UNIVERSIDAD AUTÓNOMA DE MADRID

# 32934 - CRIPTOGRAFÍA

## Información de la asignatura

**Código - Nombre:** 32934 - CRIPTOGRAFÍA

**Titulación:** 688 - Máster en Matemáticas y Aplicaciones (2016)

**Centro:** 104 - Facultad de Ciencias

**Curso Académico:** 2024/25

## 1. Detalles de la asignatura

### 1.1. Materia

Criptografía.

### 1.2. Carácter

Optativa

### 1.3. Nivel

Máster (MECES 3)

### 1.4. Curso

1

### 1.5. Semestre

Segundo semestre

### 1.6. Número de créditos ECTS

6.0

### 1.7. Idioma

Español e inglés. El curso se impartirá en inglés siempre y cuando, al menos, un alumno internacional matriculado en la asignatura lo solicite.

### 1.8. Requisitos previos

No hay.

### 1.9. Recomendaciones

Ninguna especial.

### 1.10. Requisitos mínimos de asistencia

75%

### 1.11. Coordinador/a de la asignatura

Fernando Chamizo Lorente

https://autoservicio.uam.es/paginas-blancas/

### 1.12. Competencias y resultados del aprendizaje

#### 1.12.1. Competencias / Resultados del proceso de formación y aprendizaje

***Básicas y Generales***

- Aplicar tanto los conocimientos como la capacidad de análisis y de abstracción adquiridos en la definición y planteamiento de nuevos problemas y en la búsqueda de sus soluciones tanto en contextos académicos como profesionales. Aplicar los conocimientos adquiridos y la capacidad de resolución de problemas en entornos nuevos o poco conocidos, dentro de contextos más amplios e interdisciplinares, relacionados con las matemáticas o sus aplicaciones.
- Integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información posiblemente incompleta. Estos juicios incluirán, en su caso, reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos.
- Comunicar las conclusiones matemáticas (y los conocimientos y razones últimas que las sustentan) a públicos especializados y no especializados de un modo claro y sin ambigüedades.
- Poseer las habilidades de aprendizaje que les permitan continuar estudiando de un modo autónomo, en particular, para acceder al periodo de investigación del doctorado.
- Recabar e interpretar datos, información o resultados relevantes en problemas matemáticos, científicos, tecnológicos o de otros ámbitos que requieran el uso de herramientas matemáticas, así como obtener conclusiones y exponerlas razonadamente.
- 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.
- Aplicar los conocimientos adquiridos y la capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.
- Integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.
- Comunicar las conclusiones –y los conocimientos y razones últimas que las sustentan– a públicos especializados y no especializados de un modo claro y sin ambigüedades.
- Poseer las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

***Transversales***

- Trabajo en equipo.

***Específicas***

- Conocimiento de teorías y conceptos clave y práctica en su aplicación a la resolución de problemas.
- Discriminación, tras un análisis preliminar, de las dificultades y puntos delicados en la resolución de un problema.
- Capacidad para formular simbólica y rigurosamente un problema a partir de una descripción verbal, posiblemente incompleta, de forma que se facilite su análisis y resolución.
- Capacidad para definir nuevos objetos matemáticos en términos de otros ya conocidos para utilizarlos en diferentes contextos.
- Capacidad para elegir y aplicar el procedimiento adecuado a la resolución de un problema.
- Capacidad para abstraer las propiedades estructurales (de objetos matemáticos, de la realidad observada, de otros ámbitos) distinguiéndolas de aquellas puramente ocasionales y poder comprobarlas con demostraciones o refutarlas con contraejemplos que requieran un alto nivel matemático.
- Capacidad para proponer, analizar, validar e interpretar modelos de situaciones reales complejas, utilizando las herramientas matemáticas más adecuadas a los fines que se persigan.
- Uso de medios tecnológicos y audiovisuales para la comunicación eficaz de resultados matemáticos.

- Utilización y desarrollo de aplicaciones informáticas de programación.

### 1.12.2. Resultados de aprendizaje

-

### 1.12.3. Objetivos de la asignatura

Este es un primer curso centrado en la teoría clásica de formas modulares. Aunque es un curso orientado al álgebra, es importante enfatizar la naturaleza multidisciplinar del tema, como se refleja en los contenidos. Así, por ejemplo, algunos temas de análisis complejo y teoría de números aparecerán de forma natural.

### 1.13. Contenidos del programa

1. Álgebra y geometría del grupo modular
    a. El grupo modular y el grupo theta.
    b. Dominios fundamentales y cúspides.
    c. Grupos fuchsianos, superficies de Riemann y curvas elípticas.
    d. Grupos de matrices y cifrados de Hill.
    e. Criptografía de curvas elípticas.
2. Formas modulares
    a. Definición de formas y funciones modulares.
    b. Fórmulas para la dimensión.
    c. Series de Eisenstein y sus expansiones.
    d. Más ejemplos de formas y funciones modulares.
    e. Códigos algebraico-geométricos.
3. Funciones theta
    a. La función theta de Jacobi.
    b. Sumas de cuadrados.
    c. Representación por formas cuadráticas.
    d. Observaciones sobre el empaquetamiento de esferas según Viazovska.
    e. Criptosistemas y retículos.
4. Operadores de Hecke
    a. Definición y propiedades básicas.
    b. El álgebra de Hecke.
    c. Resumen de la teoría de Atkin-Lehner.
5. Introducción a la teoría de Eichler-Shimura
    a. Funciones *L* y ecuaciones funcionales.
    b. Teoremas inversos de Hecke y Weil.
    c. Consideraciones sobre la cohomología de Eichler.

### 1.14. Referencias de consulta


[CS17] H. Cohen and F. Strömberg. *Modular forms*, volume 179 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2017. A classical approach.

[DS05] F. Diamond and J. Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[Hel02] Y. Hellegouarch. *Invitation to the mathematics of Fermat-Wiles*. Academic Press, Inc., San Diego, CA, 2002. Translated from the second (2001) French edition by L. Schneps.

[Kna92] A. W. Knapp. *Elliptic curves*, volume 40 of *Mathematical Notes*. Princeton University Press, Princeton, NJ, 1992.

[Shi94] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1.

[Zag08] D. Zagier. Elliptic modular forms and their applications. In *The 1-2-3 of modular forms*, Universitext, pages 1–103. Springer, Berlin, 2008.


## 2. Metodologías docentes y tiempo de trabajo del estudiante

### 2.1. Presencialidad

| | #horas |
|---|---|
| Porcentaje de actividades presenciales (mínimo 33% del total) | 51 |
| Porcentaje de actividades no presenciales | 99 |

### 2.2. Relación de actividades formativas

| Actividades presenciales | Nº horas |
|---|---|
| Clases teóricas en aula | 42 |
| Seminarios | |
| Clases prácticas en aula | |
| Prácticas clínicas | |
| Prácticas con medios informáticos | |
| Prácticas de campo | |
| Prácticas de laboratorio | |
| Prácticas externas y/o practicum | |
| Trabajos académicamente dirigidos | |
| Tutorías | 6 |
| Actividades de evaluación | 3 |
| Otras | |

Las clases combinarán contenido teórico y práctico. Intentaremos usar el ordenador. Sin embargo, dado que se trata de un curso orientado a los aspectos matemáticos de la criptografía, el propósito de los ejercicios de programación será entender los fundamentos teóricos más que intentar diseñar implementaciones eficientes.

## 3. Sistemas de evaluación y porcentaje en la calificación final

### 3.1. Convocatoria ordinaria

Entregas de ejercicios (50%). Examen final (50%).

#### 3.1.1. Relación actividades de evaluación

| Actividad de evaluación | % |
|---|---|
| Examen final (máximo 70% de la calificación final o el porcentaje que figure en la memoria) | 50 |
| Evaluación continua | 50 |

### 3.2. Convocatoria extraordinaria

Como en la convocatoria ordinaria.

#### 3.2.1. Relación actividades de evaluación

| Actividad de evaluación | % |
|---|---|
| Examen final (máximo 70% de la calificación final o el porcentaje que figure en la memoria) | 50 |
| Evaluación continua | 50 |

## 4. Cronograma orientativo

| Semana | Contenido | Horas presenciales | Horas no presenciales |
|---|---|---|---|
| 1-4 | Tema 1 | 10 | 18 |
| 5-7 | Tema 2 | 10 | 24 |
| 8-10 | Tema 3 | 10 | 24 |
| 11-12 | Tema 4 | 6 | 18 |
| 13-14 | Tema 5 | 6 | 18 |