# PROGRAMA DE LA ASIGNATURA
# "Criptografía"

INGENIERO EN INFORMÁTICA ( Plan 97 )

Departamento de Matemática Aplicada I

E.T.S. Ingeniería Informática

## DATOS BÁSICOS DE LA ASIGNATURA

| | |
|---|---|
| **Titulación:** | INGENIERO EN INFORMÁTICA ( Plan 97 ) |
| **Año del plan de estudio:** | 1997 |
| **Centro:** | E.T.S. Ingeniería Informática |
| **Asignatura:** | Criptografía |
| **Código:** | 260123 |
| **Tipo:** | Optativa |
| **Curso:** | Sin curso específico |
| **Período de impartición:** | Cuatrimestral |
| **Ciclo:** | 0 |
| **Área:** | Matemática Aplicada (Area responsable) |
| **Horas :** | 60 |
| **Créditos totales :** | 6.0 |
| **Departamento:** | Matemática Aplicada I (Departamento responsable) |
| **Dirección física:** | AVDA. REINA MERCEDES, S/N, 41012, SEVILLA |
| **Dirección electrónica:** | http://www.ma1.us.es/ |

## OBJETIVOS Y COMPETENCIAS

### Objetivos docentes específicos

Introducir al alumno en la criptografía, el criptoanálisis y en sus aplicaciones.

### Competencias:

**Competencias transversales/genéricas**

Capacidad de organizar y planificar

Resolución de problemas

Trabajo en equipo

**Competencias específicas**

Cognitivas(Saber)

El alumno debe conocer los fundamentos de la criptografía, tener nociones sobre los principales criptosistemas y saber evaluar su seguridad, así como saber cuáles son las principales aplicaciones de los temas estudiados en la práctica de la Informática.

Procedimentales/Instrumentales(Saber hacer)

Analizar la seguridad de un criptosistema. Implementar criptosistemas de manera segura. Evaluar la seguridad de un sistema.

Actitudinales(Ser)

Proveer al alumno de unas mínimas capacidades de abstracción, concreción, concisión, imaginación, intuición, razonamiento, crítica, objetividad, síntesis y precisión, a utilizar en cualquier momento de su vida académica o laboral, para poder afrontar con garantías de éxito los problemas que se le presenten.

## CONTENIDOS DE LA ASIGNATURA

Introducción
Necesidad de la seguridad. No sólo secreto. Ataques y defensas. Ataques pasivos. Ataques activos. Servicios de seguridad. ¿Qué es la Criptografía?. Cifrar y descifrar. Criptoanálisis. Seguridad computacional. Atacantes y sus recursos.

Fundamentos
Un poco de historia. Desplazamiento. Cifrado afín. Cifrado por sustitución. Cifrado por transposición. Cifrado de Vigenère. Cifrado XOR. Máquinas de rotores. Teoría de la información. Cifrado de Vernam. Cifrados en flujo.

Criptografía simétrica
Criptosistemas simétricos. Ventajas e inconvenientes. Cifrado por bloques. Cifrado producto. Cifrados por bloques. DES. AES. IDEA. Otros cifrados simétricos.

Criptografía de clave pública
Criptografía de clave pública. El criptosistema de mochila de Merkle-Hellman. El criptosistema RSA. El criptosistema Elgamal. Criptografía de curvas elípticas.

Aplicaciones
Sobre digital. Intercambio de claves de Diffie y Hellman. Autenticación e integridad. Funciones resumen. Firmas digitales. Firma digital RSA. Firma digital Elgamal. Certificados digitales. Algunos problemas resueltos.

## ACTIVIDADES FORMATIVAS

### Relación de actividades formativas del cuatrimestre

***Clases teóricas***

**Horas presenciales:** 24.0

**Horas no presenciales:** 26.0

**Metodología de enseñanza-aprendizaje:**

Durante 8 semanas, totalizando 24 horas presenciales organizadas según se adjunta en la temporización previa, se procederá a comentar el contenido teórico de la asignatura, con la ayuda del ordenador, ilustrando la exposición con ejemplos clarificadores. Los alumnos dispondrán de una copia de las presentaciones en ordenador a utilizar en clase, la cual estará accesible tanto en papel (en la copistería del centro), como por conexión de internet (en la página web de la asignatura en el servidor del departamento).

**Competencias que desarrolla:**

Capacidad de organizar y planificar
Resolución de problemas
Trabajo en equipo

***Prácticas de Laboratorio***

**Horas presenciales:** 22.0

**Horas no presenciales:** 25.0

**Metodología de enseñanza-aprendizaje:**

Los alumnos tendrán a su disposición en la web de la asignatura un boletín de problemas, algunos de ellos completamente resueltos, e incluyendo exámenes de convocatorias precedentes.

Durante 12 semanas, totalizando 22 horas presenciales organizadas según se adjunta en la temporización anterior, en las primeras 9 semanas se procederá a la resolución por parte del profesor, y eventualmente del alumnado, de problemas. En las últimas 3 semanas los alumnos expondrán y defenderán sus trabajos de carácter práctico en el aula.

**Competencias que desarrolla:**

Capacidad de organizar y planificar
Resolución de problemas
Trabajo en equipo

***Prácticas informáticas***

**Horas presenciales:** 8.0

**Horas no presenciales:** 4.0

**Metodología de enseñanza-aprendizaje:**

Las clases de laboratorio comenzarán a partir de la novena semana hasta la semana décima, totalizando 8 horas presenciales. En estas clases, el profesor se dedicará fundamentalmente a resolver dudas técnicas y científicas, asesorar, y a ayudar a diseñar las diferentes aplicaciones informáticas correspondientes a los trabajos prácticos dirigidos asignados.

**Competencias que desarrolla:**

Capacidad de organizar y planificar
Resolución de problemas
Trabajo en equipo

***AAD sin presencia del profesor***

**Horas presenciales:** 0.0

**Horas no presenciales:** 21.0

**Metodología de enseñanza-aprendizaje:**

Los alumnos se organizaran en  grupos. A cada grupo se le asignará un trabajo de un listado difundido en la web durante las primeras semanas del curso. Este trabajo se desarrollará a partir de un artículo internacional o algún tema de fácil documentación y actualidad en el área de la Criptografía. Este trabajo consistirá en la asimilación de estos documentos y elaboración de una memoria; si fuera posible el desarrollo de un programa informático. Las últimas semanas de clase se dedicarán a la exposición y defensa de estos trabajos por parte de todos los grupos (deberán exponer todos los integrantes del grupo). El profesor dedicará unos 60 minutos a supervisar el trabajo realizado por los grupos, previamente a la exposición.

**Competencias que desarrolla:**

Capacidad de organizar y planificar
Resolución de problemas
Trabajo en equipo

***Exámenes***

**Horas presenciales:** 6.0

**Horas no presenciales:** 0.0

**Tipo de examen:** Evaluacion alternativa

***Horas estudio del alumno (*)***

**Horas presenciales:**

**Horas no presenciales:** 14.0

## SISTEMAS Y CRITERIOS DE EVALUACIÓN Y CALIFICACIÓN

***Evaluación contínua***

El sistema de evaluación por curso comprende tres apartados distintos: exposición de un trabajo en grupo (sobre 4.5 puntos), seguimiento de las exposiciones de los trabajos (sobre 1 punto) y examen teórico-práctico (sobre 4.5 puntos).

La calificación final resulta de la suma de las tres calificaciones parciales anteriores. Se considera que un alumno supera la asignatura cuando su calificación final es 5 o superior, siempre y cuando haya obtenido un mínimo de un punto en el examen teórico-práctico, así como un punto en la exposición del trabajo en grupo.

***Examen final***

Aquellos alumnos que no hayan superado la asignatura por el sistema de evaluación por curso, o que por decisión personal renuncien a la nota de evaluación por curso, tienen la opción de superar la asignatura por medio de un examen teórico-práctico final (evaluado sobre 10 puntos), a celebrar en cada una de las convocatorias oficiales de la asignatura. Se considera que un alumno supera la asignatura cuando su calificación final es 5 o superior.