

18-9-2024

Session 3:

Discrete Logarithm problem and DHKE

**Nombre:** Álvarez García Brandon Azarael

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

**Grupo:** 7CM1

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

**Ejercicios**

Texto, Aplicación

Descripción generada automáticamente

Para estos ejercicios, he creado 3 clases diferentes, para cada punto (1,2,3), para este punto he retomado código de la practica anterior y adaptándolo a este nuevo problema, dentro de esta clase tenemos dos funciones y un constructor.

Pantalla de computadora con letras

Descripción generada automáticamente con confianza media

El constructor, es simplemente para instanciar los valores iniciales, luego extraemos de la practica anterior el algoritmo de Euclides extendido, que nos ayudara con los coeficientes, ahora incorporamos el algoritmo “Baby step – Giant Step” , esto con la finalidad de no realizar fuerza bruta, ya que al ser coeficientes grandes, podría demorar bastante, con lo que este algoritmo , hace una partición de dichas exponenciaciones y en las va guardando, posteriormente estas se van comparando, pero una partición empieza de menor a mayor y la otra partición empieza de mayor a menor, optimizando así la búsqueda, en el punto en el que coincidan devolverá esa valor ‘x’ el cual es el que estamos buscando

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Para este problema ocurre algo similar, extraemos varias funciones de nuestra practica pasada, la cual incluye, la suma de puntos, el algoritmo de Euclides extendido, aquí las funciones agregadas, serian la multiplicación escalar y el mismo algoritmo anterior, pero adaptado a curvas

Comenzamos con el constructor correspondiente a los parámetros de la curva y los puntos

Texto

Descripción generada automáticamente

El algoritmo de suma de puntos, que ha sido ligeramente refactorizado, para tratar de tener menos líneas de código, sin embargo mantiene el mismo funcionamiento. Y la multiplicación escalar , que es lo que buscamos kP para resolver el problema, donde ira doblado el punto actual en cada iteración

Texto

Descripción generada automáticamente

Y posteriormente el algoritmo mencionado, pero adaptado a Curvas, en donde debemos encontrar una x tal que P = xG.

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Para este tercer problema igual, se crea una clase aparte, en donde tenemos un constructor con un numero p y g un generador.

Texto

Descripción generada automáticamente

Posteriormente, se trato de incorporar la función de encontrar un generador correspondiente a el numero primo, debido a que no se encontró alguna función que realizara esta labor

Pantalla de computadora con letras

Descripción generada automáticamente con confianza media

Por ultimo contamos con funciones pequeñas pero que realizan la parte lógica del funcionamiento del DHKE, tenemos una función para generar una llave aleatoria, que seria la privada, en caso de querer generarla de forma aleatoria, y tenemos las funciones que computan las llaves, para generar la llave pública y la función que computa el resultado del Emisor.

Captura de pantalla de un teléfono celular

Descripción generada automáticamente

**Resultados**

Para el punto 1:

Texto

Descripción generada automáticamente

Para el punto 2:

Texto

Descripción generada automáticamente