Criptografía Código: **75.601** Créditos: **6**

ATENCIÓN: Esta información recoge los apartados del plan docente de la asignatura durante el último semestre con docencia. Al iniciar el periodo de matrícula, podrás consultar el calendario y modelo de evaluación para el siguiente semestre en Trámites / Matrícula / Horarios de las pruebas de evaluación final.

DESCRIPCIÓN

La asignatura de Criptografía tiene como objetivo fundamental formar a los alumnos en el ámbito de la criptografía moderna. Esta disciplina tiene cada vez más importancia en el mundo en que vivimos debido al creciente valor que tiene la información. Por un lado, las técnicas criptográficas son necesarias para proteger la seguridad y la privacidad de los usuarios cuando hacen uso de la tecnología y de las redes de comunicaciones. En especial es importante proteger el usuarios de actividades de vigilancia masiva que pueden llevar a cabo de forma ilegal no sólo empresas privadas sino también algunos organismos gubernamentales que actúan fuera de los circuitos legales. Por otra parte, más allá de la propia protección de los usuarios, las empresas y cualquier entidad que se relacione o utilice la tecnología necesita mecanismos que protejan sus activos digitales que, en ocasiones, pueden ser todos los activos de una compañía. Finalmente, el desarrollo de la criptografía también permite el nacimiento de nuevos paradigmas de relación entre las personas como la creación de nuevas monedas virtuales, las criptomonedas, que no dependen de ninguna entidad centralizada para poder funcionar.

El curso quiere dar un enfoque práctico de la criptografía, y es por este motivo que la asignatura se estructura conjuntamente en base a contenidos tanto teóricos como prácticos que son complementados con actividades de programación que permiten conocer los problemas reales que surgen en la implementación de sistemas criptográficos.

LA ASIGNATURA EN EL CONJUNTO DEL PLAN DE ESTUDIOS

La criptografía es una asignatura dentro del área de conocimiento de la seguridad en tecnologías de la información y de las comunicaciones. La seguridad es un área muy transversal e interdisciplinar, y por eso sus asignaturas se imparten en diferentes estudios, desde las licenciaturas de matemáticas hasta las ingenierías informáticas y de telecomunicaciones. En cuanto a la ingeniería informática o de telecomunicaciones, la asignatura de criptografía está relacionada con las otras asignaturas del área de seguridad: seguridad en redes de comunicaciones y comercio electrónico. Otras asignaturas relacionadas son el Álgebra (provee al alumno de una base en aritmética modular), la Lógica (proporciona los fundamentos lógicos), la asignatura de Grafos y Complejidad (introducen problemas complejos que tienen aplicaciones en el campo de la criptografía) y, todas las asignaturas de programación, ya que algunas de las actividades prácticas requieren conocimientos de programación.

OBJETIVOS Y COMPETENCIAS

Los objetivos de la asignatura son los siguientes:

1. Asimilar la historia, la terminología y los fundamentos de la criptografía.
2. Adquirir conocimientos básicos de aritmética modular.
3. Conocer los fundamentos teóricos de la criptografía moderna.
4. Adquirir los conocimientos necesarios para implementar cifras de clave pública y de clave privada.
5. Comprender los componentes y el funcionamiento de una infraestructura de clave pública (PKI).
6. Entender el funcionamiento de diferentes protocolos criptográficos que se utilizan en la actualidad.

Los objetivos señalados están vinculados a las competencias del Grado siguientes:

[5] Capacidad para adaptarse a las tecnologías y a los futuros entornos actualizando las competencias profesionales.

[9] Capacidad para evaluar soluciones tecnológicas y elaborar propuestas de proyectos teniendo en cuenta los recursos, las alternativas disponibles y las condiciones de mercado.

[11] Capacidad de utilizar los fundamentos matemáticos, estadísticos y físicos para comprender los sistemas TIC.

[20] Capacidad para proponer y evaluar diferentes alternativas tecnológicas para resolver un problema concreto.

CONTENIDOS

A continuación se detallan los contenidos de la asignatura agrupando en bloques temáticos los diferentes módulos que la componen:

Unidad 1: Conceptos básicos

Se estudia la terminología básica así como la evolución histórica de la criptografía. Se repasan los criptosistemas históricos más relevantes. Se introducen los conceptos más relevantes de aritmética modular para tener la base matemática suficiente para entender los criptosistemas y los protocolos criptográficos que se presentan a lo largo del curso. Este bloque incluye los módulos 1 y 2.

- Módulo 1: Introducción a la criptografía
- Módulo 2: Fundamentos matemáticos

Unidad 2: Criptografía de clave compartida

Se estudian las dos grandes familias de criptosistemas de clave compartida: cifrado de bloque y cifrado de flujo. Para cada familia se caracterizan sus propiedades principales y se estudian los criptosistemas más relevantes. Por otra parte se definen las funciones hash, incidiendo en sus propiedades y aplicaciones y analizando a fondo una de sus implementaciones más relevantes: SHA256. Este bloque incluye los módulos 3 y 4.

- Módulo 3: Criptografía de clave simétrica
- Módulo 4: Funciones hash

Unidad 3: Cifras de clave pública

Se da la caracterización de las propiedades más importantes de los criptosistemas de clave pública haciendo énfasis en temas como la distribución de claves, las firmas digitales, la combinación entre clave pública / clave simétrica, así como aspectos relevantes de implementación de la criptografía de clave pública . Finalmente, se estudian la arquitectura y los protocolos asociados a las infraestructuras de clave pública (Public Key Infrastructure, PKI). Este bloque incluye los módulos 5 y 6.

- Módulo 5: Criptografía de clave pública
- Módulo 6: Infraestructura de clave pública (PKI)

Unidad 4: Protocolos criptográficos

Se ponen en práctica las primitivas criptográficas descritas a lo largo del curso para el desarrollo de protocolos criptográficos, tales como, la compartición de secretos, las pruebas de conocimiento nulo, la transferencia inconsciente o la computación multiparte segura. Este bloque incluye el módulo 7.

- Módulo 7: Protocolos criptográficos

Actividades prácticas

Las actividades prácticas deben permitir aplicar los conocimientos teóricos adquiridos en los módulos. Siguiendo la metodología de evaluación continua, las actividades prácticas se realizarán a lo largo del curso. **Las actividades prácticas se desarrollarán con el lenguaje Python**, que dispone de una serie de librerías con funcionalidades matemáticas que permiten simplificar la implementación de sistemas criptográficos. Esto permite que el estudiante se pueda centrar en la parte conceptual de la materia y abstraerse de algunos detalles menos relevantes, que sí son necesarios para la implementación.

CONSULTA DE LOS RECURSOS DE APRENDIZAJE QUE DISPONE LA ASIGNATURA

Material	Soporte
Criptografía	PDF

RECURSOS DE APRENDIZAJE Y HERRAMIENTAS DE APOYO

El material didáctico de la asignatura se compone de 8 módulos didácticos en formato papel. Para realizar algunas de las actividades prácticas se utilizará el lenguaje de programación Python, del que encontraréis más información en el apartado de recursos del aula.

En ciertos apartados de la asignatura se proporcionará material complementario de especial interés, que el alumno podrá encontrar en el espacio de recursos del aula.

BIBLIOGRAFÍA Y FUENTES DE INFORMACIÓN

"Handbook of Applied Cryptography", Alfred J. Menezes, Paul C. van Oorschot i Scott A. Vanstone,CRC Press, 1999. http://cacr.math.uwaterloo.ca/hac/

"Understanding Cryptography", Christof Paar, Jan Pelzl, Springer, 2010.

"**Cryptography Made Simple**", Niguel P. Smart Springer, 2016.

METODOLOGÍA

Los estudiantes deben estudiar los materiales docentes de la asignatura (**módulos didácticos**) dado que estos, principalmente, son los que exponen los contenidos de la misma. Además, será necesario que realicen de manera **obligatoria** (dado que la asignatura no tiene examen) todas las actividades de evaluación continua que complementan y consolidan el aprendizaje.

En cada módulo, el estudiante encontrará un conjunto de **ejercicios de autoevaluación** de manera que pueda ser él mismo quien evalúe los conocimientos adquiridos.

El seguimiento activo de los **espacios del aula (tablón, foro)** es de primordial interés, dado que habitualmente se plantean dudas, se dan respuestas y se tratan temas relacionados con la materia de estudio.

Es importante intentar realizar un **trabajo constante de estudio y aplicación de los contenidos** dado que esta es la mejor manera de superar la asignatura. En este sentido van las propuestas de distribución temporal de aprendizajes incluidas en este documento y las otras que se puedan dar durante el curso.

Para facilitar la aplicación práctica de los contenidos y el apoyo en su experimentación dispone del **laboratorio de Criptografía**. El consultor del laboratorio os ayudará en el uso de las herramientas y sus problemáticas (y no tanto en la resolución de las dudas conceptuales sobre contenidos, tarea que lleva a cabo el consultor del aula de teoría).

INFORMACIÓN SOBRE LA EVALUACIÓN EN LA UOC

La Normativa académica de la UOC dispone que el proceso de evaluación se fundamenta en el trabajo personal del estudiante y presupone la autenticidad de la autoría y la originalidad de los ejercicios realizados.

La falta de originalidad en la autoría o el mal uso de las condiciones en las que se hace la evaluación de la asignatura es una infracción que puede tener consecuencias académicas graves.

El estudiante será calificado con un suspenso (D/0) si se detecta falta de originalidad en la autoría de alguna actividad evaluable (práctica, prueba de evaluación continua (PEC) o final (PEF), o la que se defina en el plan docente), ya sea porque ha utilizado material o dispositivos no autorizados, ya sea porque ha copiado de forma textual de internet, o ha copiado de apuntes, de materiales, manuales o artículos (sin la citación correspondiente) o de otro estudiante, o por cualquier otra conducta irregular.

La calificación de suspenso (D/0) en la evaluación continua (EC) puede conllevar la obligación de hacer el examen presencial para superar la asignatura (si hay examen y si superarlo es suficiente para superar la asignatura según indique este plan docente).

Cuando esta mala conducta se produzca durante la realización de las pruebas de evaluación finales presenciales, el estudiante puede ser expulsado del aula, y el examinador hará constar todos los elementos y la información relativos al caso.

Además, esta conducta puede dar lugar a la incoación de un procedimiento disciplinario y la aplicación, si procede, de la sanción que corresponda.

La UOC habilitará los mecanismos que considere oportunos para velar por la calidad de sus titulaciones y garantizar la excelencia y la calidad de su modelo educativo.

CONSULTA DEL MODELO DE EVALUACIÓN

Esta asignatura sólo puede superarse a partir de la evaluación continua (EC), nota que se combina con una nota de prácticas (Pr) para obtener la nota final de la asignatura. No se prevé hacer ningún examen final o prueba presencial. La fórmula de acreditación de la asignatura es la siguiente: EC + Pr.

Ponderación de las calificaciones

Opción para superar la asignatura: EC + Pr

Nota final de asignatura = Final Continuada (FC) = EC+Pr

EC = 50%

Pr = 50%

Notas mínimas:

· Pr = 5

· EC = 5

En caso de no conseguir la nota mínima en la Pr, la nota obtenida en la fórmula corresponde a la obtenida en la Pr

EVALUACIÓN CONTÍNUA

La evaluación de esta asignatura se hará exclusivamente a través de la evaluación continua que consta de:

- Cinco PECs de carácter más teórico sobre el contenido de la asignatura. Cada PEC consistirá en cuestionarios personalizados que incluirán preguntas referentes a los módulos correspondientes. Estos ejercicios deben permitir al estudiante reflexionar sobre los conceptos que se han presentado en los módulos. Los cuestionarios estarán activos entre las fechas de inicio y finalización de cada actividad, se podrá acceder a ellos a través del aula de la asignatura y su resolución también se realizará vía la aplicación que muestra el cuestionario. Cada cuestionario, atendiendo a su dificultad, se deberá resolver en un tiempo fijado, tiempo que se especificará de forma clara en cada enunciado.

Actividad	Módulos a los que hace referencia	Valoración a C
PEC-1	Módulos 1, 2	10%
PEC-2	Módulos 3	25%
PEC-3	Módulos 4	10%
PEC-4	Módulos 5	25%
PEC-5	Módulos 6,7	30%

- Tres ejercicios prácticos que servirán para ilustrar los contenidos teóricos de la asignatura.

Actividad	Módulos a los que hace referencia	Valoración a P
Prac-1	Módulos 1 y 2	30%
Prac-2	Módulos 3 y 4	30%
Prac-3	Módulos 5, 6 y 7	40%

Para superar la asignatura, es imprescindible que se entreguen todas las pruebas de evaluación continuada (PECs y Prácticas).

El hecho de entregar cualquier actividad de la evaluación continua implica que se obtendrá una nota final de EC. Así pues, la valoración de "No presentado" sólo se obtendrá si no se entrega ninguna actividad de la evaluación continua.

La nota final de la EC, que será la misma que la de la asignatura, se determinará en función de las calificaciones obtenidas en las PECs y de las prácticas a partir de la fórmula especificada en el apartado "Consulta del Modelo de Evaluación" de este plan docente. Además, también se tendrá en cuenta para la nota final de la asignatura, la participación del estudiante en el foro y haber demostrado un dominio suficiente en los aspectos fundamentales de la asignatura durante el semestre.

El seguimiento correcto de la asignatura os compromete a realizar las actividades propuestas de manera individual y según las indicaciones que pauta este Plan Docente. En caso de que no sea así, la evaluación continuada y/o las prácticas se evaluarán con una D.

Por otra parte, y siempre a criterio de los Estudios, el incumplimiento de este compromiso puede suponer que no se permita superar ninguna otra asignatura mediante evaluación continua ni en el semestre en curso ni en los siguientes.

FEEDBACK

El consultor os guiará y orientará a través del Tablón del aula para que podáis hacer un buen seguimiento de la asignatura. También responderá las dudas que vayan saliendo en el Foro del aula así como las consultas y comentarios enviados a su buzón personal.

El consultor también hará un seguimiento personalizado de la evaluación continua, revisará todas las PECs y prácticas entregadas y comentará de forma cualitativa a nivel grupal y/o individual la resolución. Estos comentarios os ayudarán a progresar en vuestro aprendizaje y a adquirir el conjunto de las competencias.