

## Formulario de Aprobación Curso de Actualización 2014

### Asignatura: Fundamentos de Criptografía

(Si el nombre contiene siglas deberán ser aclaradas)

Profesor de la asignatura<sup>1</sup>: Dr. Alfredo Viola, Profesor Titular, Instituto de Computación

Otros docentes de la Facultad: Eduardo Cota, Adjunto, Instituto de Eléctrica.  
Adrián Silveira, Ayudante, Instituto de Computación.

Docentes fuera de Facultad: Sebastián Fonseca

Instituto ó Unidad: Instituto de Computación

Departamento ó Área: Seguridad Informática

**Fecha de inicio y finalización:** Desde el 18 de agosto al 15 de setiembre. Lunes, Miércoles y Viernes.  
Horario y Salón: 18:00 a 21:00 hs. Salón de Posgrado del InCo

### Horas Presenciales: 40

(se deberán discriminar las mismas en el ítem Metodología de enseñanza)

### Arancel: \$ 10.000

(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 la 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 las horas dedicadas por el estudiante a la asignatura y su distribución 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:

2  
205

## Facultad de Ingeniería Comisión Académica de Posgrado

---

- Total de horas de dedicación del estudiante: 75

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

- Entregas de trabajo de Laboratorio
- 

### 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/>

---