Universidad Zaragoza

Curso Académico: 2023/24

29515 - Criptografía y seguridad

Información del Plan Docente

Año académico: 2023/24
Asignatura: 29515 - Criptografía y seguridad
Centro académico: 175 - Escuela Universitaria Politécnica de La Almunia
Titulación: 625 - Graduado en Ingeniería de Datos en Procesos Industriales
Créditos: 6.0
Curso: 3
Periodo de impartición: Primer semestre
Clase de asignatura: Obligatoria
Materia:

1. Información básica de la asignatura

En esta asignatura presentamos los fundamentos y las aplicaciones principales de la criptografía. Esta ciencia, conocida antiguamente como el arte de la escritura secreta, se ha convertido hoy día un compañero imprescindible del desarrollo de la sociedad de la información. Los objetivos primordiales a los cuales sirve la criptografía son la confidencialidad, la integridad y la autenticidad en el tratamiento de la información en formato electrónico.

La segunda parte versa sobre la seguridad en los sistemas informáticos y los mecanismos para alcanzarla.

Alineación con los ODS:

- Objetivo 9 Construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación

y, en concreto con las metas:

- Meta 9.c Aumentar significativamente el acceso a la tecnología de la información y las comunicaciones y esforzarse por proporcionar acceso universal y asequible a Internet en los países menos adelantados de aquí a 2030

2. Resultados de aprendizaje

El estudiante, para superar esta asignatura, deberá demostrar los siguientes resultados:

- Conocer los fundamentos de los sistemas criptográficos.
- Saber aplicar los algoritmos criptográficos tradicionales
- Identificar la seguridad y vulnerabilidad del dato.

3. Programa de la asignatura

1. Introducción a la criptografía
2. Fundamentos de criptografía
3. Criptosistemas de clave compartida: cifrado en flujo
4. Criptosistemas de clave compartida: cifrado en bloque
5. Criptosistemas de clave pública
6. Firmas digitales
7. Infraestructura de clave pública
8. Aplicaciones de la criptografía
9. Ataques contra las redes TCP/IP
10. Mecanismos de prevención
11. Mecanismos de protección

4. Actividades académicas

Actividades presenciales:

- Clases teóricas: Se explican los conceptos teóricos de la asignatura y ejemplos prácticos ilustrativos como apoyo a la teoría.
- Clases prácticas: Se realizarán problemas y casos prácticos como complemento a los conceptos teóricos estudiados.

Actividades no presenciales:

- Estudio y asimilación de la teoría expuesta en las clases magistrales.
- Comprensión y asimilación de problemas y casos prácticos resueltos en clase.
- Resolución de problemas propuestos.

- Realización de las prácticas en grupo y elaboración de informes.
- Preparación de las pruebas escritas de evaluación continua y exámenes finales.

La asignatura consta de 6 créditos ECTS, lo cual representa 150 horas de trabajo del alumno/a en la asignatura.

5. Sistema de evaluación

El estudiante deberá demostrar que ha alcanzado los resultados de aprendizaje previstos mediante las siguientes actividades de evaluación

- Trabajos prácticos (30%). Estos trabajos incluyen 2 prácticas de laboratorio y un ejercicio de diseño complejo. De cada una de las prácticas se solicitará al alumno una memoria que servirá como base para su evaluación. Para superar la asignatura el alumnado deberá obtener una nota final de prácticas de laboratorio igual o superior a 5.
- Pruebas escritas teórico-prácticas (70%) en las que se plantearán cuestiones y/o problemas del ámbito de la ingeniería de complejidad similar a la utilizada durante el curso. Se valorará la calidad y claridad de la estrategia de resolución, los conceptos usados para resolver los problemas, ausencia de errores en el desarrollo y en las soluciones, y el uso correcto de la terminología y notación. En cada una de las pruebas escritas teórico-prácticas que se realicen, el alumnado deberá obtener una nota igual o superior a 5 para superar la asignatura.

El estudiante podrá escoger entre una evaluación dividida, realizada en forma de dos pruebas escritas y la entrega de los guiones de prácticas a lo largo del cuatrimestre, o una prueba global realizada al finalizar el cuatrimestre, (que constará de un examen por parcial) y la entrega de los guiones de prácticas.