Guía docente de la asignatura

CRIPTOGRAFÍA

2021--2022

Titulación:	Grado en Matemáticas.
Plan:	394.
Código:	40035
Periodo:	primer cuatrimestre.
Carácter:	Optativa.
Nivel:	Grado.
Curso:	Cuarto.
Créditos ECTS:	6.
Lengua en que se imparte:	Castellano.
Profesor responsable:	José Enrique Marcos.
Datos de contacto:	Despacho A308.
	Teléfono: 983-185002, extensión 5002.
	E-mail: `marcosje@agt.uva.es`
Departamento:	Álgebra, Análisis Matemático, Geometría y Topología.

Situación y sentido de la asignatura.

Prerrequisitos:

Es necesario tener aprobada la asignatura "**estructuras algebraicas**" y haber cursado "**ecuaciones algebraicas**", y además tener un buen conocimiento de las estructuras de **grupo finito** y de **cuerpo finito**.

Relación con otras materias:

Es una aplicación del álgebra y teoría de números a las comunicaciones, informática, privacidad, autentificación, etc. Lo que poca gente sabe es que el verdadero fundamento de la criptografía son el **álgebra de estructuras finitas** y la teoría de números [y algo de estadística que no se impartirá]. No son meramente unos algoritmos programables en informática. Esto genera cierta frustración entre algunos alumnos de informática que desean aprender criptografía, pero no esperan ni desean ver su fundamentación matemática. Por ello, el fundamento teórico de la criptografía ha sido y será desarrollada, en buena parte, por matemáticos. Otra parte corresponde a los informáticos, que además tienen la honrosa y seria labor de implementarla adecuadamente.

Objetivos:

- Ser conscientes del fundamento matemático de la criptografía.
- Entrever una de las principales aplicaciones de las estructura algebraicas en el mundo digital.
- Conocer un poquito de la teoría de números, mediante una de sus aplicaciones.
- Entender que, en el siglo XXI, resultados que hace décadas se consideraban de matemática pura, hoy son de aplicación inmediata.
- Ver algo de la relación entre matemáticas y "computación".

Contenidos:

Cierta introducción histórica sobre criptografía.

Criptografía de clave privada.

Cifrado en flujo, sucesiones pseudoaleatorias de números.

Cifrado por bloques. Advanced Encryption Standard AES.

Criptografía de clave pública. Criptosistema RSA.

Números primos grandes. Su gran importancia en criptografía. Algoritmos de primalidad. Cómo se determinan números primos mayores que 2^{1024}. Ejemplo:

$$2^{1279} - 1 \qquad \text{es primo.}$$

Pseudoprimos.

Los grupos finitos en criptografía. Criptosistema de ElGamal. Protocolos de acuerdo para clave común.

Firma digital.

Funciones Hash criptográficas.

Introducción a la criptografía de curvas elípticas modulares.

Sistema y criterios de evaluación:

La calificación de la **primera** convocatoria:

El 65 % de la calificación corresponde a un examen final escrito.

El 16 % de la calificación es la nota un miniexamen realizado en una hora habitual de clase.

El 19 % restante corresponde a **prácticas**, sobre programación en criptografía. Esta parte no está sujeta a convocatoria extraordinaria.

Segunda convocatoria:

El 81 % de la calificación corresponde a un examen final escrito.

El 19 % es la calificación que ya se obtuvo por realizar las correspondientes prácticas de programación [sin posibilidad de segundas entregas].

Bibliografía:

- Johannes A. Buchmann, Introduction to cryptography (second edition), Editorial Springer (2004). Se puede descargar gratuitamente desde `http://almena.uva.es/`
- Raúl Durán Díaz, Luis Hernández Encinas, Jaime Muñoz Masqué, El Criptosistema RSA, Editorial RA-MA (2005). ISBN 978-84-7897-651-5
  [18.90 euros, se puede adquirir en `http://www.ra-ma.es/`

`https://en.wikipedia.org/wiki/Outline_of_cryptography`

`http://www.criptored.upm.es/paginas/docencia.htm`

`http://csrc.nist.gov/`

`https://csrc.nist.gov/publications/fips`

Se recomienda que prosigan aprendiendo **inglés** [y otros idiomas].