Escrito por Carlos Luna y Paz Morillo
Martes 12 de Mayo de 2009 16:11

1. Introducción

En este artículo se presenta la criptografía con curvas elípticas. Para ello empezaremos con la definición de curva elíptica, veremos que son conjuntos de puntos en los que se puede definir una operación denominada suma, a partir de esta suma quedará definido, de forma natural, el múltiplo de un punto como suma del punto consigo mismo un número determinado de veces. A continuación veremos cómo usar esta estructura en criptografía, concretamente veremos la utilidad del cálculo de múltiplos de un punto de una curva elíptica, como función unidireccional. Se mostrará una aplicación al intercambio de claves, así como una aplicación al cifrado de mensajes. Acabamos mostrando ejemplos de uso actual de curvas elípticas en aplicaciones cotidianas y algunas de sus ventajas frente a otras alternativas.

2. Curvas elípticas

Es bien conocido que gran parte de la investigación criptográfica actual se centra en el uso de las curvas elípticas. Lo que seguramente no es tan popular es qué son las curvas elípticas y cómo se utilizan. Este artículo trata de responder a esas preguntas.

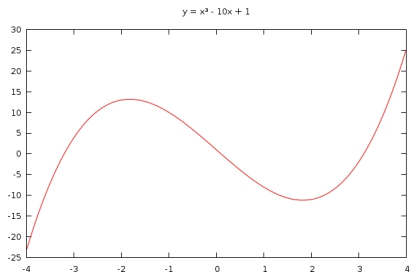
2.1. ¿Qué son las curvas elípticas?

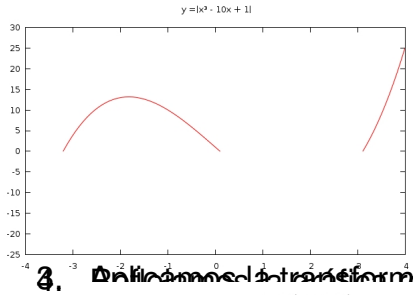
Una curva elíptica sobre un cuerpo K se define como el conjunto de puntos (x, y) de K × K que son solución de la siguiente ecuación:

$y^2 = x^3 + \alpha x + \beta$ **(1)** Donde α y β son dos parámetros que definen la curva y deben cumplir la relación $4\alpha^3 + 27\beta^2 = 0$. Es necesario, así mismo, añadir un punto más que llamaremos O y que se llamará *punto del infinito*.

Podemos dibujar con facilidad una curva elíptica sobre R siguiendo los siguientes pasos:

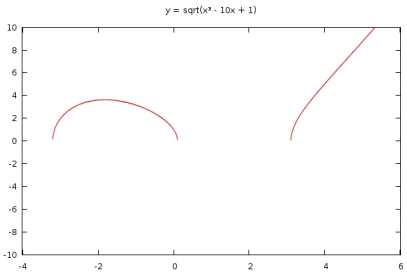
1. Dibujamos la cúbica $y = x^3 + \alpha x + \beta$
2. Eliminamos los puntos con ordenada negativa

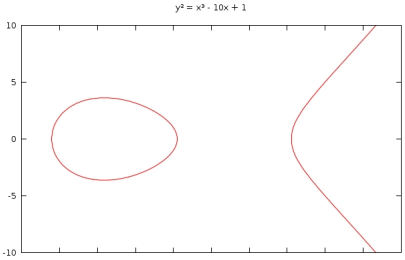




3. Aplicamos la transformación $(x, y) \to (x, \sqrt{y})$ respecto al eje de abscisas

4.





La condición $4a^3 + 27b^2 \neq 0$ garantiza que la curva elíptica sea regular, es decir, sin vértices ni

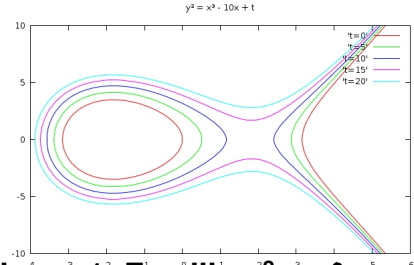


Figura 1: Familia $y^2 = x^3 - 10x + t$ con t =0, 5, 10, 15, 20

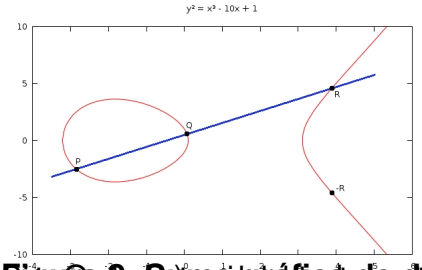


Figura 2: Suma gráfica de puntos (ver Figura 3) cede es que

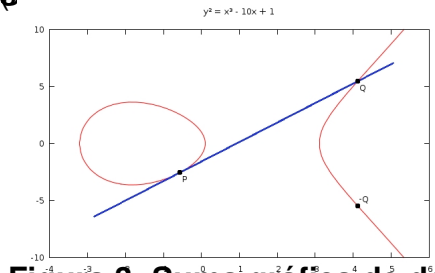


Figura 3: Suma gráfica de dos puntos

Escrito por Carlos Luna y Paz Morillo
Martes 12 de Mayo de 2009 16:11