

Formulario de Aprobación Curso de Posgrado

Asignatura: Desarrollo de la criptografía, con enfoque en Latino America

Profesor de la asignatura ¹: Dr. Joachim von zur Gathen, profesor titular, Universidad de Bonn

Profesor Responsable Local ¹: Dr. Alfredo Viola, Instituto de Computación.

Otros docentes de la Facultad:

Docentes fuera de Facultad:

Instituto ó Unidad: Computación

Departamento ó Area: Programación

Horas Presenciales: 12

Nº de Créditos: 4

Público objetivo y Cupos:

Estudiantes de posgrado en Computación, matemáticas e ingeniería eléctrica

No tiene cupo.

Objetivos:

Presentar el uso de diversos algoritmos criptográficos a lo largo de la historia de la humanidad, con énfasis en la Historia de América Latina. En este sentido se espera que el estudiante tenga conocimientos básicos de diversos algoritmos criptográficos a los efectos de entender estos usos históricos. El curso está centrado en los algoritmos usados en diversos períodos históricos y en los criptoanálisis usados para quebrarlos.

Conocimientos previos exigidos: conocimientos básicos de algoritmos criptográficos

Conocimientos previos recomendados:

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): 12
- Horas clase (práctico):
- Horas clase (laboratorio):
- Horas consulta:
- Horas evaluación:
 - o Subtotal horas presenciales:
- Horas estudio: 12

- Horas resolución ejercicios/prácticos: 36
 - Se resolverán ejercicios que aparecen en los capítulos del libro que se usen en el curso. Estos ejercicios van a ser usados como la evaluación final del curso.
 - Horas proyecto final/monografía:
 - o Total de horas de dedicación del estudiante: 60
-

Forma de evaluación: Proyecto final

Temario:

1. Los ancianos: Egiptia, Grecia, Roma
 - Sustituciones simples
 - Análisis de frecuencia
 2. La media edad: reyes y monásticos
 - Libros de códigos, en los siglos XIV, XV, XVI y XVIII.
 3. Criptografía española
 - Criptografía usada por Hernán Cortés
 4. Criptografía latino-americana
 - Criptografía usada por líderes internacionales como José Martí.
Descripción del tipo de criptografía usado.
 5. Eventos criptográficos en Latino América
 - Descripción de algoritmos criptográficos usados en eventos importantes en Latino América.
-

Bibliografía:

CryptoSchool

Joachim von zur Gathen

Sprinter (2015) ISBN-13: 978-3662484234

Datos del curso

Fecha de inicio y finalización: 2 de mayo al 12 de mayo de 2017

Horario y Salón: A confirmar
