Colegio Peruano Norteamericano Abraham Lincoln

Organización del Bachillerato Internacional

Programa del Diploma

**Exploración Matemática NS**

**Título:** Criptografía de curva elíptica

**Candidato:** Rodrigo Vargas Huaylla

**Número de Candidato:** 002202-0068

**Profesor: Jorge Luis Angles Terrones**

Lima, Perú

2018

# Tabla de contenido

## i. Introducción:

Desde pequeño, siempre tuve interés en las computadoras y el desarrollo de la tecnología en general; el hecho de saber que la matemática es la base de la creación de programas y sistemas atrajo mi interés a aprender cómo podía aplicar lo aprendido en el curso. En primer lugar, aprendí programación para entender el comportamiento desde lo más básico, y me di cuenta que mediante el uso de operaciones con distintas variables, lógica básica y creatividad se podían crear programas para resolver distintos tipos de problemas no matemáticos. A medida que mis conocimientos aumentaron fui relacionando las matemáticas a las distintas aplicaciones que utilizaba en mí día a día, entendiendo su funcionamiento.

Los avances en matemática son aplicados posteriormente en distintas áreas de la informática, tal como seria la criptografía. Siendo la criptografía el “Arte de escribir con clave secreta o de un modo enigmático” (RAE, 2018). Uno de dichos avances es la utilización de curvas elípticas en los sistemas más recientes y seguros. Investigando sobre dicho tema, decidí trabajarlo para mi exploración matemática y poder aprender a utilizarlo como sistema de seguridad para operaciones criptográficas.

Acorde a esto, plantee el siguiente objetivo para mi exploración: *Entender el comportamiento de las curvas elípticas, para aplicar sus propiedades en operaciones criptográficas.* Para lograr el presente objetivo, se definirán las propiedades de las curvas elípticas especialmente la suma de puntos, para posteriormente realizar las operaciones criptográficas de creación de número privado y él envió de mensaje.

Las curvas elípticas fueron introducidas por Diofanto en el Siglo III, en su libro “Arithmetica”, como uno de los problemas expresados, pero la naturaleza del problema tomo más de 1500 años de estudio. Fibonacci, Fermat, Euler y Newton realizaron aportes a la misma; pero en 1901, Poincaré generaliza todo lo estudiado anteriormente y los últimos aportes de la época (Wankhede, 2014).

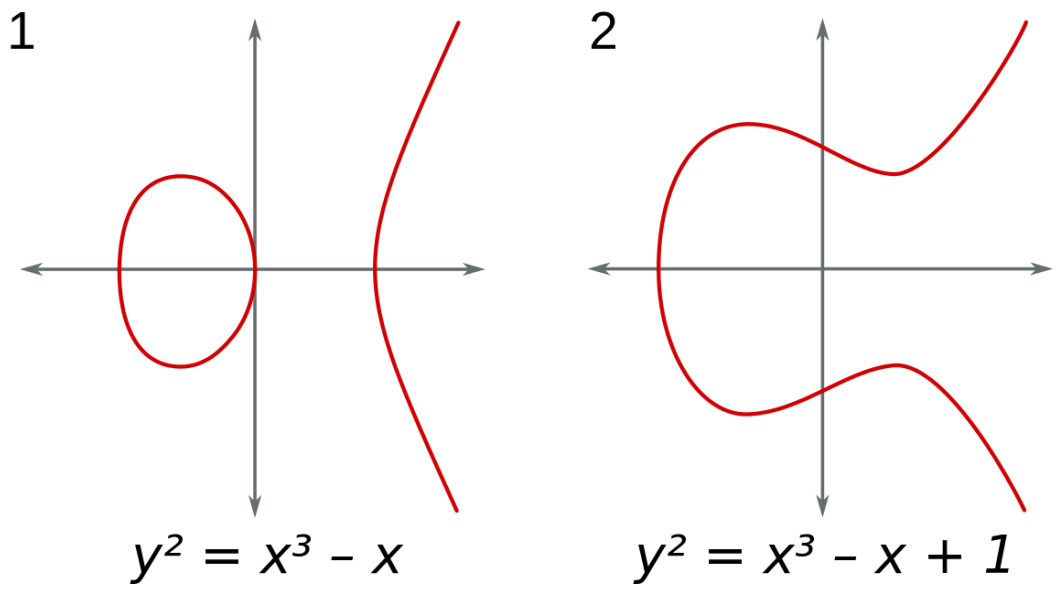
Para graficar las curvas elípticas en la presente exploración, se utilizara el programa GeoGebra.

## ii. Fundamentos de curvas elípticas:

La curva elíptica se resume al conjunto de puntos que satisfacen la ecuación: $y^2 = x^3 + ax + b$ excluyéndose $4a^3 + 27b^2 = 0$, debido a que este resultado provocaría un corte en la curva, y dejaría de ser elíptica. El conjunto de todas las curvas elípticas posibles esta descrito de la siguiente manera:

$$\{(x, y) \in \mathbb{R}^2 | \, y^2 = x^3 + ax + b \, ; 4a^3 + 27b^2 \neq 0\} \cup \{0\}$$

Gráficamente las curvas elípticas tienen la siguiente forma:




Las curvas elípticas se caracterizan por contener tres raíces reales y no ser continuas tal como la Grafica #1, o por poseer una raíz real y ser continúa como la Grafica #2.

Para poder expresar estas curvas de una manera más simplificada, debido a la infinidad de puntos posibles, se utilizan los grupos. Estos se definen como un conjunto de elementos determinados. Para las operaciones con puntos en estos grupos se presentan las siguientes propiedades:

1. Todo elemento tiene un inverso: $a + a' = 0$
2. Tiene presente a un elemento neutro: $a + 0 = 0 + a = a$
3. Clausura Lineal: Si $a, b \in G \rightarrow (a + b) \in G$, siendo $G$ el grupo.
4. Asociativa: $(a + b) + c = a + (b + c)$
5. Conmutativa: $a + b = b + a$

Dicho esto, el grupo se define de la siguiente manera: $\{(x, y) \in E | y^2 = x^3 + ax + b\}$ es decir, puntos que satisfagan la ecuación de la curva elíptica.

El inverso de un punto $P$ es simétrico al eje $x$, cumpliéndose la primera propiedad. Esto es debido a que $y$ tiene dos soluciones, las cuales solo difieren en el signo.

Cualquier línea recta que se sobreponga una curva elíptica, tendrá únicamente tres puntos de intersección. Por eso se dice que se presenta la operación suma dentro de la curva elíptica en la relación de 3 puntos alineados, cumpliéndose la expresión $P + Q + R = 0$ siendo tres puntos del grupo $E$. Esta suma no se refiere a la suma de las coordenadas, sino una forma de expresar el comportamiento de los tres puntos en una recta y cumplir el comportamiento de la curva como grupo.

La expresión previa es fundamental para el presente sistema criptográfico, nos permite entender que trazar una recta entre dos puntos, se obtiene un tercer punto en dicha recta. Posteriormente se explicara el comportamiento de las operaciones que surgen de dicha propiedad.

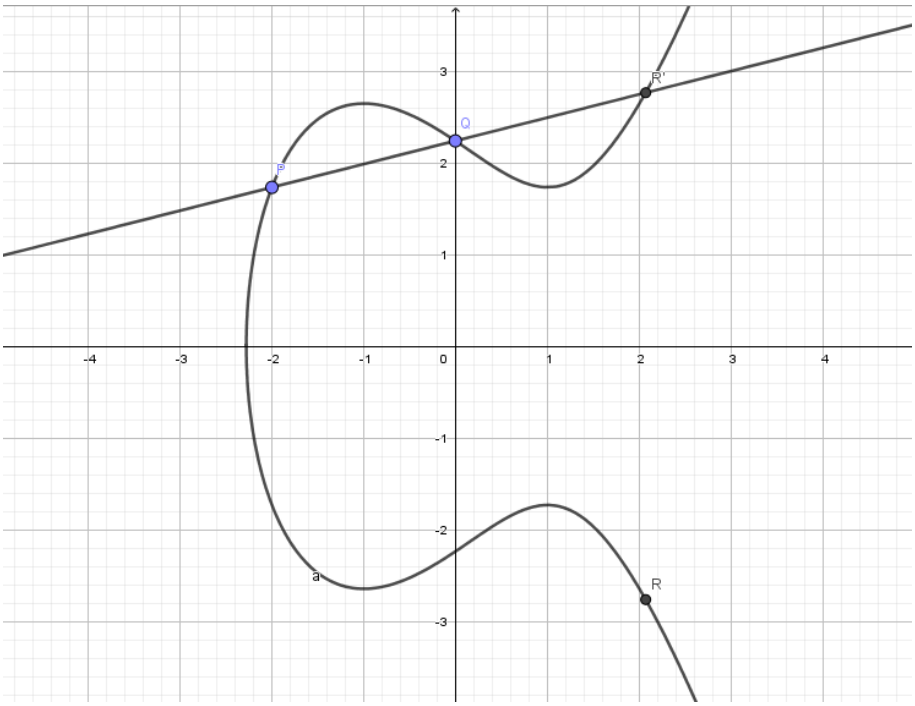
## iii. Suma y multiplicación de puntos:

Expresando a las soluciones de la curva elíptica como un grupo $E$, donde los $P + Q + R = 0$, lo cual se puede expresar de la forma $P + Q = -R$, siendo estos tres pertenecientes a una recta de gradiente $m = \frac{Q_y - P_y}{Q_x - P_x}$, y que tiene la forma $P_{(x,y)} + \lambda \times m_{(P,Q)} = -R_{(x,y)}$ donde el punto $R$ pertenece a la curva y $\lambda$ es un parámetro.

De manera algebraica se obtiene el punto desconocido $R$, es necesario el conocimiento de los otros dos puntos para determinar la ecuación de la recta que contiene a los tres puntos. Se realiza el siguiente procedimiento:

1. Siendo $P$ y $Q$ puntos dentro de la curva elíptica $y^2 = x^3 + ax + b$
2. Se obtiene la pendiente $m = \frac{Q_y - P_y}{Q_x - P_x}$ para la ecuación de la recta de forma $y = mx + c$.
3. Remplazar los valores para obtener el intercepto $Y$ de la ecuación.
4. Igualar $y^2$ para obtener los tres valores de $x$, los cuales son los valores de los tres puntos de intersección $P$, $Q$ y $R$.

Se puede visualizar en una curva elíptica de ecuación $y^2 = x^3 - 3x + 5$ con puntos $P(-2, \sqrt{3})$ y $Q(0, \sqrt{5})$, con el cual se obtiene el punto $R$.




Debido a la gráfica se entiende la existencia del punto $R$, de manera algebraica se procede a encontrar las respectivas coordenadas. Siendo $m = \frac{\sqrt{5}-\sqrt{3}}{2}$ la pendiente de la recta que pasa por ambos puntos, se realiza el siguiente procedimiento para obtener el valor $x$ de $R$.

$$y = \left(\frac{\sqrt{5}-\sqrt{3}}{2}\right)x + \sqrt{5}$$

$$y^2 = \left(\frac{4-\sqrt{15}}{2}\right)x^2 + \left(5-\sqrt{15}\right)x + 5$$

$$\left(\frac{4-\sqrt{15}}{2}\right)x^2 + \left(5-\sqrt{15}\right)x + 5 = x^3 - 3x + 5$$

$$0 = x^3 - \left(\frac{4-\sqrt{15}}{2}\right)x^2 + \left(\sqrt{15}-8\right)x = x\left[x^2 - \left(\frac{4-\sqrt{15}}{2}\right)x - 8 + \sqrt{15}\right]$$

Los valores de $x$ que satisfacen dicha ecuación son los siguientes: 0, -2, y 2.06. Se remplaza dicho valor para obtener el valor $y$ para posteriormente reflejarlo.

$$y = \left(\frac{\sqrt{5}-\sqrt{3}}{2}\right)(2.06) + \sqrt{5} = 2.76$$

Las coordenadas del punto $R$ son $(2.06, -2.76)$, debido al reflejo en el eje $X$ para el cumplimiento de la ecuación $P + Q + R = 0$.

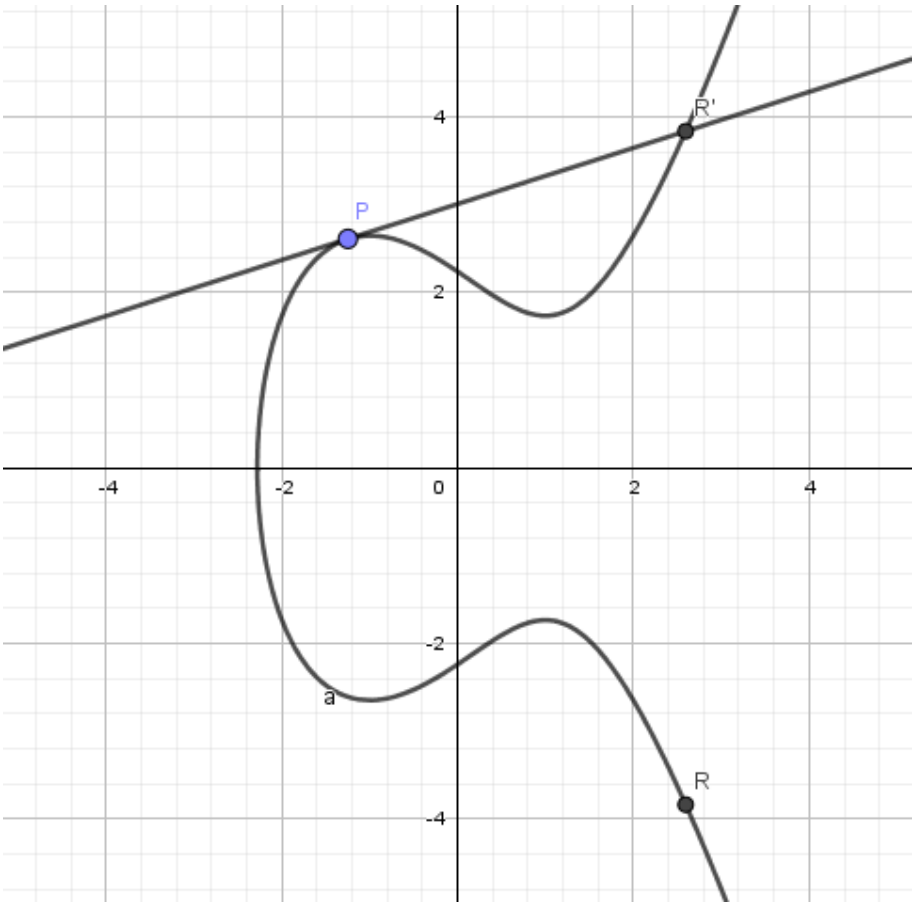
Este método sirve para sumar distintos puntos, la principal excepción se presenta cuando $P = Q$, es decir cuando se quiere obtener el resultado de $2P =$

$-R$ cuando $R$ es un punto desconocido. Se aplica el concepto de derivada para encontrar la tangente que pasa por un único punto, debido a que $P$ y $Q$ están ubicados en el mismo lugar, manteniéndose la estructura de los 3 puntos alineados.

De manera algebraica, la derivada nos permite llegar a determinar la pendiente en el punto, utilizando derivación implícita se sabe que $\frac{dy}{dx} = \pm\frac{3x^2+a}{2\sqrt{x^3+ax+b}} = \frac{3x^2+a}{2y}$.

Utilizando la curva generada anteriormente, teniendo como nuevo punto $P(-1.25, 2.61)$, se obtiene $2P = -R$ utilizando la derivada en $P$.

$$f'(-1.25) = \frac{3((-1.25)^2 - 1)}{2\sqrt{(-1.25)^3 - 3(-1.25) + 5}} = 0.324$$




Hallándose la derivada podemos igualar la recta y la curva elíptica para obtener los puntos de intersección.

$$y = 0.324x + b$$

$$2.61 - 0.324(-1.25) = 3.015$$

$$y = 0.324x - 3.015$$

$$y^2 = 0.105x^2 - 1.95x + 9.09 = x^3 - 3x + 5$$

La multiplicación escalar otorga facilidad para obtener el resultado de $nP = R$ siendo $n \in \mathbb{N}$. Realizar sumas repetidas toma mucho tiempo, pero sabemos cómo sumar dos puntos distintos y sumar dos puntos iguales, lo cual nos serviría mucho transformar $n$ a un número binario, donde su descomposición polinómica nos permite utilizar los conocimientos de suma y multiplicación de puntos.

Se visualiza en el siguiente ejemplo como se aplica para un valor de $n = 14$, el cual se expresa su numeración en base 2.

$$n = 14 = 1110_2$$

$$n = 2^3 + 2^2 + 2^1$$

$$12P = 2^3P + 2^2P + 2P$$

Utilizando los parámetros anteriores, se utiliza la curva elíptica para obtener el punto resultante. En la gráfica se pueden visualizar los valores de $2^nP$ siendo $n = 0,1,2,3$. Para posteriormente dar la suma de los puntos para hallar su multiplicación escalar. Se utilizan los parámetros establecidos en el ejemplo anterior y se realizan las operaciones en puntos.

Realizando el procedimiento anterior se obtiene que:

- $P = (-1.25,2.61)$
- $2P = (2.61, -3.87)$

La ecuación de la recta de la tangente en dicho punto es $y = -2.25x + 2$, se procede a igualar la presente función lineal con la curva elíptica.

$$5.06x^2 - 9x + 4 = x^3 - 3x + 5$$

$$0 = x^3 - 5.06x^2 + 6x + 1$$

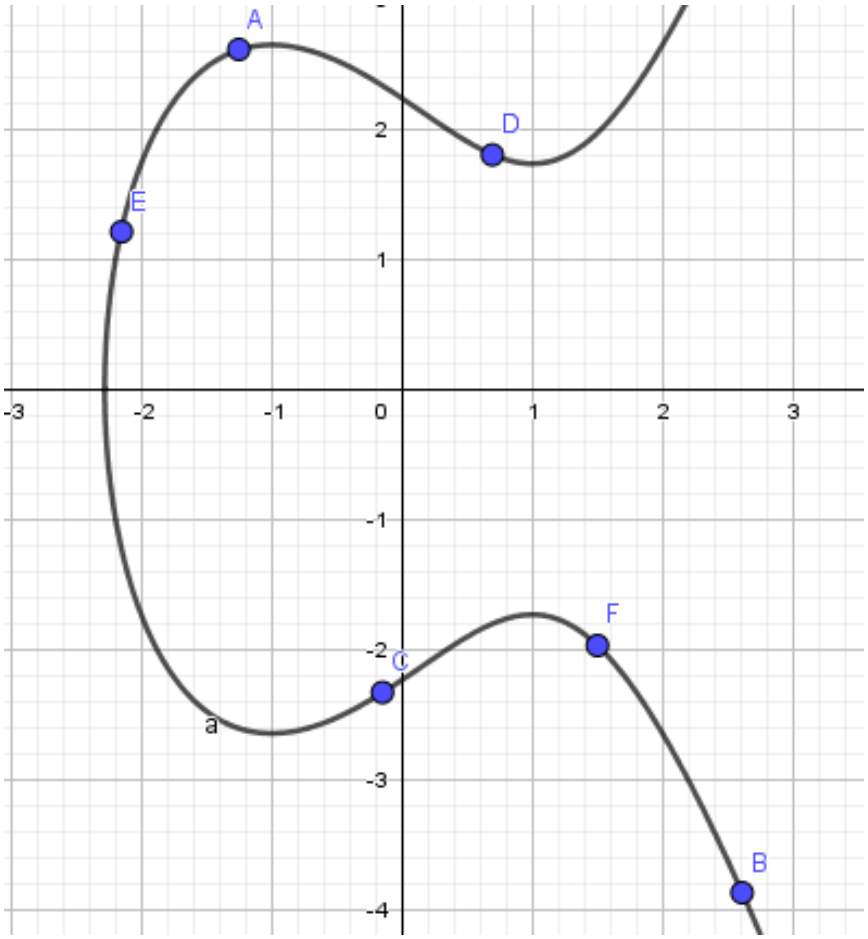
Utilizando mi calculadora grafica la solución restante es $x = -0.148$, obteniéndose $4P = (-0.148, -2.33)$. Continuándose el procedimiento anterior:

$$y = 0.629x - 2.24$$

$$0.396x^2 - 2.82x + 5.02 = x^3 - 3x + 5$$

$$0 = x^3 - 0.396x^2 - 0.18x - 0.02$$

$$8P = (0.696,1.80)$$




Siendo A=P, B=2P, C=4P, D=8P, E=6P, F=14P.

Se procede a sumar los resultados para llegar al resultado que se expresa en la gráfica reconociendo que $P + Q = -R$

$$2P + 4P = -6P$$

$$6P + 8P = -14P$$

Ya entendiendo el comportamiento de las curvas elípticas determinamos los dos procedimientos criptográficos, siendo seleccionados el intercambio de llaves Diffie Hellman y el envío de mensaje encriptado.

## iv. Intercambio de llaves Diffie Hellman:

Este protocolo criptográfico fue introducido por Whitfield Diffie y Martin Hellman, cual tiene como base de seguridad la dificultad de obtener la inversa del número generado. Este fue planteado utilizando como base la aritmética modular, pero se puede adaptar utilizando las curvas elípticas. El presente método tiene como objetivo la creación de un número privado entre dos usuarios, compartiéndose valores en un medio público.

El intercambio de llaves Diffie Hellman puede ser utilizado como concepto en las curvas elípticas, aprovechando las propiedades geométricas multiplicación escalar de puntos para compartir y generarlos; presentando el siguiente planteamiento:

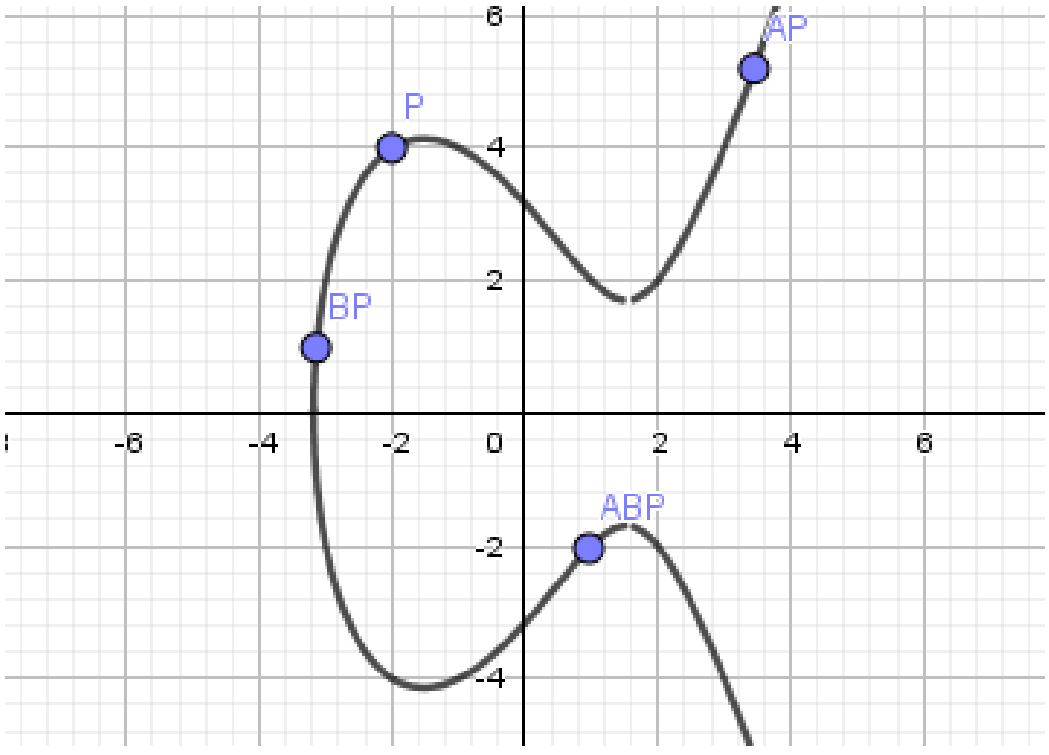
- Emisor: Alice
- Receptor: Bob
- Objetivo: Generar un numero privado utilizando un medio público.

El número generado se interpreta como un punto. Se utilizan las operaciones con puntos creándose el siguiente protocolo:

1. Se tiene un punto común el cual es utilizado por Alice y Bob, ambos usuarios generan un número privado aleatorio.
2. Alice y Bob realizan operaciones para crear $nP$, enviándose mutuamente el punto resultante.
3. Multiplicando el punto por el número privado, ambos obtienen un mismo punto sin tener que compartirlo, con esto se genera un punto $R$, siendo utilizable también como numero si fuera necesario.

Lo conocido por el resto de usuarios desconocidos es el punto común $P$, la curva elíptica y el punto $nP$ de cada uno ($aP$ y $bP$). Lo conocido únicamente por Alice y Bob es el punto resultante ($abP$) y los valores $n$ privados.

De manera gráfica se puede expresar utilizando el siguiente método: Siendo $P$ un punto público en una función $y^2 = x^3 - 7x + 3$



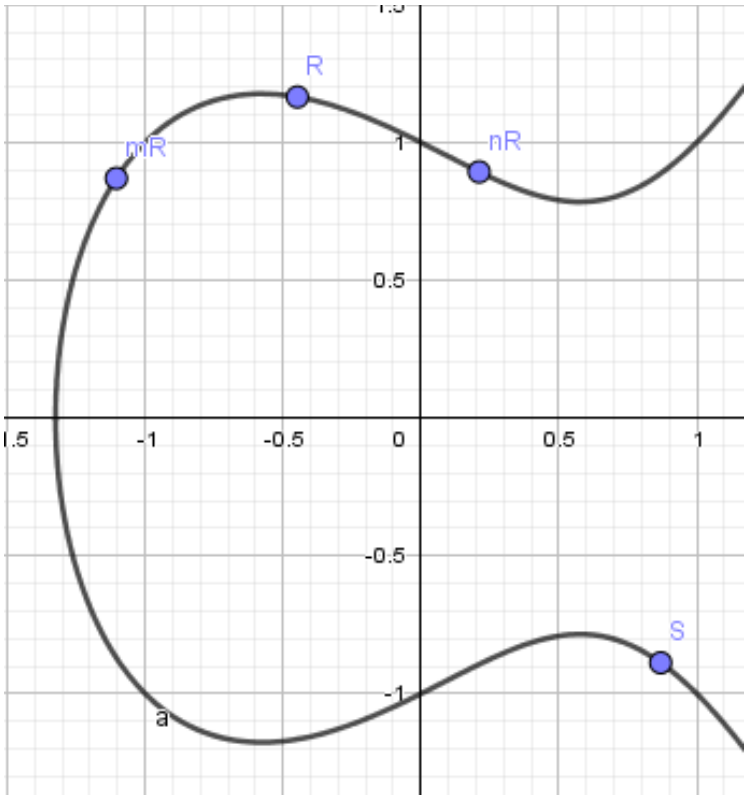
Para aumentar la complejidad del sistema de creación de puntos, se puede repetir el progreso distintas veces. En primer lugar se parte de un punto público y se crea uno privado, para poder descifrar de manera externa se tiene que probar la multiplicación escalar hasta encontrar el valor constante en ambos puntos, y posteriormente encontrar el punto producto.

Si aumentamos la cantidad de procesos, se aumenta la dificultad de obtener el punto general. Repetir el proceso en una segunda ocasión, siendo $c$ y $d$ los números aleatorios privados, se envían los puntos $c(abP)$ y $d(abP)$ para obtener $(cd)(abP)$, aumentando la seguridad del cifrado.

## v. Intercambio de mensajes encriptados:

Para el envío de mensajes se utiliza el punto generado previamente y la operación suma para enviar dicho mensaje. Realizando el siguiente protocolo.

1. Cada usuario en la red posee un número público único, Alice quien es el emisor, conoce el número de Bob y realiza una multiplicación entre ese número y el punto generado.
2. Este punto $n_B R$ le sirve a Alice para poder sumar el punto $m_A R$ el cual cumple el rol de mensaje. Por consiguiente Alice envía a Bob el resultado de la suma de ambos puntos $(m_A + n_B)R$.
3. Bob recibe este punto y resta el suyo para obtener el mensaje $(m_A + n_B)R - n_B R = m_A R$.



Continuándose con el ejemplo previo de manera gráfica se obtienen los siguientes puntos, siendo $R$ el punto obtenido anteriormente y $m_A R$ el mensaje a transmitirse, el cual solo puede ser descifrado por el receptor, el cual conoce su número público y el punto generado.

Para poder hacer este sistema más difícil, se divide el mensaje en varias partes, utilizándose distintos puntos base. Para poder descifrar un mensaje en curva elíptica se necesita descifrar el punto privado por cada parte del mensaje.

## vi. Aplicación de operaciones criptográficas:

Para lograr mi objetivo de aplicar dichas operaciones criptográficas de manera efectiva, planteare un algoritmo para enviar un mensaje privado buscando una seguridad máxima para el usuario. Utilizando como ejemplo el siguiente problema:

*Eduardo quiere enviarle la clave de su tarjeta de crédito a Ricardo, para que él pueda realizar un pago de $10000 lo más antes posible. En el pueblo de ambos ha ocurrido una crisis tecnológica, solo pueden utilizar el servicio inseguro y publico del estado. Ambos son estudiantes de informática y conocen el método de curva elíptica para enviar el mensaje, utilizan dicho procedimiento.*

En primer lugar se establecen los parámetros para el problema.

- Emisor: Eduardo
  - Numero Privado: 2 Numero Publico: 7.
- Receptor: Ricardo
  - Numero Privado: 4. Numero Publico: 4
- Curva Elíptica: $y^2 = x^3 - x + 1$
- Punto Base: $P = (-0.5,1.17)$

En primer lugar se procede a crear un punto privado siguiendo el procedimiento del intercambio de llaves. Se procede a realizar la operación $2^n P$ para los valores $n = 0,1,2$.

$$P \rightarrow (-0.5,1.17)$$

$$y = -0.107x + 1.120$$

$$0.011x^2 - 0.240x + 1.254 = x^3 - x + 1$$

$$2P \rightarrow (1.011, -1.012)$$

$$y = -1.022x - 0.087$$

$$1.044x^2 + 0.178x + 0.008 = x^3 - x + 1$$

$$4P \rightarrow (-1.031, -0.967)$$

Eduardo y Ricardo envían sus números privados $nP$ por el medio, $2P$ y $4P$ respectivamente. La obtención de la llave generada como sabemos se obtiene mediante la multiplicación escalar del número generado. Se redefine $2P = E$ y $4P = R$ y la llave generada es igual a $4E$ y a $2R$. En función del punto $P$ es igual a $8P$ en el presente caso, pero ambos usuarios no saben dicho resultado.

Cada usuario realiza las siguientes operaciones al obtener el punto del otro usuario. Lo realizado por Eduardo es lo siguiente:

$$E \rightarrow (1.011, -1.012)$$

$$2E \rightarrow (-1.031, -0.967)$$

$$y = -1.022x - 0.087$$

$$1.044x^2 + 0.178x + 0.008 = x^3 - x + 1$$

$$4E \rightarrow (1.031, -0.967)$$

Lo realizado por Ricardo es lo siguiente:

$$R \rightarrow (-1.031, -0.967)$$

$$y = -1.022x - 0.087$$

$$1.044x^2 + 0.178x + 0.008 = x^3 - x + 1$$

$$2R \rightarrow (1.031, -0.967)$$

Podemos observar en el presente ejemplo que ambos usuarios llegan al mismo punto sin compartir sus números privados, simplemente realizando operaciones con puntos con $P$ y el $nP$ del otro usuario.

Se redefine el punto base como $G \rightarrow (1.031 - 0.967)$ y se realiza el envió de mensaje por parte de Eduardo. Para esto obtiene $n_R G$ siendo $n_R$ el número público de Ricardo, a este se le adiciona el mensaje enviado por Eduardo, escrito en los valores de $x$ del punto $m_E G$. El punto que se envía es $(m_E + n_R)G$, para que Ricardo mediante la resta de $n_R G$ pueda obtener el punto $m_E G$.

El código que quiere enviar Eduardo es 0837, por ende se define al valor de $x = -0.837$ en el punto mensaje, el valor $y$ no es necesario que sea positivo o negativo, por ende Eduardo decide que sea negativo. Definiéndose $m_E G$ como $m_E G \rightarrow (-0.837, 1.118)$.

Se obtiene el punto $n_R G$ para posteriormente enviar $(m_E + n_R)G$, de la siguiente manera:

$$n_R G = 4G$$

$$G \rightarrow (1.031 - 0.967)$$

$$y = -1.061x + 0.127$$

$$2G \rightarrow (-0.900, -1.082)$$

$$y = -0.661x - 1.677$$

$$4G = n_R G \rightarrow (2.237, 3.156)$$

Recordando que la estructura de la suma de puntos es $P + Q = -R$, se realiza la siguiente operación teniéndose los puntos $m_E \rightarrow (-0.837, -1.118)$ y $n_R \rightarrow (2.237, 3.156)$.

$$m_E + n_R = -(m_E + n_R)G$$

$$y = 1.390x + 0.047$$

$$(m_E + n_R)G \rightarrow (0.532, -0.786)$$

Enviándose dicho punto queda concluida la operación criptográfica. En síntesis los datos que se transmiten por el medio son:

- Curva Elíptica: $y^2 = x^3 - x + 1$
- Punto Base: $P = (-0.5, 1.17)$
- Numero público de Ricardo y Eduardo, 7 y 4 respectivamente.
- Puntos $nP$ de ambos, sin conocerse el valor de $n$ en ambos usuarios.
- El punto $(m_E + n_R)G$ sin conococerse el valor del punto privado $G$.

## vii. Conclusión y evaluación:

Como pudimos evidenciar en el ejemplo, el presente método es seguro debido a dos factores importantes. El primero es la incapacidad de resolver división de puntos en un escalar, es decir uno puede obtener la multiplicación de $nP = G$ conociendo el escalar y el punto base, pero no se puede obtener el escalar privado conociendo solamente $P$ y $G$. El segundo factor es el aumento de dificultad operativa mediante el incremento del escalar para poder operar el punto, siendo la tecnología grafica fundamental para poder realizar dichas operaciones de manera más rápida.

Para mejorar la seguridad del sistema se tienen que utilizar valores muchos más amplios, existe dificultad para realizar dicha operación de manera individual y aritmética, debido a distintos factores pero principalmente el redondeo. El redondeo provoco que existan soluciones de las ecuaciones cubicas de forma compleja pero con parte imaginaria despreciable, este

problema fue solucionado al hallar los puntos de intersección de manera gráfica, lo cual me aseguraba la existencia y el entendimiento de dicho punto.

De igual manera el uso de la tecnología es fundamental para poder aumentar la seguridad, no solo de manera gráfica, sino utilizando un software simple utilizando el algoritmo ideado. Utilizando estos principios incluso podríamos crear un sistema de mensajería autónomo para dos usuarios. La presente investigación contribuye a entender el funcionamiento de este sistema criptográfico, el cual se toma como punto de partida para la creación de sistemas más complejos, complementando distintos métodos como la aritmética modular o el análisis.

Pude durante esta exploración lograr mi objetivo, comprendiendo las propiedades de las curvas elípticas y los grupos que podían generarse mediante estas, y crear un algoritmo para envió de mensaje utilizando las propiedades de suma y multiplicación de puntos en las curvas elípticas. A futuro planteo seguir aprendiendo sobre este mismo tema, debido a mi interés en las Ciencias de la Computación como carrera universitaria. También reconozco la importancia de los sistemas criptográficos de seguridad para el desarrollo de aplicaciones, al aprender este tema y utilizarlo para futuros proyectos de esta índole.

## viii. Bibliografía:


Certicom Research. (21 de Mayo de 2009). *SEC 1: Elliptic Curve Cryptography.* Obtenido de http://www.secg.org/sec1-v2.pdf

Chambers, A. (20 de Julio de 2015). *Elliptic cryptography*. Obtenido de plus magazine: https://plus.maths.org/content/elliptic-cryptography

Corbellini, A. (17 de Mayo de 2015). *Elliptic Curve Cryptography: a gentle introduction*. Obtenido de http://andrea.corbellini.name/2015/05/17/elliptic-curve-cryptography-a-gentle-introduction/

Ivorra Castillo, C. (s.f.). *Curvas Elipticas.* Recuperado el 23 de Febrero de 2018, de Universitat de València: https://www.uv.es/ivorra/Libros/Elipticas.pdf

Schulz, R.-H. (s.f.). *RSA or ECC.* Recuperado el 15 de Febrero de 2018, de Freie Universität Berlin: http://page.mi.fu-berlin.de/rhschulz/Krypto/RSA_or_ECC.pdf

Weisstein, E. (s.f.). *Elliptic Curve*. Recuperado el 21 de Febrero de 2018, de MathWorld Wolfram: http://mathworld.wolfram.com/EllipticCurve.html