Programa de Asignatura

Nombre de la Asignatura	Criptografía
Créditos	**10 (diez)**
Objetivo de la Asignatura	Dar un curso de criptografía orientado a estudiantes de ingeniería. En este sentido se espera balancear tanto aspectos teóricos como aspectos algorítimicos 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.
Metodología de enseñanza	Se dictarán quince semanas de clases teórico-prácticas, a razón de cuatro horas semanales. La evaluación consistirá en la entrega de trabajos obligatorios con una carga total estimada de 50 hs.
Temario	· Introducción . Criptosistemas básicos de clave privada. AES. . RSA y el problema de factorización. . ElGamal y el problema del logaritmo discreto. . Funciones de Hash y aplicaciones. . Firmas Digitales. . Números pseudoaleatorios . Manejo de claves e infraestructura de clave pública. . Aplicaciones.
Bibliografía Básica:	. *CryptoSchool.* Joachim von zur Gathen. Springer. ISBN-13: 978-3662484234, 2015. (Disponible en el Portal Timbó) . *Introduction to Modern Cryptography, Second Edition.* Jonathan Katz y Yehuda Lindell. Chapman & Hall/CRC Cryptography and Network Security Series. ISBN-13: 978-1466570269. 2015. (Accesible en Internet) <u>Complementaria:</u> . *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.

Conocimientos previos exigidos y recomendados

Se sugiere conocimientos previos en matemáticas discretas. Es recomendable también tener experiencia en programación.

3
TRF

Anexo:

1) Cronograma tentativo.

· Introducción	6 hs.
. Criptosistemas básicos de clave privada. AES.	6 hs.
. RSA y el problema de factorización.	8 hs.
. ElGamal y el problema del logaritmo discreto.	8 hs.
. Funciones de Hash y aplicaciones.	4 hs.
. Firmas Digitales.	6 hs.
. Números pseudoaleatorios	10 hs.
. Manejo de claves e infraestructura de clave pública.	6 hs.
. Aplicaciones.	6 hs.
· Obligatorios	50 hs.
. Lectura para preparar clases	40 hs.

2) Modalidad del curso y procedimiento de evaluación.

Se realizarán clases presenciales para profundizar los temas que los estudiantes deberán tener leídos (con material previalmente entregado) y de resolución y discusión de problemas. Se espera que las clases sean interactivas, con activa participación estudiantil, y basado en las dudas que puedan surgir en la lectura previa o en los ejercicios propuestos.

La cantidad de trabajos obligatorios que los estudiantes deberán realizar dependerá de los recursos asignados para el dictado del curso y la cantidad de estudiantes. Se estiman entre 2 y 5 trabajos obligatorios.
La evaluación final será mediante la evaluación de los trabajos obligatorios, debiendo tener un mínimo del 60% del puntaje total de los mismos para poder aprobar el curso (No se exigen mínimos en cada trabajo).

3) Materia.

- **Ingeniería en Computación (plan 97)**

  Arquitectura, Sistemas Operativos y Redes de Computadoras.

- **Licenciatura en Computación**

  Arquitectura, Sistemas Operativos y Redes de Computadoras.

4) Previaturas

- **Ingeniería en Computación (plan 97)**

  Examen aprobado de Matemática Discreta 1, Matemática Discreta 2 y Programación 3.

- **Licenciatura en Computación**

  Examen aprobado de Matemática Discreta 1, Matemática Discreta 2 y Programación 3.

- **Ingenería en Computación (plan 87)**

  Las previas definidas en forma general para todas las electivas técnicas, no tiene previas especificas.

5) Observaciones

Para el plan 87 de Ingeniería en Computación debe valer como electiva técnica, acreditándose una electiva completa.

6) Esta asignatura no adhiere a resolución del consejo sobre condición de libre

APROB. RES. CONSEJO DE FAC. ING.
de fecha 26.7.16 Exp. 060120-001170-16