



CriptoCert Certified Crypto Analyst

Versión: 20190404 (www.cryptocert.com)

Temario

El presente índice correspondiente al temario de la certificación **CriptoCert Certified Crypto Analyst** permite a los potenciales candidatos hacerse una idea general del material y contenidos que se cubren en la certificación. Los candidatos que opten a la certificación recibirán un índice más detallado junto a la documentación oficial, de más de 800 páginas.

1. Introducción a la seguridad

- 1.1. Amenazas en seguridad informática
- 1.2. Protección de activos
- 1.3. Definiciones de seguridad
 - 1.3.1. ¿Qué es la seguridad informática?
 - 1.3.2. ¿Qué es la seguridad de la información?
- 1.4. Principios de la seguridad
 - 1.4.1. Confidencialidad
 - 1.4.2. Integridad
 - 1.4.3. Disponibilidad
- 1.5. Otros servicios de la seguridad
 - 1.5.1. Autenticación
 - 1.5.2. Control de acceso
 - 1.5.3. No repudio
 - 1.5.4. Trazabilidad
- 1.6. ¿Qué es la criptografía?
- 1.7. Hechos históricos en la criptografía

2. Teoría de números, teoría de la información, complejidad algorítmica

- 2.1. Teoría de números: matemática discreta
 - 2.1.1. Operaciones modulares
 - 2.1.2. Conjunto completo de restos CCR
 - 2.1.3. Conjunto reducido de restos CRR
 - 2.1.4. Función de Euler
 - 2.1.5. Propiedades de las operaciones en \mathbb{Z}_n
 - 2.1.6. Homomorfismo de los enteros
 - 2.1.7. Operaciones típicas en un módulo
 - 2.1.8. Inversos aditivos y multiplicativos
 - 2.1.9. Algoritmo Extendido de Euclides AEE
 - 2.1.10. Producto y potencia dentro de un módulo
 - 2.1.11. Raíces primitivas
 - 2.1.12. Anillos en la exponenciación modular
 - 2.1.13. Algoritmo de exponenciación rápida AER
 - 2.1.14. Cálculos en campos de Galois (GF)
- 2.2. Teoría de la información
 - 2.2.1. Información y teoría de la información
 - 2.2.2. Cantidad de información de un mensaje



CriptoCert Certified Crypto Analyst

- 2.2.3. Incertidumbre e información
- 2.2.4. Grados de indeterminación
- 2.2.5. Entropía de los mensajes
- 2.2.6. Propiedades de la entropía
- 2.2.7. Codificación óptima con el método Huffman
- 2.2.8. Ratio real y ratio absoluta del lenguaje
- 2.2.9. Redundancia del lenguaje
- 2.2.10. Distancia de unicidad
- 2.2.11. Modelo de cifrador aleatorio
- 2.2.12. Cantidad de trabajo Q en un criptoanálisis
- 2.3. Complejidad algorítmica
 - 2.3.1. Operaciones bit en suma y multiplicación
 - 2.3.2. La función $O(n)$
 - 2.3.3. Algoritmos de complejidad polinómica
 - 2.3.4. Algoritmos de complejidad no determinista
 - 2.3.5. Problemas de tipo NP

3. Introducción e historia de la criptografía

- 3.1. Conceptos básicos de criptografía
 - 3.1.1. Criptología, criptografía y criptoanálisis
 - 3.1.2. Esquema de un sistema de cifra
 - 3.1.3. Principios de Kerckhoffs
 - 3.1.4. Técnicas de difusión y confusión
 - 3.1.5. Compresión, codificación y cifrado
 - 3.1.6. Ataques comunes en la criptografía
- 3.2. Breve historia de la criptografía
 - 3.2.1. Los comienzos (siglos V y II a.C.)
 - 3.2.2. Cifrado del César (siglo I a.C.)
 - 3.2.3. Disco de Alberti (1466)
 - 3.2.4. Cilindro de Jefferson (1795)
 - 3.2.5. El escarabajo de oro (1843)
 - 3.2.6. Cifrador de Playfair (1854)
 - 3.2.7. Disco de Wheatstone (1860)
 - 3.2.8. Cilindro de Bazeries (1901)
 - 3.2.9. El telegrama de Zimmermann (1917)
 - 3.2.10. Máquina Enigma (1923)
 - 3.2.11. Turing (1943) y Shannon (1949)
- 3.3. Algoritmos criptográficos clásicos
 - 3.3.1. Clasificación de los sistemas clásicos
 - 3.3.2. Cifrado por Escítala
 - 3.3.3. Cifrado por columnas y filas
 - 3.3.4. Cifrado rail fence
 - 3.3.5. Sustitución monoalfabética
 - 3.3.6. Sustitución polialfabética
 - 3.3.7. Sustitución poligrámica



CriptoCert Certified Crypto Analyst

4. Introducción a la criptografía moderna

- 4.1. Clasificación de los sistemas de cifra
- 4.2. De la cifra clásica a la moderna
- 4.3. Clasificación de la cifra moderna
- 4.4. Algoritmos de cifra moderna
- 4.5. Cifrado en flujo y cifrado en bloque
 - 4.5.1. Cifrado en flujo
 - 4.5.2. Estructura de la cifra flujo
 - 4.5.3. Cifrado en bloque
 - 4.5.4. Características de la cifra en bloque
- 4.6. Cifrado simétrico y cifrado asimétrico
 - 4.6.1. Criptografía simétrica CS o de clave secreta
 - 4.6.2. Criptografía asimétrica CA o de clave pública
 - 4.6.3. Confidencialidad e integridad en CS
 - 4.6.4. Confidencialidad e integridad en CA
 - 4.6.5. Comparativa entre la cifra simétrica y la cifra asimétrica
 - 4.6.6. Sistemas de cifra híbridos

5. Criptografía simétrica

- 5.1. Cifra simétrica en flujo
 - 5.1.1. Introducción a la cifra simétrica en flujo
 - 5.1.2. Fundamentos de la cifra simétrica en flujo
 - 5.1.3. Principios de la cifra simétrica en flujo
 - 5.1.4. Algoritmos de cifra simétrica en flujo
 - 5.1.5. Criptoanálisis de los algoritmos de cifra simétrica en flujo
 - 5.1.6. Resumen: Cifra simétrica en flujo
- 5.2. Cifra simétrica en bloque
 - 5.2.1. Introducción a la cifra simétrica en bloque
 - 5.2.2. Principios de la cifra simétrica en bloque
 - 5.2.3. Modos de cifra en sistemas simétricos en bloque
 - 5.2.4. Vectores de inicialización (IVs)
 - 5.2.5. Relleno o padding
 - 5.2.6. Algoritmos de cifra simétrica en bloque
 - 5.2.7. Criptoanálisis de los algoritmos de cifra simétrica en bloque

6. Criptografía asimétrica

- 6.1. Introducción a la cifra asimétrica
 - 6.1.1. Propiedades de la cifra asimétrica
 - 6.1.2. Cifrado de números
 - 6.1.3. Confidencialidad e integridad con cifra asimétrica
- 6.2. Intercambio de clave de Diffie y Hellman DH
 - 6.2.1. Algoritmo de Diffie y Hellman
 - 6.2.2. Seguridad del algoritmo de Diffie y Hellman
 - 6.2.3. Ataque por fuerza bruta al algoritmo de DH
 - 6.2.4. Características del PLD en DH
 - 6.2.5. Ataque Man-In-The-Middle a DH



CriptoCert Certified Crypto Analyst

- 6.3. Algoritmo de cifra RSA
 - 6.3.1. Principios de RSA
 - 6.3.2. Cifrado y descifrado con RSA
 - 6.3.3. Claves parejas y números no cifrables en RSA
 - 6.3.4. Ataques a RSA
- 6.4. Algoritmo de Elgamal
 - 6.4.1. Principios del algoritmo de Elgamal
 - 6.4.2. Cifrado y descifrado con Elgamal
 - 6.4.3. Cifrado Elgamal de bloques de texto
- 6.5. Criptografía con curvas elípticas ECC
 - 6.5.1. Introducción a las curvas elípticas
 - 6.5.2. Curvas elípticas en criptografía
 - 6.5.3. Cifrado y descifrado con curvas elípticas
 - 6.5.4. Seguridad de la criptografía con curvas elípticas

7. Funciones hash

- 7.1. Contexto de las funciones hash
- 7.2. Características y propiedades de las funciones hash
 - 7.2.1. ¿Qué es una función hash?
 - 7.2.2. Seguridad asociada a una función hash
 - 7.2.3. Preimágenes de las funciones hash
 - 7.2.4. Propiedades de las funciones hash
- 7.3. Utilización de las funciones hash en seguridad
 - 7.3.1. Ejemplos de las funciones hash en seguridad
- 7.4. Algoritmos de hash
 - 7.4.1. Tabla comparativa de los algoritmos de hash
 - 7.4.2. Listado de algoritmos de hash
 - 7.4.3. ¿Qué algoritmo de hash debería usar (y con qué longitud de hash)?
 - 7.4.4. Construcción de las funciones hash
 - 7.4.5. MD5
 - 7.4.6. SHA-1
 - 7.4.7. Comparativa entre las funciones hash MD5 y SHA-1
 - 7.4.8. SHA-2 (SHA-256)
 - 7.4.9. SHA-3 (Keccak)
 - 7.4.10. Comparativa de velocidad en funciones hash
- 7.5. Criptoanálisis de las funciones hash
 - 7.5.1. Pseudo-colisiones y funciones de compresión
 - 7.5.2. Ataques de extensión de la longitud
 - 7.5.3. Ataques de preimágenes
 - 7.5.4. Ataques de colisiones
 - 7.5.5. Ataques basados en la paradoja del cumpleaños
 - 7.5.6. Vulnerabilidades de MD5 y SHA-1
 - 7.5.7. Utilización de múltiples funciones hash simultáneamente

8. Autenticación

- 8.1. Autenticación con sistemas asimétricos
- 8.2. Autenticación con sistemas simétricos: MAC y HMAC



CriptoCert Certified Crypto Analyst

8.3. MAC (Message Authentication Code)

8.3.1. Poly1305

8.3.2. SipHash

8.4. HMAC (keyed-Hash Message Authentication Code)

8.4.1. Creación de MACs a partir de funciones hash (HMAC)

8.4.2. Creación de MACs a partir de cifradores en bloque (CBC-MAC)

8.4.3. Galois Counter Message Authentication Code (GMAC)

8.5. Cifrado autenticado (AE, Authenticated Encryption)

9. Firma digital

9.1. Principios de la firma digital

9.2. Algoritmos asimétricos de firma digital

9.2.1. Firma RSA

9.2.2. Firma Elgamal

9.2.3. Firma DSA

9.2.4. Firma ECDSA

9.3. Algoritmos simétricos de firma digital

9.3.1. Firma Desmedt

9.4. Tabla comparativa

10. Certificados digitales

10.1. Infraestructuras de clave pública (PKI)

10.2. Fundamentos de los certificados digitales. X509v3

10.3. Autenticación y firma digital

10.4. Revocación de certificados

10.5. Estándares PKCS

10.6. Otras alternativas: Let's Encrypt, Lemur

11. Claves criptográficas. Fortalezas, debilidades y gestión

11.1. Elección de las claves

11.2. Protección y almacenamiento de claves

11.2.1. Elección de claves

11.2.2. Longitud de claves

11.3. Ataques a claves criptográficas

11.3.1. Diccionarios

11.3.2. Canal lateral

11.3.3. Computación cuántica

12. Algoritmos de derivación de claves

12.1. Funciones de derivación de claves (KDF y HKDF, Hash-based Key-Derivation Functions)

12.2. Key stretching y tipos de ataques sobre contraseñas/claves

12.2.1. Semillas: Uso de sal y pimienta para el almacenamiento de hashes

12.2.2. Algoritmos de derivación de claves



CriptoCert Certified Crypto Analyst

13. Herramientas de cifrado

13.1. Herramientas de aprendizaje de criptografía

13.1.1. Herramientas de terceros

13.1.1.1. Cryptool

13.1.1.2. Crypton

13.1.2. Herramientas propias

13.1.2.1. SAMCrypt

13.1.2.2. Criptoclásicos v2.1

13.1.2.3. safedes

13.1.2.4. AESPhere

13.1.2.5. FlujoLab

13.1.2.6. CriptoRES

13.1.2.7. ExpoCrypt

13.1.2.8. genRSA v2.1

13.1.2.9. RingRSA

13.1.2.10. LegionRSA

13.2. Herramientas para prácticas de criptografía

13.2.1. Cifrado de software

13.2.1.1. GPG

13.2.1.2. PGP

13.2.1.3. OpenSSL

13.2.2. Cifrado de discos duros

13.2.2.1. Veracrypt

13.2.2.2. BitLocker

13.2.2.3. FileVault2

13.2.2.4. LUKS

13.2.3. Recopilatorio de herramientas prácticas en criptografía: Prims Break

14. Esteganografía y estegoanálisis

14.1. Historia de la esteganografía (negación plausible, etc.)

14.2. Técnicas de ocultación en contenido digital (multimedia, sistemas de ficheros, protocolos, etc.)

14.3. Herramientas de esteganografía

14.4. Técnicas de estegoanálisis

14.5. Herramientas de estegoanálisis

15. Criptografía cuántica y postcuántica

15.1. Funcionamiento de los ordenadores cuánticos (Quantum bits, gates)

15.1.1. Conceptos básicos y estado actual

15.1.2. Seguridad de los criptosistemas

15.2. Recomendaciones criptográficas

15.3. Protocolos de criptografía cuántica (fotones, fibra óptica, aire, satélite, BB82, etc.)

Autores: Alfonso Muñoz, Jorge Ramió y Raúl Siles (CriptoCert)