MAESTRÍA EN CIENCIAS DE LA COMPUTACIÓN
PROPUESTA DE CURSO DE POSGRADO

1- DATOS GENERALES DE LA ACTIVIDAD CURRICULAR	
1.1 Título del Curso	Tópicos Formales en Criptografía
1.2 Área temática[1]	Teoría de la Computación

2- COMPOSICION DEL EQUIPO DOCENTE	
2.1 Responsable a cargo de la actividad curricular	Mg. Gerardo Parra
2.2 Docentes	

3- CARGA HORARIA					
Carga horaria teórica	30 hs.				
Carga horaria práctica	30 hs.				
Carga horaria total	60 hs.				
Distribución horaria semanal	Lu	Ma	Mie	Jue	Vie
Fecha de inicio sugerida					

4- BREVE RESUMEN DE CONTENIDOS (hasta 400 palabras)

Introducción a la Criptografía. Criptosistemas Clásicos. Definiciones Formales. Encriptación de Clave Simétrica. Criptografía de Clave Pública. RSA. Tópicos Avanzados.

5- CONOCIMIENTOS PREVIOS REQUERIDOS

Se requieren sólidos conocimientos en diseño de algoritmos y en conceptos clásicos de teoría de la computación.

6- OBJETIVOS

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.

[1] Corresponde a uno de los siguientes tópicos: Algoritmos y Lenguajes; Teoría de la Computación; Ingeniería de Software, Bases de Datos y Sistemas de Información; Arquitecturas, Sistemas Operativos y Redes.

7- CONTENIDOS (organizados en unidades, ejes, módulos, otros)

Unidad I: Introducción a la Criptografía.
Nociones básicas de criptografía. Criptosistemas Clásicos. Sistemas Monoalfabéticos y Polialfabéticos.

Unidad II: Encriptación de Clave Simétrica.
Conceptos básicos. Stream Ciphers. Block Ciphers. Modos de operación.

Unidad III: Criptografía de Clave Pública.
Conceptos básicos. Aritmética modular. RSA. Funciones Hash. Logaritmos Discretos.

Unidad IV: Tópicos Avanzados.
Otras Bases de Criptosistemas. Nociones de algoritmos probabilísticos. Variantes alternativas.

8- PROPUESTA DIDÁCTICA (metodología de trabajo de clases teóricas y prácticas)

La propuesta metodológica consiste en el dictado de clases teóricas donde se introducen los conceptos fundamentales del curso y de clases prácticas de ejercitación de los conceptos presentados a nivel teórico.
Las clases teóricas se desarrollarán mediante una exposición oral, con la ayuda de algún recurso didáctico visual, de los temas por parte del Profesor. Durante las clases prácticas, los estudiantes resolverán los ejercicios y problemas propuestos para las unidades temáticas. Se promoverán actividades grupales de exposición de ciertos temas con el objetivo de profundizar aspectos teóricos y/o prácticos.
Del total de las 60 hs asignadas al curso, se dedicará un porcentaje equitativo de tiempo entre las clases teóricas, las clases prácticas y la atención de consultas personalizadas. Se utilizará la Plataforma de Educación a Distancia (PEDCo) como soporte de material didáctico y como mecanismo de comunicación entre los docentes y los estudiantes.

9- MODALIDAD DE EVALUACIÓN Y CONDICIONES DE ACREDITACIÓN[2]

Se proponen dos instancias de evaluación. La primera consistirá en la realización de un examen sobre los contenidos teóricos y/o prácticos de las unidades. La segunda consistirá en el desarrollo de un trabajo final de los temas abarcados en el curso. La calificación final se obtendrá ponderando las notas de las dos evaluaciones.

[2] Son condiciones mínimas para la aprobación de todos los cursos: cumplir con un mínimo del 80% de asistencia a las clases, realizar las tareas y aprobar las evaluaciones que se hayan propuesto en el programa, con una calificación no menor a 7 (puntos). Los trabajos de evaluación pautados y la calificación de los alumnos deberán realizarse dentro de los 60 días posteriores a la finalización del curso.

10- BIBLIOGRAFÍA DE LECTURA OBLIGATORIA CORRESPONDIENTE A CADA UNIDAD Y GENERAL

BIBLIOGRAFÍA BÁSICA:

1. A. Salomaa. **Public-Key Cryptography**. Springer; 2nd edition. 1996.

2. H. Delfs and H. Knebl. **Introduction to Cryptography: Principles and Aplications**. Springer; 2nd edition. 2010.

3. Chuck Easttom. **Modern Cryptography: Applied Mathematics for Encryption and Information Security**. McGraw-Hill Education; 1 edition (October 12, 2015).

BIBLIOGRAFÍA DE CONSULTA:

1. Abhijit Das, C. E. Veni Madhavan. **Public-Key Cryptography: Theory and Practice.** Pearson. 2009.

2. Steven D. Galbraith. **Mathematics of Public Key Cryptography.** Cambridge University Press. 2012.

2. Juraj Hromkovic. **Theoretical Computer Science. Introduction to Automata, Computability, Complexity, Algorithmics, Randomization, Communication, and Cryptography**. Springer-Verlag. 2004.

11- INFRAESTRUCTURA E INSUMOS REQUERIDOS[3]

Para las clases teóricas se requerirá un proyector de multimedia. Se estima que el curso necesitará contar con la colaboración de un auxiliar docente.

12 – OTRA INFORMACIÓN RELEVANTE

[3] Deberá constar aquí si la realización del curso requiere contar con instalaciones especiales (laboratorio, sala de informática, equipamiento audiovisual, etc.). Explicitar si se estima que el curso debe tener un número máximo determinado de asistentes para poder ser dictado.