Cuerpos finitos y criptografía

Florence Gillibert

Pontificia Universidad Católica de Valparaíso

Fecha: Jueves 19 de Octubre de 2017
Sala: Aula
Hora: 11:45 - 13:00

Abstract:

Hablaremos del problema del logaritmo discreto en un subgrupo multiplicativo de un cuerpo finito. Explicaremos como la dificultad de resolver este problema puede ser explotada en algunos protocolos de criptografía, como el protocolo de intercambio de clave de Diffie Hellman y el criptosistema de ElGamal.

Contacto
Enzo Fuentes M.
email: enzo.fuentes.m@gmail.com
webpage: http://ima.ucv.cl/seminarios/coloquio-ima/