Formulario de aprobación de curso de posgrado/educación permanente

Asignatura: Fundamentos de Criptografía
(Si el nombre contiene siglas deberán ser aclaradas)

Modalidad: (posgrado, educación permanente o ambas)	**Posgrado**	X
	Educación permanente	X

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

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

Otros docentes de la Facultad: Ing. Bruno Scarone, Gr. 1, Instituto de Computación
(título, nombre, grado, instituto)

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

[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)

[Si es curso de posgrado]
Programa(s) de posgrado: Especialización en Seguridad Informática y Maestría en Seguridad Informática

Instituto o unidad: Instituto de Computación

Departamento o área: Seguridad Informática

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

Nº de Créditos: 5
[Exclusivamente para curso de posgrado]
(de acuerdo a la definición de la UdelaR, un crédito equivale a 15 horas de dedicación del estudiante según se detalla en el ítem Metodología de enseñanza)

Público objetivo: Profesionales y estudiantes interesados en Seguridad Informática. Estudiantes del Diploma en Seguridad Informática

Cupos: No tiene cupo
(si corresponde, se indicará el número de plazas, mínimo y máximo y los criterios de selección. Asimismo, se adjuntará en nota aparte los fundamentos de los cupos propuestos. Si no existe indicación particular para el cupo máximo, el criterio general será el orden de inscripción, hasta completar el cupo asignado)

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)

Descripción de la metodología:
[Obligatorio]

- 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 públ

Bibliografía:

D. Stinson, M. B. Paterson. Cryptography: Theory and Practice, FourthEdition (Discrete Mathematics and Its Applications) 4th Edition. CRC Press. 2018.

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
(título del libro-nombre del autor-editorial-ISBN-fecha de edición)

Datos del curso

Fecha de inicio y finalización: 8 de marzo al 9 de abril de 2021

Horario y Salón: Lunes, miércoles y viernes de 18 a 21 hs.

Arancel: $19.500
[Si la modalidad no corresponde indique “no corresponde”. Si el curso contempla otorgar becas, indíquelo]

Arancel para estudiantes inscriptos en la modalidad posgrado: $19.500
Arancel para estudiantes inscriptos en la modalidad educación permanente: $19.500