CURSO:

TÓPICOS FORMALES EN CRIPTOGRAFÍA

Mg. Gerardo Parra

Secretaría de Investigación y Posgrado

Facultad de Informática

INSCRIPCIÓN Y CONSULTAS

TELÉFONO:
(+54) 294490300 – int. 644/649

SITIO WEB:
https://www.fi.uncoma.edu.ar/index.php/investigacion-y-postgrado-86-investigacion-y-postgrado-cursos/

CORREO ELECTRÓNICO:
posgradofai@fi.uncoma.edu.ar

El objetivo general del curso es presentar los fundamentos teóricos y prácticos de la criptografía moderna. En todos los casos, se hará énfasis en las posibles aplicaciones.

Los objetivos específicos son:

- Introducir los aspectos formales de la criptografía.
- Analizar los criptosistemas clásicos y estudiar los beneficios de los criptosistemas modernos.

Se discutirán tópicos referidos a:

- Nociones básicas de criptografía. Criptosistemas Clásicos. Sistemas Monoalfabéticos y Polialfabéticos.
- Conceptos básicos de encriptación de clave simétrica. Stream Ciphers. Block Ciphers. Modos de operación.
- Conceptos básicos de criptografía de clave pública. Aritmética modular. RSA. Funciones Hash. Logaritmos Discretos.
- Otras Bases de Criptosistemas. Nociones de algoritmos probabilísticos. Variantes alternativas.

SON ADMITIDOS AL CURSO:
GRADUADOS Y ALUMNOS AVANZADOS DE CARRERAS INFORMÁTICAS,
Interesados con conocimientos en diseño de algoritmos y en conceptos clásicos de teoría de la computación.

FECHAS Y HORARIOS: Días Miércoles 07, 14, 21, 28 y Viernes 30 de agosto 2024 de 16 a 20 hs

ARANCEL: 20.000 pesos

(para los inscriptos en la Maestría en Ciencias de la Computación, rige el acuerdo arancelario según su categoría como estudiante matriculado).

CERTIFICADO: curso con evaluación. Se emitirá certificado de aprobación o asistencia según corresponda.