Conference: Interdisciplinary Congress of Renewable Energies, Industrial Maintenance, Mechatronics and Information Technology

BOOKLET

RENIECYT - LATINDEX - Research Gate - DULCINEA - CLASE - Sudoc - HISPANA - SHERPA UNIVERSIA - E-Revistas - Google Scholar

DOI - REDIB - Mendeley - DIALNET - ROAD - ORCID

Title: Criptografía basada en curvas elípticas Criptografía

Authors: RAMÍREZ-HERNÁNDEZ, Héctor David, CONTRERAS-JUÁREZ, Roberto, ESPINOZA-HERNÁNDEZ, Nelva Betzabel y SÁNCHEZ-MENDOZA, Eduardo.

Editorial label ECORFAN: 607-8695
BCIERMMI Control Number: 2019-283
BCIERMMI Classification (2019): 241019-283

Pages: 13
RNA: 03-2010-032610115700-14

ECORFAN-México, S.C.
143 – 50 Itzopan Street
La Florida, Ecatepec Municipality
Mexico State, 55120 Zipcode
Phone: +52 1 55 6159 2296
Skype: ecorfan-mexico.s.c.
E-mail: contacto@ecorfan.org
Facebook: ECORFAN-México S. C.
Twitter: @EcorfanC

www.ecorfan.org

Holdings
Mexico Colombia Guatemala
Bolivia Cameroon Democratic
Spain El Salvador Republic
Ecuador Taiwan of Congo
Peru Paraguay Nicaragua

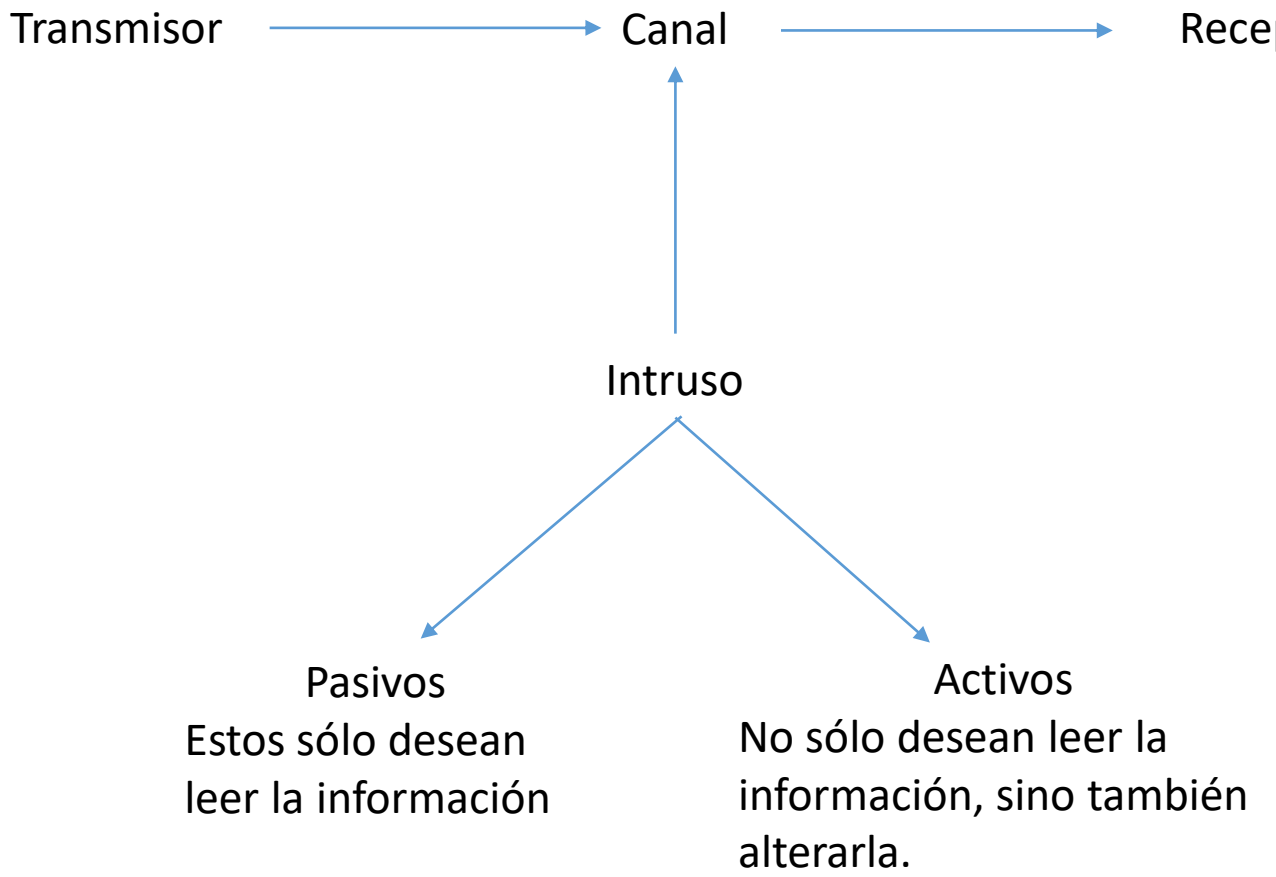
INTRODUCCIÓN

En la película “Juegos de Guerra” (1983), David Lightman es un joven que tiene una gran habilidad con los ordenadores por ello les saca el mayor partido posible, con cosas como falsear las notas del instituto y conseguir cambiar de curso. Un día busca en la red cómo entrar en el sistema de las compañías que crean juegos de ordenador para poder acceder a los juegos que todavía no han salido al mercado.

David accidentalmente se conecta a un ordenador del Departamento de Defensa de Estados Unidos que tiene el control absoluto del arsenal nuclear del país. Como gran admirador de los ordenadores el joven empieza a jugar a lo que cree que es otro juego de simulación (una guerra entre EEUU y Rusia).

Pronto se da cuenta de que no se trata de un juego más y con la ayuda del doctor Falken y de su novia tendrán que luchar por evitar un conflicto mundial: la Tercera Guerra Mundial.

Actualmente, en la era de la información, la necesidad de ocultar datos relevantes se ha incrementado hasta convertir a la criptografía en una herramienta fundamental para el manejo de información de forma segura en cualquier campo de trabajo, sea éste informático, privado, empresarial o de seguridad nacional, entre otros.



¿Cómo proteger la información enviada de intrusos?

CRIPTOGRAFÍA: es la práctica y el estudio de técnicas de cifrado y descifrado de información, es decir, de técnicas para codificar un mensaje haciéndolo ininteligible (cifrado) y recuperar el mensaje original a partir de esa versión ininteligible (descifrado).

Etimológicamente hablando, el origen de la palabra criptografía procede del griego κρμπτοζ (kryptos) = secreto; γραφϱιν (graphein) = escribir, es decir, el arte de escribir de manera secreta.

Curvas Elípticas

La criptografía de curvas elípticas (ECC) pertenece a la criptografía asimétrica, debido a que se utilizan dos tipos de llaves distintas, una pública y una privada, en la que el conocimiento de la llave pública no permite determinar el conocimiento de la clave privada.

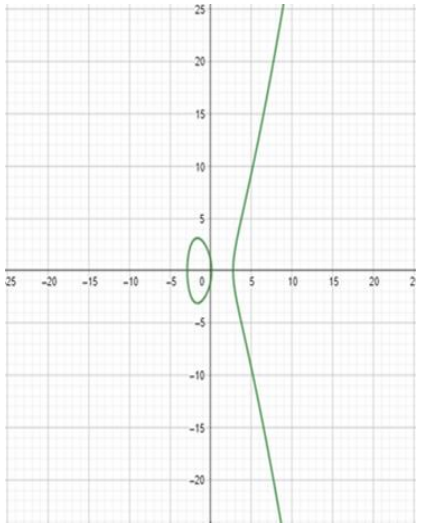
La criptografía de curvas elípticas fue propuesta en 1985 por Neal Koblitz (Koblitz, 1987) y Víctor Miller (Miller, 1986). Desde entonces una gran cantidad de investigaciones se han realizado para tener implementaciones eficientes y seguras de estos esquemas criptográficos.

Definimos de manera general a las curvas elípticas de la siguiente forma.

Sea K un campo. Una curva elíptica sobre K, es la curva plana sobre K definida por la ecuación de Weierstrass:

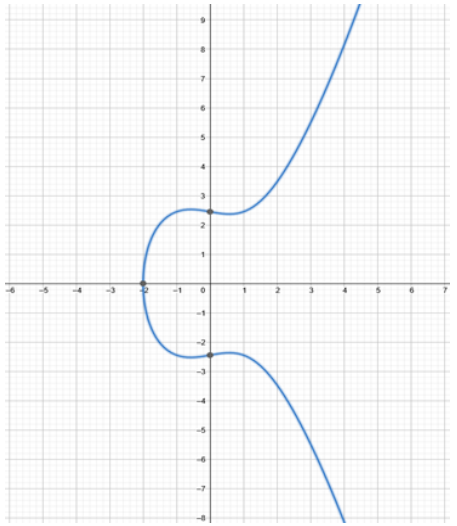
$$y^2 = x^3 + ax + b,$$

donde $x, y, a, b \in K$.



Curva elíptica $y^2 = x^3 - 8x + 1$

Ejemplos de curvas elípticas definidas sobre $\mathbb{R}$.



Curva Elíptica $y^2 = x^3 - x + 6$

A la expresión $\Delta = 4a^3 + 27b^2$ se le conoce como el discriminante de la curva elíptica. Se verifica que para que la curva elíptica no tenga raíces múltiples es necesario que $\Delta \neq 0$.

Una curva elíptica definida sobre el campo de $GF(p)$, denotada por $E(GF(p))$, esta formada por las variables a y b dentro del campo de $GF(p)$. Las curvas elípticas incluyen todos los puntos de (x, y) que satisface la ecuación de una curva elíptica módulo p. Esto es, una curva elíptica sobre $GF(p)$ tiene por ecuación:

$$y^2 \ mod \ p = (x^3 + ax + b) \ mod \ p,$$

donde $a, b, x, y \in GF(p)$.

De manera análoga, si $x^3 + \ ax \ + \ b$ contiene factores no repetidos, o equivalentemente si

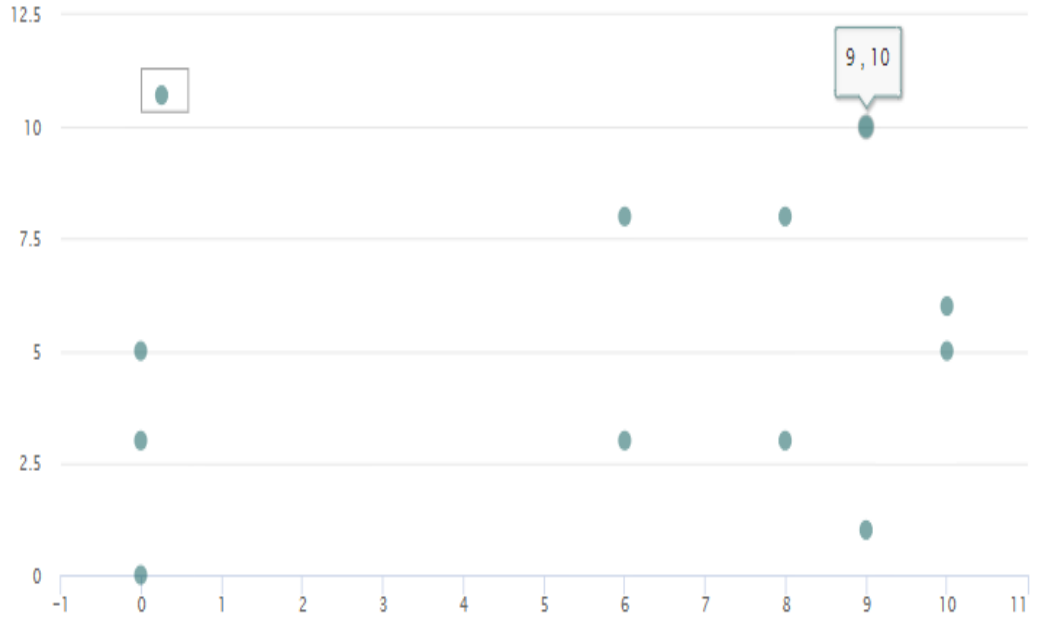
$$4a^3 \ + \ 27b^2 \neq 0 \ mod \ p$$

entonces la curva elíptica se puede utilizar para la criptografía. Una curva elíptica sobre el campo de $GF(p)$ tiene los puntos correspondientes en la curva elíptica, junto con un punto especial ∞, el cual se le llama punto en infinito o punto cero.

Ejemplo: Consideremos la curva elíptica sobre $GF(11)$. Con $a = 6$ y $b = 10$, la ecuación de la curva elíptica es $y^2 = x^3 + 6x + 10$. Los puntos que pertenecen a esta curva son: (0,3), (0,5), (6,3), (6,8), (8,3), (8,8), (9,1), (9,10), (10,5), (10,6) incluyendo a ∞.

La cardinalidad de puntos de una curva elíptica se denota por $\#E(GF(p))$. En este ejemplo

$$\#E(GF(p)) = 11.$$



Estructura de grupo

Desde el punto de vista algebraico, la ley de grupo para una Curva Elíptica representada por la ecuación de *Weierstrass,* se define de acuerdo con las siguientes propiedades:

- $P_1 + \infty = P_1$
- Si $P_1 = (x_1, y_1)$, entonces $-P_1 = (x_1, -y_1)$.
- Sean $P_1 = (x_1, y_1)$ y $P_2 = (x_2, y_2)$ puntos de la curva elíptica con $P_1, P_2 \neq \infty$. Entonces si $x_1 = x_2$ pero $y_1 \neq y_2$ o $P_1 = P_2$ y $y_1 = 0$ entonces $P_1 + P_2 = \infty$. En otro caso

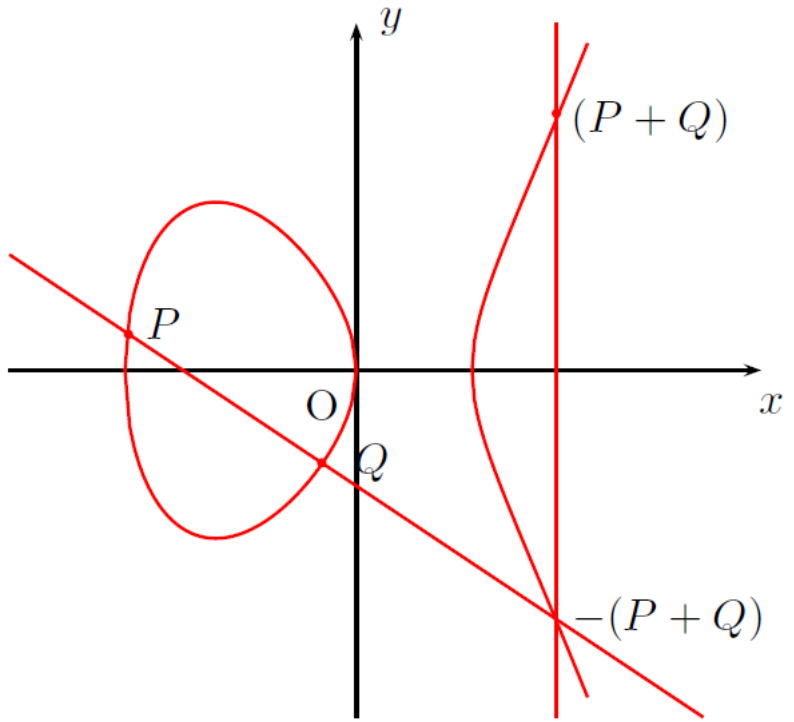
$$P_1 + P_2 = P_3 = (x_3, y_3) \text{ con}$$

$$x_3 = m^2 - x_1 - x_2,$$

$$y_3 = m(x_1 - x_3) - y_1$$

$$m = \begin{cases} \dfrac{3x_1^2 + a}{2y_1} & x_1 = x_2 \\ \dfrac{y_2 - y_1}{x_2 - x_1} & x_1 \neq x_2 \end{cases}$$

La curva elíptica $E(GF(p))$ dotada de la operación suma definida anteriormente forma un grupo abeliano.



Protocolo Criptográfico

Para llevar a cabo la encriptación y desencriptación usando curvas elípticas, es necesario realizar múltiples operaciones que nos permiten establecer los mecanismos de seguridad que se necesitan en el resguardo de la información.

1. Proporcionar un número primo p y los coeficientes a y b, para formar la curva elíptica de la forma (*2*) cumpliendo la condición (*3*). Para mostrar este paso, consideremos los coeficientes a = 9, b = 13 y el número primo p = 19. Con estos parámetros se obtiene la curva

$$y^2 = (x^3 + 9x + 13)\ mod\ 19,$$

   cumpliendo con la condición de que $\Delta \neq 0$.

2. Para el siguiente paso se necesita determinar el número de puntos con los que cuenta la curva elíptica, $\#E(GF(p))$. Para nuestro propósito, utilizamos el cálculo de los residuos cuadráticos para determinar $\#E(GF(p))$. Para ello , dados un número primo p y un entero cualquiera x, el símbolo de Legendre está definido de la siguiente manera:

$$\left(\frac{x}{p}\right) = \begin{cases} 1\ si\ x\ es\ un\ residuo\ cuadrático \\ -1\ si\ x\ no\ es\ residuo\ cuadrático \\ 0\ si\ x\ es\ múltiplo\ de\ p \end{cases}$$

Una vez calculado el número de Legendre, se conoce la cantidad de puntos que tiene la curva, que en nuestro caso es

#E(GF(p)) = 21.

Ahora para calcular todos los puntos de la curva se toman los valores mostrados en la tabla 1 y se utiliza la formula $H = (x - p)^2$ dando como resultado la tabla 2.

x	z	residuo		y	H
0	13	-1		0	0
1	4	1		1	1
2	1	1		2	4
3	10	-1		3	9
4	18	-1		4	16
5	12	-1		5	6
6	17	1		6	17
7	1	1		7	11
8	8	-1		8	7
9	6	1		9	5
10	1	1		10	5
11	18	-1		11	7
12	6	1		12	11
13	9	1		13	17
14	14	-1		14	6
15	8	-1		15	16
16	16	1		16	9
17	6	1		17	4

Cuando obtenemos los valores de x, z, y H en las tablas (1) y (2) respectivamente, se aplica el algoritmo de la Figura 2 para encontrar todos los puntos que pertenecen a la curva $E(GF(p))$.

Entrada: a$arrayXZ$, a$arrayYH$
Salida: Puntos de la curva E(GF(p))

1: $count \leftarrow 0$
2: **for** ($i = 0$ **to length arrayXZ) do**
3: $z \leftarrow arrayXZ[i] -> getZ()$ **//función para obtener el valor de** z
4. **for** ($j = 1$ **to length arrayYH) do**
5: **if** ($z = \boldsymbol{arrayYH[j] -> getH()}$) **then**
6: $arrayPoint[count] \leftarrow (arrayXZ[i] -> getX(), arrayYH[j] -> get\ Y())$
7 $count \leftarrow +1$
8: **if (isGen(**$arrayPoint[count]$**))** **then**
9: **return** $arrayPoint[count]$
10: **EndIf**
11: **Endif**
12: **Endfor**
13: **Endfor**

Para fines de ilustración en nuestro ejemplo se calcularon el orden de cada uno de los puntos de la curva obteniendo la tabla siguiente. En la práctica esto no es necesario, puesto que sería demasiado costoso, ya que al ser un método que necesita calcular el símbolo de Legendre desde 0 hasta $p-1$ este se vuelve inviable a medida que el p crece.

x	y	Orden
1	2	21
1	17	21
2	1	7
2	18	7
6	6	21
6	13	21
7	1	21
7	18	21
9	5	21
9	14	21
10	1	3
10	18	3
12	5	7
12	14	7
13	3	21
13	16	21
16	4	7
16	15	7
17	5	21
17	14	21

Cifrado de datos

Para realizar el cifrado de los datos, se debe contar con los siguientes parámetros:

- el número primo p
- los coeficientes a y b
- la cardinalidad de puntos de la curva elíptica $\#E(GF(p))$,
- un punto generador G de la curva,
- valores M y h con $Mh < p$,
- $llaveSA$ (llave secreta del usuario A), $llaveSB$ (llave secreta del usuario B) en donde $mcd(llaveSA, llaveSB) = 1$.

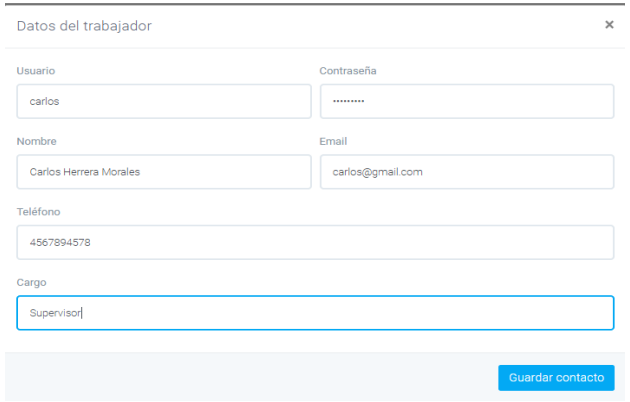
Ejemplo:

$$p = 500009, a = 15567, b = 7896,$$
$$\#E(GF(p)) = 499879, G = (241479, 71146),$$
$$M = 456, h = 123,$$
$$LlaveSA = 24528$$
$$LlaveSB = 11923$$

Así, nuestra curva a considerar es:

$$y^2 = (x^3 + 15567x + 7896) \ mod\ 500009$$

Supongamos que tenemos un usuario que se va a registrar en una plataforma y lo que interesa cifrar es la contraseña. Para nuestro caso la contraseña es carlos123 e ingresa sus datos en un formulario.



Procedemos a cifrar la contraseña del usuario de la siguiente manera:

Paso 1. Codificar el mensaje, para ello usamos el código ascii que comprende del 0 al 255.

Inicializamos con $j = 1$. Sabiendo que el ascii de la letra c es 99 se realizan los siguientes pasos:

Paso 1. 1 Calculamos

$x = ascii(c)\,(h) + j = 99\,(123) + 1 = 12178$, y se sustituye este resultado en la ecuación de la curva elíptica, esto es,

$$y^2 = (x^3 + 15567x + 7896) =$$

$$12178^3 + 15567(12178) + 7896 = 334992,$$

dado que no existe valor de y que cumpla con esta ecuación, se aumenta a $j = 2$ y se reinicia el proceso.

Paso 1.2 $x = ascii(c)\,h + j = 99\,(123) + 2 = 12179$, y se sustituye este resultado en la ecuación de la curva elíptica, esto es,

$$y^2 = (x^3 + 15567x + 7896)$$

$$= 12179^3 + 15567(12179) + 7896 = 290136$$

este número si tiene raíz cuadrada que es igual a 161435.

Por tanto, la codificación de la letra c es $(12179\,, 161435\,)$. Repetimos este proceso para cada una de las letras y números obtenemos:

$$c = (\,12179\,, 161435\,)$$
$$a = (\,11936\,, 218659\,)$$
$$r = (\,14023{,}101746)$$
$$l = (\,13285{,}115296)$$
$$o = (\,13656{,}29398)$$
$$s = (\,14147{,}176240)$$
$$1 = (\,6031{,}183341)$$
$$2 = (\,6152{,}153375)$$
$$3 = (\,6277{,}52620)$$

Paso 2. Se calcula la llave pública de A:

$$llavePA = LlaveSA * G\_$$
$$= 24528\,(\,241479\,, 71146\,)$$
$$= (\,253513\,, 78497\,),$$

entonces la pareja es igual

$$A = (\,24528\,, (253513\,, 78497)\,).$$

Paso 3. Se calcula la llave pública de B: $llavePB = LlaveSB * G =$ $11923\,(241479\,, 71146) = (\,339894\,, 358573\,)$, entonces la pareja es igual $B = (\,4562\,, (339894{,}358573)\,)$.

Paso 4. Ciframos la letra c eligiendo un entero aleatorio $k = 205887$ y multiplicamos ese número por el punto G, esto es,

$$kG = 205887(241479{,}71146)$$
$$= (45235{,}155942).$$

Paso 5. Sumando la codificación de la letra

$$c + k(llavePB)$$

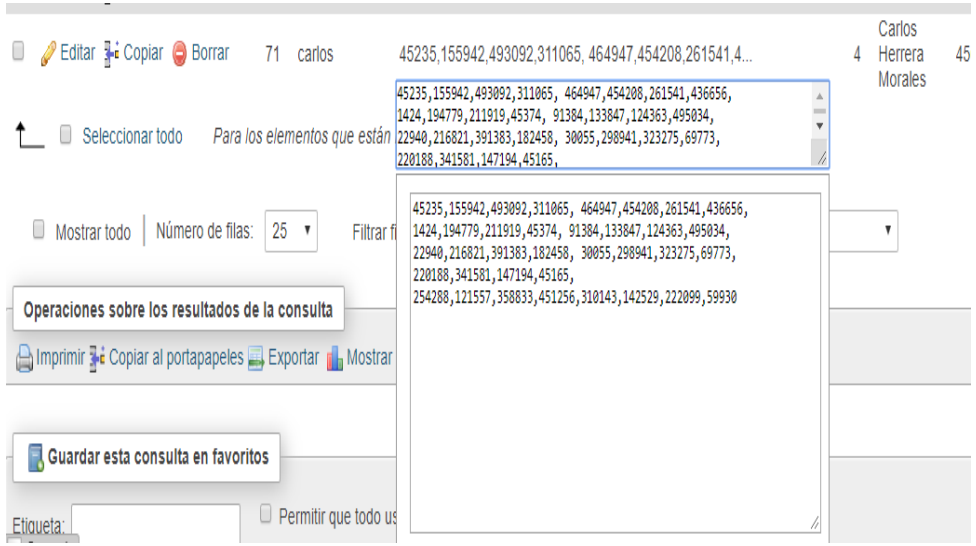
se obtiene:

$$(12179{,}161435) + 205887(339894{,}358573)$$
$$= (12179{,}161435\,) + (237547{,}189319)$$
$$= (493092{,}311065).$$

Paso 6. Se unen los resultados obtenidos en los pasos 4 y 5 para que la pareja de coordenadas quede como: $(\,(45235{,}155942)\,, (493092{,}311065)\,)$.

Repetimos estos pasos para cada uno de los caracteres restantes, obteniendo los siguientes resultados

Coordenadas Asignadas	k
(45235,155942,493092,311065)	205887
(464947,454208,261541,436656)	425387
(1424,194779,211919,45374)	294652
(91384,133847,124363,495034)	258306
(22940,216821,391383,182458)	99447
(30055,298941,323275,69773)	340580
(220188,341581,147194,45165)	162281
(254288,121557,358833,451256)	470133
(310143,142529,222099,59930)	92723



Conclusiones

- Se muestran los conceptos matemáticos para la realización de los algoritmos de cifrado y descifrado usando criptografía en curvas elípticas.
- Dado que actualmente las plataformas móviles o web recaban mucha información confidencial, se observó la necesidad de aportar un método de cifrado de esta información para que no pueda ser utilizada de manera incorrecta. Al hacer uso de una programación en PHP, se propone una librería que puede ser implementada para estos propósitos.
- La dificultad que se presenta es la de calcular el número de puntos que contiene una curva elíptica, para ello será necesario establecer la programación adecuada para que logremos contar con este dato de una manera eficiente y poder trabajar con valores de números primos aún más grandes. Es por ello que, como trabajo a futuro se pueda realizar la implementación del algoritmo de Schoff para este propósito.

Referencias

- Amalraj, J., Raybin, J. (2016). A survey paper on cryptography techniques. IJCSMC, Vol. 5, Issue 8, 55 – 59.
- Diffie, W. & Hellman, M. (1976). New directions in cryptography. IEEE transactions on Information Theory, 22(6), 644-654.
- ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE transactions on information Theory, 31, 469-472
- Gómez, J. (2002). Criptografía y curvas elípticas. La Gaceta de la RSME, Vol. 5, 737-777.
- Granados, G. (2006). Introducción a la criptografía. Revista Digital Universitaria, Vol. 7, No. 7, 1-17.
- Gupta, V., Stebila, D. y Chang, S. (2004). Integrating Elliptic Curve Cryptography into the Web's Security Infrastructure. Sun Microsystems, Inc., 402-403.
- Hankerson, D., Menezes, A. and Vanstone, S. (2004). Guide to Elliptic Curve Cryptography. Springer-Verlag New York, Inc.
- Koblitz, N. (1987). Elliptic curve in cryptography. American Mathematical Society J. Comput. Math., 207–209.
- Miller, V. S. (1986). Use of elliptic curves in cryptography. In Lecture notes in computer sciences; 218 on Advances in cryptology. CRYPTO 85, USA. Springer-Verlag New York, Inc., 417– 426,
- Kawahara, Y. Takagi, T. and Okamoto E. (2006). Efficient Implementation of Tate Pairing on a Mobile Phone Using Java. In Computational Intelligence and Security, vol. 2, 1247 - 1252, Berlin.
- Katz, J., Lindell, Y. (2015) Introduction to Modern Cryptography. NY: Chapmann & Hall Book/CRC.
- Schoff, N. (1995). Counting points on elliptic curves over _finite _fields, Journal de Théorie des Nombres de Bordeaux 7, 219-254.

ECORFAN®