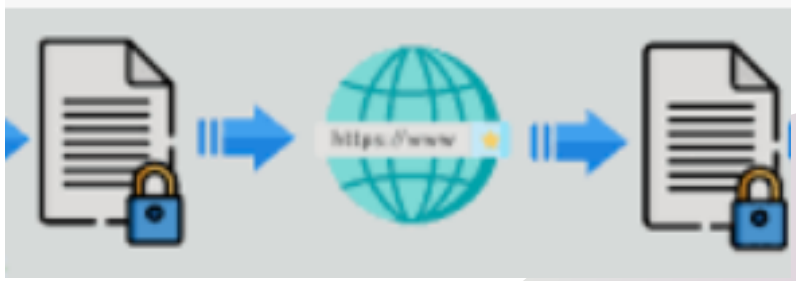
JULNAM

Objetivo

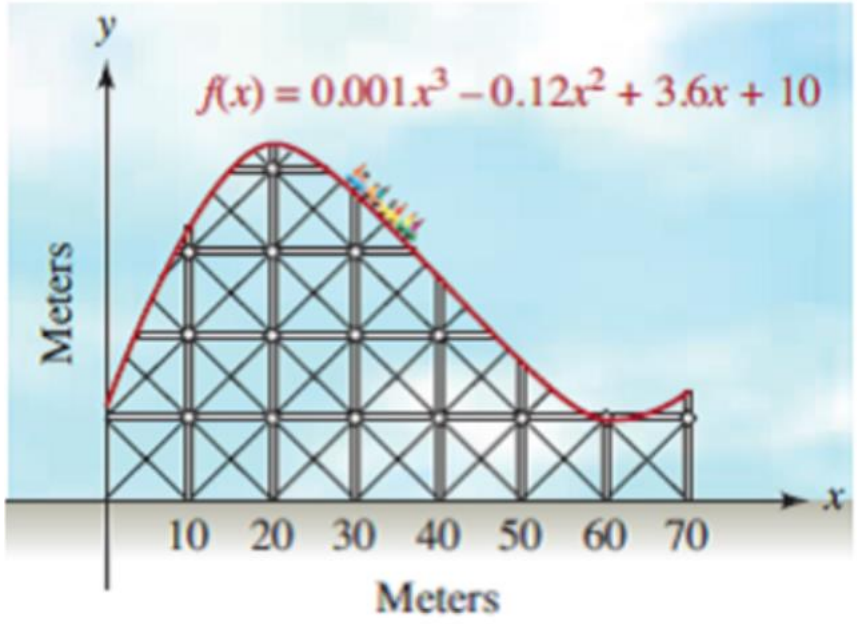
Implementar un mecanismo (en Python o Julia) de firma digital con criptografía asimétrica con el protocolo ECDH (Elliptic-curve Diffie–Hellman) de intercambio con llaves privadas.



Justificación de cómo ayuda al alumno a comprender el tema

La aplicación de las funciones polinomiales (en esta secuencia una función con radical como lo es una curva elíptica) son variados y se utilizan para resolver muchos problemas en otras ciencias, por mencionar los siguientes:

-En construcción, ingeniería civil y arquitectura

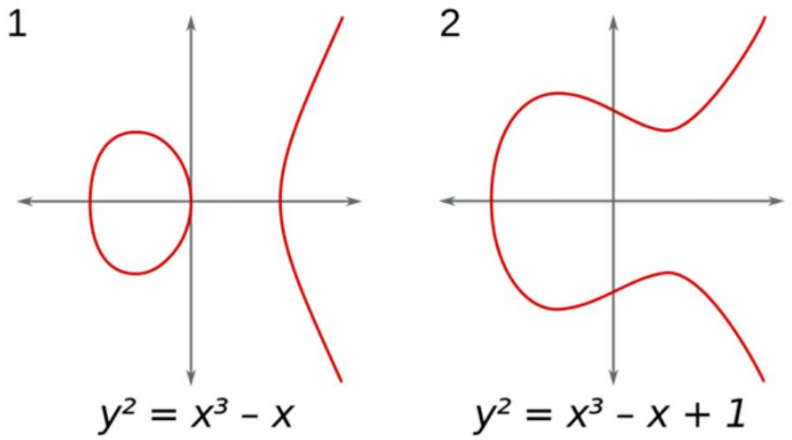


Diseñando una montaña rusa con polinomios

En Ingeniería forestal, por ejemplo, necesitamos la geometría para calcular áreas, pero también los polinomios en problemas como calcular cuántos árboles necesitamos replantar después de haber talado una zona de un bosque.

-El uso de polinomios en el área de la salud es amplio, desde el cálculo de las dosis más adecuadas de un medicamento, o el peso de un paciente enfermo en función del tiempo. Por poner solo un ejemplo, si queremos modelizar el ritmo circadiano en pacientes con hipertensión, buscamos la curva que mejor se adapte a nuestros datos, en este caso un polinomio de grado cuatro, lo que nos permite optimizar las dosis del medicamento contra la hipertensión.

-Finalmente, las curvas elípticas son usadas en criptografía, y no son más que expresiones polinómicas en dos variables, que también se pueden expresar como funciones con radicales, tal y como muestran estos dos ejemplos:



1.- $y = \sqrt{x^3 - x}$

2.- $y = \sqrt{x^3 - x + 1}$