21 DOS

Facultad de Ingeniería
Comisión Académica de Posgrado

Formulario de aprobación de curso de posgrado/educación permanente

Asignatura:
Generación aleatoria en criptografía

Modalidad:

Posgrado	[X]
Educación permanente	[ ]

Profesor de la asignatura [1]:
Dr. Joachim von zur Gathen, Universidad de Bonn, Alemania.

Profesor Responsable Local [1]:
Dr. Alfredo Viola, grado 5 DT, Instituto de Computación.

Otros docentes de la Facultad:

Docentes fuera de Facultad:
Dr. Joachim von zur Gathen, Universidad de Bonn, Alemania.

[Si es curso de posgrado]
Programa(s) de posgrado: Maestría/Doctorado en Informática, Maestría en Ingeniería Matemática.

Instituto o unidad: Computación

Departamento o área: Programación

Horas Presenciales:
12 hs.

Nº de Créditos:

4

Público objetivo:

Estudiantes de grado y de posgrado interesados en los fundamentos matemáticos de la criptografía.

Cupos:

No tiene

Objetivos: El curso es de gran importancia en relación al uso práctico de la criptografía pero además con fuertes componentes teóricos. La generación aleatoria uniforme de números es tema de fundamental importancia y fuente de graves problemas prácticos. Además de las implicancias prácticas, en el curso se van a ver profundos vínculos de este problema con otras áreas de la Ciencia de la Computación como el de Complejidad Computacional.

Conocimientos previos exigidos: criptografía , fundamentos de probabilidad.

Conocimientos previos recomendados: fundamentos de complejidad computacional.

Metodología de enseñanza:

Descripción de la metodología:

Son cuatro clases de tres horas cada una en una semana, en un régimen intensivo. Son clases teórico prácticas en donde se fomenta la participación estudiantil.

Detalle de horas:

- Horas de clase (teórico): 12
- Horas de clase (práctico):
- Horas de clase (laboratorio):
- Horas de consulta:
- Horas de evaluación:
    - Subtotal de horas presenciales:
- Horas de estudio: 12
- Horas de resolución de ejercicios/prácticos: 36
- Horas proyecto final/monografía:
    - Total de horas de dedicación del estudiante: 60

Forma de evaluación:

Resolución de ejercicios en un trabajo final evaluado en 36 horas totales.

Temario:

1. Generatorios aleatorios basados en experimentos físicos.
2. Generadores pseudoaleatorios.
3. Distinguidores y predictores.
4. Generadores aleatorios con buenas propiedades teóricas (Nisan-Wigderson y Blum-Blum-Schub).

Bibliografía:

Joachim von zur Gathen.
CryptoSchool.
Springer,
ISBN 978-3-662-48425-8
2015.

Notas del curso.

4| CUATRO.

Facultad de Ingeniería
Comisión Académica de Posgrado

Datos del curso

Fecha de inicio y finalización: 3 al 7 de febrero 2020

Horario y Salón: A confirmar

Arancel:

No corresponde.

Arancel para estudiantes inscriptos en la modalidad posgrado:
Arancel para estudiantes inscriptos en la modalidad educación permanente: