

TÉCNICAS Y PROTOCOLOS CRIPTOGRÁFICOS

Curso Académico: (2015 / 2016)

Fecha de revisión: 18-05-2015

Departamento asignado a la asignatura:

Coordinador/a: PERIS LOPEZ, PEDRO

Tipo: Optativa Créditos ECTS : 4.5

Curso : 1 Cuatrimestre : 1

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

Ninguno

OBJETIVOS

Análisis y diseño de protocolos criptográficos.
 Conocimiento y capacidad de uso de las técnicas criptoanálisis clásicas y modernas.
 Análisis y diseño de primitivas criptográficas.
 Implementación algoritmos y protocolos criptográficos.

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

- 1.1 Protocolos criptográficos.
- 1.2 Protocolos criptográficos ultraligeros.
- 2.1 Primitivas criptográficas clásicas.
- 2.2 Primitivas criptográficas modernas.
- 3.1 Criptoanálisis de protocolos criptográficos.
- 3.2 Criptoanálisis de primitivas criptográficas.
- 4.1 Implementación de algoritmos y protocolos criptográficos.

SISTEMA DE EVALUACIÓN

La evaluación de la asignatura se realizará a través de un único 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: 75%.
- Presentación y contestación a las preguntas: 25%.

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

BIBLIOGRAFÍA BÁSICA

- Christopher Swenson Modern Cryptanalysis: Techniques for Advanced Code Breaking, John Wiley & Sons Ltd.
- Mark Stamp, Richard M. Low Applied Cryptanalysis: Breaking Ciphers in the Real World, Wiley-Blackwell.
- Menezes, A. J.; Vanstone, P. C van Handbook of Applied Cryptography, CRC Press. 1996.
- Pastor, J; Sarasa, M. A Criptografía Digital. Fundamentos y Aplicaciones, Colección Textos Docentes. Zaragoza, 1998..
- Pedro Peris-Lopez Lightweight Cryptography in Radio Frequency Identification Systems: Analysis and

Design of Protocols and Cryptographic Primitives, VDM Verlag Dr. Müller.

- Schneier, B. Applied Cryptography. Protocols, Algorithms and Source code in C, 2ª edición. John Wiley, 1996..
- Stallings, William Cryptography and network security, 3ª edición. Prentice Hall, 2003..
- Wenbo Mao Modern Cryptography: Theory and Practice , Prentice Hall.

BIBLIOGRAFÍA COMPLEMENTARIA

- Antoine Joux Algorithmic Cryptanalysis, Chapman & Hall/CRC.
- Dmitry Khovratovich New Methods in Symmetric Cryptanalysis: How to break ciphers and hash functions , LAP LAMBERT Academic Publishing.
- Elementary Cryptanalysis Ele Abraham Sinkov, Mathematical Association of America.
- Helen Fouche Gaines Cryptanalysis , Dover Publications Inc..