

11-9-2024

**Nombre:** Álvarez García Brandon Azarael

**Nombre de la materia:** Selected topics in cryptography

**Grupo:** 7CM1

**Nombre de la profesora:** Dra. Sandra Díaz Santiago

Session 2:

Group operations on elliptic curves

Texto

Descripción generada automáticamente**Programming exercises**

Para las funciones hacemos uso de la clase que cree en la practica pasada, con el fin de ahorrar código e implementar una mejoría en la clase, para esta función, simplemente evaluamos y^2 y comprobamos si está en las raíces, de ser así, devolveremos verdadero, de lo contrario falso

Texto

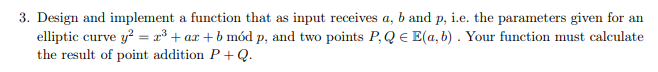
Descripción generada automáticamente

De la practica anterior, se creo una función para generar los puntos, esta misma se reutiliza, con la característica de invertir la coordenada ’y’ y aplicar el modulo como se muestra en la formula (x, -y mod p).

La función devolverá los puntos de la recta, pero de forma negada, al inicio se agrega la representación del punto al infinito (0,1,0)

Pantalla de computadora con letras

Descripción generada automáticamente con confianza media



Para esta función, esta dividida en dos partes, la primera consiste en la creación de una función para el calculo del coeficiente de Bezout, necesario para el calculo de S, ya que al realizarlo de forma directa, arrojaba pseudovalores.

Texto

Descripción generada automáticamente

Una vez teniendo esta función, ahora si se trabaja con la función de suma de puntos P+Q.

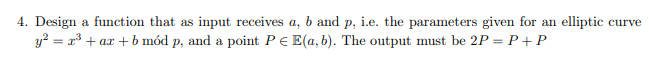
Primeramente, se tratan los casos especiales vistos en clase, para poder minimizar los errores a la hora del calculo de la suma de los puntos

Texto

Descripción generada automáticamenteTexto

Descripción generada automáticamente

Aquí se observa primero se tratan los casos especiales en donde se trata el punto al infinito, en caso de que no se trate ningún caso especial , se comprueba que ambos puntos pertenezcan a la recta, ya que para poder realizar esta operación, ambos deben pertenecer, si pertenecen ambos puntos, se procede a realizar el cálculo respectivo usando aquí el algoritmo de Euclides extendido, para nuestro coeficiente S, si este resulta 0, se trata del punto al infinito, ya que seria el inverso del punto que estamos tratando, y si ambos puntos son iguales solo mandamos a llamar la función designada para el doblado de puntos.



Para esta función resulta de forma mas sencilla ya que se trata de un solo punto, al igual que la función anterior, se comprueba el caso especial del punto al infinito y se compruebe que este punto pertenezca a la recta, de ser así simplemente volveríamos a realizar el cálculo, pero esta vez para P+P

Captura de pantalla de computadora

Descripción generada automáticamente

**Pruebas**

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Imagen que contiene Texto

Descripción generada automáticamenteTexto

Descripción generada automáticamente