www.criptocert.com

Temario general

VERSIÓN: **20190721**

Temario ***general reducido*** de la certificación técnica profesional **CriptoCert Certified Crypto Analyst**.

1. **Módulo 1. Introducción a la seguridad y a la criptografía**
   - 1.1. Introducción a la seguridad
   - 1.2. Seguridad informática y seguridad de la información
     - 1.2.1. Amenazas en seguridad informática
     - 1.2.2. Protección de activos
     - 1.2.3. Seguridad Informática
     - 1.2.4. Seguridad de la información
   - 1.3. Principios de la seguridad informática
     - 1.3.1. Confidencialidad, integridad y disponibilidad
   - 1.4. Otros servicios de la seguridad
     - 1.4.1. Autenticación, control de acceso, no repudio y trazabilidad
   - 1.5. Hitos en la criptografía y definición
     - 1.5.1. Claude Shannon y la teoría de la información
     - 1.5.2. Horst Feistel y el algoritmo DES
     - 1.5.3. Diffie y Hellman y el intercambio de clave
     - 1.5.4. ¿Qué es la criptografía?
   - 1.6. ¿Cómo estudiar la criptografía?
     - 1.6.1. El papel de las matemáticas en la criptografía
     - 1.6.2. Importancia de la historia en la criptografía actual

2. **Módulo 2. Teoría de números, teoría de la información, complejidad algorítmica**
   - 2.1. Teoría de números
     - 2.1.1. Matemática discreta
       - 2.1.1.1. Principios de la aritmética modular: Operaciones modulares, números primos y compuestos, conjunto de restos, función $\phi(n)$ de Euler…

2.1.1.2. Propiedades, inversos y operaciones en Zn: Homomorfismo de los enteros, cálculo de inversos con Teorema Extendido de Euclides…

2.1.1.3. Exponenciación modular y raíces primitivas: Producto y potencia en un módulo, formación de anillos, raíces primitivas, exponenciación con el Algoritmo de Exponenciación Rápida…

2.1.1.4. Campos de Galois y curvas elípticas en criptografía

2.2. Teoría de la información

2.2.1. Introducción: Definición de información y de teoría de la información

2.2.2. Cantidad de información de un mensaje: En función de su extensión, su utilidad y su probabilidad

2.2.3. Incertidumbre e información: Cantidad de información y grado de indeterminación

2.2.4. Entropía de los mensajes

2.2.5. Codificación óptima

2.2.6. Ratio del lenguaje: Ratio absoluta y real, redundancia del lenguaje…

2.2.7. Distancia de unicidad

2.3. Complejidad algorítmica

2.3.1. Introducción: Operaciones bit en la suma, multiplicación, función O(n), órdenes de complejidad, problemas P y NP…

3. Módulo 3. Fundamentos e historia de la criptografía

3.1. Conceptos básicos de criptografía

3.1.1. Introducción a la criptología: Esquema, principios de Kerckhoffs, técnicas de difusión y confusión, permutaciones, sustituciones y cifradores de producto, compresión, codificación y cifrado…

3.2. Breve historia de la criptografía: ejemplos de cifrado…

3.3. Algoritmos criptográficos clásicos

3.3.1. Clasificación de los sistemas clásicos

3.3.1.1. Transposición o permutación: principios y ejemplos de cifrado…

3.3.1.2. Sustitución monoalfabética: principios y ejemplos de cifrado y criptoanálisis…

3.3.1.3. Sustitución polialfabética: principios y ejemplos de cifrado y criptoanálisis…

3.3.1.4. Sustitución poligrámica: principios y ejemplos de cifrado y criptoanálisis…

4. Módulo 4. Introducción a la criptografía moderna

4.1. De la cifra clásica a la cifra moderna

4.1.1. Inflexión entre cifra clásica y cifra moderna: Claude Shannon, DES, Diffie y Hellman…

4.1.2. Clasificación de la cifra moderna
4.1.2.1. Según la clave: Cifrado simétrico o asimétrico
4.1.2.2. Según el tratamiento de la información: Cifrado en flujo o en bloque
4.1.3. Cifrado en flujo
4.1.4. Cifrado en bloque
4.1.5. Cifrado simétrico o de clave secreta
4.1.6. Cifrado asimétrico o de clave pública
4.1.6.1. Comparativa entre la cifra simétrica y la cifra asimétrica: seguridad de la cifra y de la clave, gestión de claves, espacio de claves, vida de las claves, intercambio de claves, autenticación y firma digital, velocidad de cifra…
4.1.7. Usos de sistemas de cifra híbridos
4.1.8. Utilización de múltiples algoritmos simultáneamente

5. Módulo 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
5.1.2.1. Características y conceptos: Características de las secuencias cifrantes, rachas de dígitos y autocorrelación fuera de fase
5.1.2.2. Postulados de Golomb (G1, G2 y G3)
5.1.3. Principios de la cifra simétrica en flujo
5.1.3.1. Generadores de bits (pseudo)aleatorios
5.1.3.2. Tipos de cifradores simétricos en flujo: estado y contador
5.1.3.3. Clasificación práctica de los cifradores simétricos en flujo: hardware y software
5.1.3.4. Tests de aleatoriedad (Diehard, Golomb, NIST STS…)
5.1.4. Algoritmos de cifra simétrica en flujo
5.1.4.1. Tabla comparativa de los algoritmos de cifra simétrica en flujo
5.1.4.2. ¿Qué algoritmo de cifra simétrica en flujo debería usar (y con qué longitud de clave)?
5.1.4.3. Registros de desplazamiento: FSR, LFSR y NLFSR
5.1.4.3.1. FSR: Feedback Shift Registers, generadores LFSR (lineales), polinomios, M-secuencias, mejora de la complejidad lineal, generadores NLFSR (no lineales)…
5.1.4.4. A5 (A5/1)
5.1.4.4.1. Algoritmo de cifra A5/1 y su seguridad, esquema, función mayoría y periodo…

5.1.4.5. RC4
5.1.4.5.1. Algoritmo de cifra RC4, características, rutinas KSA y PRGA…
5.1.4.6. Salsa20
5.1.4.6.1. Salsa20 Core
5.1.4.6.2. Funciones de ronda de columnas y de filas
5.1.4.6.3. Función Quarter-Round (QR)
5.1.4.7. ChaCha20
5.1.4.7.1. Funciones de ronda de columnas y de filas
5.1.5. Criptoanálisis de los algoritmos de cifra simétrica en flujo
5.1.5.1. Ataque de Berlekamp-Massey sobre LFSR
5.1.5.2. Ataques sobre el algoritmo A5/1
5.1.5.3. Criptoanálisis de RC4 en redes Wi-Fi WEP
5.1.5.4. Criptoanálisis de RC4 en TLS (comunicaciones web)
5.1.5.5. Criptoanálisis de Salsa20 (y ChaCha20)
5.1.5.6. Resumen de errores comunes en cifradores simétricos 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
5.2.1.1. Características y estructura de la cifra simétrica en bloque
5.2.2. Principios de la cifra simétrica en bloque
5.2.2.1. Tamaño de bloque y número de vueltas
5.2.2.2. Esquemas de Feistel y Redes de sustitución y permutación (SPNs, Substitution-Permutation Networks)
5.2.3. Modos de cifra en sistemas simétricos en bloque: ECB, CBC y PCBC, CFB, OFB, CTR, GCM, FPE, XTS…
5.2.4. Vectores de inicialización (IVs)
5.2.5. Relleno o padding
5.2.6. Algoritmos de cifra simétrica en bloque
5.2.6.1. Tabla comparativa de los algoritmos de cifra simétrica en bloque
5.2.6.2. Cifradores simétricos en bloque más conocidos
5.2.6.3. ¿Qué algoritmo de cifra en bloque debería usar (y con qué longitud de clave)?
5.2.6.4. DES: Algoritmo DES, la función F y obtención de las subclaves, cifrado y descifrado con el algoritmo DES, las Cajas-S del algoritmo DES, espacio de claves del algoritmo DES…
5.2.6.5. 3DES (EDE)
5.2.6.6. AES: Algoritmo AES y características, esquema general de cifra con AES, funciones SubBytes, ShiftRows, MixColumns, AddRoundKey, expansión de la clave y descifrado en AES
5.2.6.7. Comparativa cifra en bloque vs. cifra en flujo

7. Módulo 7. Criptografía asimétrica

- 7.1. Introducción a la cifra asimétrica
- 7.2. Confidencialidad e integridad con cifra asimétrica
- 7.3. Intercambio de clave de Diffie y Hellman DH
  - 7.3.1. Algoritmo de intercambio de clave de DH: Seguridad, ataque por fuerza bruta, DH y el problema del logaritmo discreto, ataques MitM…
- 7.4. Algoritmo RSA
  - 7.4.1. Principios de RSA: Generación de claves RSA, seguridad y parámetros
  - 7.4.2. Cifrado y descifrado con RSA
    - 7.4.2.1. Operaciones de cifrado y descifrado: confidencialidad e integridad, descifrado RSA con el Teorema Chino del Resto TCR…
  - 7.4.3. Claves parejas y números no cifrables en RSA
    - 7.4.3.1. Claves privadas y públicas parejas
    - 7.4.3.2. Números no cifrables en RSA: características y distribución
  - 7.4.4. Optimal Asymmetric Encryption Padding (OAEP)
  - 7.4.5. Ataques comunes a RSA
    - 7.4.5.1. Ataque a RSA basado en la factorización entera del módulo n
    - 7.4.5.2. Ataque a RSA basado en el cifrado cíclico
    - 7.4.5.3. Ataque a RSA basado en la paradoja del cumpleaños
    - 7.4.5.4. Ataque acústico a RSA por canal lateral
- 7.5. Algoritmo de Elgamal
  - 7.5.1. Principios del algoritmo de Elgamal
  - 7.5.2. Operaciones de cifrado y descifrado con Elgamal
- 7.6. Criptografía con curvas elípticas ECC
  - 7.6.1. Limitaciones de la criptografía asimétrica
  - 7.6.2. Curvas elípticas en criptografía. Definiciones
    - 7.6.2.1. Tipos de curvas elípticas en criptografía
    - 7.6.2.2. Tamaño de la clave en curvas elípticas
  - 7.6.3. Curvas de Weierstrass
    - 7.6.3.1. Operaciones sobre una curva elíptica
    - 7.6.3.2. Representación geométrica de operaciones
    - 7.6.3.3. Operaciones sobre una curva elíptica en un cuerpo finito
  - 7.6.4. Curvas elípticas aplicadas
    - 7.6.4.1. Escenarios de uso
    - 7.6.4.2. Distribución o intercambio de claves criptográficas: ECDH, y Curve 25519 y X25529
    - 7.6.4.3. Firma digital con curvas elípticas. ECDSA
    - 7.6.4.4. Cifrado y descifrado con curvas elípticas
  - 7.6.5. Seguridad de las curvas elípticas
    - 7.6.5.1. Ataques a ECDLP
    - 7.6.5.2. Recomendaciones de seguridad

8. Módulo 8. Autenticación

8.1. Autenticación de mensajes

8.1.1. Definiciones

8.1.2. Ataques a la identidad y a la integridad

8.2. Mecanismos de autenticación

8.2.1. Fundamentos

8.2.2. Autenticación con sistemas asimétricos

8.2.3. Autenticación con sistemas simétricos

8.2.3.1. Funciones HMAC y MAC (Message Authentication Code)

8.3. Cifrado autenticado

8.3.1. Fundamentos y esquemas genéricos

8.3.2. AES GCM

9. Módulo 9. Firma digital

9.1. Firma digital en España

9.2. Características de una firma digital

9.3. Cómo usar la firma digital. Recomendaciones

9.4. Algoritmos asimétricos de firma digital

9.4.1. Autenticación asimétrica via hash

9.4.2. Algoritmo asimétrico de firma RSA

9.4.2.1. Firma digital y verificación con RSA

9.4.2.2. El problema de las claves públicas parejas

9.4.3. Algoritmo asimétrico de firma ElGamal

9.4.3.1. Firma digital y verificación con ElGamal

9.4.3.2. Seguridad de la firma digital ElGamal

9.4.3.3. Ataques a la firma digital ElGamal

9.4.4. Algoritmo asimétrico de firma DSA

9.4.4.1. Firmas digitales DSA y DSS

9.4.4.2. Firma digital y verificación con DSA

9.4.4.3. Seguridad de la firma digital DSA y ECDSA

10. **Módulo 10. Certificados digitales**

10.1. El problema de la distribución de claves criptográficas

10.2. Infraestructuras de clave pública y autoridades de certificación

10.3. Certificados Digitales. Principios básicos

10.3.1. Tipos de certificados digitales

10.3.2. Estándar PKCS (Public-Key Cryptography Standards)

10.4. Fundamentos de los certificados digitales X.509v3

10.4.1. ¿Qué contiene un certificado digital?

14. Módulo 14. Esteganografía y estegoanálisis

- 14.1. Limitaciones de la criptografía
- 14.2. Protegiendo comunicaciones. Esteganografía
- 14.3. Un poco de cultura esteganográfica
- 14.4. Esteganografía en la actualidad
  - 14.4.1. Problema del prisionero
  - 14.4.2. Esquemas esteganográficos
  - 14.4.3. El caso DeCSS
- 14.5. Tendencias de uso en esteganografía
  - 14.5.1. Canales encubiertos en protocolos de comunicación
  - 14.5.2. Esteganografía en sistemas de ficheros y sistemas operativos
    - 14.5.2.1. Formatos de los ficheros
    - 14.5.2.2. Formatos comprimidos
    - 14.5.2.3. Alternate Data Stream (ADS-NTFS)
  - 14.5.3. Esteganografía en tecnologías web
  - 14.5.4. Esteganografía textual y lingüística
    - 14.5.4.1. Esteganografía textual
    - 14.5.4.2. Esteganografía lingüística: textos existentes y estegotextos
  - 14.5.5. Esteganografía multimedia: audio, video, e imágenes
- 14.6. Estegoanálisis
  - 14.6.1. Definiciones y principios
  - 14.6.2. Herramientas de estegoanálisis
  - 14.6.3. Mecanismos de detección de información oculta

15. Módulo 15. Criptografía cuántica y postcuántica

- 15.1. Computación cuántica
  - 15.1.1. Conceptos básicos
  - 15.1.2. Estado actual
  - 15.1.3. Seguridad de los criptosistemas
  - 15.1.4. Recomendaciones criptográficas
- 15.2. Criptografía cuántica y postcuántica
  - 15.2.1. Criptografía cuántica
  - 15.2.2. Criptografía postcuántica