Formulario de Aprobación Curso de Posgrado

Asignatura: Criptografía

(Si el nombre contiene siglas deberán ser aclaradas)

Profesor de la asignatura [1]: Alfredo Viola, Prof. Titular Gr. 5
(título, nombre, grado o cargo, Instituto o Institución)

Profesor Responsable Local [1]:
(título, nombre, grado, Instituto)

Otros docentes de la Facultad:
(título, nombre, grado, Instituto)

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

Programa(s): Maestría en Informática PEDECIBA, Doctorado en Informática PEDECIBA

Instituto ó Unidad: Instituto de Computación.
Departamento ó Area: Programación

Horas Presenciales: 60

Nº de Créditos: 10

Público objetivo y Cupos: **Estudiantes de posgrado en informática. El curso no tiene cupos.**

Objetivos: Dar un curso de criptografía básico. En este sentido se espera balancear tanto aspectos teóricos como aspectos algorítimicos y aspectos orientados al uso de la criptografía en la práctica profesional. Se estudiarán también diversos aspectos relacionados con los estándares NIST. De haber tiempo, se espera completar con algunos datos de la historia de la criptografía que ayuden a ilustrar diversos conceptos.

Conocimientos previos exigidos: Matemáticas discretas.
Conocimientos previos recomendados: Fundamentos de estructuras de datos y algoritmos, probabilidad, álgebra.

Metodología de enseñanza:

- Horas clase (teórico-práctico): 50
- Horas clase (práctico): Incluídas arriba
- Horas clase (laboratorio): 5
- Horas consulta: 5
- Horas evaluación: 0
    - Subtotal horas presenciales: 60
- Horas estudio: 30
- Horas resolución ejercicios/prácticos: 60
- Horas proyecto final/monografía: 0
    - Total de horas de dedicación del estudiante: 150

Forma de evaluación:

La evaluación final se realizará mediante la resolución de ejercicios sacados del libro de texto consistiendo en 4 obligatorios (15 % cada uno), y 2 laboratorios con entrega de informe (20% cada uno).

Es importante aclarar que la participación en clase no es obligatoria, pero se recomienda su presencia debido a que la metodología usada ayuda mucho a la comprensión de los temas dictados en el curso.

Temario:

1. Introducción
2. Criptosistemas básicos de clave privada. AES.
3. RSA y el problema de factorización.
4. ElGamal y el problema del logaritmo discreto.
5. Funciones de Hash y aplicaciones.
6. Firmas Digitales.
7. Números pseudoaleatorios
8. Manejo de claves e infraestructura de clave pública.
9. Aplicaciones.

Bibliografía:

1. Joachim von zur Gathen (2015). CryptoSchool. Springer. ISBN-13: 978-3662484234.

Datos del curso

Fecha de inicio y finalización: **25 de febrero al 6 de julio de 2019**

Horario y Salón: Martes y jueves de 8:00 a 10:00 en salón 305