Curvas elípticas en criptografía

14, 16, 18 y 21 de Marzo

Profesor Dr. Joachim von zur Gathen, Department of Computer Science at the Universität Bonn.
Responsable Local: Dr. Alfredo Viola, Instituto de Computación, FING, UDELAR.

Temario:

- Curvas elípticas como grupos
- El tamaño de una curva elíptica
- Calcular el tamaño
- Polinomios de división
- Logaritmo discreto sobre curvas elípticas especiales
- Seguridad práctica con clave pública
- Las curvas NIST

Hora: de 18:00 a 21:00 durante los días de dictado.
Evaluacion: una carpeta de ejercicios de resolución individual.
Mail de contacto: Dr. Álvaro Martín, almartin@fing.edu.uy

PEDECIBA · FACULTAD DE INGENIERIA · CSIC