Curso Académico: (2019 / 2020)**Fecha de revisión: 02/05/2019 11:50:10**

Departamento asignado a la asignatura:**Coordinador/a: PERIS LOPEZ, PEDRO****Tipo: Optativa Créditos ECTS : 3.0****Curso : 1 Cuatrimestre : 1**

OBJETIVOS

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

1. Protocolos
 - 1.1 Protocolos criptográficos estándares
 - 1.2 Protocolos criptográficos ultraligeros.
2. Primitivas criptográficas
 - 2.1 Primitivas criptográficas clásicas.
 - 2.2 Primitivas criptográficas modernas.
3. Criptoanálisis
 - 3.1 Criptoanálisis de protocolos criptográficos.
 - 3.2 Criptoanálisis de primitivas criptográficas.
4. Implementaciones hardware
 - 4.1 Implementación protocolos criptográficos
 - 4.2. Implementación de primitivas criptográficas

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

Peso porcentual del Examen/Prueba Final:	100
Peso porcentual del resto de la evaluación:	0

La evaluación de la asignatura se realizará a través de un trabajo de investigación sobre protocolos criptográficos que se realizará durante el transcurso de la asignatura. El trabajo tendrá una componente teoría y práctica (programación en el lenguaje elegido por el alumno). La lista de trabajos será publicada por el profesor y los posibles trabajos serán seleccionados de dicha lista, o bien, podrán ser propuestos por el alumno siempre y cuando el profesor le de su aprobación. El alumno tendrá que entregar una memoria del trabajo, así como todo el código desarrollado. A su vez, se tendrá que realizar una exposición en público presentando y explicando brevemente el trabajo realizado.

La calificación de la asignatura se realizará de la siguiente manera:

- Memoria y código desarrollado: 85%.
- Presentación y contestación a las preguntas: 15%.

Alternativamente, la calificación de la asignatura podría realizarse mediante un examen con ejercicios prácticos (100% de la calificación).

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, John 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.