Formulario de Aprobación Curso de Posgrado 2016

Asignatura: Criptografía

Profesor de la asignatura [1]: Dr. Alfredo Viola, grado 5, 40 hs. DT, Instituto de Computación.

Profesor Responsable Local [1]:

Otros docentes de la Facultad: Adrián Silveira (grado 2, InCo), Sebastián Fonseca (Grado 1, InCo).

Docentes fuera de Facultad:

Instituto ó Unidad: Computación
Departamento ó Area: Programación

Fecha de inicio y finalización: Agosto 2016 a Noviembre 2016

Horario y Salón: Martes y Jueves de 8:00 a 10:00 horas

Horas Presenciales: 64 hs.

Nº de Créditos: 10

Público objetivo y Cupos: Estudiantes de grado y posgrado en computación interesados en fundamentos criptográficos y sus usos en la práctica profesional. NO hay cupo.

Objetivos:
Dar un curso de criptografía orientado a estudiantes de ingeniería. En este sentido se espera balancear tanto aspectos teóricos como aspectos algorítmicos y aspectos orientados al uso de la criptografía en la práctica profesional. Se estudiarán también diversos aspectos relacionados con los estándares NIST. De haber tiempo, se espera completar con algunos datos de la historia de la criptografía que ayuden a ilustrar diversos conceptos.

Se espera que quienes tomen el curso, terminen teniendo no sólo fundamentos básicos sobre la criptografía, sino que también ideas claras sobre su uso en la profesión.

Conocimientos previos exigidos: Matemáticas discretas, álgebra, fundamentos de estructuras de datos y algoritmos, probabilidad.

Conocimientos previos recomendados:

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)

Se espera que las clases sean interactivas y con importante participación de los estudiantes. El libro de referencia puede ser accedido por el Portal Timbó, así que el contenido de las clases se puede leer previamente del libro. Se espera también integrar los ejercicios prácticos, obligatorios y laboratorios como parte integral del curso. En este sentido, se espera discutir también ejercicios previamente seleccionados, y tratando de mostrar al resolverlos los conceptos teóricos más importantes vistos en clase.

El curso durará 16 semanas con una carga de 4 horas de teórico-práctico.

- Horas clase (teórico-práctico): 64
- Horas clase (práctico):
- Horas clase (laboratorio):
- Horas consulta:
- Horas evaluación:
    - Subtotal horas presenciales: 64
- Horas estudio: 40
- Horas resolución ejercicios/prácticos: 46
- Horas proyecto final/monografía:
    - Total de horas de dedicación del estudiante: 150

Forma de evaluación: Ejercicios de práctico y laboratorio a ser entregados al docente.

Temario:

1. · Introducción
2. . Criptosistemas básicos de clave privada. AES.
3. . RSA y el problema de factorización.
4. . ElGamal y el problema del logaritmo discreto.
5. . Funciones de Hash y aplicaciones.
6. . Firmas Digitales.
7. . Números pseudoaleatorios
8. . Manejo de claves e infraestructura de clave pública.
9. . Aplicaciones.

Bibliografía:

. *CryptoSchool.* Joachim von zur Gathen. Springer. ISBN-13: 978-3662484234, 2015.

. *Introduction to Modern Cryptography*, *Second Edition*. Jonathan Katz y Yehuda Lindell. Chapman & Hall/CRC Cryptography and Network Security Series. ISBN-13: 978-1466570269. 2015.

Complementaria:

. *Handbook of Applied Cryptography, Fifth Edition.* Alfred J. Menezes, Paul C. van Oorschot y Scott A. Vanstone. CRC Press ISBN: 0-8493-8523-7 (2001). En línea en http://cacr.uwaterloo.ca/hac/

. *Cryptography: Theory and Practice, Third Edition.* Douglas Stinson. Chapman and Hall/CRC. ISBN-13: 978-1584885085. 2005.

. *Cryptography Engineering: Design Principles and Practical Applications*. Niels Ferguson, Bruce Schneier y Tadayoshi Kohno. Wiley. ISBN-13: 978-0470474242. 2010.

. *Everyday Cryptography: Fundamental Principles and Applications.* Keith M. Martin. Oxford University Press. ISBN-13: 978-0199695591. 2012.