PROPUESTA MODULO DE TALLER (*para aprobación por la Comisión de Carrera*)

Nombre Actividad Específica	*Generación aleatoria en criptografía*
Proponente	*Instituto de Computación*
Responsable	*Joachim von zur Gathen (Universidad de Bonn, Alemania)*
Responsable en INCO o FING	*Alfredo Viola (viola@fing.edu.uy)*
Objetivo	*El módulo taller es de gran importancia en relación al uso práctico de la criptografía, pero además con fuertes componentes teóricos. La generación aleatoria uniforme de números es tema de fundamental importancia y fuente de graves problemas prácticos. Además de las implicancias prácticas, en el taller se van a ver profundos vínculos de este problema con otras áreas de la Ciencia de la Computación como el de Complejidad Computacional. El taller va a estar dirigido por un líder mundial experto en el tema.*
Descripción	El taller va a consistir en 4 sesiones interactivas de 3 horas cada una, distribuidas a lo largo de una semana. Es parte de una visita científica que el Dr. von zur Gahten va a realizar a fines de enero y principios de febrero. Aprovechamos su visita para discutir sobre este tema tan fundamental (no sólo en criptografía) y el cual no se presenta con esta profundidad en los cursos que dicta la Facultad de Ingeniería. La idea es que los estudiantes lean antes el material (que va a estar disponible en el EVA del Módulo Taller) y en las reuniones se discutan los aspectos fundamentales y los estudiantes hagan sus contribuciones. La evaluación final consistirá en un proyecto final de carácter individual.
Aporte a / tareas concretas del estudiante	El tema de generación uniforme aleatoria de grandes números es central en muchas áreas, más allá de la criptografía. Entender bien la dificultad del problema y herramientas para resolverlo es esencial. En este contexto además de ver aspectos prácticos se van a ver vínculos profundos con otras áreas, como el de la Complejidad Computacional. El Taller no sólo va a aportar conocimiento en el tema de generación aleatoria uniforme de grandes números, sino también en varios aspectos fundamentales de la Complejidad Computacional como los de distinguidores y predictores. Los estudiantes no sólo van a tener que participar diariamente en las sesiones de trabajo, sino que además van a tener que realizar un trabajo final.
Carga horaria total	*60 hs. (4 créditos)*
Carga horaria sem.	*24 hs. de reuniones y su preparación (12 horas cada uno) y 36 horas de trabajo final.*
Fecha inicio	*3 de febrero de 2020*
Fecha fin	*7 de febrero de 2020 (fecha de fin de clases presenciales)*
Conocimientos requeridos	*Fundamentos de criptografía y probabilidad (no necesariamente teniendo cursos previos).*
Cupo de estudiantes	*No hay cupos.*
Forma de Selección	*No corresponde.*
Método de Evaluación	*Participación en las reuniones y trabajo final.*

_____
Firma docente responsable
inco – fing

aprobado Comisión Carrera fecha: