS

BENEFICIOS

- Al terminar el curso los estudiantes aprenderán fundamentos de la simetría moderna y la clave de criptografía incluyendo detalles de algoritmos como Feistel Networks, DES y AES.