

Criptografía

Presentación de la asignatura

Somos las profesoras Itziar Baragaña, del Departamento de Ciencia de la Computación e Inteligencia Artificial de la Universidad del País Vasco/Euskal Herriko Unibertsitatea, y Alicia Roca, del Departamento de Matemática Aplicada de la Universidad Politécnica de Valencia.

Las dos formamos parte del Grupo de Análisis Matricial y Aplicaciones “GAMA” de la UPV/EHU (<http://www.ehu.eus/es/web/gama>)

Hemos impartido la asignatura de Criptografía durante varios cursos en nuestras respectivas Universidades. Esperamos que la materia os resulte interesante, y que nuestra experiencia os pueda servir de ayuda.

Resumen del programa

Introducción a la Criptografía
Cifrado en flujo
Cifrado simétrico en bloque
Criptografía de clave pública
Protocolos de autenticación

Plan de trabajo

El curso está organizado en 6 semanas.

La materia a estudiar se presenta en vídeos y en las correspondientes transparencias. Cada vídeo tiene asignados unos ejercicios de autoevaluación. Es muy importante realizarlos y comprobar las soluciones para el adecuado progreso en el curso. Recomendamos realizar cada parte tras el vídeo con el que esté relacionada.

Cada semana habrá que realizar una o dos prácticas. La primera práctica (Práctica 0) contiene indicaciones precisas sobre la realización de todas ellas. Se pide leerla con atención.

La tarea concreta a realizar cada semana está indicada en la “Guía de la semana” correspondiente.

Evaluación

Cada semana habrá que contestar un test de evaluación y entregar la tarea encomendada en cada práctica. El plazo de presentación terminará al finalizar la semana.