Criptografía y seguridad informática

Curso Académico: (2020 / 2021) **Fecha de revisión: 10-07-2020**

Departamento asignado a la asignatura: Departamento de Informática

Coordinador/a: GONZALEZ-TABLAS FERRERES, ANA ISABEL

Tipo: Obligatoria Créditos ECTS : 6.0

Curso : 3 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

AF1.CLASES TEÓRICO-PRÁCTICAS. Conocimientos que deben adquirir los alumnos.Estos recibirán las notas de clase y tendrán textos básicos de referencia para facilitar el seguimiento de las clases y el desarrollo del trabajo posterior.Se resolverán ejercicios, prácticas problemas por parte del alumno y se realizarán talleres y prueba de evaluación para adquirirlas capacidades necesarias.Para asignaturas de 6 ECTS se dedicarán 44 horas como norma general con un 100% de presencialidad.(excepto aquellas que no tengan examen que dedicarán 48 horas)
AF2.TUTORÍAS. Asistencia individualizada (tutorías individuales) o en grupo (tutorías colectivas) a los estudiantes por parte del profesor. Para asignaturas de 6 créditos se dedicarán 4 horas con un 100% de presencialidad.
AF3.TRABAJO INDIVIDUAL O EN GRUPO DEL ESTUDIANTE. Para asignaturas de 6 créditos se dedicarán 98 horas 0% presencialidad.
AF8.TALLERES Y LABORATORIOS. Para asignaturas de 3 créditos se dedicarán 4 horas con un 100% de presencialidad. Para las asignaturas de 6 créditos se dedicarán 8 horas con un 100% de presencialidad.
MD1.CLASE TEORÍA. Exposiciones en clase del profesor con soporte de medios informáticos y audiovisuales, en las que se desarrollan los conceptos principales de la materia y se proporcionan los materiales y la bibliografía para complementar el aprendizaje de los alumnos.
MD2.PRÁCTICAS. Resolución de casos prácticos, problemas, etc. planteados por el profesor de manera individual o en grupo.
MD3.TUTORÍAS. Asistencia individualizada (tutorías individuales) o en grupo (tutorías colectivas) a los estudiantes por parte del profesor. Para asignaturas de 6 créditos se dedicarán 4 horas con un 100% de presencialidad.
MD6.PRÁCTICAS DE LABORATORIO. Docencia aplicada/experimental a talleres y laboratorios bajo la supervisión de un tutor.

SISTEMA DE EVALUACIÓN

SE1.EXAMEN FINAL. En el que se valorarán de forma global los conocimientos, destrezas y capacidades adquiridas a lo largo del curso. El porcentaje de valoración varía para cada asignatura en un rango entre el 60% y el 0%.
SE2.EVALUACIÓN CONTINUA. En ella se valorarán los trabajos, presentaciones, actuación en debates, exposiciones en clase, ejercicios, prácticas y trabajo en los talleres a lo largo del curso. El porcentaje de valoración varía para cada asignatura en un rango entre el 40 y el 100 % de la nota final.

Se podrá requerir la obtención de un rendimiento mínimo en el examen final.

Peso porcentual del Examen Final:	20
Peso porcentual del resto de la evaluación:	80

BIBLIOGRAFÍA BÁSICA

- 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.
- Jean-Philippe Aumasson Serious Cryptography: A Practical Introduction to Modern Encryption , Random House LCC US .
- W. STALLINGS CRYPTOGRAPHY AND NETWORK SECURITY. (5ª EDICIÓN), PRENTICE HALL.