

4-9-2024

**Nombre:** Álvarez García Brandon Azarael

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

**Grupo:** 7CM1

**Nombre del profesor:** Dra. Sandra Díaz Santiago

Session 1:

Points in an elliptic curve

**Introducción teórica del tema**

Criptografía de curva elíptica En 1985, los matemáticos Neal Koblitz y Victor Miller presentaron de manera independiente una propuesta para usar curvas elípticas sobre cuerpos finitos en la elaboración de esquemas de cifrado.

En criptografía, no se usan las curvas elípticas basadas en números reales, ya que esto produce errores de redondeo. Por eso, se utilizan curvas elípticas definidas sobre cuerpos finitos, que se pueden representar por medio de la siguiente ecuación:

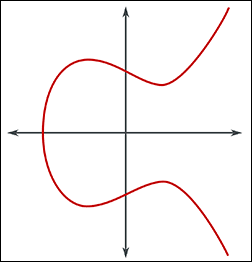
𝑦 2 = 𝑥 3 + 𝑎𝑥 + 𝑏 𝑚𝑜𝑑 𝑝

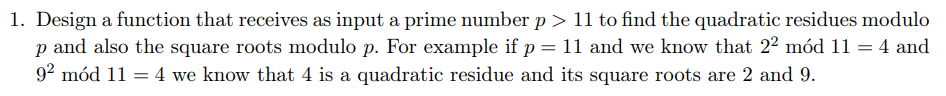
𝑑𝑜𝑛𝑑𝑒 4𝑎 3 + 27𝑏 2𝑚𝑜𝑑𝑝 ≠ 0

Esta criptografía de curva elíptica se caracteriza por tener un número de puntos finito, cuyas coordenadas serán únicamente números enteros. Esa característica es de suma importancia para este algoritmo de cifrado, ya que permite hacer cálculos de forma eficiente y sin errores de redondeo.

Los algoritmos de cifrado normalmente se basan en problemas matemáticos cuya solución aún no ha sido hallada. De esta forma, se garantiza que la función no sea reversible a manos de un tercero malicioso.

Se basa en el problema del logaritmo elíptico, también conocido como problema del logaritmo discreto en curvas elípticas para el cual hoy en día aún no se le ha encontrado una solución, lo cual hace que este algoritmo continúe siendo criptográficamente seguro.



**Ejercicios de programación**

Texto

Descripción generada automáticamente

Para todas las funciones cree una clase llamada ElipticCurve en donde pondría toda la lógica de las funciones, para esta función basta con instanciar un conjunto para guardar todos los residuos cuadráticos y se define como conjunto, ya que Python omite valores repetidos y una variable sr, para las raíces cuadradas y se define como un diccionario para relatar la posiciones de dichas raíces, lo que se realiza es recorrer los números desde 1 a p (donde p es un numero primo) e ir guardando esos residuos y comprobar si ese residuo coincide con alguna raíz y se añade, al final retorna el conjunto de residuos cuadráticos y el diccionario de raíces cuadradas.

Captura de pantalla de computadora

Descripción generada automáticamente

Imagen que contiene Texto

Descripción generada automáticamenteAdicionalmente cree esta función que lo único que realiza es generar parámetros a,b,p para las funciones, en donde genero números aleatorios de 1 a p-1 y evaluó si corresponden a una curva elíptica , si no vuelvo a generar estos valores, en caso de que correspondan, retorno los valores generados.

Pantalla de computadora con letras

Descripción generada automáticamente con confianza media

Para esta función es evaluar con todos los elementos del conjunto p, en los bucles no se coloca p-1 , ya que no realiza este ultimo recorrido por tanto no es necesario y solo se evalúa la función y los resultados se van guardando en una lista que al final se retorna.

Imagen que contiene Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Para esta última función se instancia en el main, ya que instancio un objeto de mi clase EllipticCurve e incorporo estas funciones dentro de buildCurve , retornando los valores necesarios de la curva o de dichas funciones, genero a,b,p con mi función y genero los valores de result que corresponde a los valores evaluados de la curva, qr y sr de mi nueva función creada buildCurve, posteriormente imprimo los datos y los escribo en un archivo de texto solicitado.

**Screen shots del programa en funcionamiento.**

Texto

Descripción generada automáticamentePrueba 1:

Texto

Descripción generada automáticamentePrueba 2:

Captura de pantalla de computadora

Descripción generada automáticamentePrueba 3: