

Formulario de Aprobación Curso de Actualización 2011

Asignatura: Fundamentos de Criptografía

Profesor de la asignatura ¹: Dr. Alfredo Viola
Gr. 5, 40 hs. DT
Instituto de Computación

Otros docentes de la Facultad: (A CONFIRMAR)

Docentes fuera de Facultad:
(título, nombre, cargo, Institución, país)

Instituto ó Unidad: COMPUTACIÓN
Departamento ó Area: PROGRAMACIÓN

Fecha de inicio y finalización: (A CONFIRMAR)
Horario y Salón: (A CONFIRMAR)

Horas Presenciales: 30 hs.

Arancel: \$ 7.000

Público objetivo y Cupos:

Orientado a profesionales interesados en temas relacionados con la Seguridad Informática.

Objetivos: Presentar al estudiante los principios fundamentales de la criptografía, en donde se integren aspectos teóricos con laboratorios experimentales.

Conocimientos previos recomendados: Algún fundamento en álgebra, y experiencia mínima en seguridad informática. Conocimientos básicos de probabilidad.

Metodología de enseñanza:

20 hs. de clases teórico-prácticas.
10 hs. de laboratorio.

Forma de evaluación: Resolución de trabajos de laboratorio, y una entrega obligatoria con ejercicios resueltos.

Temario:

1. Algunos requerimientos de seguridad. Aproximación criptográfica en la propuesta de soluciones.
2. Criptografía de clave privada.
3. Criptografía de clave pública.
4. Promitivas criptográficas.
5. Infraestructura de Clave Pública (PKI).

Bibliografía: Menezes, van Oorschot, Vanstone: Handbook of Cryptography
<http://www.cacr.math.uwaterloo.ca/hac/>