

Propuesta Módulo de Taller

Taller de Criptografía Moderna

Proponente: Instituto de Computación.

Responsable: Alfredo Viola

Objetivo:

En este seminario está orientado a estudiantes de grado y posgrado en Computación e Ingeniería Matemática. El objetivo es presentar conceptos fundamentales de la criptografía moderna, en un formato tipo seminario, con material a ser recomendado en el curso. Se espera que este seminario permita al estudiante poder cursar posteriormente cursos mas avanzados de criptografía.

Aporte a/ tareas concretas del estudiante:

Se espera que el estudiante adquiera conceptos fundamentales de criptografía moderna ya sea en cifrado en bloques como de cifrado en flujo. Estos conceptos incluyen temas tales como cifrados de clave simétrica y clave pública, autenticación de mensajes, firmas digitales y distribución de claves.

La metodología consiste en la presentación de diversos temas por parte de los estudiantes y la discusión en clase de dichas presentaciones. Se evaluará la participación en clase, la presentación de los temas y un trabajo final.

Carga horaria total y créditos: 120 horas (60 horas de clase + 60 horas de trabajo personal), generando un total de 8 créditos.

Carga horaria semanal: 4 horas de clases (dos veces por semana por 2 horas) + trabajo personal en casa de preparación y lectura de las clases.

Fecha de inicio: Miércoles 8 de setiembre. Se agradece enviar mail a viola@fing.edu.uy, para confirmar interes en participar del taller.

Fecha de finalización: 17 de diciembre

Conocimientos requeridos:

Cupos de estudiantes: 20 estudiantes

Forma de selección: Por sorteo

Horario: Lunes y Miércoles de 8:00 a 10:00 hs. (Salón GRIS, Instituto de Mecánica de los Fluídos e Ingeniería Ambiental - IMFIA).