CAPITULO VII

En esta parte realizaremos el estudio de la Curva Elíptica y como primera aproximación en la disertación de este tópico, el análisis se llevará a cabo en el campo de los números reales. De forma general podemos decir que la Curva Elíptica, la cual se denota como , es la gráfica de la siguiente ecuación:

(7.1) . Donde .

La expresión (7.1) se le conoce como la ecuación de Weierstrass [1]. Ahora bien, para que haya tres raíces diferentes en la expresión (7.1), de las cuales al menos una es real, se debe cumplir que . Cuando la Curva Elíptica cumple con esta propiedad se dice que es no-singular.

Queda claro que hay un conjunto de puntos que son solución de la ecuación (7.1). En este orden de ideas, sea , entonces, se denota al conjunto de todas las soluciones sobre una Curva Elíptica como sigue: .

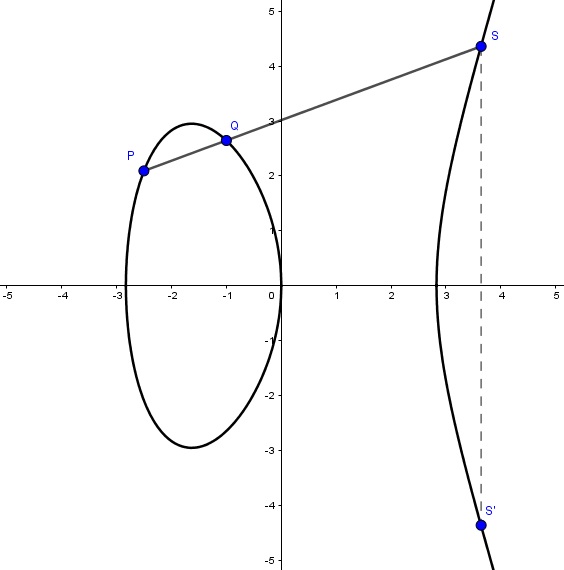


Figura 7.1. Gráfica de la Curva Elíptica .

En este punto es conveniente, presentar un ejemplo que muestre la gráfica de una curva en particular.

La Figura 7.1 representa la gráfica en el plano cartesiano de la curva .

Es simple observar que esta curva particular tiene el elemento constante igual a cero.

**VII.1. La operación de suma en el conjunto .**

Supongamos que el punto de la Figura 7.1 tiene como coordenadas a y las coordenadas del punto son . Entonces, se pueden dar los siguientes tres casos:

1. Que las abscisas .
2. Que se cumpla y las ordenadas .
3. Que las abscisas y las ordenadas sean iguales; i.e., y .

Cuando se está en el primer caso, claramente se tienen dos puntos diferentes, como por ejemplo, el caso que se presenta en la Figura 7.1. En esta situación, la línea recta que pasa por los puntos se intersecta con la gráfica de la Curva Elíptica en el punto . Entonces, se define la suma de como el punto .

Esto es, si se sigue que .

Ahora bien, de acuerdo con nuestro curso de Geometría Analítica se puede obtener la línea recta que pasa por los puntos y [2]. Una vez calculada la línea recta, usando a la expresión (7.1) es posible calcular el punto y por lo tanto al punto .

Entonces, la pendiente de la ecuación se calcula como sigue:

(7.1.1)

La ordenada al origen o término constante se obtiene como:

(7.1.2) , o también de la forma .

Por otro lado, para encontrarlas las coordenadas del punto , se iguala la ecuación de la recta con la curva , esta ecuación se escribe a continuación:

(7.1.3) .

Si desarrollamos el lado izquierdo de la expresión (7.1.3) y posteriormente se reagrupa de acuerdo al exponente de la variable, obtenemos lo siguiente:

(7.1.4) .

Ahora hagamos el siguiente razonamiento: como estamos analizando el primer caso, implica que . Por lo tanto, la tercera raíz es real y además diferente de .

Lo que implica que la expresión (7.1.4) se puede escribir como el producto de tres binomios, esto es:

(7.1.5) .

Si realizamos el producto de la expresión (7.1.5) y reagrupamos de acuerdo con el orden del exponente, tenemos que el coeficiente del término cuadrático es: .

Por lo tanto, , se sigue que:

(7.1.6) .

Entonces, es posible calcular la ordenada del punto , ya que sería de signo contrario a la ordenada del punto . Con esta información es simple darse cuenta que:

(7.1.7) .

Continuando con nuestra discusión, veremos que sucede cuando se cumple que y . Si observamos la Figura 7.1 no es complicado darse cuenta que cuando los puntos y cumplen con esta condición, entonces, uno es imagen del otro con relación al eje de la abscisa.

Por lo tanto, la línea recta que une ambos puntos forma un ángulo de 90° con respecto al eje de la abscisa. Se sigue que la pendiente de esta recta, denotada como , es la tangente trigonométrica de 90° el cual es un valor no acotado, esto es,.

Entonces, si decimos que el punto es el inverso aditivo de o viceversa; se sigue que . En conclusión, cuando se cumple que y , la suma de los dos puntos se define como el idéntico aditivo, que en este caso resulta ser . También, se menciona que este elemento algunos autores lo denotan como sin embargo, en este libro lo escribiremos como. Además, por definición diremos que para cualquier punto que sea solución de la ecuación (7.1), digamos , se cumple que .

Con relación al tercer rubro, y se toma a la línea tangente a la curva en el punto . En este escenario, la pendiente de la recta es la derivada de en el punto .

Entonces, , donde la pendiente .

Por lo tanto, si conocemos la pendiente y un punto, , la línea recta queda determinada. Se sigue que se puede calcular las coordenadas del punto , siguiendo un procedimiento similar al del caso uno.

En este orden de ideas, la pendiente es:

(7.1.8)

A partir de esta información, no es complicado calcular las expresiones (7.1.6) y (7.1.7) para los valores . A continuación se escribe la expresión para la abscisa .

(7.1.9)

El cálculo de da como resultado el mismo valor de la expresión (7.1.7). Entonces, dado lo anterior se concluye que la suma de dos puntos está definida.

Para terminar esta parte se menciona que la suma cumple con las siguientes propiedades [3]:

1. La suma es cerrada en el conjunto solución
2. La suma es conmutativa
3. La suma es asociativa.

**VII.2. La Curva Elíptica Discreta.**

Una vez entendida la suma de puntos para la Curva Elíptica en el conjunto de los reales, ésta se puede extender para el caso discreto.

Definición 7.2.1.- Suponga que se da un primo , de tal forma que el problema del logaritmo discreto sea imposible de resolver, de acuerdo a la tecnología que se tiene en este momento. Además, se tiene la Curva Elíptica ; donde las constantes . Entonces, se dice que un punto es solución de la curva si cumple con:

7.2.1

También, las constantes cumplen con , asimismo, existe un punto llamado punto al infinito que es el elemento nulo [4].

Con base en la expresión 7.2.1, se define la operación “suma” sobre el conjunto de soluciones , teniendo en cuenta que todas las operaciones se realizan en la aritmética módulo , se procede de la siguiente manera:

Dados dos puntos y donde se cumple que ; entonces .

Ahora bien, de acuerdo con las expresiones: 7.1.1, 7.1.6, 7.1.7, 7.1.8 y 7.1.9 de la sección anterior los valores de , se calculan de acuerdo a las siguientes relaciones:

7.2.2. Si ; o bien si y , entonces:

7.2.3. .

Una vez que se conoce el valor de , las variables se calculan de la siguiente manera:

7.2.4. mod. si . En caso de que y , entonces:

7.2.5. mod. .

Por otro lado, el valor de la variable se calcula como:

7.2.6 .

En este punto es conveniente ilustrar con un ejemplo lo anteriormente expuesto.

Ejemplo 7.2.1. Suponga que se tiene la curva , también, es simple comprobar que el punto = es una solución de la curva. Con esta información se ilustran los cálculos de y .

Primero verificaremos que el punto es solución de .

El lado izquierdo de la ecuación de la curva nos queda: 140. Con relación al lado derecho de la equivalencia se tiene que: Por lo tanto, se concluye que el punto es solución de la curva .

Con relación al cálculo . Por lo que, el valor de se obtiene como sigue: , de aquí que

Entonces, mod. , lo cual nos queda . Finalmente, el cálculo de es como sigue:, por lo que

Por lo tanto, Para el cálculo de se debe considerarse que , por lo que el cálculo de la pendiente debe tener en cuenta que .

En este orden de ideas,, entonces, De aquí, , por lo que

Ahora bien, el valor de Se sigue que entonces 3

Con relación a cómo construir una Curva Elíptica en el conjunto , no es un problema sencillo de resolver. En realidad no hay un procedimiento que realice el cálculo de manera directa. A continuación veremos algunos teoremas y lemas, que nos dan una idea de cómo podríamos obtener una Curva Elíptica de la forma:

7.2.2.

Se inicia con el Teorema 7.2.1, el cual se enuncia a continuación [5]:

Teorema 7.2.1. Dado un primo impar y una constante . También, denotemos a como el número de soluciones de la ecuación 7.2.2. Además, el primo se escribe de la forma donde son enteros positivos, y también es par; asimismo, se cumple que . Entonces, si la constante no es potencia cuarta módulo de algún elemento del campo , y si es potencia cuadrada módulo de algún elemento del campo .

Por otra parte, hay también otras condiciones que deben cumplirse; esto es, que la Curva Elíptica del tipo 7.2.2 sea no-singular, no-supersingular y que no sea de traza uno [6]. Lo anterior implica lo siguiente: que cumpla con para que la curva sea no-singular; además, si nos garantiza que la curva es no-supersingular, y la tercera que para que la curva no sea de traza uno.

Ahora bien, el teorema 7.2.1 nos deja algunas cosas por resolver; por ejemplo, ¿cómo saber cuándo no es potencia cuarta módulo de algún elemento del campo ?

Para resolver la última pregunta se enuncia el siguiente lema:

Lema 7.2.1. Considere que se tiene una Curva Elíptica de la forma: donde . Adicionalmente, se cumple con la condición Entonces, si es potencia cuarta de algún elemento del campo implica que se cumple que .

Demostración. Supongamos que es potencia cuarta de algún elemento de . Entonces, existe un tal que se cumple que Por otro lado, sabemos que lo cual implica que . Por lo tanto, es cierto que , sin embargo, lo anterior implica que . Utilizando el teorema del pequeño Fermat se sabe que Por lo tanto,

En este punto hemos demostrado que si es potencia cuarta de algún elemento del campo , entonces, es cierto que ; por lo tanto si implica que no es potencia cuarta de ningún elemento del campo módulo

Ahora bien, para que sea cierto de que hay un elemento del conjunto cuyo cuadrado módulo sea , se utiliza el criterio de Euler; esto es, debe cumplirse que [7].

Continuando con nuestro análisis, se va requerir que encontremos un subconjunto, del conjunto total de soluciones, con un número primo de soluciones; esto es, encontrar un factor primo del número total de soluciones Con este objetivo en mente, primero demostraremos que el número total de soluciones es divisible de manera entera entre 4. En otras palabras, se cumple que

Lema 7.2.2. Supongamos que las condiciones establecidas en el teorema 7.2.1 se cumplen, entonces

De acuerdo con el teorema 7.2.1 es cierto que , con impar y par. Lo anterior implica que es impar, además, se conoce que el número total de soluciones es , el cual se puede escribir de la siguiente manera: por lo que Sin embargo, es par y por lo tanto es divisible entre 4, de la misma forma es divisible entre 4, entonces, se concluye que

El lema anterior es toral para encontrar un factor primo del número De hecho, en el cálculo de una Curva Elíptica se pide que el número sea primo, dicho primo se denotará como .

Otro aspecto importante en la generación de una Curva Elíptica es el elemento generador o primitivo. Este elemento, punto de la curva, debe cumplir con la siguiente propiedad: si es el primitivo es cierto que . Por lo tanto, se inicia proponiendo una solución de la ecuación 7.2.2 y posteriormente se verifica si dicha solución cumple con la propiedad donde es módulo

A continuación escribiremos un teorema que nos aclara un poco más la construcción de una Curva Elíptica.

Teorema 7.2.2. Suponga que se tiene una Curva Elíptica, definida sobre un campo , donde es un primo mayor que 3. Entonces, existen dos enteros positivos tal que hay un isomorfismo entre los siguientes conjuntos: También, se cumple que y

La aplicación particular que se emplea aquí es y , considerando que es un factor primo del número de soluciones , el cual se calcula como .

Se debe aclarar que no siempre es primo, sin embargo, se buscan otros valores para de tal manera que el entero positivo sea primo.

**VII.3. Generación de Curvas Elípticas.**

En esta parte se ve cómo se realiza el cálculo de una Curva Elíptica de la forma , utilizando los teoremas, lemas y desarrollos de la sección anterior.

Iniciamos resolviendo el problema de cómo encontrar una solución inicial de la curva . De hecho, el problema se plantea de otra manera; esto es, dado un punto y un primo se busca una constante , tal que el punto sea solución de la curva .

Este problema se resuelve calculando la constante de la siguiente manera:

7.3.1.

Por otro lado, la constante debe cumplir con no ser potencia cuarta de algún elemento del conjunto , además, si debe ser potencia cuadrada de algún elemento del campo .

Por lo que debe ser cierto que y . Si se cumple con estas dos condiciones, se continúa con el proceso de calcular una Curva Elíptica, de otra manera se elige otro punto.

También, se debe comprobar que el punto es un elemento generador del subconjunto de con soluciones. Lo anterior implica que debe cumplir lo siguiente:

En caso contrario, se debe proponer otro punto y realizar el cálculo de nuevamente, y posteriormente verificar si se cumple la condición

Por cierto, el proceso del cálculo de una Curva Elíptica se ilustra mediante un diagrama de flujo en la Figura 7.3.1.

Como puede observar hay una serie de requisitos que se deben satisfacer antes de encontrar una Curva Elíptica.

Sin embargo, si este proceso se lleva a cabo de manera paralela con 16 procesadores, la probabilidad de encontrar una Curva Elíptica es muy alta [8].

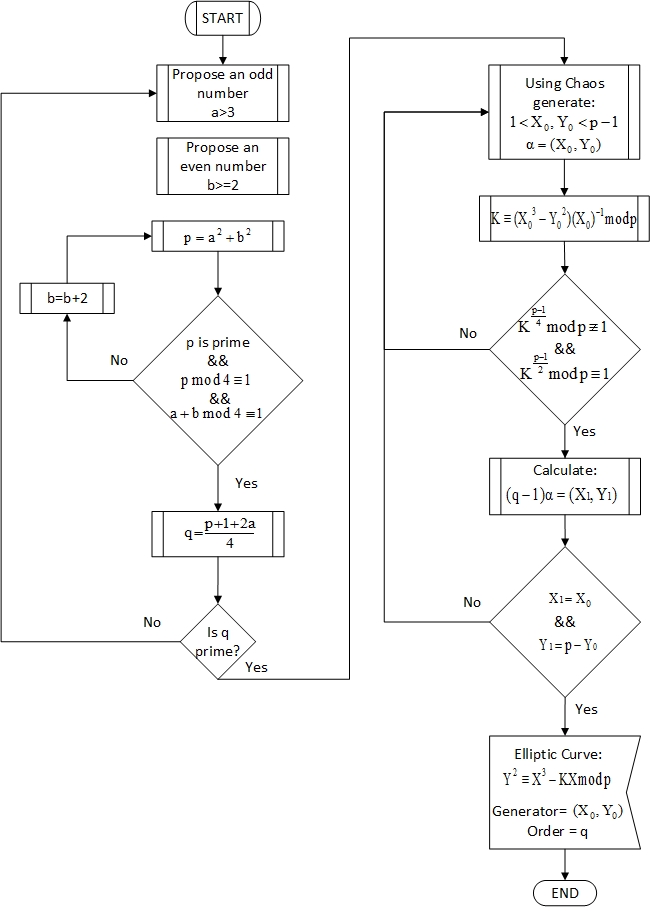


Figura 7.3.1. Diagrama de flujo para el cálculo de una Curva Elíptica.

Consideramos que es importante desarrollar un ejemplo para ilustrar lo anteriormente mencionado.

Ejemplo 7.3.1. Digamos que se tiene la curva del ejemplo 7.2.1 , y también el punto = . Primero veremos cuál es el valor de la constante para este punto, por lo que llevaremos a cabo los cálculos que se indican en la ecuación 7.3.1. De aquí se obtiene

Posteriormente, no es complicado verificar que Asimismo, es cierto que .

Además, el primo se construyó de acuerdo con los siguientes valores: y , se sigue que , y también se cumplen los siguientes requerimientos: 3, y

En este orden de ideas, el valor de nos da como resultado , lo cual puede constatarse que es primo.

Ahora bien, lo que resta por comprobar es que el punto es un elemento generador, por lo que se debe cumplir lo siguiente:.

Antes de realizar las operaciones para encontrar al punto , es conveniente mencionar cómo se realizan estas operaciones; esto es, una de las formas sería sumar 96 veces el punto No obstante, llevarlo a cabo de esta forma no es práctico. A continuación ilustraremos como se realiza esta operación.

Se inicia expresando a 96 de manera binaria, o sea, 96 = 110 0000‬. Posteriormente, se sigue el procedimiento de ir doblando los valores de hasta el bit más significativo contando a partir de la posición cero.

En nuestro caso, el bit más significativo tiene la posición 6, por lo que calculan los puntos: Después que se alcanzó el bit más significativo, de regreso solamente se suman los resultados donde aparecen bits igual a uno. Para esta situación particular se tiene que; .

Entonces, los pasos para llevar a cabo la operación se muestra a continuación:

Si denotamos el punto como , tenemos que: y finalmente

Ahora bien, de regreso solamente tenemos un bit igual a uno, el cual corresponde a la posición 5 y que es . Entonces,por lo que . Observe que .

Entonces, se concluye que el punto es un elemento generador.

**VII.4. Cifrado de información con la Curva Elíptica.**

Se inicia este punto diciendo que el criptosistema que se desarrolla con la Curva Elíptica es asimétrico, esto es, es de llave pública. Por otra parte, es importante señalar que con este criptosistema solamente se cifran puntos de la curva, sin embargo, daremos algunas ideas de cómo cifrar la llave del criptosistema simétrico; esto es, lo que se conoce como la distribución de llaves.

A continuación se ilustra de manera esquemática la forma en que se cifran los puntos de la curva.

El cifrado de un texto plano,, se realiza como sigue:

7.4.1. .

Donde el entero se elige al azar y además cumple que , y el punto , teniendo en cuenta que es un elemento generador.

Con respecto al punto, éste se calcula como sigue:

7.4.2. , con .

El punto es público y el entero es privado, además, éste entero cumple con lo siguiente: . También, se señala que tanto como son públicos.

El procedimiento de descifrado se muestra en la expresión 7.4.3.

7.4.3. .

El resultado de la expresión anterior es , porque , sin embargo, esto último es igual a .

En este punto, los autores consideran que es conveniente mostrar un ejemplo con la intención de aclarar ideas.

Ejemplo 7.4.1. Suponga que se tiene la curva , y que se desea enviar cifrado el punto calculado en el ejemplo 7.2.1. Esto es, 3, además, considere que el generador y el número de soluciones del subconjunto donde se aplicará el esquema de cifrado son los siguientes: y . En este orden de ideas, suponga que y .

Entonces, el punto público es , por lo que En general, si se conoce el punto no se sigue inmediatamente que . Por otro lado, recordemos que el valor privado es

Continuando con los cálculos,, de donde Con relación al punto , se tiene que por lo que y finalmente

Ahora bien, con respecto al proceso de descifrado se realizan los siguientes cálculos.

Con este objetivo en mente primero calculamos , entonces, primero se encuentra la pendiente, o sea . Llevando a cabo los cálculos tenemos que .

Entonces, la coordenada , por lo que Con respecto al cálculo de tenemos que .

Se sigue y por lo tanto .

Sin embargo, nosotros deseamos lo cual se logra cambiando la segunda coordenada por .

Entonces, Se sigue que,

De la misma forma que antes, para calcular la suma de dos puntos diferentes se inicia con , por lo que .

Continuando con nuestros cálculos, restan por obtener a . En este orden de ideas,, por lo que

Para la coordenada , se sigue que

Entonces, como se esperaba.

Como puede observarse, la Curva Elíptica solamente cifra puntos de ella misma.

En este sentido habrá que definir un procedimiento para cifrar la llave del criptosistema simétrico. En la sección que sigue daremos algunas técnicas para lograrlo.

**VII.5. Protocolos para el envío de llaves de sistema simétricos.**

En la práctica no hay una norma que nos indique cómo enviar la llave de un criptosistema simétrico utilizando la Curva Elíptica, pero en esta obra se hacen algunas sugerencias para hacerlo.

La primera que se describe es la siguiente: consideremos que se quiere enviar una llave de un sistema simétrico, digamos AES-128. La llave es una cadena de 128 bits, la cual tiene asociado un número entero, denotémoslo como Por otro lado, se tiene un punto de la curva que se desea cifrar, digamos que es .

Entonces, el remitente para enviar la llave realiza la siguiente operación: . De aquí, la propuesta es enviarle al destinatario las variables .

El destinatario procede de la siguiente manera: utilizando a obtiene el punto de acuerdo con el procedimiento descrito anteriormente.

Una vez realizado esto, como es público el destinatario puede calcular . Una vez hecho lo anterior, se realiza el producto .

Conociendo el valor de es simple obtener el la llave , y con ello descifrar el mensaje encriptado. A continuación mostramos un ejemplo con la intención de ilustrar los conceptos descritos anteriormente.

Ejemplo 7.5.1. Supongamos que se tienen los datos mostrados en el ejemplo 7.4.1. Además, suponga que la llave y que el punto que se encripta es . Con esta información se desea enviar la llave al destinatario.

Entonces, con los datos del ejemplo 7.4.1 se calculan las variables y la llave se convierte en entero, lo cual nos da . Con estos datos es simple calcular a lo cual da como resultado .

De aquí, el remitente envía los siguientes variables: y 109. Una vez que el destinatario recibe estos valores, usando a obtiene el punto como se hizo en el ejemplo 7.4.1.

Por otra parte, encuentra el inverso multiplicativo de , lo cual nos da .

Entonces, para obtener el valor entero de la llave el destinatario lleva a cabo la operación que sigue:. Posteriormente, convierte en binario a 281 obteniendo la cadena .

Otro protocolo para enviar la llave consiste en lo siguiente: una vez que se decide cuál es el punto que se va enviar, se procede como sigue: primero se convierten a binario los enteros ; denotemos estas cadenas como .

Después, se toma como la llave a la cadena de ceros y unos que se forma a partir del punto decimal a la derecha del producto , donde el símbolo representa la operación de concatenación, y es el número transcendente 3.14159.

Se aclara, que el número de bits que se toman a la derecha del punto decimal del producto , depende del criptosistema simétrico que se emplee; esto es, si el sistema fuera AES-128 entonces se tomarían 128 bits; sin embargo, si utilizamos el criptosistema AES-256, entonces, tomaríamos 256 bits.

Posteriormente, el remitente envía el punto encriptado al destinatario. Una vez que éste, el destinatario, descifra el punto encriptado haciendo uso de ; obtiene a y finalmente, convierte en binario sus coordenadas y después las concatena para obtener la llave.

Algunas reflexiones con relación al procedimiento descrito anteriormente.

Es claro que es un proceso muy simple, y su complejidad para resolverlo se basa en el problema del logaritmo discreto [9].

Sin embargo, tiene el inconveniente de tener solamente el número de llaves igual a , el cual es muy inferior a todas las posibilidades que nos da elegir aleatoriamente, la llave del sistema simétrico.

Pero si el número es lo suficientemente grande este problema puede reducirse.

Por otra parte, en este proceso se utilizó al número , sin embargo, se puede usar cualquier otro número transcendente, como por ejemplo, el número transcendente .

Entonces, como puede observarse se pueden desarrollar un gran número de esquemas de comunicación segura robustos, empleando este procedimiento [10].

Ejercicios

1.- Dada la curva , muestre que el punto es solución de la curva. Además, calcule y .

2.- Dados los valores de y encuentre lo siguiente:

a) El primo y muestre que mod. 4 ≡ 1, además, que +

b) El orden de la Curva, además, muestre que es primo.

c) Si α = (55211, 443096) calcule el valor de y muestre que no es potencia cuarta de ningún elemento de ; además, muestre que si es potencia cuadrada de algún elemento de .

3.- Desarrolle el software para encontrar Curvas Elípticas, siguiendo el diagrama de flujo mostrado en la Figura 7.3.1. Muestre que α = (55211, 443096) es un elemento generador para la curva del problema anterior.

4.- Diga cuál es la expresión de la Curva Elíptica del problema 1. Además, calcule lo solicitado en los siguientes incisos.

a) Considerando que 921 es la clave privada realice los cálculos necesarios para encontrar la clave pública .

b) Calcule el punto y cífrelo, esto es, calcule los valores de . También, realice el proceso de descifrado.

5.- Utilizando el punto realice la operación , considerando que son cadenas de bits. Tome los primeros 12 bits después del punto decimal como la llave hipotética de un sistema simétrico, y posteriormente, lleve a cabo los cálculos necesarios para el envío de dicha llave.

Bibliografía

[1] Carstensen-Opitz, Celine and Fine, Benjamin and Moldenhauer, Anja and Rosenberger, Gerhard, “Abstract Algebra: Applications to Galois Theory, Algebraic Geometry, Representation Theory and Cryptography”, Walter de Gruyter GmbH \& Co KG, 2019.

[2] Larson Ron, Hostetler Robert, Edwars Bruce, “Cálculo con geometría analítica Tratado de Geometría Analítica”, Mcgraw-Hill, edición, ISBN 9701052749, 2006.

[3] Gallian J., “Cont**e**mporary abstract algebra”, seventh edition, Brooks/Cole, 2011.

[4]. HemanthChakravarthy M. and Kannan E., Hybrid Elliptic Curve Cryptography Using Ant Colony Based Authentication System for Cloud Computing, Journal of Engineering and Applied Sciences, 2015.

[5]. Washington, L. C. “Elliptic Curves: Number Theory and Cryptography”, CRC press, 2008.

[6] Stinson R Douglas, Paterson B. Maura. “CRYPTOGRAPHY: Theory and practice”, CRC Press / Chapman & Hall Book, 2020.

[7]. Douglas R. Stinson. “CRYPTOGRAPHY: Theory and practice”, Chapman and Hall/ CRC Press, 2006.

[8] V. M. Silva–García, R. Flores–Carapia, C. Rentería–Márquez, B. Luna–Benoso, J. C. Chimal–Eguía, IMAGE CIPHER APPLICATIONS USING THE ELLIPTICAL CURVE AND CHAOS, International Journal of Applied Mathematics & Computer Science, Vol. 30. No 2, 2020.

[9] Hner, Thomas and Jaques, Samuel and Naehrig, Michael and Roetteler, Martin and Soeken, Mathias, Improved quantum circuits for elliptic curve discrete logarithms, International Conference on Post-Quantum Cryptography, Springer, pp. 425--444, 2020.

[10] VÍCTOR MANUEL SILVA GARCÍA, MARLON DAVID GONZÁLEZ RAMÍREZ, ROLANDO FLORES CARAPIA, EDUARDO VEGA-ALVARADO, AND EDUARDO RODRÍGUEZ ESCOBAR, A Novel Method for Image Encryption Based on Chaos and Transcendental Numbers, IEEE Access, Vol. 7, 2019.