



## FICHA TÉCNICA DE LA ASIGNATURA

<b>Datos de la asignatura</b>	
<b>Nombre completo</b>	Criptografía, Firma electrónica y Blockchain
<b>Código</b>	DTC-MCS-512
<b>Título</b>	Máster en Ciberseguridad
<b>Impartido en</b>	Máster Universitario en Ingeniería de Telecomunicación y Máster en Ciberseguridad [Primer Curso] Máster en Ciberseguridad [Primer Curso]
<b>Nivel</b>	Master
<b>Cuatrimestre</b>	Semestral
<b>Créditos</b>	6,0 ECTS
<b>Carácter</b>	Optativa
<b>Departamento / Área</b>	Departamento de Ciencias de la Computación e Inteligencia Artificial
<b>Responsable</b>	Rafael Palacios Hielscher

<b>Datos del profesorado</b>	
<b>Profesor</b>	
<b>Nombre</b>	Luis Hernández Encinas
<b>Departamento / Área</b>	Departamento de Ciencias de la Computación e Inteligencia Artificial (DCIA)
<b>Correo electrónico</b>	lhernandez@icai.comillas.edu
<b>Profesor</b>	
<b>Nombre</b>	Raúl Olivar Merchant
<b>Departamento / Área</b>	Departamento de Ciencias de la Computación e Inteligencia Artificial (DCIA)
<b>Correo electrónico</b>	rolivar@icai.comillas.edu
<b>Profesor</b>	
<b>Nombre</b>	Alonso Alfredo Rodríguez Rodríguez
<b>Departamento / Área</b>	Departamento de Ciencias de la Computación e Inteligencia Artificial (DCIA)
<b>Correo electrónico</b>	aarodriguez@icai.comillas.edu
<b>Profesor</b>	
<b>Nombre</b>	Luis Hernández Álvarez
<b>Departamento / Área</b>	Departamento de Ciencias de la Computación e Inteligencia Artificial (DCIA)
<b>Correo electrónico</b>	lhalvarez@comillas.edu

## DATOS ESPECÍFICOS DE LA ASIGNATURA

<b>Contextualización de la asignatura</b>
<b>Aportación al perfil profesional de la titulación</b>



La asignatura está orientada a formar a los alumnos en los conceptos teóricos de la criptografía y su uso práctico en mundo de la TI a través de la firma digital y las cadenas de blockchain.

Desde el punto de vista criptográfico se presentarán los hechos históricos (sistemas de cifrado clásicos, medievales y las máquinas de cifrado empleadas a lo largo del siglo XX) y los conceptos elementales que definen la criptología actual (seguridad, confidencialidad, integridad, disponibilidad, identificación, etc.). Se explicarán los fundamentos básicos y problemas matemáticos que son la base de la seguridad de la criptología moderna. Una vez aprendidos estos fundamentos, se estudiarán con profundidad los protocolos de intercambio de clave (DH y ECDH), los criptosistemas simétricos (TDES y AES) y asimétricos (RSA y ECC) de uso más extendido en la actualidad, así como los principales protocolos criptográficos que garantizan la autenticación de los intervinientes en una comunicación (RSA, DSA, ECDSA) y la integridad de la información intercambiada (SHA-1, SHA-2, etc.)

Como primer elemento práctico del uso de la criptografía se presentará su uso en los sistemas de firma digital. Se presentarán las bases que sustentan todo el sistema, desde los certificados a las Autoridades de Certificación y Prestadores de Servicios de Confianza. Se repasarán las bases legales en las que se sustenta todo el modelo, los distintos tipos de firma desde los puntos de vista funcionales y técnicos y sus aportaciones a los procesos de Negocio y la transformación digital. Como ejemplos prácticos se desarrollarán pruebas con un sistema abierto (openSSL) y con un sistema de firma en la nube certificado según el Reglamento EU 910/2014 eIDAS. Desde el punto de vista de la seguridad y sitios web se presentará el uso de protocolos como SSL/TLS como elementos para garantizar la confianza en la navegación y las transacciones.

En los capítulos relativos a BlockChain se va a estudiar el funcionamiento de las redes blockchain convencionales. Primero se comentará el funcionamiento de las redes públicas más populares. Se profundizará en el estudio de la red de Bitcoin y la de Ethereum. Se presentarán los principales y más conocidos ataques a este tipo de redes incidiendo en los objetivos y situaciones en las que la red es más vulnerable. Se comentarán las redes Semi-Permissionadas y sus ventajas y posibles aplicaciones. Se estudiarán las redes privadas o semipermissionadas y las herramientas más habituales que nos podemos encontrar a la hora de comenzar un desarrollo ad-hoc. Para afianzar

conocimientos se realizarán prácticas en las que el alumno deberá utilizar los conocimientos adquiridos en teoría.

## Prerrequisitos

Esta asignatura no tiene prerrequisitos

## Competencias - Objetivos

### Resultados de Aprendizaje

La asignatura está orientada a formar a los alumnos en los conceptos teóricos de la criptografía y su uso práctico en mundo de la TI a través de la firma digital y las cadenas de blockchain.

Desde el punto de vista **criptográfico** se presentarán los hechos históricos (sistemas de cifrado clásicos, medievales y las máquinas de cifrado empleadas a lo largo del siglo XX) y los conceptos elementales que definen la criptología actual (seguridad, confidencialidad, integridad, disponibilidad, identificación, etc.). Se explicarán los fundamentos básicos y problemas matemáticos que son la base de la seguridad de la criptología moderna. Una vez aprendidos estos fundamentos, se estudiarán con profundidad los protocolos de intercambio de clave (DH y ECDH), los criptosistemas simétricos (TDES y AES) y asimétricos (RSA y ECC) de uso más extendido en la actualidad, así como los principales protocolos criptográficos que garantizan la autenticación de los intervinientes en una comunicación (RSA, DSA, ECDSA) y la integridad de la información intercambiada (SHA-1, SHA-2, etc.)

Como primer elemento práctico del uso de la criptografía se presentará su uso en los sistemas de **firma digital**. Se presentarán las bases que sustentan todo el sistema, desde los certificados a las Autoridades de Certificación y Prestadores de Servicios de Confianza. Se repasarán las bases legales en las que se sustenta todo el modelo, los distintos tipos de firma desde los puntos de vista funcionales y técnicos y sus aportaciones a los procesos de Negocio y la transformación digital. Como ejemplos prácticos se desarrollarán pruebas con un sistema abierto (openSSL) y con un sistema de firma en la nube certificado según el Reglamento EU 910/2014 eIDAS. Desde el punto de



vista de la seguridad y sitios web se presentará el uso de protocolos como SSL/TLS como elementos para garantizar la confianza en la navegación y las transacciones.

El los capítulos relativos a **BlockChain** se va a estudiar el funcionamiento de las redes blockchain convencionales. Primero se comentará el funcionamiento de las redes públicas más populares. Se profundizará en el estudio de la red de Bitcoin y la de Ethereum. Se presentarán los principales y más conocidos ataques a este tipo de redes incidiendo en los objetivos y situaciones en las que la red es más vulnerable. Se comentarán las redes Semi-Permissionadas y sus ventajas y posibles aplicaciones. Se estudiarán las redes privadas o semi-permissionadas y las herramientas más habituales que nos podemos encontrar a la hora de comenzar un desarrollo ad-hoc. Para afianzar conocimientos se realizarán prácticas en las que el alumno deberá utilizar los conocimientos adquiridos en teoría.

## BLOQUES TEMÁTICOS Y CONTENIDOS

### Contenidos – Bloques Temáticos

## Criptografía

### Introducción a la criptografía

Conceptos básicos

Hechos históricos

Criptografía y Criptoanálisis

### Generadores de números aleatorios

Entropía

Postulados de Golomb

TRNG

PRNG

### Criptosistemas simétricos

cifrado en stream

cifrado en bloque

### Fundamentos matemáticos para criptografía

Algoritmos

Complejidad computacional

Aritmética modular

Estructuras algebraicas

Problemas computacionalmente difíciles

Curva elípticas

Funciones de resumen (HASH)

Protocolos de intercambio de claves (DH)

Criptosistemas asimétricos

RSA

ElGamal

ECC

### Infraestructura de clave pública

Digital signatures (RSA, ECC, DSA, ECDSA, etc.)

Digital certificates

### Software: Cryptool



# Firma Electrónica

## **Certificados y PKI**

- Repasso a los fundamentos de seguridad y criptografía
- Conceptos básicos de certificados
- Conceptos básicos de Autoridades de Certificación
- PKI y Prestadores de Servicios de Certificación
- Formatos y tipos de firmas
- Repasso de conceptos
- Firma electrónica. Formatos técnicos
- Firma electrónica. Requisitos para llegar a una firma electrónica
- Firma electrónica. Tipos de firma desde la perspectiva funcional
- Firma electrónica. Tipos de firma desde la perspectiva legal
- Firma electrónica. Ejemplos básicos de tipos de firma

## **Ejemplos básicos de firma**

- Introducción a OpenSSL
- Uso de funciones hash
- Uso de cifrado simétrico
- Creación de claves y certificado de nuestra CA
- Validación y uso del certificado de nuestra CA
- Parseo de estructuras ASN.1
- Creación de claves y petición de certificado de un usuario
- Firma del certificado de usuario por parte de la CA
- Creación de un PCKS#12 de usuario partiendo de claves y cert
- Firma de ficheros binarios y firma con Acrobat

## **Legislación de firma**

- Un poco de historia...
- ¿Qué es elDAS?
- Los actores principales... los PCSC o QTSP
- La estrella de la fiesta... la firma electrónica
- La certificación de los dispositivos y los entornos de firma
- La que queda por venir
- La firma como transformador de procesos
- La firma digital como elemento de transformación
- Un caso real... firma de contratos laborales
- Solución propuesta, definición funcional del nuevo modelo
- Demo/Práctica sobre un entorno real

## **Confianza en sitios web**

- Seguridad en Internet y certificados SSL
- Necesidades para poner en marcha el sistema
- Las raíces de confianza y los navegadores
- Tipos de certificados y los niveles de seguridad
- ¿Y para nuestro sitio web?
- La gestión de los certificados como elemento clave del negocio



# Blockchain

Introducción a las redes Blockchain

Historia

Qué es blockchain

Tipos de redes blockchain

## **Red Bitcoin**

Operación

Nodos

Algorítmica

Wallets

## **Red Ethereum**

Operación

Algorítmica

EVM

Ataques y deficiencias de seguridad

Conceptos

Tipos de Ataques

## **Redes Semi-Permissionadas**

Conceptos

Redes

## **Redes Permissionadas**

Conceptos

Redes

Herramientas

Casos de uso de blockchain

Criptografía

# Introducción a la criptografía

- Conceptos básicos
- Hechos históricos
- Criptografía y Criptoanálisis

# Generadores de números aleatorios

- Entropía
- Postulados de Golomb
- TRNG
- PRNG



## Criptosistemas simétricos

- cifrado en stream
- cifrado en bloques

## Fundamentos matemáticos para criptografía

- Algoritmos
- Complejidad computacional
- Aritmética modular
- Estructuras algebraicas
- Problemas computacionalmente difíciles
- Curva elípticas

## Funciones de resumen (HASH)

## Protocolos de intercambio de claves (DH)

## Criptosistemas asimétricos

- RSA
- ElGamal
- ECC

## Infraestructura de clave pública

- Digital signatures (RSA, ECC, DSA, ECDSA, etc.)
- Digital certificates

## Software: Cryptool

### Firma Electrónica

## Certificados y PKI

- Repaso a los fundamentos de seguridad y criptografía
- Conceptos básicos de certificados
- Conceptos básicos de Autoridades de Certificación
- PKI y Prestadores de Servicios de Certificación

## Formatos y tipos de firmas

- Repaso de conceptos
- Firma electrónica. Formatos técnicos
- Firma electrónica. Requisitos para llegar a una firma electrónica
- Firma electrónica. Tipos de firma desde la perspectiva funcional
- Firma electrónica. Tipos de firma desde la perspectiva legal



- Firma electrónica. Ejemplos básicos de tipos de firma

## Ejemplos básicos de firma

- Introducción a OpenSSL
- Uso de funciones hash
- Uso de cifrado simétrico
- Creación de claves y certificado de nuestra CA
- Validación y uso del certificado de nuestra CA
- Parseo de estructuras ASN.1
- Creación de claves y petición de certificado de un usuario
- Firma del certificado de usuario por parte de la CA
- Creación de un PCKS#12 de usuario partiendo de claves y cert
- Firma de ficheros binarios y firma con Acrobat

## Legislación de firma

- Un poco de historia...
- ¿Qué es elDAS?
- Los actores principales... los PCSC o QTSP
- La estrella de la fiesta... la firma electrónica
- La certificación de los dispositivos y los entornos de firma
- La que queda por venir

## La firma como transformador de procesos

- La firma digital como elemento de transformación
- Un caso real... firma de contratos laborales
- Solución propuesta, definición funcional del nuevo modelo
- Demo/Práctica sobre un entorno real

## Confianza en sitios web

- Seguridad en Internet y certificados SSL
- Necesidades para poner en marcha el sistema
- Las raíces de confianza y los navegadores
- Tipos de certificados y los niveles de seguridad
- ¿Y para nuestro sitio web?
- La gestión de los certificados como elemento clave del negocio

### Blockchain

#### Blockchain

## Introducción a las redes Blockchain

- Historia
- Qué es blockchain
- Tipos de redes blockchain



## Red Bitcoin

- Operación
- Nodos
- Algorítmica
- Wallets

## Red Ethereum

- Operación
- Algorítmica
- EVM

## Ataques y deficiencias de seguridad

- Conceptos
- Tipos de Ataques

## Redes Semi-Prmisionadas

- Conceptos
- Redes

## Redes Permisionadas

- Conceptos
- Redes
- Herramientas

## Casos de uso de blockchain

### METODOLOGÍA DOCENTE

#### Aspectos metodológicos generales de la asignatura

- Lecciones en clase
- Prácticas de laboratorio

### EVALUACIÓN Y CRITERIOS DE CALIFICACIÓN

#### Sistema de evaluación:

- Criptografía (42%). Examen.
- Firma Digital (33%). Examen.
- Blockchain (25%): Examen (20%) + Labs (5%)



Al margen de esta ponderación en las notas de cada una de las partes de la asignatura para la obtención de la nota global, para poder aprobar la asignatura completa, el alumno deberá haber obtenido, al menos, un 3 en cada una de ellas de forma separada. Si la nota de alguna de las partes es menor que 3, el alumno deberá volver a examinarse en la convocatoria extraordinaria de la parte en cuya nota haya obtenido menos de 3.

## Calificaciones

### Sistema de evaluación:

- Criptografía (42%). Examen.
- Firma Digital (33%). Examen.
- Blockchain (25%): Examen (20%) + Labs (5%)

Al margen de esta ponderación en las notas de cada una de las partes de la asignatura para la obtención de la nota global, para poder aprobar la asignatura completa, el alumno deberá haber obtenido, al menos, un 3 en cada una de ellas de forma separada. Si la nota de alguna de las partes es menor que 3, el alumno deberá volver a examinarse en la convocatoria extraordinaria de la parte en cuya nota haya obtenido menos de 3.

## Normas de Uso de la IA

La IA puede utilizarse para actividades previas a la tarea, como la lluvia de ideas, la descripción y la investigación inicial. Este nivel se centra en el uso de la IA para la planificación, las síntesis y la generación de ideas, pero las evaluaciones deben hacer hincapié en la capacidad de desarrollar y refinar estas ideas de forma independiente.

La IA puede utilizarse para ayudar a completar la tarea, incluida la generación de ideas, la redacción, la retroalimentación y la evaluación. Los estudiantes deben evaluar y modificar críticamente los resultados sugeridos por la IA, demostrando su comprensión.

En todo caso, el uso de la IA tiene que estar citado y las fuentes verificadas de forma independiente por el alumno.

No se permite el uso de la IA en ninguna de las pruebas de examen, ni en los tests de evaluación del rendimiento

## BIBLIOGRAFÍA Y RECURSOS

En cumplimiento de la normativa vigente en materia de **protección de datos de carácter personal**, le informamos y recordamos que puede consultar los aspectos relativos a privacidad y protección de datos que ha aceptado en su matrícula entrando en esta web y pulsando "descargar"

<https://servicios.upcomillas.es/sedeelectronica/inicio.aspx?csv=02E4557CAA66F4A81663AD10CED66792>