Técnicas y Protocolos Criptográficos

Curso Académico: (2020 / 2021) **Fecha de revisión: 07-09-2020**

Departamento asignado a la asignatura: Departamento de Informática

Coordinador/a: CAMARA NUÑEZ, MARIA CARMEN

Tipo: Optativa Créditos ECTS : 3.0

Curso : 1 Cuatrimestre : 1

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE Y RESULTADOS DEL APRENDIZAJE.

Competencias básicas:

1) Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación.

2) Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.

3) Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

Competencias generales:

1) Capacidad para comprender y aplicar métodos y técnicas de investigación en el ámbito de la Ingeniería Informática.

2) Capacidad de concebir, diseñar o crear, poner en práctica y adoptar un proceso sustancial de investigación o creación.

3) Saber transmitir de un modo claro y sin ambigüedades a un público especializado o no, resultados procedentes de la investigación científica y tecnológica o del ámbito de la innovación más avanzada, así como los fundamentos más relevantes sobre los que se sustentan;

Competencias específicas:

1) Capacidad de análisis crítico de documentos técnicos y científicos en el ámbito de la Ingeniería Informática.

2) Conocer el significado de la investigación científica.

3) Capacidad para conocer y analizar los algoritmos criptográficos, y evaluar sus vulnerabilidades.

4) Comprender los mecanismos de gestión de claves.

El estudiante adquirirá capacidad de uso, análisis y diseño en las siguientes áreas de conocimiento:

1) Protocolos criptográficos.

2) Técnicas de criptoanálisis clásicas y modernas.

3) Análisis y diseño de primitivas criptográficas.

4) Implementación de algoritmos y protocolos criptográficos.

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

Bloque 1. Introducción

a. Introducción a ciberseguridad.

Bloque 2. Protocolos

a. Protocolos criptográficos estándares
b. Protocolos criptográficos ultraligeros

Bloque 3. Criptoanálisis
a. Criptoanálisis de protocolos criptograficos

Bloque 4. Ciberseguridad en dispositivos con capacidades restringidas
a. Vulnerabilidades
b. Ataques
c. Contramedidas

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

Actividades formativas:

1) Clases teórico prácticas

2) Tutorías

3) Trabajo individual del estudiante

4) Trabajo en equipo de los estudiantes

Metodologías docentes:

1) 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 proporciona la bibliografía para complementar el aprendizaje de los alumnos.

2) Lectura crítica de textos recomendados por el profesor de la asignatura: Artículos de prensa, informes, manuales y/o artículos académicos, bien para su posterior discusión en clase, bien para ampliar y consolidar los conocimientos de la asignatura.

3) Elaboración de trabajos e informes de manera individual o en grupo.

4) Exposición en clase sobre un texto o artículo de investigación recomendado por el profesor.

SISTEMA DE EVALUACIÓN

Se establece el siguiente sistema de evaluación:

1. Convocatoria ordinaria - evaluación continua

A. Examen final (30% de la nota final)
-La nota mínima será de 4.0 para superar la asignatura

B. Prácticas de laboratorio (70% de la nota final)

2. Convocatoria ordinaria - evaluación no continua
A. Examen final (100% de la nota final)
-La calificación máxima obtenible será de 6 puntos
-Será necesario obtener 5 puntos para superar la asignatura.
-El examen contendrá ejercicios específicos para comprobar la adquisición de competencias relativas a los trabajos.

3. Convocatoria extraordinaria
La calificación de los estudiantes en la convocatoria extraordinaria se ajustará a las siguientes reglas:

a. Si el estudiante siguió el proceso de evaluación continua, el examen tendrá el mismo valor porcentual que en la convocatoria ordinaria, y la calificación final de la asignatura tendrá en cuenta la nota de la evaluación continua y la nota obtenida en el examen final.

b. Si el estudiante no siguió el proceso de evaluación continua, tendrá derecho a realizar un examen en la convocatoria extraordinaria con un valor del 100 % de la calificación total de la asignatura. Este examen podrá contener preguntas pertinentes a las actividades realizadas durante el curso. En esta asignatura no se permite la reentrega de los

trabajos en esta convocatoria.

Peso porcentual del Examen Final:	30
Peso porcentual del resto de la evaluación:	70

BIBLIOGRAFÍA BÁSICA

- Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone Handbook of Applied Cryptography, CRC Press.

- Christopher Swenson Modern Cryptanalysis: Techniques for Advanced Code Breaking, ohn Wiley & Sons Ltd .

- Colin Boyd and Anish Mathuria Protocols for Authentication and Key Establishment , Springer .

- Dr Sandeep Kumar Sood Authentication Protocols: CRYPTANALYSIS OF PASSWORD BASED AUTHENTICATION AND KEY AGREEMENT PROTOCOLS, LAP LAMBERT Academic Publishing.

- Mark Stamp and Richard M. Low Applied Cryptanalysis: Breaking Ciphers in the Real World, Wiley-Blackwell.

- Pedro Peris-Lopez Lightweight Cryptography in Radio Frequency Identification Systems. Analysis and Design of Protocols and Cryptographic Primitives. , Verlag Dr. Muller (VDM), 2010