

FUNDAMENTOS DE CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA

Curso 2023 / 24

6 ECTS

2 horas Teoría + 2 horas Prácticas

(1º Cuatrimestre)

Francisco de Borja Rodríguez Ortiz (teoría y prácticas)

Luis Fernando Lago Fernández (prácticas)

Escuela Politécnica Superior

Universidad Autónoma de Madrid

Datos generales de la asignatura

- ♦ Profesor del grupo 146 – Francisco de Borja Rodríguez Ortiz
 - Despacho B-328
 - Tutorías: por cita a petición del estudiante
- ♦ Profesor de la asignatura
 - Teoría: Francisco de Borja Rodríguez Ortiz (coordinador)
 - Prácticas: Francisco de Borja Rodríguez Ortiz y Luis Fernando Lago Fernández.
- ♦ Horario Teoría (Grupo 146)
 - Miércoles 16h a 18h
- ♦ Horario Prácticas (comienzan la semana del 25 de septiembre).
 - Grupo 1462: martes 18h a 20h (Luis Fernando Lago Fernández).
 - Grupo 1461: jueves 18h a 20h (Francisco de Borja Rodríguez Ortiz).
- ♦ Prueba intermedia (tentativa)
 - 08 noviembre, horario de clase
- ♦ Prueba final
 - Martes 16 de enero, 2023 mañana

Datos generales de la asignatura

- ♦ Leer la guía de la asignatura

[https://secretaria-virtual.uam.es/doa/consultaPublica/look\[conpub\]BuscarPubGuiaDocAs?entradaPublica=true&idiomaPais=es.ES&_anoAcademico=2023&_centro=350&_planEstudio=773](https://secretaria-virtual.uam.es/doa/consultaPublica/look[conpub]BuscarPubGuiaDocAs?entradaPublica=true&idiomaPais=es.ES&_anoAcademico=2023&_centro=350&_planEstudio=773)

¿POR QUÉ CRIPTOGRAFÍA Y SEGURIDAD?

- ◆ Hoy en día se quiere formar a profesionales que puedan evaluar en un Departamento de Sistemas de Información la seguridad y protección de datos del mismo.
- ◆ Por lo tanto, las empresas actuales demandan más perfiles profesionales de informáticos con conocimiento y fundamentos en seguridad de la información.
- ◆ La herramienta fundamental para llevar a buen término ese objetivo es la criptografía y el criptoanálisis.
- ◆ En este curso se pretenden transmitir los fundamentos básicos de la criptografía y seguridad de la información.
- ◆ Se pretende dar al alumno una base profunda de la fortaleza y la debilidad de los diversos métodos de cifrado que existen.

¿POR QUÉ CRIPTOGRAFÍA Y SEGURIDAD?

- ♦ Los alumnos necesitarán discernir con certeza aquellos conceptos que subyacen a los algoritmos de cifrado que les permitan valorar el grado de fiabilidad y eficiencia para una aplicación cualquiera.
- ♦ El objetivo final del curso no consiste en que se hayan memorizado los métodos más punteros de cifrado y de *hashing*, sino que cuando se les ponga en sus manos un algoritmo de cifrado cualquiera sepan determinar con la ayuda de los conceptos aprendidos:
 - cómo es de seguro,
 - cuál es su eficiencia
 - en qué circunstancias puede ser utilizado
 - e incluso modificarlo para adaptarlo a un problema concreto

¿POR QUÉ CRIPTOGRAFÍA Y SEGURIDAD?

- ♦ El curso contiene los temas fundamentales siguientes
 - Introducción
 - Métodos clásicos de cifrado
 - Cifrado perfecto y distancia de unicidad
 - Cifrado simétricos por bloques: DES y AES
 - Criptografía de clave pública: RSA
 - MAC y Hash
- ♦ + 3 prácticas (estás son aplicación directa de la teoría).
 - Para mas detalle se puede consultar:

[https://secretaria-virtual.uam.es/doa/consultaPublica/look\[conpub\]BuscarPubGuiaDocAs?entradaPublica=true&idiomaPais=es.ES&_anoAcademico=2023&_centro=350&_planEstudio=773](https://secretaria-virtual.uam.es/doa/consultaPublica/look[conpub]BuscarPubGuiaDocAs?entradaPublica=true&idiomaPais=es.ES&_anoAcademico=2023&_centro=350&_planEstudio=773)

Bibliografía

1. D. R. Stinson, "Cryptography: Theory and Practice" (Básica).
2. W. Stallings, "Cryptography and Network Security: Principles and Practice" (Básica).
3. A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, "Handbook of Applied Cryptography" (Complementaria).
4. B. Schneier, "Applied Cryptography" (Complementaria).
5. J. Van der Lubbe, "Basic Methods of Cryptography" (Complementaria).
6. Pieprzyk, J., Hardjono, T., Seberry, J., "Fundamentals of Computer Security". (Complementaria)
7. N. Koblitz, "A Course in Number Theory and Cryptography" (Complementaria específica de Teoría de Números).

Bibliografía

8. Ramanujachary Kumanduri, Cristina Romero, "Number Theory with Computer Applications". (Complementaria específica de Teoría de Números)
9. "Introducción a la Criptografía". Caballero, Pino. Ra-Ma, Textos Universitarios (Complementaria).
10. Simon Singh, "Los códigos secretos". (Complementaria, divulgación).
11. Simon Singh, "The Code Book. " (Complementaria, divulgación).
12. Joan Daemen, Vicent Rijmen, "The design of Rijndael AES-The Advanced Encryption Standard". (Complementaria AES).

Grupos de prácticas

- ◆ Grupos de prácticas
 - Apuntarse en la hoja de clase por parejas
 - Dos grupos
 - Antes del miércoles 20 sep

Evaluación

Sólo si sube la nota

10%

60% Teoría ≥ 5 para hacer media

90%

Prueba intermedia (08 nov, tentativa)
Liberatorio con ≥ 6

Examen final (16
enero)

Ejer-
cicios y
Tareas

40% Prácticas ≥ 5 (cada práctica ≥ 3) para hacer media

- ♦ Prueba intermedia liberatoria (≥ 6)
 - La nota del parcial liberado se traslada a la nota del examen final, escalada a la puntuación de la parte correspondiente
 - La prueba intermedia cubrirá un 45% aproximadamente de la materia
- ♦ Ejercicios
 - Entrega de al menos ~20 ejercicios de las hojas de problemas (5 de cada hoja).
 - Se fijarán dos entregas antes de la primera prueba y prueba final.
 - Entrega en pdf vía Moodle
- ♦ Tareas de evaluación continua
 - Entrega libre a lo largo del curso, según se vayan poniendo, pdf via Moodle.
- ♦ Convalidación de prácticas: me tenéis que escribir (≥ 7 , ≥ 3 teoría)