Formulario de Aprobación Curso de Actualización 2017

Asignatura: Fundamentos de Criptografía

(Si el nombre contiene siglas deberán ser aclaradas)

Profesor de la asignatura [1] **:**Dr. Alfredo Viola, Profesor Titular, Instituto de Computación
(título, nombre, grado o cargo, Instituto o Institución)

Profesor Responsable Local
(título, nombre, grado, Instituto)

Otros docentes de la Facultad: Sebastián Fonseca, Ayudante, Instituto de Computación.

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

Instituto ó Unidad: Instituto de Computación
Departamento ó Area: Seguridad Informártica

[1] Agregar CV si el curso se dicta por primera vez.
(Si el profesor de la asignatura no es docente de la Facultad se deberá designar un responsable local)

Horas Presenciales: 40
(se deberán discriminar las mismas en el ítem Metodología de enseñanza)

Público objetivo y Cupos: Profesionales y estudiantes interesados en Seguridad Informática. Estudiantes del Diploma en Seguridad Informática.
No tiene cupo

Objetivos: El objetivo de este curso es que los estudiantes conozcan los fundamentos matemáticos de la criptografía, las principales primitivas criptográficas, así como algunas prácticas de uso que las hacen vulnerables.

Conocimientos previos exigidos: Ninguno

Conocimientos previos recomendados: Álgebra Lineal, Probabilidad

Metodología de enseñanza:
(comprende una descripción de la metodología de enseñanza y de las horas dedicadas por el estudiante a la asignatura, distribuidas en horas presenciales -de clase práctica, teórico, laboratorio, consulta, etc.- y no presenciales de trabajo personal del estudiante)

- Horas clase (teórico): 10
- Horas clase (práctico): 10
- Horas clase (laboratorio):10
- Horas consulta:10
- Horas evaluación:

- Subtotal horas presenciales: 40

- Horas estudio: 25
- Horas resolución ejercicios/prácticos: 10
- Horas proyecto final/monografía:
  - Total de horas de dedicación del estudiante: 75

Forma de evaluación: El curso se evaluará a partir de:

- Entregas de trabajo de Laboratorio individuales

Temario:

1. Primitivas de seguridad
2. Criptografía de clave privada
3. Criptografía de clave pública
4. Primitivas criptográficas
5. Infraestructura de clave pública

Bibliografía:

Menezes, P. van Oorschot, S. Vanstone, Handbook of Applied Cryptography. CRC Press. 1997.
http://www.cacr.math.uwaterloo.ca/hac/
(título del libro-nombre del autor-editorial-ISBN-fecha de edición)

Datos del curso

Fecha de inicio y finalización: 13 de marzo al 7 de abril

Horario y Salón: Lunes, Miércoles y Viernes de 18 a 21 hs. Salón 701.

Arancel: $13.500