# Criptografía y seguridad informática

**Curso Académico: ( 2019 / 2020 )** **Fecha de revisión: 23-04-2020**

**Departamento asignado a la asignatura: Departamento de Informática**

**Coordinador/a: GONZALEZ-TABLAS FERRERES, ANA ISABEL**

**Tipo: Obligatoria Créditos ECTS : 6.0**

**Curso : 4 Cuatrimestre : 1**

## REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

Programación
Estadística
Matemática Discreta

## OBJETIVOS

Los objetivos de esta asignatura son que el estudiante reconozca la importancia actual de la criptografía y de las tecnologías que permiten su tratamiento, los puntos débiles de éstas y las amenazas que sufren. Así mismo, el alumno debe terminar conociendo los principios, métodos y medios de los sistemas de seguridad. Para lograr estos objetivos el alumno debe adquirir una serie de conocimientos, capacidades y actitudes.

Por lo que se refiere a los conocimientos, al finalizar el curso el estudiante será capaz de:
- Conocer en profundidad los fundamentos matemáticos de la criptografía y criptoanálisis, con especial atención a la teoría de números.
- Dominar los principales criptosistemas y los algoritmos de cifrado actuales más característicos.
- Dominar los sistemas de firma y verificación basados en clave pública
- Conocer los problemas asociados a la gestión de claves y sus diversas soluciones.
- Entender los fundamentos de las medidas de seguridad, con especial atención a los sistemas y protocolos criptográficos, sus principios métodos y medios.
- Reconocer los diversos sistemas de autenticación, sus ventajas e inconvenientes.
- Diferenciar los objetivos de la seguridad de la información

Por lo que atañe a las capacidades se pueden desglosar en específicas y genéricas (destrezas).
En cuanto a las capacidades específicas, el alumno será capaz de:
- Resolver problemas de la teoría de números en su aplicación a la criptografía. (P.O.: a)
- Reconocer las ventajas, inconvenientes y usos de los sistemas de clave secreta y pública. (P.O.: a, c)
- Cifrar y descifrar en distintos entornos, detectando posibles ataques (P.O.: a, c)
- Firmar y verificar en distintos entornos, detectando posibles ataques (P.O.: a, c)
- Diseñar y aplicar los mecanismos de seguridad oportunos (principalmente criptográficos) para un sistema de información. (P.O.: a, c, e)
- Aplicar los mecanismos de autenticación pertinentes a un sistema de información (P.O.: a, c, e)

En cuanto a las capacidades generales o destrezas, durante el curso se trabajarán:
- La capacidad para encontrar y seleccionar las informaciones relevantes para solucionar un problema concreto. (P.O.: a, b)
- La capacidad para aplicar conocimientos multidisciplinares a la resolución de un determinado problema. (P.O.: a, c, e, g)
- La capacidad para investigar un sistema particular en un entorno concreto y hallar sus vulnerabilidades y amenazas. (P.O.: a, b)

En cuanto a las actitudes el alumno tras cursar el curso debería tener:
- Una actitud crítica respecto de la seguridad que ofrece un sistema de información particular, en un entorno dado y unos riesgos determinados. (P.O.: i)
- Una actitud recelosa respecto de la seguridad supuesta de los sistemas y protocolos criptográficos implementados en los sistemas. (P.O.: i)

En relación con las competencias básicas establecidas en el artículo 3 sobre competencias RD

1393/2007 modificado por el RD 861/2010, en esta asignatura se aborda la competencia CB1:
- Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio.

En relación con las competencias según lo establecido el apartado 5 del Anexo II de la Resolución de 8 de junio de 2009, de la Secretaría General de Universidades (BOE de 4 de Agosto de 2009) en esta asignatura se aborda la competencia CGB3:
- Capacidad para comprender y dominar los conceptos básicos de matemática discreta, lógica, algorítmica y complejidad computacional, y su aplicación para la resolución de problemas propios de la ingeniería.

## DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

1. Fundamentos matemáticos de la criptografía.
1.1. Teoría de números
1.2. Aritmética modular
1.3. Cálculo de inversos
1.4. Logaritmos discretos
1.5. Cuerpos de Galois
2. Criptografía
2.1. Introducción
2.2. Criptografía clásica y criptoanálisis
2.3. Criptosistemas simétricos
2.4. Funciones resumen y MAC
2.5. Criptosistemas asimétricos
2.6. Generación y distribución de claves
2.7. Criptosistemas de firma digital
2.8. Infraestructuras de clave pública
3. Autenticación de usuarios
4. Introducción a la seguridad en las tecnologías de la información
4.1. Vulnerabilidades y amenazas
4.2. Medidas y mecanismos

## ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

La metodología docente incluirá:

(1) Clases magistrales (2,5 ECTS). Los profesores presentarán un resumen de los conocimientos que los alumnos deben adquirir y se espera que el alumno participe activamente durante la clase. Para facilitar su desarrollo los alumnos recibirán el material básico de la asignatura (las notas de clase, las referencias a los textos bibliográficos básicos y el material complementario) en la herramienta web oportuna. Los alumnos leerán y estudiarán este material (trabajo del alumno). (P.O.: a, c, g, i)
(2) Problemas (2,0 ECTS). El alumno, guiado por el profesor durante las clases de problemas, resolverá ejercicios que le servirán para aplicar los conocimientos adquiridos. Los alumnos resolverán problemas adicionales fuera del tiempo de clase (trabajo del alumno). (P.O.: a, c, g, i)
(3) Prácticas (1,5 ECTS) en laboratorio / aula informática. El alumno aprenderá el uso de las principales herramientas criptográficas de defensa. Se publicarán las instrucciones de las prácticas para que el alumno las realice. Se ofrecerán sesiones en las que el profesor dará soporte a los alumnos en la realización de las prácticas. Los alumnos completarán las tareas solicitadas en cada práctica fuera del tiempo de clase (trabajo del alumno). (P.O.: a, b, c, e, g, i)

## SISTEMA DE EVALUACIÓN

La evaluación se basará en los siguientes criterios:

1) Entrega de resultados de las prácticas en aulas informáticas y tests: 30% (P.O.: a, b, c, e, g, i)
La nota se calculará como la suma de las notas obtenidas en las diferentes actividades de evaluaciones de las prácticas.
2) Exámenes de teoría y problemas: 70% (P.O.: a, c, g, i)
2.1) Examen de evaluación continua: 30% (durante el curso).
2.2) Examen de final (obligatorio). Conjunto de teoría y problemas: 40%. Para superar la asignatura se debe obtener un mínimo de puntos en el examen final.

ALGORITMO EVALUACIÓN CONTINUA:

NOTA_TOTAL = NOTA_PRAC + NOTA_EX + NOTA_EX_FINAL;

IF NOTA_EX_FINAL<2 THEN
--IF NOTA_TOTAL>5 THEN
----NOTA_TOTAL=4,5
--END_IF
END_IF

Podrían ofrecerse actividades adicionales de evaluación optativas que no se tendrán en cuenta para asignar las matrículas de honor, aunque sí contarán en la nota final del estudiante.

| | |
|---|---|
| **Peso porcentual del Examen Final:** | 40 |
| **Peso porcentual del resto de la evaluación:** | 60 |

## BIBLIOGRAFÍA BÁSICA


- A. MENEZES HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS.
- A.I. González-Tablas Ferreres y P. Martín González Recopilación de problemas de examen 2010-2015. Criptografía y Seguridad Informática, CopyRed, 2016
- J. PASTOR; M.A. SARASA; J.L. SALAZAR CRIPTOGRAFÍA DIGITAL. FUNDAMENTOS Y APLICACIONES. (2ª EDICIÓN), PRENSAS UNIVERSITARIAS DE ZARAGOZA.
- W. STALLINGS CRYPTOGRAPHY AND NETWORK SECURITY. (5ª EDICIÓN), PRENTICE HALL.