

www.criptocert.com

Temario general: Practitioner

VERSIÓN: **20201013**

Temario general del diploma técnico profesional **CriptoCert Crypto Practitioner**.

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…

Copyright © 2020 CriptoCert S.L. (www.criptocert.com)
Todos los derechos reservados.

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…

Copyright © 2020 CriptoCert S.L. (www.criptocert.com)
Todos los derechos reservados.

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
5.1.4. 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…

Copyright © 2020 CriptoCert S.L. (www.criptocert.com)
Todos los derechos reservados.

5.1.4.5. RC4

5.1.4.5.1. Algoritmo de cifra RC4, características, rutinas KSA y PRGA…

5.1.5. 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: listado.

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, y esquema general de cifra con AES.

5.2.7. Resumen: Cifra simétrica en bloque

6. Módulo 6. Funciones hash

6.1. Contexto de las funciones hash

6.2. Características y propiedades de las funciones hash: seguridad, preimágenes y propiedades

6.3. Utilización de las funciones hash en seguridad

6.4. Algoritmos de hash

6.4.1. Tabla comparativa de los algoritmos de hash

6.4.2. Listado de algoritmos de hash

6.4.3. ¿Qué algoritmo de hash debería usar (y con qué longitud de hash)?

6.4.4. Construcción de las funciones hash

6.4.5. MD5

6.4.5.1. Etapas y bloques de la función hash MD5 y esquema

Copyright © 2020 CriptoCert S.L. (www.criptocert.com)
Todos los derechos reservados.

6.4.6. SHA-1
6.4.6.1. Esquema de la función hash SHA-1
6.4.7. Comparativa entre las funciones hash MD5 y SHA-1
6.4.8. SHA-2 (SHA-256)
6.5. Resumen: Funciones hash

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
7.5. Algoritmo de Elgamal
7.5.1. Principios del algoritmo de Elgamal
7.5.2. Operaciones de cifrado y descifrado con Elgamal
7.6. Introducción a la criptografía con curvas elípticas ECC

Copyright © 2020 CriptoCert S.L. (www.criptocert.com)
Todos los derechos reservados. All rights reserved.

NOTA: El temario indicado anteriormente para el diploma CriptoCert Crypto Practitioner se ha diseñado para que sea acorde con el nivel de un diploma. Detalles más específicos y de mayor profundidad en algunos módulos, así como otros temas relacionados con la criptografía actual y futura, se cubren en la certificación CriptoCert Certified Crypto Analyst (https://www.criptocert.com/CriptoCert_Analyst.html).