

Criptografía sobre curvas elípticas

Dr. José de Jesús Galaviz Casas

Universidad Nacional Autónoma de México
Facultad de Ciencias

Resumen

Se revisan algunos de los conceptos básicos de criptografía. Se enfoca luego la criptografía de clave pública y se establecen las desventajas de eficiencia inherentes al trabajar en ella sobre campos finitos. Esto da pie para hablar de las curvas elípticas como una alternativa viable y cada vez más usada.