Criptografía con curvas elípticas

Josep M. Miret Biosca

Dpto. Matemática
Escuela Politécnica Superior, Universidad de Lleida
C/ Jaume II, 69, 25001-Lleida
miret@eps.udl.es

En los últimos años, la criptografía con curvas elípticas ha adquirido una creciente importancia, llegando en la actualidad a formar parte de los estándares industriales. Si bien se han diseñado variantes con curvas elípticas de criptosistemas clásicos, como el RSA, su principal logro se ha conseguido en los criptosistemas basados en el problema del logaritmo discreto, como los de tipo ElGamal. En este caso, los criptosistemas elípticos garantizan la misma seguridad que los construídos sobre el grupo multiplicativo de un cuerpo finito primo, pero con longitudes de clave mucho menores.

Mostraremos, pues, las buenas propiedades de estos criptosistemas, así como los requerimientos básicos para que una curva sea criptográficamente útil, abordando uno de los problemas que aparecen: el cálculo del cardinal de su grupo de puntos. Veremos, finalmente, métodos para descartar curvas criptográficamente no útiles, o bien para generar, a partir de una curva elíptica buena, más curvas que también lo sean.