Versión: 20190404 (www.criptocert.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.

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

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

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. SAMCript

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. ExpoCript

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)