Formulario de Aprobación Curso de Posgrado 2011

Asignatura: Curvas elípticas en criptografía

Profesor de la asignatura: Dr. Joachim von zur Gathen, Full Professor Aachen-Bonn Institute of Technology, Alemania

Profesor Responsable Local: Dr. Alfredo Viola Gr. 5 DT Instituto de Computación

Instituto ó Unidad: Instituto de Computación

Departamento ó Area: Programación

Fecha de inicio y finalización: 14, 16, 18, 21 de marzo de 2011

Horario y Salón: 18 a 21 hs. (salón a confirmar)

Horas Presenciales: 15 horas

Nº de Créditos: 3

Público objetivo y Cupos: Estudiantes avanzados de grado en Computación e Ingeniería Eléctrica y estudiantes de posgrado en Computación, Ingeniería Matemática e Ingeniería Eléctrica.

Objetivos: Presentar a los estudiantes con los principios básicos del uso de curvas elípticas en criptografía.

Conocimientos previos exigidos: estructuras de datos y algoritmos, probabilidad, y matemáticas discretas

Conocimientos previos recomendados: Fundamentos de álgebra, algoritmia y programación.

Metodología de enseñanza:
12 hs. de clases teóricas + consultas (se consideran 15 hs. presenciales y 27 hs. de carga de trabajo del estudiante).
Examen final domiciliario con ejercicios a resolver, evaluado en una carga de trabajo de 25 hs.

Forma de evaluación:
Examen final domiciliario con ejercicios a resolver.

Temario:
1. Curvas elípticas como grupos.
2. El tamaño de una curva elíptica.
3. Calcular el tamaño.
4. Polinomios de división.
5. Logaritmo discreto sobre curvas elípticas especiales.
6. Seguridad práctica con clave pública.
7. Las curvas NIST.

Bibliografía:

Material presentado por el profesor basado en el nuevo libro que está escribiendo sobre el tema.