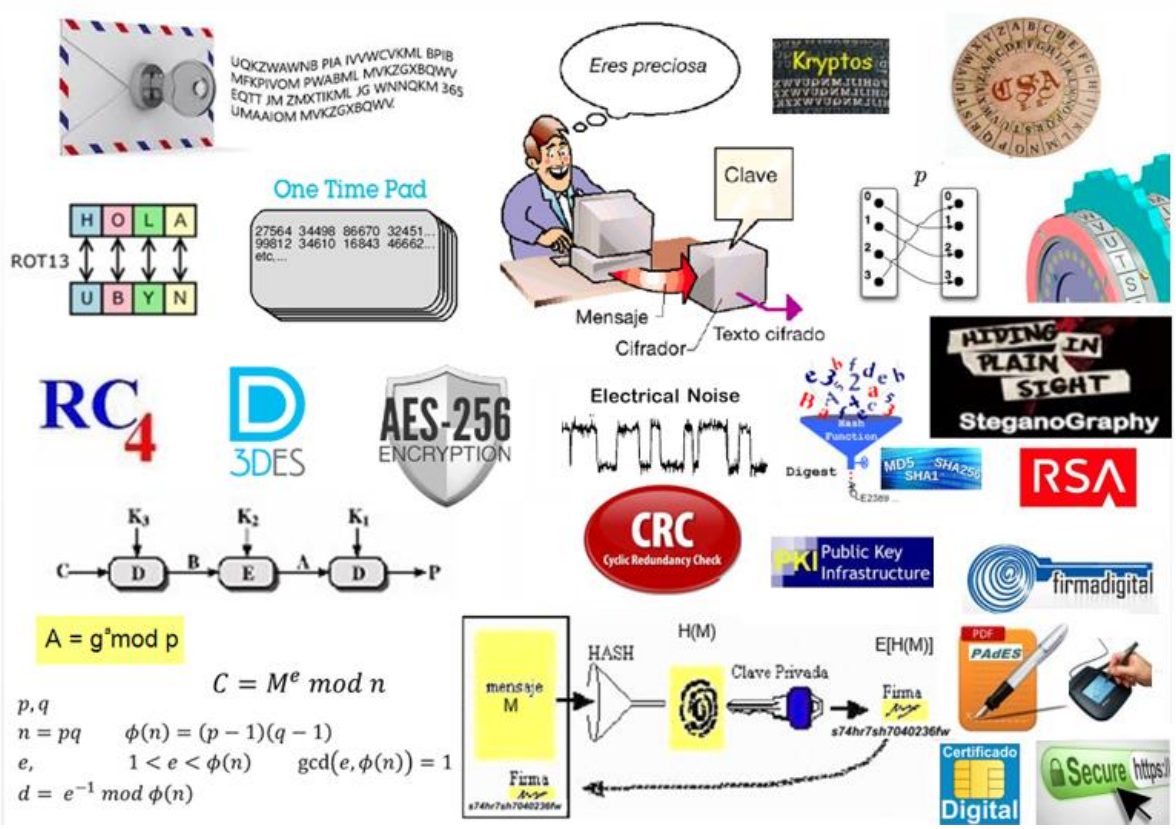
CRIPTOGRAFÍA Y FIRMA ELECTRÓNICA

CURSO TEÓRICO-PRÁCTICO



DIRIGIDO A: Estudiantes, profesionales y técnicos superiores en informática, computación, sistemas, telecomunicaciones o área afín, así como gerentes de sistemas, gerentes de seguridad (CISO),administradores de sistemas, consultores, analistas, desarrolladores, programadores, pentesters, auditores, peritos forense, investigadores de criptomonedas.

REQUISITOS DESEABLES: Conocimientos en el área de telecomunicaciones, redes y protocolos, especialmente TCP/IP. Conocimientos de computación (hardware, software, programación) y de sistemas operativos operativos (Windows, Linux). Conocimientos básicos de seguridad informática. Conocimiento instrumental del idioma inglés.

MODALIDAD Y DURACIÓN: El curso se realiza a distancia y se utiliza un DVD como material de apoyo, el cual se puede obtener en físico o descargarlo de Internet. En el DVD se encuentran las presentaciones de las clases, hiperenlaces, libros electrónicos, guías para las experiencias prácticas, así como los programas y herramientas para efectuar dichas prácticas. La metodología utilizada combina clases y lecturas con experiencias prácticas. El participante avanza a su propio ritmo, de acuerdo a su disponibilidad de tiempo. Se pueden realizar consultas en línea (Skype, WhatsApp, teléfono) y por correo electrónico. La duración del curso es de 6 semanas y se requieren unas 24 horas de dedicación (entre teoría y práctica) para completar el adiestramiento. Se entrega un certificado de aprobación.

EQUIPAMIENTO: El participante debe disponer de PC o laptop de buenas prestaciones y acceso a Internet. Las imágenes forenses que se usan para ciertas prácticas son de varios GB y se deben descargar de Internet. Para las prácticas (opcionales) de *Forénsica en Dispositivos Móviles* se requiere un teléfono celular con sistema operativo Android y que eventualmente se pueda "rootear".

DOCENTE: Ing. Vincenzo Mendillo - Profesor Titular (UCV - USB - UNIMET - UCAB)

- Ingeniero Electricista (Especialidad: Telecomunicaciones) - Universidad Central de Venezuela

- Master of Science in Electronics - University of Southampton
- Live Senior Member IEEE - Institute of Electrical and Electronics Engineers
- Miembro de CriptoRed - Red de Criptografía y Seguridad de la Información
- Coordinador del Diplomado STIT en Seguridad en Tecnología Informática y Telecomunicaciones.
- Primer presidente y miembro fundador de ASOVESINFO (Asociación Venezolana de la Seguridad de la Información)

EVALUACIÓN: A lo largo del curso el participante deberá realizar una serie de actividades por su cuenta. La realización con esmero, dedicación y constancia de las actividades planificadas, determinará el nivel de conocimientos, destrezas y competencias que el participante habrá adquirido al completar el curso. La evaluación del aprendizaje se realiza básicamente mediante cuestionarios y exámenes parciales (tests) sobre la teoría e informes sobre las prácticas. Para aprobar el curso se requiere que la nota final sea de al menos 50%.

- 4 cuestionarios sobre los tópicos de teoría: 30% de la nota final
- 2 exámenes parciales (tests) sobre los tópicos de teoría: 30% de la nota final
- 6 informes sobre 6 experiencias prácticas: 50% de la nota final

Se otorgará la mención honorífica a los participantes que hayan aprobado los exámenes parciales con un promedio de al menos el 80% y que hayan entregado 8 informes.

CONTENIDO PROGRAMÁTICO

1. CRIPTOGRAFÍA Y PROTECCIÓN DE LA CONFIDENCIALIDAD

Parte 1

Criptología, criptografía, criptoanálisis y esteganografía. Criptografía clásica. Cifrado por sustitución y por transposición. Criptografía moderna. El algoritmo DES (*Data Encryption Standard*) y Triple DES. Otros algoritmos de cifrado (IDEA, SAFER, CAST, Blowfish, RC2, RC4, RC5, AES, Serpent, Twofish). Algoritmos en telefonía celular. Encriptación en discos duros y medios extraíbles. OTFE (*On The Fly Encryption*) con PGPdisk, TrueCrypt, EFS (*Encrypted File System*), BitLocker. PBE (*Password Based Encryption*). Desarrollos futuros: Criptografía cuántica. Distribución de claves criptográficas. Uso de KDC (*Key Distribution Center*). Generación de números aleatorios.

Parte 2

Criptografía de clave pública. Ataque del hombre en el medio (MiTM) Sistema DH (*Diffie-Hellman*). Sistema RSA (*Rivest-Shamir-Adleman*). Criptografía de curva elíptica (ECC). Bases matemáticas: Exponencial discreta, factorización de números primos. Aplicaciones: Firma digital, distribución de la clave de sesión, digital envelope, criptomonedas (Bitcoin).

Parte 3

Esteganografía e información oculta. Técnicas esteganográficas. Canales encubiertos. Huevos de Pascua. Estegoimagen. Estegoanálisis. Marca de agua digital.

2. INTEGRIDAD Y AUTENTICIDAD DE LA INFORMACIÓN

Parte 1

El problema de la integridad de datos. Medios físicos de transmisión y almacenamiento. Ruido térmico. Filtros eléctricos. Relación señal a ruido S/N. Ruido impulsivo e interferencia. Fuentes de interferencia electromagnética (EMI). Cable trenzado y cable coaxial. Fibra óptica. Atenuación y distorsión en los cables. Ecualización de la línea. El problema de la diafonía. Medios de transmisión inalámbricos. Interceptación y jamming. Medios transportables (cinta magnética, memoria SD, CD-ROM, DVD). Control de errores (paridad, CRC). Corrección de errores (Hamming, confirmación). Chequeo de integridad mediante hash. Árbol de hashes (Merkle tree) y blockchain. Funciones hash: MD5, SHA, RIPEMD, Whirpool. Uso de MAC (*Message Authentication Code*) y HMAC.

Parte 2

Firma electrónica. Código Seguro de Verificación (CSV). Firma electrónica avanzada/cualificada. Modos de firma (implícito, explícito). Firmas múltiples: Cofirma y contrafirma. Normativa nacional e internacional: ESIGN, EIDAS. Firma digital. Generación con RSA y DSA. Sobre digital (*digital envelope*). PGP. Certificados digitales X.509. Estándares PKCS. Obtención y revocación de certificados digitales. Certificados digitales para servidores web. Seguridad con EV-SSL. Certificados de raíz y certificados autofirmados (*self-signed*).

Generación de certificados con OpenSSL, MakeCert, SelfSSL. Infraestructura de clave pública (PKI). Autoridades de certificación (CA). Aplicaciones de PKI: Navegación segura con HTTPS, banca en línea, compras por Internet, correo electrónico seguro, VPN, fechado digital (*time stamp*). Formatos de firma electrónica: PKCS#7, CMS, XMLdSig, CAdES, XAdES, PAdES, ODF, OOXML. Modos de operación de firma XML (*detached, enveloping, enveloped*). Productos y servicios. @Firma (Gobierno de España). Factura electrónica.

PRÁCTICAS DE ADIESTRAMIENTO

1. Criptografía clásica y moderna
   Objetivo: Familiarizarse con los principios y aplicaciones de la criptografía clásica y moderna para proteger la confidencialidad de la información que se almacena y procesa en los sistemas informáticos y que se transmite por las redes de comunicación.
   Plataforma: Windows

2. Criptografía de clave pública
   Objetivo: Familiarizarse con los principios y aplicaciones de la criptografía de clave pública, y especifícamente con los sistemas RSA (Rivest-Shamir-Adleman) y DH (Diffie-Hellman), utilizados para garantizar la confidencialidad, integridad, autenticidad y no repudio de las transacciones electrónicas y de los documentos digitales.
   Plataforma: Windows

3. Marcas de agua, esteganografía e información oculta
   Objetivo: Familiarizarse con los principios y aplicaciones de las marcas de agua (para clasificar la información o proteger la propiedad intelectual) y de la esteganografía (para esconder y camuflar la información).
   Plataforma: Windows

4. Protección de datos en laptops y medios extraibles
   Objetivo: Familiarizarse con las técnicas para la protección de los datos en dispositivos móviles como laptops y memorias USB, los cuales frecuentemente son extraviados o robados, con el riesgo de que personas extrañas tengan acceso a información confidencial.
   Plataforma: Windows

5. Navegación segura en Internet con SSL/TLS y HTTPS
   Objetivo: Familiarizarse con la operación de los protocolos SSL/TLS y HTTPS, utilizados para establecer una sesión segura entre cliente y servidor, protegiendo la confidencialidad, integridad y autenticidad de los datos de los usuarios que navegan por redes públicas como Internet.
   Plataforma: Windows/Linux

6. Certificados digitales e infraestructura de clave pública PKI
   Objetivo: Familiarizarse con la gestión de los certificados digitales X.509 utilizados para firmar y encriptar mensajes y documentos. Además aprender cómo se generan e instalan certificados digitales para servidores web Apache mediante OpenSSL.
   Plataforma: Windows/Linux

7. Firma digital y sellado de tiempo
   Objetivo: Familiarizarse con el uso de la función hash, firma digital y sellado de tiempo para asegurar la integridad, autenticidad y no repudio de las transacciones electrónicas y de los documentos digitales.
   Plataforma: Windows

8. Correo electrónico seguro
   Objetivo: Familiarizarse con el uso de HTTPS, certificados digitales y firma digital para asegurar la confidencialidad, integridad, autenticidad y no repudio de los mensajes que se envían a través del correo electrónico.
   Plataforma: Windows/Linux