

# CRIPTOGRAFÍA Y FIRMA ELECTRÓNICA

The collage illustrates various cryptographic and digital security concepts:

- One Time Pad:** A diagram showing a message "HOLA" being encrypted with a key "UBYN" using the XOR operation. A stack of pads is shown with numbers like 27564, 34498, 86670, 32451, 99812, 34610, 16843, 46662, etc.
- ROT13:** A diagram showing the letters H, O, L, A being shifted 13 positions to become U, B, Y, N.
- AES-256 ENCRYPTION:** A shield icon representing the Advanced Encryption Standard.
- RSA:** A red logo for the RSA cryptosystem.
- PKI Public Key Infrastructure:** A blue logo for Public Key Infrastructure.
- Digital Signature:** A diagram showing a message "mensaje M" being hashed (H(M)) and then signed with a private key (Clave Privada) to produce a signature "Firma" and its corresponding hash "E[H(M)]".
- Steganography:** A logo for "HIDING IN PLAIN SIGHT SteganoGraphy" with a gear and a key.
- Other elements:** "Kryptos" logo, "Eres preciosa" speech bubble, "Clave" (key) box, "Mensaje" (message) and "Texto cifrado" (encrypted text) labels, "Cifrador" (cipher) box, "Electrical Noise" waveform, "Digest" (MD5, SHA1, SHA256), "CRC Cyclic Redundancy Check", "firmadigital" logo, "Certificado Digital" (Digital Certificate), and "Secure https" icon.

CURSO DIRIGIDO A: Estudiantes y profesionales en las áreas de computación, informática, telecomunicaciones y sistemas.

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.
- Presidente y miembro fundador de [ASOVESINFO](#) (Asociación Venezolana de la Seguridad de la Información)

MODALIDAD: El curso tiene una duración de 6 semanas y se realiza a distancia, de forma no-presencial, utilizando un CD-ROM como material de apoyo, complementado con consultas en línea o por correo electrónico. En ese CD-ROM se encuentran las presentaciones de las clases, artículos técnicos y libros electrónicos, guías para las experiencias prácticas, así como los programas y herramientas para efectuar dichas prácticas.

EQUIPAMIENTO: Disponer de PC o laptop de buenas prestaciones y acceso a Internet, preferiblemente sin restricciones impuestas por proxies y firewalls.

REQUISITOS DESEABLES: Conocimientos en el área de telecomunicaciones, redes y protocolos, especialmente TCP/IP. Familiaridad con el uso de computadoras, sistemas operativos (Windows, Linux, Android), redes de área local (LAN), redes inalámbricas Wi-Fi, Internet. Conocimiento instrumental del idioma inglés.

EVALUACIÓN: A lo largo del curso, el participante deberá realizar una serie de actividades. 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 mediante cuestionarios y exámenes parciales (tests) sobre la teoría e informes sobre las prácticas.

- 4 cuestionarios sobre la teoría: 30%
- 2 exámenes parciales (tests) sobre la teoría: 30%
- 6 informes sobre 6 experiencias prácticas: 40%

---

## 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, dinero digital (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. Ecuación 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). 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: E-SIGN, 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 específicamente 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 extraíbles  
*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