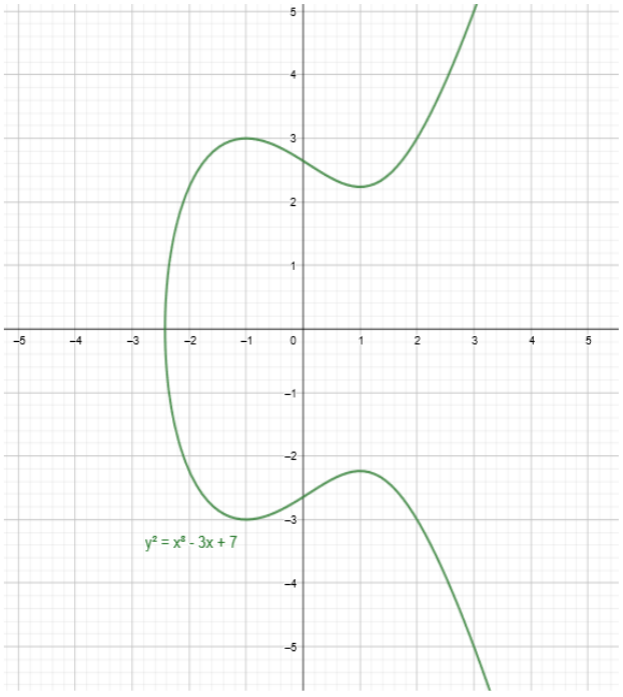
Las Curvas Elípticas y La Criptografía



$$y^2 = x^3 + 5x + 28$$

Pseudònim: Turing

Contenido

Abreviaciones

Las abreviaciones mostradas a continuación han sido usadas para facilitar la lectura de la monografía:

- A.Mod Aritmética Modular
- AEE Algoritmo Extendido de Euclides
- AES Sistema de Encriptación Avanzada (Advanced Encryption System)
- DHEC Protocolo de Intercambio de Claves Diffie-Hellman en Curvas Elípticas
- EC Curva/s Elíptica/s
- ECC Criptografía en Curvas Elípticas (Elliptic Curve Cryptography)
- ECDSA Algoritmo para el Criticado de llave con Curvas Elípticas (Elliptic Curve Digital Signature Algorithm)
- Kpriv Clave privada
- Kpúb Clave pública
- NIST Instituto Naciona de Seguridad y Tecnología de los E.E.U.U (National Institut of Security and Technology)
- NSA Agencia de Seguridad Nacional de los E.E.U.U. (National Security Agency)
- P.G. / G Punto Generador
- RSA Protocolo de Intercambio de Claves RSA (Rivest – Shamir – Adleman)

Índice de Tablas, Gráficos e Ilustraciones

Introducción

En esta monografía se va explorar la criptografía desde un punto de vista matemático siguiendo la siguiente pregunta: ¿Hasta qué punto el uso de las Curvas Elípticas y la Matemática Modular (Protocolo Diffie-Hellman en Curva Elípticas) son un sistema más eficiente en comparación el RSA? Esta pregunta es planteada debido a la predominancia del sistema criptográfico RSA en la mayoría de ámbitos tecnológicos[1]. Sin embargo, la Criptografía en Curvas Elípticas (ECC) ha sido utilizada ya en servidores de Internet como Google Inc., Bitcoin o la NSA (National Security Administration)[2].

El objetivo de este estudio es comparar cuál de ambos sistemas es el más eficiente teniendo en cuenta la longitud de clave, cuál es su ratio de aumento al exigir más seguridad y cuáles son las implicaciones de estos parámetros a la eficiencia del sistema criptográfico. La hipótesis inicial sugería que ECC es mejor sistema en términos de seguridad, pero no de eficiencia, ya que como se ha explicado, en ámbitos de mucha seguridad sí se utiliza, pero en contextos donde no se requiere tanta se sigue usando RSA. Esto hace pensar que RSA es más eficiente ya que si no predominaría ECC.

Como es una investigación matemática se plantearán inicialmente las Curvas Elípticas como concepto matemático, estudiando sus propiedades y cómo se define un grupo abeliano con ellas. A continuación, se introducirán aquellos aspectos necesarios de la matemática modular para entender el funcionamiento de la criptografía. Con ambos conceptos se explicará el Protocolo de Intercambio de Claves Diffie-Hellman en Curvas Elípticas, el cual llevará a estudiar las Curvas Elípticas dentro de la matemática modular. Posteriormente, se describirá el Protocolo de Intercambio de Claves RSA, que requiere de la matemática estudiada y plantea un esquema diferente. Para entenderlos mejor se dará un ejemplo de los protocolos de forma didáctica. Finalmente se destacarán el principal punto débil de la Criptografía en Curvas Elípticas y sus ventajas respecto al RSA,

[1] Olenski, Julie. «ECC 101: What is ECC and why would I want to use it?» 29 de May de 2015. Artículo. 27 de Setiembre de 2018. <https://www.globalsign.com/en/blog/elliptic-curve-cryptography/>.

[2]Sullivan, Nick. «A (relatively easy to understand) primer on elliptic curve criptography.» *arstechnica* (2013). Artículo Digital. 22 de Setiembre de 2018. <https://arstechnica.com/information-technology/2013/10/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/3/>.

Frenkel, Edward. «How did the NSA hack our email?» 22 de Deciembre de 2013. Vídeo Didactico. 27 de Junio de 2018. <https://www.youtube.com/watch?v=ulg_AHBOIQU>.

Ryckwalder, Eric. *The Math Behind Bitcoin*. 19 de Octubre de 2014. Artículo. 27 de Setiembre de 2018. <https://www.coindesk.com/math-behind-bitcoin/>.

según los parámetros ya descritos. Además, hay una introducción a la criptografía al inicio y unas conclusiones finales.

Durante las diferentes secciones en las que se divide la monografía, se hará uso de ecuaciones matemáticas, definiciones y teoremas, así como ejemplos y observaciones de relevancia, usando un formato matemático. Las herramientas usadas han sido Microsoft Excel y Geogebra, ejemplificando algoritmos y representado curvas. Las principales fuentes secundarias de información son trabajos y teoría de nivel universitario, docencias grabadas y distribuidas en Internet, además de libros especializados.

Por último, el valor de esta investigación está en que se extraerán conclusiones de relevancia actual, en una sociedad que comparte tantos datos continuamente y donde buscar una mayor eficiencia en este proceso beneficiará a nuestro planeta, al ahorrar en recursos naturales. Determinar cuál sería el sistema más eficiente y seguro permitirá entender la tendencia actual hacia la criptografía en curvas elípticas, aparte de ver cómo las matemáticas tienen una clara aplicación real y de importancia para todos.

SECCIÓN 1: Criptografía

La criptografía es la ciencia que estudia el cifrado y descifrado de un mensaje con el objetivo de mantener seguro y secreto el mensaje para el emisor y el receptor/es. Esta ciencia se remonta hasta la época romana hasta nuestros días[3], la cual es básica para permanecer secreto nuestros datos cuando usamos Internet, el correo electrónico o hacemos E-commerce.

Tipos de Claves

Para realizar una comunicación entre dos usuarios (persona humana o servidor), es necesario establecer un protocolo de actuación. Este protocolo puede ser de clave privada o pública:

Clave Privada/Simétrica

El usuario emisor cifrará el mensaje mediante un algoritmo de encriptación que usará una clave única para ese cifrado en concreto. El mensaje será enviado mediante un canal de comunicación (Internet) hasta el receptor. Éste se encargará de aplicar un algoritmo de desencriptación que solo dará el mensaje aplicando la misma clave utilizada por el emisor.

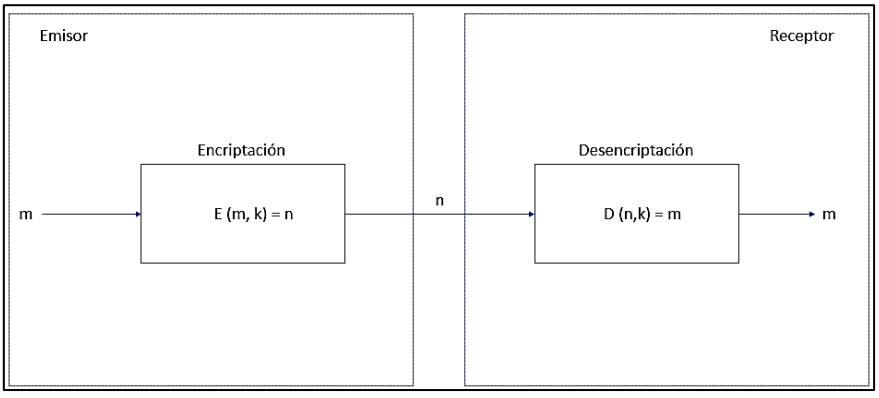


Ilustración 4: Encriptación Simétrica

Como vemos, hay una simetría en el protocolo y se caracterizan por ser altamente seguros y rápidos.

[3] Paar, Christof y Jan Pelzl. *Understanding Cryptography: A Textbook for Students and Practisioners*. Londres: Springer, 1998. Libro.

Clave Pública/Asimétrica

Para los protocolos de clave pública, tenemos el mismo esquema, con la dificultad de que los usuarios no pueden acordar cual es la clave que se utilizará. Sin embargo, en la década de los 70, se obtuvo la solución: el cifrado asimétrico. Ambos usuarios tendrán dos pares de claves diferentes: usuario A tiene clave privada A y la clave pública; mientras que el usuario B tiene la clave privada B y la clave pública. La clave pública permite encriptar el mensaje, pero solo mediante una de las dos privadas, se puede desencriptar el mensaje. Por tanto, el emisor cifrará con la clave pública y el receptor descifrará con su clave privada.

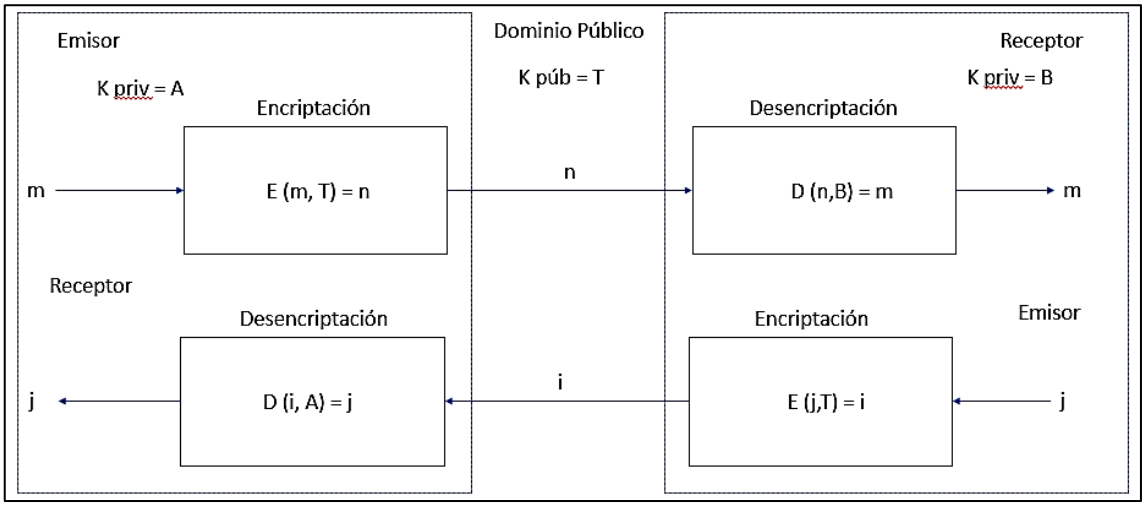


Ilustración 5: Encriptación Asimétrica

El espacio central es el dominio púbico y es accesible a cualquiera de la red. Por este motivo es importante asegurar que este esquema se repite sin alteraciones de terceras personas. Por ello, se utilizarán certificados de usuario, de clave de seguridad y de mensaje; habiendo entidades que los subministran.

Por último, los protocolos asimétricos requieren un intercambio de claves, lo cual será el objeto de estudio en esta monografía. Estos intercambios de clave son una Función Hash:

- La función tiene una inversa ineficiente para la computación (única dirección)
- Dos valores de entrada no pueden dar un mismo resultado (fenómeno conocido como colisión)

Es básico que se cumplan estas condiciones para propiciar una buena comunicación.

SECCIÓN 2: Curvas Elípticas

Uno de los campos de mayor interés en las matemáticas es la Geometría Algebraica, la cual hace un estudio de expresiones algebraicas relacionándolas con conceptos de geometría. Una parte importante de su estudio son las curvas planas, y en especial: la **curva elíptica (EC)**.

2.1. Expresión Matemática de una Curva Elíptica

Una EC viene definida sobre un cuerpo[4] $\mathbb{K}$ mediante lo que se conoce como:

Ecuación de Weierstrass en el plano afín[5]:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (1)$$

con $a_1, \ldots, a_6 \in \mathbb{K}$

2.2. Ecuación de la Curva Elíptica en Criptografía

Cuando el cuerpo elegido tiene una característica[6] de cuerpo distinta a 2 y 3 (denotado como car($\mathbb{K}$) ≠ 2, 3) se puede simplificar la ecuación (1)[7]. Primero se divide por 2 y se completa cuadrados; y a continuación se realiza un cambio de variable para dar paso a una versión más conocida de la ecuación de una EC:

> **Definición 1 (Curva elíptica)** *(Sesma)***:** *Sea $\mathbb{K}$ un cuerpo, con car($\mathbb{K}$) ≠ 2, 3, la curva elíptica E definida sobre $\mathbb{K}$ en el plano afín $\mathbb{A}$ viene definida por:*
>
> $$E(\mathbb{K}) = \{(x, y) \in \mathbb{A}^2_{\mathbb{K}} \mid y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\} \qquad (2)$$
>
> *donde A y B son constantes que pertenecen a un cuerpo $\mathbb{K}$ y $\mathcal{O} \coloneqq (0 : 1 : 0)$*

[4] Un cuerpo $\mathbb{K}$ es un conjunto de elementos con unas operaciones definidas, y en concreto, con la operación multiplicación conmutativa. Fuente: Román, Juan de Burgos. MATEMÁTICAS II Definiciones, Teoremas y Resultados Segunda Edición. Madrid: García-Maroto Editores, S.L, 2010. Libro Impreso.

[5] García, Sara N. Matheu. «Curvas Elípticas.» Trabajo de Final de Grado. Universidad de Murcia, 2015. Documento. 19 de Junio de 2018. <https://www.um.es/documents/118351/1884002/TFG_MATHEU+GARCIA.pdf/0f3f6eb9-5ef7-4483-b41f-525bf7ef1160>.

[6] La característica de cuerpo $\mathbb{K}$ es aquel número entero positivo n tal que: $1 \oplus \overset{n}{\ldots} \oplus 1 = 0$
Si existe tal entero positivo, se dice que éste es la característica de $\mathbb{K}$; por el contrario, si no existe, entonces la característica de $\mathbb{K}$ es 0. Fuente: Ibid (Román)

[7] Ver en el anexo la transformación de la ecuación (1) a (2) en el Documento 1: Transformación de la ecuación de Weiertrass a simplificada.

2.2.1. Elemento Neutro

Una EC forma un grupo abeliano el cual se define como:

> **Definición *2 (*Grupo Abeliano*)*** *(Román): Sea* $\mathbb{G}$ *un grupo con un conjunto de elementos y unas operaciones definidas (suma o multiplicación) que cumplen con la propiedad conmutativa y asociativa.*

Para que sea posible cumplir con esta propiedad, es necesario un elemento neutro para la suma tal que:

$$a + 0 = a$$

Como en EC, la suma de puntos sigue unas operaciones distintas al cuerpo de los $\mathbb{K}$ (ver en Suma de Puntos), es necesario el uso de un punto en el infinito $\mathcal{O}$, al cual llamamos **elemento neutro**, situado en el infinito en el eje de las ordenadas y confirmará esta propiedad.[8][9]

2.2.2. Simetría

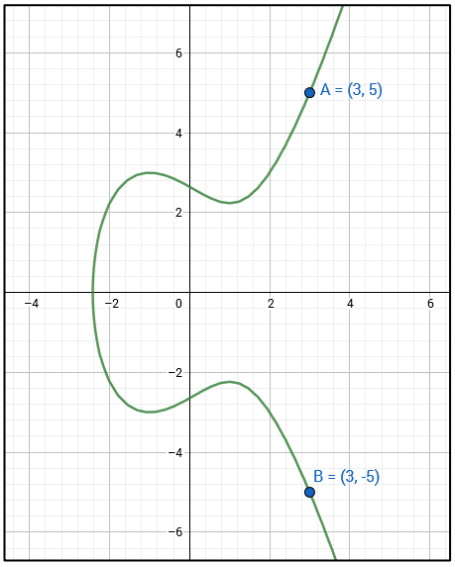
Una de las principales propiedades de las EC es su simetría respecto al eje x, ya que permite operar con las propiedades de un grupo abeliano. Esta simetría sucede por lo siguiente:

$$(y)^2 = y^2 \qquad (-y)^2 = y^2 \qquad y = \pm\sqrt[2]{x^3 + Ax + B}$$

[8] Existen otras explicaciones para la existencia de un elemento neutro/punto en el infinito, pero se cree que está es la de mejor comprensión:

- Ibid (García)
- L, Delgado, Vallejo R. y Mutis W. & Castillo J. «Estructura de Grupo de las Curvas Elípticas.» *Revista Sigma, Universida de Nariño* (2009): 20-37. Artículo. 19 de Junio de 2018. <https://www.researchgate.net/publication/28296289_La_Estructura_de_Grupo_de_las_Curvas_Elipticas>.

[9] En el Anexo 1: Puntos Singulares: Nodos y Cúspides se pueden encontrar otras propiedades importantes.



Ejemplo:

$$y^2 = x^3 - 3x + 7$$

Para *x = 3*

$$y = \pm\sqrt[2]{3^3 - 3 \cdot (3) + 7}$$

$$y = +5$$

$$y = -5$$

Gráfico 1: Simetría respecto al eje X

2.2.3. Discriminante y j-invariante

El discriminante es una propiedad de cada curva que nos indica como son las raíces de la ecuación, dependiendo del valor que el discriminante tome (Rotger y Ayuso):

$$\Delta = 4A^3 + 27B^2$$

- Si Δ = 0 existen raíces múltiples.
- Si Δ = 0 y A = 0 la $E(\mathbb{K})$ tiene un punto singular cúspide.
- Si Δ = 0 y A ≠ 0 la $E(\mathbb{K})$ tiene un punto singular nodo,

El j-invariante es aquella propiedad de la ecuación de una $E(\mathbb{K})$ para saber que dos EC pueden ser la misma si se realiza cambios de variable. En caso de tener diferente *j*-invariante seguro que son diferentes. Se calcula a continuación (Sesma):

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}$$

Y en caso de coincidir se realiza el siguiente Teorema:

> **Teorema 1** *(Sesma): Sean* $E_1(\mathbb{K})$ ***y*** $E_2(\mathbb{K})$ *dos curvas con* j_1 *y* j_2 *respectivamente. Si* $j_1 = j_2$ *entonces existe* $\mu \neq 0 \in \mathbb{K}$ *tal que:*
>
> $$A_2 = \mu^4 A_1 \qquad B_2 = \mu^6 B_1$$

2.3. Operaciones con las Curvas Elípticas

Las EC forman un grupo abeliano como ya se ha descrito anteriormente, donde sus elementos se conocen como **puntos racionales** y sus operaciones son **la suma** y la **multiplicación escalar** (la suma k-repetida del mismo punto racional).

2.3.1. Suma de Puntos

La suma de puntos tiene forma analítica[10]:

i) Trazar una secante entre dos puntos

ii) Encontrar el 3r punto de intersección entre la secante y $E(\mathbb{K})$

iii) Hacer reflexión del punto respecto eje de las abscisas

Sabemos que hay tres puntos de intersección con la siguiente demostración:

$$Ecuación\ de\ \mathbb{E}: y^2 = x^3 + Ax + B$$
$$Ecuación\ de\ la\ recta: y = mx + n$$

Por tanto:

$$(mx + n)^2 = x^3 + Ax + B$$
$$(m^2x^2 + 2mnx + n^2) = x^3 + Ax + B$$
$$0 = x^3 + m^2x^2 + (2m + A)x + B + n^2$$

Siendo la solución una ecuación de tercer grado, con 3 soluciones donde la curva y la recta intersecan.

También se puede realizar mediante unas expresiones algebraicas cumpliendo la siguiente proposición:

Proposición 1 *(Sesma): Sean P = (x_1, y_1) y Q = (x_2, y_2) dos puntos racionales de $E(\mathbb{K})$ y sea F = P + Q = (x3, y3):*

- $Si\ x_1 \neq x_2\ entonces \begin{cases} x_3 = m^2 - x_1 - x_2 \\ y_3 = m(x_1 - x_3) - y_1 \end{cases} \quad con\ m = \frac{y_2 - y_1}{x_2 - x_1}$

- $Si\ x_1 = x_2\ e\ y_1 \neq y_2\ entonces\ P + Q = \mathcal{O}$

Ejemplo: *Sea la curva $y^2 = x^3 - 3x + 7$ y P = ($\sqrt{5}$, -2) y Q = (3, 5). Ahora P + Q = F:*

$$m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{5 - \sqrt{5}}{3 - (-2)} = 1 - \frac{\sqrt{5}}{5}$$

[10] Sesma, Iciar. *Criptografía en Curvas Elípticas*. Trabajo de Final de Grado. Logroño, 2015. Documento. 19 de Junio de 2018. <https://biblioteca.unirioja.es/tfe_e/TFE001034.pdf>.

$$\begin{cases} x_3 = m^2 - x_1 - x_2 = \left(1 - \frac{\sqrt{5}}{5}\right)^2 - (-2) - 3 \approx -0{,}69 \\ y_3 = m(x_1 - x_3) - y_1 = \left(1 - \frac{\sqrt{5}}{5}\right)\left((-2) - 3\right) - \sqrt{5} \approx -2{,}96 \end{cases}$$

Por tanto, F = (-0,69; -2,96)

De forma analítica observamos la segunda parte de la proposición:

$$- \; Si \; x_1 = x_2 \; e \; y_1 \neq y_2 \; entonces \; P + Q = \mathcal{O}$$

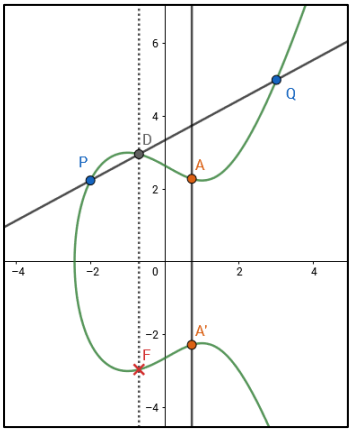


Gráfico 2:Suma de Puntos

A = (0,73; 2,28) y A' = (0,73; -2,28) cumplen con ambas igualdades, por lo que su suma es el elemento neutro o suma. Esto es porque el segmento que une los dos puntos, no corta por otro 3r punto de la curva que no sea el elemento neutro.

Antes de continuar veamos cómo se cumple la siguiente proposición:

> **Proposición 2** *(Sesma)*: *La suma de puntos definida sobre una EC descrita anteriormente, forma un grupo abeliano, ya que cumple con:*
>
> - *Conmutatividad:* $P_1 + P_2 = P_2 + P_1$
> - *Elemento Neutro:* $P + \mathcal{O} = P$
> - *Elemento Inverso:* $P + P' = \mathcal{O}$, *siendo* $P' = -P = (x, -y)$
> - *Asociatividad:* $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$

2.3.2. Multiplicación Escalar

La operación más utilizada en criptografía es la multiplicación escalar, la cual consiste en multiplicar un escalar por un punto. Por ejemplo: 2 · P = P + P. Por tanto, el escalar dice cuántas veces debe sumarse un mismo punto. Para hacerlo, hay un método analítico[11]:

i) Trazar la recta tangente al punto, por este motivo no puede ser una recta singular

ii) Encontrar el segundo punto de intersección entre la tangente y $E(\mathbb{K})$

iii) Hacer reflexión del punto respecto eje de las abscisas

Y también otro algebraico que se utiliza una segunda proposición:

Proposición 3 *(Sesma): Sean P = (x_1, y_1) un punto racional de $E(\mathbb{K})$ y sea*

F = 2 · P = P + P = (x_2, y_2)

$$-Si\ x_1 = x_2\ e\ y_1 = y_2\ \ entonces \begin{cases} x_2 = m^2 - 2x_1 \\ y_2 = m(x_1 - x_3) - y_1 \end{cases} \quad con\ m = \frac{3x_1^2 + A}{2y_1}$$

Ejemplo:

$$m = \frac{3x_1^2 + A}{2y_1} = \frac{3 \cdot 3^2 + (-3)}{2 \cdot 5} = 2{,}4$$

$$x_2 = m^2 - 2x_1 = 2{,}4^2 - 2 \cdot (3) = -0{,}24$$
$$y_2 = m(x_1 - x_2) - y_1 = (2{,}4)\big(3 - (-0{,}24)\big) - 2 = 2{,}78$$

Por tanto, F = 2 · P = (-0,24; 2,78)

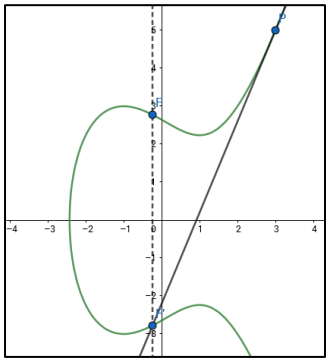


Gráfico 3: Multiplicación de un punto por el escalar 2

[11] Ibid (Sesma)

Para usar la multiplicación escalar, es necesario hacer uso de las 2 proposiciones anteriores, alternándolas para conseguir sumar el punto P las n veces requeridas. Uno método de hacerlo es mediante el siguiente lema:

> **Lema 1** *(Sesma)**: Sean P = (x_1, y_1) un punto racional de $E(\mathbb{K})$ y sea k ∈ $\mathbb{N}$, el procedimiento para calcular kP (multiplicación escalar) sea:*

1. *Se crean tres variables: a, Q_1 y Q_2. Se les asignará el valor de k, elemento neutro (**$\mathcal{O}$**) y P respectivamente*
2. *Evaluamos si el valor de a es par o impar.*
   - *Si a es par, asignamos $a = \frac{a}{2}, Q_1 = Q_1$ y $Q_2 = 2Q_2$*
   - *Si a es impar, asignamos $a = a - 1, Q_1 = Q_1 + Q_2$ y $Q_2 = Q_2$*
3. *Si a ≠ 0 volver al paso 2 con los nuevos valores*
4. *Si a = 0 entonces kP = Q_1*

Para demostrar este lema, se ha diseñado un algoritmo con el programa Excel, disponible en:

https://drive.google.com/file/d/1BC6gQyBXkaKJSUvKGD5hu7QEhpgJfZGk/view?usp=sharing

Ejemplo: Sea P = (3, 5) perteneciente a $E(\mathbb{K})$ definida por: $y^2 = x^3 - 3x + 7$ y realice la siguiente operación de grupo: 5P.

Con el Algoritmo[12]:

	k	P			A
INTRODUCE VALUES		x	y		
	7	3	5		-3

Tabla 1: Valores de Entrada del Algoritmo 1

[12] En el link con partido se puede observar este algoritmo y otros, la descripción de todo el documento está en el Anexo 1: Excel de Algoritmos

ALGORITHM	A	Q1	Q1	Q2	Q2
		X	Y	X	Y
Step 1-Asign Values	7	i	i	3	5
Step2- Proceed	6	3	5	3	5
Step 3 - Avaluation	Continue	Continue	Continue		
Step2- Proceed	3	3,00	5,00	-0,24	2,78
Step 3 - Avaluation	Continue	Continue	Continue		
Step2- Proceed	2	-2,29	-1,37	-0,24	2,78
Step 3 - Avaluation	Continue	Continue	Continue		
Step2- Proceed	1	-2,29	-1,37	0,74	-2,28
Step 3 - Avaluation	Continue	Continue	Continue		
Step2- Proceed	0	1,64	2,55	0,74	-2,28
Step 3 & Step 4 - The answer point is in the previous step	DONE	Above Cell is X value	Above Cell is Y value		

Tabla 2:Ejecución del Algoritmo 1

Analíticamente:

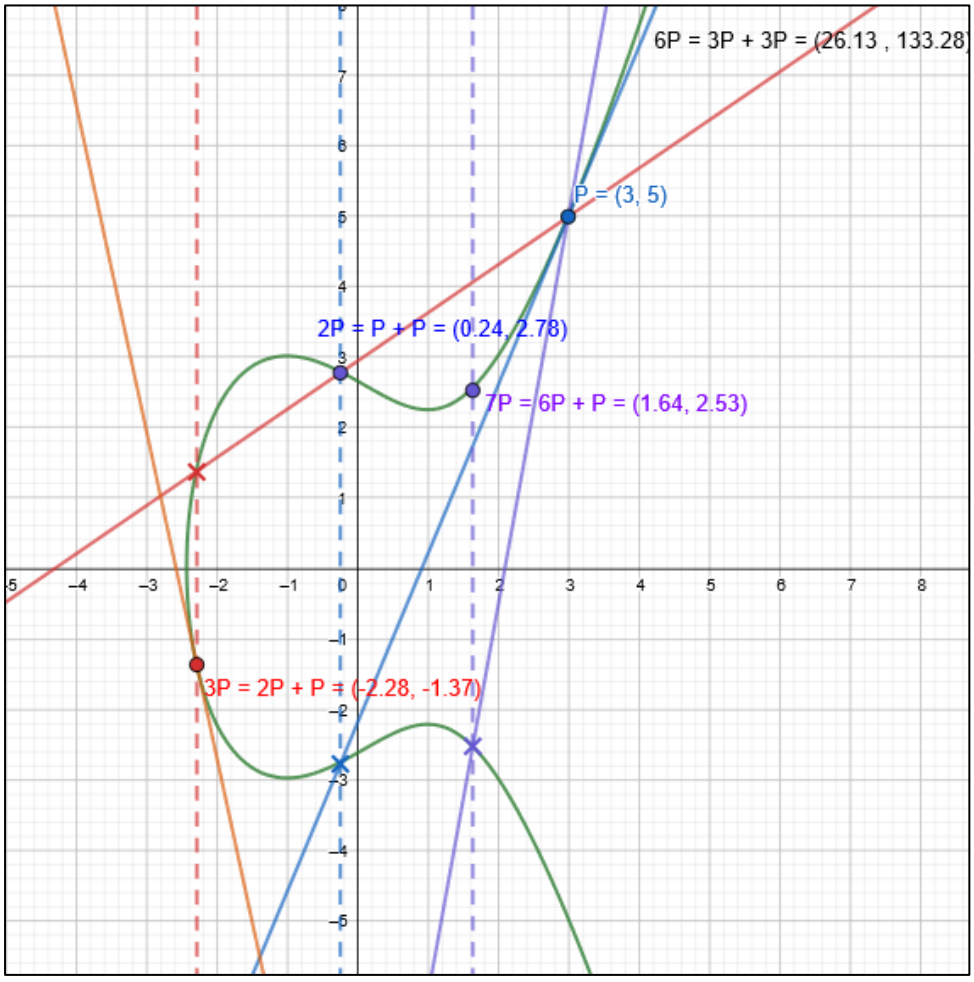


Gráfico 4: Multiplicación de un punto por el escalar 7

SECCIÓN 3: Matemática Modular

En criptografía y computación uno de los principales problemas es que cuerpos como los números reales o raciones son infinitos. Por este motivo, se trabaja con conjuntos cerrados de elementos, finitos; sin embargo, los números siguen siendo infinitos. Como solución, la aritmética modular (A.Mod) proporciona un sistema donde cualquier número queda representado en un grupo.

3.1. Funcionamiento

La A.Mod se define dentro de un conjunto $\mathbb{Z}_m$:

> **Definición *3* (Conjunto)** *(Aritmética Modular)*: *Sea* $\mathbb{Z}_m$ *un conjunto definido por números enteros empezando por el 0 y siendo el último m-1:*
>
> $$\mathbb{Z}_m = \{0, 1, 2, 3, \dots, m-1\}$$
>
> **El conjunto* $*_{\mathbb{Z}_m}$ *excluye el 0.*

m establecerá la relación entre los elementos del conjunto y el conjunto de números enteros ($\mathbb{K}$) mediante la siguiente relación:

> **Proposición 4** (Aritmética Modular): Sea $\mathbb{Z}_m$ un conjunto cerrado, D y q números entero cualquieras, y r un elemento de $\mathbb{Z}_m$ tal que:
>
> $$D = m \cdot q + r \qquad D \equiv r \; mod(m)$$
>
> Apareciendo un nuevo operador llamado modular y estableciendo que un número entero D es congruente al número r en módulo m.

Ejemplo:

$$19 = 17 \cdot 1 + 2 \qquad 19 = 2 \; mod \; (17)$$

$$35 = 7 \cdot 5 + 0 \qquad 35 = 0 \; mod \; (7)$$

Observamos en el último ejemplo como el elemento 0 es congruente a cualquier múltiplo de m.

3.1.1. Suma

En A.Mod podemos realizar la operación de la suma como en la aritmética lineal, buscando un elemento congruente al resultado final:

$$30 + 33 = 63 \equiv 12\ mod\ (17)$$

$$35 + 17 = 52 \equiv 1\ mod\ (17)$$

3.1.2. Multiplicación y División

La multiplicación se comporta de la misma forma que la suma, pero para que siga siendo conmutativa y asociativa, siendo un grupo abeliano es necesario estudiar el elemento inverso. Se dice que todo número tiene su inverso, el cual al multiplicarse ambos, el resultado es 1, siendo este el elemento neutro de la multiplicación:

Elemento Inverso $7 \cdot 3 = 42 \equiv 1\ mod\ (17)$

Elemento Neutro $7 \cdot 1 \equiv 7\ mod\ (17)$

Como observamos, dos números enteros positivos, al ser multiplicado da 1. Denotaremos al inverso modular como a^{-1} y por tanto:

$$a \cdot a^{-1} = 1\ mod\ (m)$$

Y al ser conmutativo, propiedad de grupo abeliano:

$$a \cdot b = 1 = b \cdot a \quad por\ tanto\ a^{-1} = b \quad y \quad b^{-1} = a$$

A esta manera de operar la llamaremos división y para encontrar cualquier inverso de un elemento, debemos hacer uso del Algoritmo Extendido de Euclides 7(AEE)[13].

$$\frac{12}{12}\ mod(53) = 12 \cdot 12^{-1} \equiv 1\ mod\ (53) \rightarrow 12 \cdot x \equiv 1\ mod\ (53) \rightarrow \overbrace{x = 31}^{A.E.E}$$
$$\rightarrow 12 \cdot 31 \equiv 1\ mod\ (53)$$

[13] Ver el Algoritmo en Anexo 1: Documento 2: Algoritmo Extendido de Euclides

Alguna de las características básicas para que se cumpla esta operación es y sea un anillo conmutativo[14]:

- El máximo común divisor de un elemento y *m* debe ser 1: mcd (a, m) = 1
    - Por tanto, para que todos los elementos tengan inverso, ***m* debe ser primo**.
        - Por consecuencia, si en ECC necesitamos grupo abelianos, se va a trabajar con grupos circulares primos $\mathbb{Z}_p$.

[14] Ver definición en Anexo 2: Documento 4: Definiciones

SECCIÓN 4: Protocolo Diffie Hellmann en Curvas Elípticas

A continuación, se mostrará cómo se combinan las dos secciones anteriores para generar el Protocolo Diffie-Hellmann en Curvas Elipticas (ECDH).

4.1. Elementos

Parámetros de la Ecuación

Para el intercambio de claves, se utiliza una curva con la siguiente ecuación:

> ***Definición* 3** (Sesma)**:** Sea una curva $\mathbb{E}$ formada sobre un campo $\mathbb{Z}_p$, está formada por el conjunto de elementos (x, y) ∈ $\mathbb{Z}_p$, tales que:
>
> $$E(\mathbb{Z}_p) = \left\{(x, y) \in \mathbb{A}^2_{\mathbb{Z}_p} \;\middle|\; y^2 = x^3 + Ax + B \; mod\; (m)\right\} \cup \{\mathcal{O}\} \qquad (3)$$
>
> donde $A, B \in \mathbb{Z}_p$ y cumple con $4 \cdot A^3 + 27 \cdot B^2 \neq 0 \; mod\; (m)$

Recordemos que el punto en el infinito ($\mathcal{O}$) sirve para cumplir con las características de grupo y se decide de forma arbitraria.

Para ver un ejemplo de la nueva definición, se toma los parámetros: A= -3, B= 7 y p = 17.

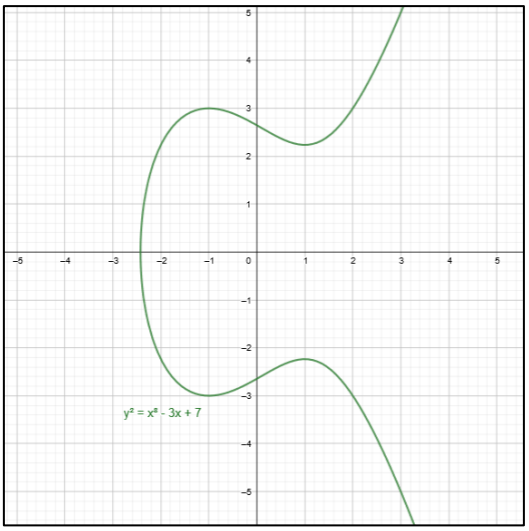


Gráfico 5: EC sobre los números Reales

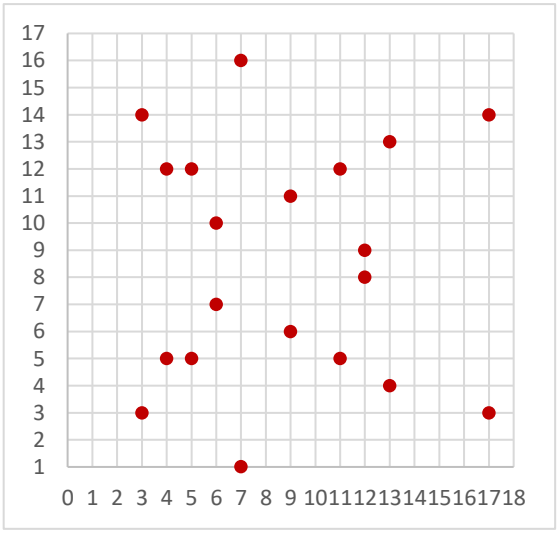


Gráfico 6: EC sobre el conjunto $\mathbb{Z}_{17}$. [17]

En ambos casos se conservará una simetría, sobre el eje x ó sobre y = 8,5.

[15] Definida sobre $\mathbb{Z}_{17}$**,** con un total de 20 puntos más el punto en el infinito, es decir: 21.

Para conocer el total de puntos de una EC, denotados como $\#E$, que será crucial conocerlo para determinar la seguridad de una curva, se puede computar, en caso de que sean parámetros pequeños, pero normalmente se usará el Teorema de Hasse:

> ***Teorema 2 (Teorema de Hasse)*** (Tolkov) *y* (Gee)*:* Sea una curva $\mathbb{E}$ formada sobre un campo $\mathbb{Z}_p$, está formada por el conjunto de elementos (x, y) ∈ $\mathbb{Z}_p$, el total de elementos se define entre los siguientes límites:
>
> $$p - 2\sqrt{p} < \#\mathbb{E} < p + 2\sqrt{p}$$
>
> Reestructurado posteriormente como:
>
> $$|\#E - (p+1)| \leq 2\sqrt{p}$$
>
> O también:
>
> $$-1 < \frac{N-p}{2\sqrt{p}} < 1$$

Así se puede aproximar entre que valores estará el total de puntos de una curva. Por ejemplo:

Para una curva con los siguientes parámetros: A= -3, B= 7 y p = 17.

$$17 - 2\sqrt{17} < \#\mathbb{E} < 17 + 2\sqrt{17}$$

$$12{,}754 < \#\mathbb{E} < 29{,}246$$

Y como se ha mostrado anteriormente $\#\mathbb{E} = 21$.[16]

Punto Generador

Para trabajar con ECC, se necesita usar un grupo de elementos finitos, a fin de poder computarse en un tiempo razonable. Estos grupos son los llamados grupos cíclicos, los cuales parten de un elemento primitivo, llamado generador (P.G.), y se forma un grupo delimitado con sus operaciones. Por tanto, cualquier elemento de nuestra EC puede ser

[16] Además, es importante que el primo no sea un divisor del discriminante, ya que en el campo definido, el nuevo discriminante sería 0. Por lo que al final se dice que si p|Δ, entonces E tiene una mal reducción a modulo.Fuente: Ibid (Tolkov)

un generador, pero interesa que incluya a todos los puntos de la curva para asegurar mayor seguridad.[17]

Orden del Grupo Cíclico

Una vez escogido el P.G. de la EC que funcionará como elemento primitivo es necesario computar todos sus puntos hasta llegar al punto en el infinito. Para computar el grupo cíclico se utilizará la multiplicación escalar, aplicando A.Mod a cada cálculo.[18]

$$Si\ x_1 \neq x_2\ entonces \begin{cases} x_3 = m^2 - x_1 - x_2\ mod\ (p) \\ y_3 = m(x_1 - x_3) - y_1\ mod\ (p) \end{cases} \quad con\ m = \frac{y_2 - y_1}{x_2 - x_1}\ mod\ (p)$$

$$- Si\ x_1 = x_2\ e\ y_1 \neq y_2\ entonces\ P + Q = \mathcal{O}$$

$$Si\ x_1 = x_2\ e\ \ y_1 = y_2\ \ entonces \begin{cases} x_2 = m^2 - 2x_1\ mod\ (p) \\ y_2 = m(x_1 - x_3) - y_1\ mod\ (p) \end{cases} \quad con\ m = \frac{3x_1^2 + A}{2y_1} mod\ (p)$$

Fijándonos sin embargo en cómo se calcula la m: calculando primero el denominador, y encontrando su inverso con el AEE y multiplicándolo por el numerador.

Cofactor

Es un parámetro usado para determinar la seguridad de la curva e idealmente debería ser 1 y no mayor de 4. Se calcula como (Pierce):

$$Cofactor\ (h) = \frac{\#\ E\ (\mathbb{Z}/\mathbb{Z}_p)}{ord\ (G)}$$

[17] Para escoger el punto generador podemos aplicar el siguiente *Teorema* (Paar y Pelzl, Understanding Cryptography: A Textbook for Students and Practisioners)*:* Los puntos de una curva elíptica junto con el punto en el infinito $\mathcal{O}$ tienen subgrupos cíclicos. Bajo ciertas condiciones todos los puntos de la curva elíptica forman un grupo cíclico. Por tanto, cualquier elemento de nuestra EC puede ser un generador, pero interesa que incluya a todos los puntos de la curva para asegurar mayor seguridad.

[18] Ver como se realiza el cálculo en: Anexo 1: Excel de Algoritmos

Puntos Computados

Por último, será necesario que ambas partes (emisor y receptor) eligen de forma secreta e independiente un entero positivo, el cual será su clave privada. Una vez seleccionado de forma aleatoria, se realiza una multiplicación escalar con este entero y el generador, el cual dará un elemento del grupo cíclico. Ambos enviarán este elemento y será de dominio público. Cada uno cogerá el punto del otro, y lo multiplicará por su escalar, consiguiendo el mismo elemento del grupo cíclico y siendo éste la clave pública.

4.2. Ejemplo

Elijamos el grupo cíclico y los parámetros de la curva

$$\mathbb{Z}/\mathbb{Z}_{13} : \{0, 1, 2, \dots, 12\}$$

$$E\ (\mathbb{Z}/\mathbb{Z}_{13}): y^2 \equiv x^3 - 3x + 7\ \ mod\ (13)$$

Conjunto de Puntos de la Recta:

Para el elemento 0:

x→ $0^3 - 3 \cdot 0 + 7 \equiv 7\ mod\ 13$

y → $0^2 \equiv 0\ mod\ 13$

Para todos los $\mathbb{Z}/\mathbb{Z}_{13}$:

Elementos del Campo: $\mathbb{Z}/\mathbb{Z}_{13}$	$x^3 - 3x + 7\ \ mod\ (13)$	$y^2\ mod\ (13)$	X	Y1	Y2
0	**7**	0			
1	**5**	1			
2	9	4	2	3	10
3	12	9	3	5	8
4	**7**	**3**			
5	0	**12**	5	0	
6	10	10	6	6	7
7	4	10	7	2	11
8	1	12	8	1	12
9	7	3			
10	2	9			
11	5	4			
12	9	1	12	3	10

Tabla 3: Computación de la EC sobre un Grupo Circular[19]

[19] Esta tabla muestra una primera columna con los elementos el anillo usado $\mathbb{Z}/\mathbb{Z}_{13}$, a continuación, se sustituye en las dos siguientes columnas dichos elementos con la operación descrita en el encabezamiento. El color verde indica que el número está en ambas columnas y por tanto creará un punto racional de la EC. Si el color es rojo indica lo contrario. La siguiente columna indica la coordenada *x* del punto racional, el cual es un elemento de $\mathbb{Z}/\mathbb{Z}_{13}$. Las dos siguientes son las coordenadas *y* de dos puntos diferentes que comparten la misma x (debido a la simetría), siendo *y* el elemento de $\mathbb{Z}/\mathbb{Z}_{13}$ que iguala $y^2 \equiv x^3 - 3x + 7\ \ mod\ (13)$, correspondiente a *x*.

Por tanto, los puntos son:

X	Y
2	3
2	10
3	5
3	8
5	0
6	6
6	7

X	Y
7	2
7	11
8	1
8	12
12	3
12	10
$\mathcal{O}$	$\mathcal{O}$

Tabla 4:Puntos Racionales de EC

Un total de 14 puntos ya que añadimos el punto en el infinito, tal y como se definió en la ecuación (2).

Los Puntos de la Curva se representan a continuación:

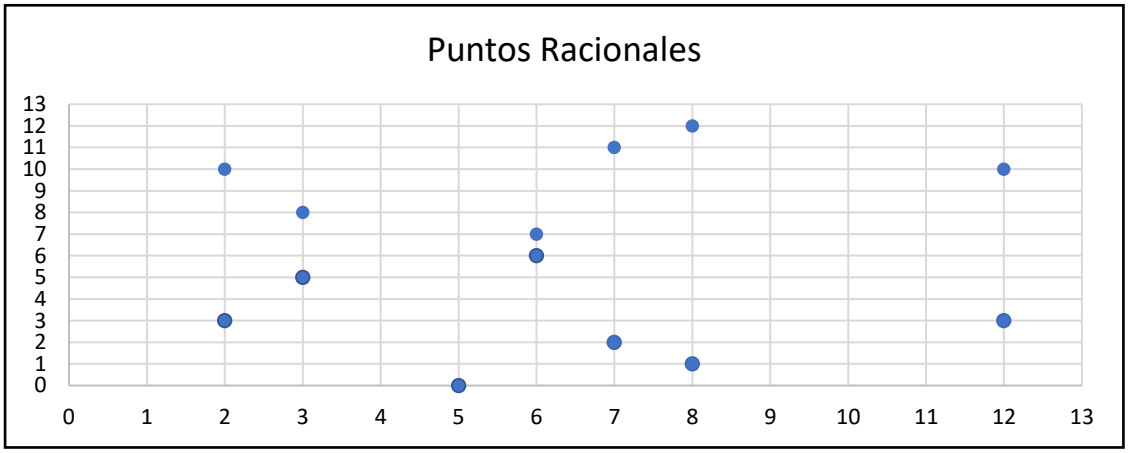


Gráfico 5: Puntos Racionales de EC en el Plano Cartesiano

Ahora necesitaremos crear el grupo cíclico con un generador:

$$G: (12, 3)$$

Para 2G:

$$m = \frac{3x_1^2 + A}{2y_1} \; mod\ (p) = \frac{3 \cdot (12)^2 + (-3)}{2 \cdot 3} \; mod\ (13) = (429) \cdot (6)^{-1} \equiv 0 \cdot 11 \; mod\ (13) \equiv$$
$$\equiv 0 \; mod\ (13)$$

$$x_2 = m^2 - 2x_1 \; mod\ (p) = 0^2 - 2 \cdot (12) \; mod\ (13) \equiv 2 \; mod\ (13)$$

$$y_2 = m(x_1 - x_2) - y_1 \; mod\ (p) = (0)\big(12 - (2)\big) - 3 \; mod\ (13) \equiv 10 \; mod\ (13)$$

$$2G = (2, 10)$$

Siguiendo el Lema 1[20], se computan todos los puntos

	X	Y
G	12	3
2G	2	10
3G	3	5
4G	8	12
5G	7	2
6G	6	6
7G	5	0

	X	Y
8G	6	7
9G	7	11
10G	8	1
11G	3	8
12G	2	3
13G	12	10
14G	$\mathcal{O}$	

Tabla 5:Grupo Cíclico a partir del Punto Generador

Fijase en el punto 14 G, computado del siguiente modo:

$$14G = G + 13G = (12, 3) + (12, 10)$$

Y 13G es (12, 10), el cual puede ser representado como (12, -3) ya que:

$$-3 \equiv 10 \; mod \; (13)$$

Por lo que 13 G = - G, siendo entonces:

$$G + 13G = (12, 3) + (12, 10) = (12, 3) + (12, -3) = G + (-G) = \mathcal{O}$$

Según la propiedad de elemento inverso de un grupo.

A partir de aquí:

$$15G = G + 14G = G + \mathcal{O} = G = (12, 3)$$

$$16G = G + 15G = G + G = 2G = (2, 10)$$

[20] Ver (Sesma) en la sección Multiplicación y División

Formando así un grupo cíclico que represente a cualquier escalar positivo.

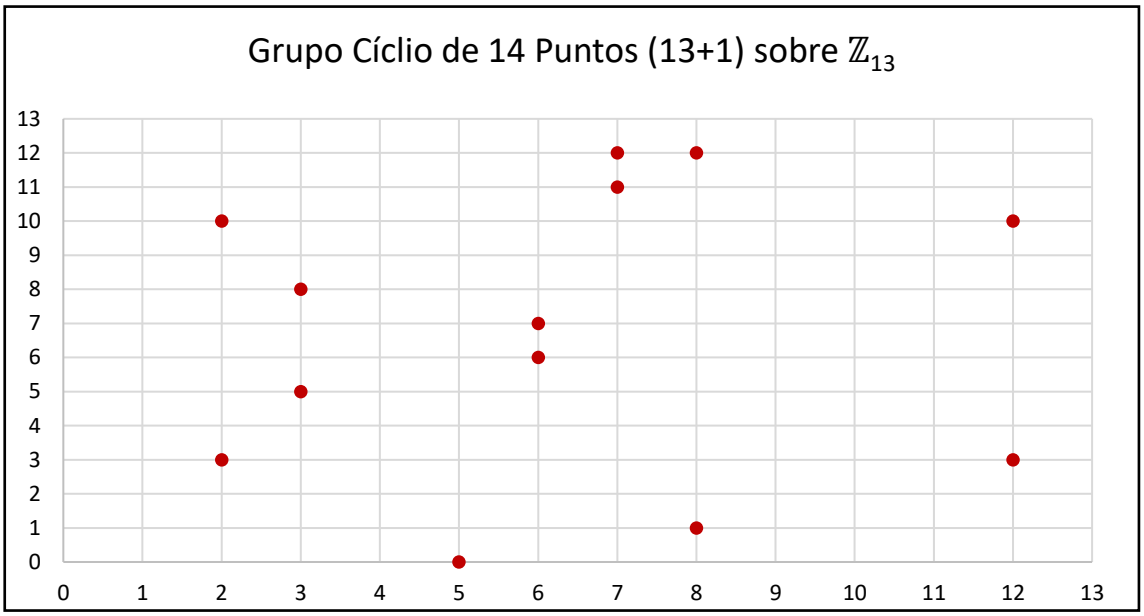


Gráfico 6: Grupo Cíclico del P.G. en el plano cartesiano

Por ahora tenemos:

$$\mathbb{Z}/\mathbb{Z}_{13} : \{0, 1, 2, \dots, 12\}$$

$$E\ (\mathbb{Z}/\mathbb{Z}_{13}) : y^2 \equiv x^3 - 3x + 7\ \ mod\ (13)$$

$$\#\ E\ (\mathbb{Z}/\mathbb{Z}_{13}) = 14$$

$$G : (12, 3)$$

$$ord\ (G) = 14$$

$$Cofactor\ (h) = \frac{\#\ E\ (\mathbb{Z}/\mathbb{Z}_{13})}{ord\ (G)} = \frac{14}{14} = 1$$

Cofactor ideal para el intercambio de claves ECDH.

Veamos ahora como funcionaría en este caso el Protocolo ECDH.

Alice	**Dominio Público**	**Bob**
	Datos Iniciales	
Elección de un escalar para la clave privada (α):	$E: y^2 = x^3 + Ax + B\ mod\ (p)$	**Elección de un escalar para la clave privada (β):**
4	p = 13	12
Computando:	A = - 3	**Computando:**
4G = (8, 12)	B = 7	12G = (2, 3)
	G = (12, 3)	
* * *	n = 14	* * *
Recibe:	h = 1	**Recibe:**
βG = (2, 3)	* * *	αG = (8, 12)
Computa:	Información computada	**Computa:**
$\alpha \cdot \beta G = 4 \cdot \beta G = 4 \cdot (2, 3) = (6, 6)$	αG = (8, 12)	$\beta \cdot \alpha G = 12 \cdot \alpha G = 12 \cdot (8, 12) = (6, 6)$
Clave Pública: (6, 6)	βG = (2, 3)	**Clave Pública:** (6, 6)
	* * *	
	Clave Pública: (6, 6)	

Ilustración 1: Esquema del Protocolo de Intercambio de Claves Diffie-Hellman en Curvas Elípticas

Comprobación:

Alice computa: $\alpha \cdot \beta G = 4 \cdot 12\ G = 48\ \cdot (2, 3) \equiv 6 \cdot (2, 3)\ mod\ (13) = 6G = (6, 6)$

Bob computa: $\beta \cdot \alpha G = 12 \cdot 4\ G = 48 \cdot (2,\ 3) \equiv 6 \cdot (2, 3)\ mod\ (13) = 6G = (6, 6)$

Computando ambos la misma Kpúb

Si alguien quisiera alguna de las claves privadas debería ser capaz de resolver el Problema del Logaritmo Discreto en ECDH:

αG = (8, 12) ó βG = (2, 3)

Para poder descifrar la Kpúb $\alpha\beta G$ =(6, 6)

A partir de aquí, se utilizará algoritmos de encriptación como el AES, ya que aumentará la velocidad de la comunicación, y encriptarán con la Kpúb y desencriptarán con Kpriv

4.3. Problema del Logaritmo Discreto en Curvas Elípticas

La complejidad de todo el protocolo reside en el siguiente problema:

> ***Definición 4*** (Paar y Pelzl, Understanding Cryptography: A Textbook for Students and Practisioners)**:** *Dada la curva elíptica* $E\ (\mathbb{Z}/\mathbb{Z}_m)$*, considere un elemento primitivo (generador) P y otro elemento T. El problema del logaritmo*[21] *discreto reside en encontrar un entero d, que cumpla 1 ≤ d ≤ #E, tal que:*
>
> $$\overbrace{P + P + \cdots + P}^{d} = dP = T$$

Si alguien del dominio público es capaz de encontrar el entero *d*, habrá deducido la clave privada de un usuario, y podrá computar la pública, pudiendo acceder a la información tras aplicar esta clave a los algoritmos de cifrado y descifrado. Debemos tener en cuenta que en dominio público se conoce G (punto generador) y deberá descubrir $\alpha\ o\ \beta$, para calcular una u otra clave privada.[22]

[21] A pesar de no exigir un logaritmo, el nombre es este debido a que el Protocolo Diffie-Hellmman sin curvas elípticas presenta el mismo problema, donde el entero *d* es un exponente y es necesario realizar un logaritmo a un grupo circular. Como ECDH es una variante de este último, se mantiene el nombre.

[22] Hasta hoy, el mejor ataque conocido para desvelar la clave pública es el de Rho Pollard el cual está basado en el algortimo *baby-step giant-step* y los pasos requeridos para su ejecución responden a $\sqrt{m}$, siendo *m* el número primo que creará el grupo cíclico. Fuentes: Ibid (Paar y Pelzl, Understanding Cryptography: A Textbook for Students and Practisioners) y Ibid (Sesma)

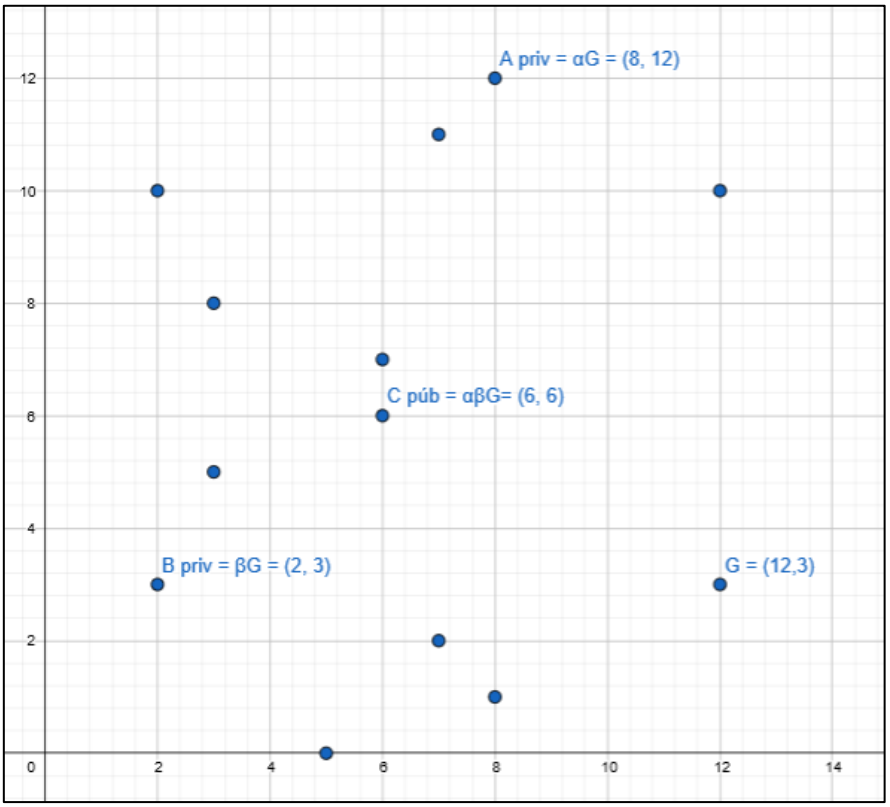


Gráfico 7: Ejemplo del Problema del Logaritmo Discreto

SECCIÓN 5: Comparativa respecto RSA

5.1. RSA y su valor

En 1977 se inventó un algoritmo para clave pública llamado RSA, basado en el problema de factorizar números primos de muchas cifras[23]. Como en el protocolo anterior, el algoritmo generará una clave pública y una clave privada.

Los primeros pasos los realizará el receptor:

1- Escoger números primos largos: *p* y *q*.

2- Calcular $n = p \cdot q$

3- Calcular la función phi:

$$\varphi(n) = \prod_{i=n}^{n} (p_i^{e_i} - p_i^{e_i - 1})$$

Esta función sirve para calcular el número de primos relativos del campo $\mathbb{Z}_n$ respecto a *n*. Sin embargo, en RSA se utiliza porque es necesario conocer su descomposición factorial, y si no se conocen p y q, no se podrá calcular. En RSA se simplifica la fórmula como, ya que los dos son primos

$$\varphi(n) = (p-1) \cdot (q-1)$$

4- Escoger la clave pública: $e \in \mathbb{Z}_{\varphi(n)}$ y que sea co-primo con $\varphi(n)$, es decir el M.C.D$(e, \varphi(n))$ = 1

5- Calcular la clave privada: *d*, tal que:

$$d \cdot e \equiv 1 \; mod \; (\varphi(n))$$

La clave pública será *n* y *e*.
La clave privada será *d*.

A partir de aquí se aplica un algoritmo para encriptar y desencriptar el mensaje, y se ve así, como funciona cada clave:

El emisor cogerá las claves y realizará el siguiente cálculo para encriptar el mensaje *x*:

$$y = e_{c.púb}(x) \equiv x^e \; mod \; (n)$$

El mensaje encriptado será *y*.

El receptor para desencriptar *y* calculará:

$$x = d_{c.priv}(y) \equiv y^d \; mod \; (n)$$

Y el mensaje será desencriptado como *x*.

Así, ha habido un intercambio de claves y se ha transmitido ya el mensaje.

[23] Ibid (Paar y Pelzl, Understanding Cryptography: A Textbook for Students and Practisioners)

Veamos un ejemplo:

Alice	**Dominio Público**	**Bob**
x = 8		1- $p = 5$ y $q = 11$ 2- $n = p \cdot q = 55$ 3- $\varphi(55) = (5-1) \cdot (11-1) = 40$ 4- $e = 7$ 5- $7 \equiv 23\ mod\ (40)$
	Clave pública: n = 55; e = 7	
$y = e_{c.púb}(8) \equiv 8^7\ mod\ (55) = 2$		
	Mensaje encriptado: y = 2	
		$x = d_{c.priv}(2) \equiv 2^{23}\ mod\ (55) = 8$

Ilustración 2: Esquema del Protocolo de Intercambio de Claves y Cifrado RSA

Comprobación[24]:

$$(x^e)^d \equiv x^{de} \equiv x\ mod\ n \qquad 8^{7^{23}} = 8\ mod\ 55$$

$$d \cdot e = 1 + t \cdot \varphi(n) \qquad 7 \cdot 23 = 1 + t \cdot 40$$

$$x^{de} \equiv x^{1+t\cdot\varphi(n)} \equiv x^{t\cdot\varphi(n)} \cdot x \equiv x^{\varphi(n)^t} \cdot x\ mod\ n \qquad 8^{7\cdot 23} \equiv 8^{1+t40} \equiv 8^{t40} \cdot 8 \equiv 8^{40^t} \cdot 8\ mod\ 55$$

Teorema de Euler: $\boldsymbol{x^{\varphi(n)} \equiv 1\ mod\ (n)}$

$$1 \equiv 1^t \equiv x^{\varphi(n)^t}\ mod\ n \qquad 1 \equiv 1^t \equiv 8^{40^t}\ mod\ 55$$

$$x^{de} \equiv x^{\varphi(n)^t} \cdot x \equiv 1 \cdot x\ mod\ n \qquad 8^{7\cdot 23} \equiv 8^{40^t} \cdot 8 \equiv 1 \cdot 8\ mod\ n$$

[24] Ibid (Paar y Pelzl, Understanding Cryptography: A Textbook for Students and Practisioners)

5.2. Ventajas ECDH respecto RSA

A continuación, se mostrará un análisis de las ventajas de ECDH respecto del estandarizado RSA. Sin embargo, es importante destacar el principal punto negativo de ECC:

- El NIST (National Institut of Security in Technology) es la principal institución de referencia para la criptografia y criptosistemas. Este organismo publicó un sistema de generación de Números Aleatorio: "The Dual Elliptic Curve Deterministic Random Bit Generator " (Dual_EC_DRBG). Este algoritmo es más ineficiente respecto a otros por la larga computación requerida y además se ha demostrado no ser totalmente seguro, significando que se puede predecir sus resultados. Este resultado es el utilizado como clave privada en el DH-ECC y por tanto pone en peligro todo el sistema[25].

Esta desventaja obliga a combinar las ECC con otros protocolos informáticos (RSA, AES, SHA…), los cuales ayudan se encargan de solventar el Dual_EC_DRBG, y posibles ataques como el Man-in-the-Middle[26].[27]

5.2.1. Longitud de Clave

El factor más importante para determinar la seguridad de un sistema criptográfico es la longitud de clave que se utilizará para el intercambio de claves y el cifrado del mensaje.

En ECDHE la longitud de clave viene determinada por los bits del primo elegido para la ecuación (3). En RSA la longitud de clave depende de los bits del número n ($n = p \cdot q$), el cuáles también un número primo.

Estos dos parámetros son los que permitirán descifrar el intercambio de claves, por lo que se evalúa cuál es su longitud necesaria en base a los ataques que pueden recibir y la dificultad que interpone estos dos valores. A continuación, se ve los Millones de Instrucciones por Segundo (MIPS) durante un año necesarios para romper la seguridad

[25] Frenkel, Edward. «How did the NSA hack our email?» 22 de Deciembre de 2013. Vídeo Didactico. 27 de Junio de 2018. <https://www.youtube.com/watch?v=ulg_AHBOIQU>.

[26] Ibid (Paar, Lecture 24: Man-in-the-middle Attack, Certificates and PKI by Christof Paar)

[27] Ver ejemplos de cómo se combinan los protocolos de criptografía en el Anexo 1: Ejemplos de EC usadas en la actualidad

con los mejores algoritmos hasta el momento, así como los pasos que ejecutara el algoritmo:

- Para ECDH[28]:

Tamaño de m (bits)	Pasos necesarios	MIPS años
160	2^{80}	$9{,}6 \cdot 10^{11}$
186	2^{93}	$7{,}9 \cdot 10^{15}$
234	2^{117}	$1{,}6 \cdot 10^{23}$
354	2^{177}	$1{,}5 \cdot 10^{41}$
326	2^{213}	$1{,}5 \cdot 10^{42}$

Tabla 6: Seguridad de ECDH ante el ataque Rho Pollard

- Para RSA[29]:

Tamaño de n	MIPS año
512	$3 \cdot 10^4$
768	$2 \cdot 10^8$
1024	$3 \cdot 10^{11}$
1280	10^{14}
1536	$3 \cdot 10^{16}$
2048	$3 \cdot 10^{20}$

Tabla 7: Seguridad de RSA ante el ataque general de criba del cuerpo de números

Como podemos observar, los MIPS necesarios para 326 bits de ECDH son 10^{22} más que 2048 bits de RSA.

Para comparar la seguridad aportada por ambos sistemas, se va a comparar sus longitudes de claves con el sistema de encriptación simétrica AES, el cuál es el estándar de comparación más usado[30].

Seguridad (Bits)	Algoritmo de encriptación Simétrica[31]	RSA Longitud de clave (Bits)	ECDHE Longitud de clave (Bits)
80	Skipjack	1024	160
112	3DES	2048	224
128	AES-128	3072	256
192	AES-192	7680	385
256	AES-256	15360	512

Tabla 8: Datos Proporcionados por el NIST de comparación de seguridad

[28] Molinero, Francisco Javier Brotons. *Modelo de Criptoprocesador de Curvas Elípticas en GF (2m) basado en Hardware reconfigurable*. Tesis Doctoral. Universidad de Alicante. Alicante, 2016. Documento. 23 de Setiembre de 2018. <https://rua.ua.es/dspace/bitstream/10045/54171/1/tesis_brotons_molinero.pdf>.

[29] Ibid (Molinero)

[30] Vanstone, Scott. «ECC Holds Key to Next-Gen Cryptography.» *EE TImes Connecting the Global Electronic Community* (2004). 23 de Setiembre de 2018. <https://www.eetimes.com/document.asp?doc_id=1207181>.

[31] Ver más información en el Anexo 1: Tipos de Clave en la Criptografía

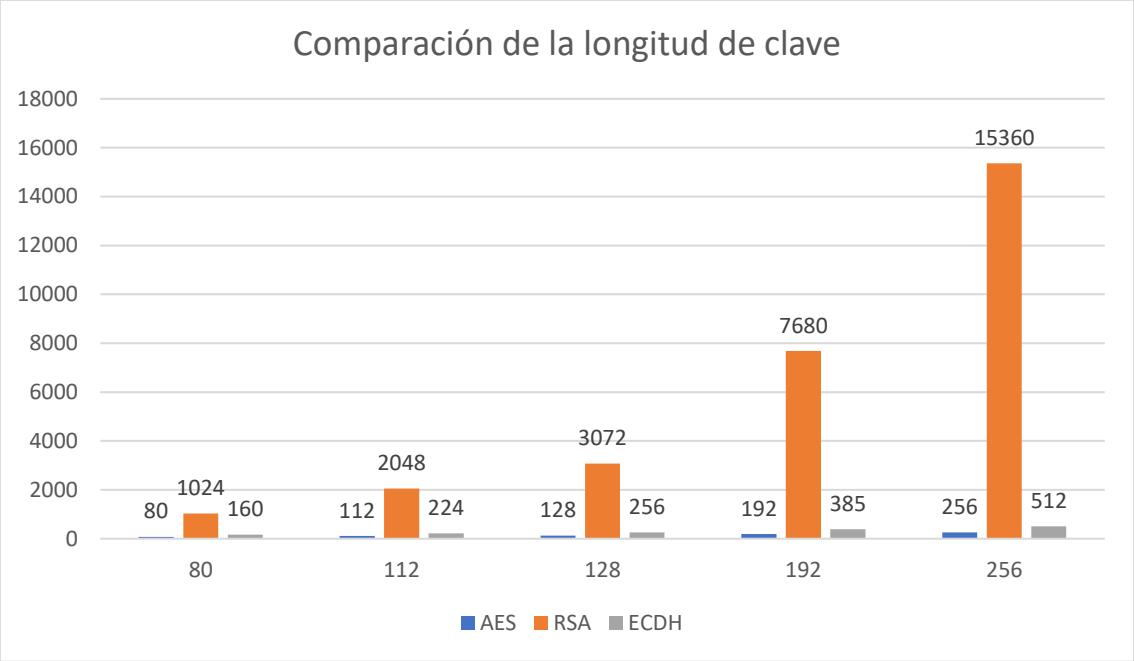


Gráfico 8: Grafico de Barras Comparando la L.de Clave de cada sistema

Un ejemplo real de los parámetros utilizados en ECDH por Google.com son los de la curva P-384[32]:

$$y^2 = x^3 + Ax + B \ mod \ (m)$$

A=115792089210356248762697446949407573530086143415290314195533631308867097853948

B=10583637251521421293261297800472684091144410159937255548352563140394674012 91

m=115792089210356248762697446949407573530086143415290314195533631308867097853951

[32] Sullivan, Nick. «A (relatively easy to understand) primer on elliptic curve criptography.» *arstechnica* (2013). Artículo Digital. 22 de Setiembre de 2018. <https://arstechnica.com/information-technology/2013/10/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/3/>.

5.2.2. Ratio de aumento de Seguridad

Por otra parte, el aumento de seguridad para un sistema implicará mayor longitud de clave, pero existe una característica muy notable entre ambos sistemas cuando se aumenta la seguridad[33]:

Tiempo de Ruptura (MIPS año)	Tamaño de clave RSA (bits)	Tamaño de clave ECC (bits)	Relación entre claves RSA/ECC
10^4	512	106	5:1
10^8	768	132	6:1
10^{11}	1024	160	7:1
10^{20}	2048	210	10:1
10^{78}	21000	600	35:1

Tabla 9: Comparación de la L. de clave con el Ratio entre RSA y ECC

Como podemos ver, la ratio de seguridad aumenta de forma muy notable, por lo que significaría que ECDH es un sistema más seguro y eficiente para estandarizar entre diferentes grados de seguridad.

Este hecho sucede a causa de que el tiempo de los mejores algoritmos para romper cada criptosistema aumenta de forma diferente. En RSA los pasos requeridos aumentan de forma semi-exponencial, en cambio para ECDH es completamente exponencial[34].

Es importante destacar que la longitud de clave utilizada también determinará el proceso de cifrado del mensaje, no solo el intercambio de claves, y deben coincidir ambos en los bits deseados. Así, si se quiere aumentar la seguridad pública, se verá ralentizada también la computación del cifrado.

[33]Ibid (Molinero)
[34]Ibid (Vanstone)

5.3. Implicaciones en la Eficiencia

Una vez analizados estas dos características de seguridad de cada protocolo es importante analizar sus implicaciones en la eficiencia del sistema, ya que a mayor longitud de clave se exige:

- Mayor capacidad de almacenamiento.
- Mayor capacidad de computación.
- Mayor longitud del certificado de clave.
- Más energía para la computación.
- Más tiempo[35] para realizar la computación.
- Mayor amplitud de banda para transportar la clave y el mensaje *a posteriori*.

Por todas estas repercusiones, podemos deducir que para tener una comunicación más eficiente se debe optar por la menor longitud de clave posible, siempre que certifique la seguridad necesaria. En la comparativa estudiada es mejor el Protocolo ECDH.

[35] Ver en el Anexo 2: Documento 3: Gráfico comparativo del Tiempo de computación

Conclusión

La Criptografía en Curvas Elípticas hace uso de estructuras algebraicas que forman un conjunto de elementos con unas operaciones y propiedades definidas que lo convierten en un grupo abeliano. Además, para la criptografía se utiliza la matemática modular, la cual hace uso de los grupos cíclicos y evita el concepto de números infinitos. Cuando se convierte el grupo abeliano de las Curvas Elípticas (EC) a un grupo cíclico, creado por a partir punto generado y mediante las operaciones definidas en las EC, se consiguen los elementos necesarios para crear un Protocolo de Intercambio de Claves para un sistema criptográfico asimétrico: Protocolo Diffie-Hellman en Curvas Elípticas (ECDH). Gracias a las operaciones definidas, la dificultad del problema está en el logaritmo discreto y en la actualidad los algoritmos utilizados para romperlo siguen siendo ineficientes.

Por otra parte, existe el protocolo RSA, el cual se basa en la factorización de números primos, usa la matemática modular para realizar el intercambio de claves forma segura y secreta. En la actualidad es un sistema más empleado para el uso doméstico[36] (de baja seguridad) mientras que grandes empresas tecnológicos e instituciones optan por ECDH[37]. Ambos sistemas se usan combinados con otros algoritmos para evitar ataques y dar mayor protección, así como más velocidad, por lo que podemos concluir que un sistema por si solo tienen más riesgos.

Sin embargo, tras hacer una comparación de ambos sistemas, donde las EC tienen dos desventajas principales, podemos ver como ECDH presenta longitudes de clave menores y esto se acaba traduciendo en mayor eficiencia, lo que hace al protocolo más adecuado para los dispositivos pequeños y de baja capacidad de computación y almacenaje. Esto contradice a la hipótesis inicial, donde se creía que ECDH era menos eficiente por tener menos uso en ámbitos de poca seguridad, pero después del análisis se sugiere que es a causa de que es un sistema más nuevo y que hasta la década de los 2000 no se conocían todas sus cualidades.

La metodología usada en esta monografía ha permitido una gran compresión de ambos sistemas tanto desde un punto de vista matemático como criptográfico, sin embargo, no se han realizado simulaciones lo que hubiera permitido respaldar los datos extraídos

[36]Ibid (Olenski)
[37]Ibid (Vanstone)

de fuentes secundarias. Además, más investigación se podría realizar sobre grupos cíclicos de base 2, los cuales usan polinomios y presentan pequeñas alteraciones. A más, solo se han evaluado las EC en el intercambio de claves, pero podrían ser utilizadas para certificados de seguridad (ECDSA) o en la propia encriptación.

Bibliografía

Acosta, Miguel Ángel Olalla. «Capítulo 3 - El anillo de los números enteros.» s.f. Universidad de Sevilla. Teoría Universitaria. 1 de Agosto de 2018. <https://rodas5.us.es/file/a774213d-a15a-41df-816c-e633fb1a5876/1/03-Presentacion-Enteros.pdf>.

Aguirre, Jorge Ramió. «Capítulo 7 - Teoría de los Númeors.» 1 de Marzo de 2006. Universidad Politécnica de Madrid. Presentación Universitaria. 1 de Agosto de 2018. <http://www.deic.uab.es/material/26118-07TeoriaNumeros.pdf>.

«Aritmética Modular.» Universiad de Murcia, s.f. Presenación. 5 de Julio de 2018. <http://webs.um.es/pacovera/miwiki/lib/exe/fetch.php?id=inicio&cache=cache&media=aritmeticamod.pdf>.

Castillo, Carlos Ivorra. «Curvas Elíptica.» s.f. Universitat de Valencia. Teoría Asignatura. 20 de Junio de 2018. <https://www.uv.es/ivorra/Libros/Elipticas.pdf>.

Frenkel, Edward. «How did the NSA hack our email?» 22 de Deciembre de 2013. Vídeo Didactico. 27 de Junio de 2018. <https://www.youtube.com/watch?v=ulg_AHBOIQU>.

García, Sara N. Matheu. «Curvas Elípticas.» Trabajo de Final de Grado. Universidad de Murcia, 2015. Documento. 19 de Junio de 2018. <https://www.um.es/documents/118351/1884002/TFG_MATHEU+GARCIA.pdf/0f3f6eb9-5ef7-4483-b41f-525bf7ef1160>.

Gee, Toby. *Elliptic Curves*. Imperial College London. Londres, 18 de Julio de 2014. Recorded Lecture. 27 de Junio de 2018. <https://www.youtube.com/watch?v=6eZQu120A80>.

Grooten, Martijn. «Elliptic Curve Cryptography for those who are afraid of maths.» 3 de June de 2015. Conferencia. 27 de Junio de 2018. <https://www.youtube.com/watch?v=yBr3Q6xiTw4>.

Gutierrez, Pedro. *GenBeta*. 15 de Enero de 2013. Artículo. 24 de Setiembre de 2018. <https://www.genbeta.com/desarrollo/que-son-y-para-que-sirven-los-hash-funciones-de-resumen-y-firmas-digitales>.

L, Delgado, Vallejo R. y Mutis W. & Castillo J. «Estructura de Grupo de las Curvas Elípticas.» *Revista Sigma, Universida de Nariño* (2009): 20-37. Artículo. 19 de Junio de 2018. <https://www.researchgate.net/publication/28296289_La_Estructura_de_Grupo_de_las_Curvas_Elipticas>.

Langley, Adam. *Google Security Blog*. 17 de Setiembre de 2015. 23 de Setiembre de 2018. <https://security.googleblog.com/2015/09/disabling-sslv3-and-rc4.html>.

Menezes, Alfred J., Paul C van Oorsshot y Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996. Libro Digital. 1 de Julio de 2018.

Microsoft. Vers. https://docs.microsoft.com/en-us/windows/desktop/secauthn/cipher-suites-in-schannel. 31 de Mayo de 2018. 23 de Setiembre de 2018.

Molinero, Francisco Javier Brotons. *Modelo de Criptoprocesador de Curvas Elípticas en GF (2m) basado en Hardware reconfigurable*. Tesis Doctoral. Universidad de Alicante. Alicante, 2016. Documento. 23 de Setiembre de 2018. <https://rua.ua.es/dspace/bitstream/10045/54171/1/tesis_brotons_molinero.pdf>.

Muñoz, José Peña. «LA ARITMÉTICA MODULAR.» 2012. *Descartes.* Ministerio de Educación, Cultura y Deporte. Web Didáctica. 5 de Julio de 2018. <http://serbal.pntic.mec.es/jpem0100/cesar/01.html>.

Olenski, Julie. «ECC 101: What is ECC and why would I want to use it?» 29 de May de 2015. Artículo. 27 de Setiembre de 2018. <https://www.globalsign.com/en/blog/elliptic-curve-cryptography/>.

Paar, Christof. «Lecture 11: Number Theory for PKC: Euclidean Algorithm, Euler's Phi Function & Euler's Theorem.» 30 de Enero de 2014. Ruhr Univerity Bochun. Recorded Lecture. 27 de Junio de 2018.

—. «Lecture 12: The RSA Cryptosystem and Efficient Exponentiation by Christof Paar.» 30 de Enero de 2014. Ruhr Bochum University. Recorded Lecture. 28 de Junio de 2018. <https://www.youtube.com/watch?v=QSlWzKNbKrU&list=PL6N5qY2nvvJE8X75VkXglSrVhLv1tVcfy&index=12>.

—. «Lecture 16: Introduction to Elliptic Curves by Christof Paar.» 30 de Eneo de 2014. Ruhr Bochum University. Recorded Lecture. 28 de Junio de 2018. <https://www.youtube.com/watch?v=vnpZXJL6QCQ&list=PL6N5qY2nvvJE8X75VkXglSrVhLv1tVcfy&index=16>.

—. «Lecture 17: Elliptic Curve Cryptography (ECC) by Christof Paar.» 30 de Enero de 2014. Ruhr Bochum University. Recorded Lecture. 28 de Junio de 2018. <https://www.youtube.com/watch?v=zTt4gvuQ6sY&index=17&list=PL6N5qY2nvvJE8X75VkXglSrVhLv1tVcfy>.

—. «Lecture 2: Modular Arithmetic and Historical Ciphers by Christof Paar.» 30 de Enero de 2014. Ruhr University Bochum. Recorded Lecture. 30 de Junio de 2018. <https://www.youtube.com/watch?v=W1SY6qKZrUk>.

—. «Lecture 24: Man-in-the-middle Attack, Certificates and PKI by Christof Paar.» 30 de Enero de 2014. Ruhr Bochum University. Recorded Lecture. 8 de Julio de 2018.

<https://www.youtube.com/watch?v=B9UirR9YDnQ&index=24&list=PL6N5qY2nvvJE8X75VkXglSrVhLv1tVcfy&pbjreload=10>.

Paar, Christof y Jan Pelzl. *Understanding Cryptography: A Textbook for Students and Practisioners*. Londres: Springer, 1998. Libro.

Palacios, Manuel. «pcmap.unizar.es.» Otoño de 2002. Teoria Universitaria. 26 de Setiembre de 2018. <http://pcmap.unizar.es/~mpala/A_L_lecci/3grupos.pdf>.

Pierce, Robert. *Elliptic Curve Diffie Hellman*. 10 de Desembre de 2014. Video Didáctico. 29 de Julio de 2018. <https://www.youtube.com/watch?v=F3zzNa42-tQ>.

Pound, Mike. «Elliptic Curve - Computerphile.» 16 de Enerro de 2018. Video Didáctico. 27 de Junio de 2018. <https://www.youtube.com/watch?v=NF1pwjL9-DE>.

Raedy, Willy. «Elliptic Curve Cryptography Tutorial - Understanding ECC through the Diffie-Hellman Key Exchange.» 8 de Agosto de 2017. Recorded Lecture. 29 de Agosto de 2018. <https://www.youtube.com/watch?v=gAtBM06xwaw>.

Robshaw, M.J.B. y Yiqun Lisa Yin. «Elliptic Curve Cryptosystems.» Estudio Comparativo. 1997. Documento. 17 de Agosto de 2018.

Román, Juan de Burgos. *MATEMÁTICAS II Definiciones, Teoremas y Resultados Segunda Edición*. Madrid: García-Maroto Editores, S.L, 2010. Libro Impreso.

Rotger, Llorenç Huguet y Josep Rifà Comà & Juan Gabriel Tena Ayuso. «Criptografía con Curvas Elípticas.» Teoría de Asignatura. Universitat Oberta de Catalunya, s.f. Documento. 3 de Julio de 2018. <https://www.exabyteinformatica.com/uoc/Informatica/Criptografia_avanzada/Criptografia_avanzada_(Modulo_4).pdf>.

Ruiz, C. «AMPLIACIÓN DE MATEMÁTICAS - GRUPOS CíCLICOS.» s.f. Universidad Complutense de Madrid. Teoría Universitaria. 4 de Julio de 2018.

Ryckwalder, Eric. *The Math Behind Bitcoin*. 19 de Octubre de 2014. Artículo. 27 de Setiembre de 2018. <https://www.coindesk.com/math-behind-bitcoin/>.

Sandoval, Miguel Morales. «2003.» 2003. INAOE. Teoría Universitaria. 5 de Julio de 2018. <https://www.tamps.cinvestav.mx/~mmorales/documents/Criptograf.pdf>.

Sesma, Iciar. *Criptografía en Curvas Elípticas*. Trabajo de Final de Grado. Logroño, 2015. Documento. 19 de Junio de 2018. <https://biblioteca.unirioja.es/tfe_e/TFE001034.pdf>.

Sullivan, Nick. «A (relatively easy to understand) primer on elliptic curve criptography.» *arstechnica* (2013). Artículo Digital. 22 de Setiembre de 2018. <https://arstechnica.com/information-technology/2013/10/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/3/>.

Tolkov, Igor. *Counting points on elliptic curves: Hasse's theorem and recent developments*. Scientific Paper. Washington, 2009. Documento. 04 de Julio de 2018. <https://www.math.washington.edu/~morrow/336_09/papers/Igor.pdf>.

Vanstone, Scott. «ECC Holds Key to Next-Gen Cryptography.» *EE TImes Connecting the Global Electronic Community* (2004). 23 de Setiembre de 2018. <https://www.eetimes.com/document.asp?doc_id=1207181>.

Wagnon, John. «Elliptic Curve Cryptography Overview.» 14 de Octubre de 2015. Vídeo Didáctico. 27 de Junio de 2018. <https://www.youtube.com/watch?v=dCvB-mhkT0w>.

Anexo 1: Excel de Algoritmos

Para esta monografía se ha creado un Excel para realizar los cálculos y algoritmos mencionados en las diferentes secciones. Este Excel es modificable después de descargarlo en: https://drive.google.com/file/d/1BC6gQyBXkaKJSUvKGD5hu7QEhpgJfZGk/view?usp=sharing

El archivo presenta diferentes hojas:

- **DATA-1:** se observa una tabla que realiza el Lema 1 (Multiplicación Escalar, sobre el cuerpo de número reales)
- **Multiplicación escalar sobre Z:** se introducen los parámetros que computará DATA-1 y muestra los resultados de la multiplicación escalar
- **DATA-**2: se computan los puntos racióneles de una curva elíptica sobre un grupo cíclico
- **Puntos de la Curva**: Se introducen los parámetros para DATA-2 y se muestran los puntos en el plano cartesiano, así como los puntos finales
- **Multiplicación escalar sobre Zm**: se computa la multiplicación escalar sobre un grupo cíclico. Se introduce los puntos en la parte superior y la respuesta se encuentra en la tabla del escalar, donde aparece el resultado "Above Cell is X/Y result"
- **RSA**: permite ver cómo funciona el algoritmo descrito, pero presenta muchas limitaciones debido a la dificultad de escoger las claves

Tipos de Clave en la Criptografía

Para entender las diferencias de longitud de clave es necesario conocer los tipos de clave hay y su complejidad. Toda la información ha sido extraída de (Paar y Pelzl, Understanding Cryptography: A Textbook for Students and Practisioners):

Tipos de Claves

Para realizar una comunicación entre dos usuarios (persona humana o servidor), es necesario establecer un protocolo de actuación. Este protocolo puede ser de clave privada o pública:

Clave Privada/Simétrica

El usuario emisor cifrará el mensaje mediante un algoritmo de encriptación que usará una clave única para ese cifrado en concreto. El mensaje será enviado mediante un canal de comunicación (Internet) hasta el receptor. Éste se encargará de aplicar un algoritmo de desencriptación que solo dará el mensaje aplicando la misma clave utilizada por el emisor.

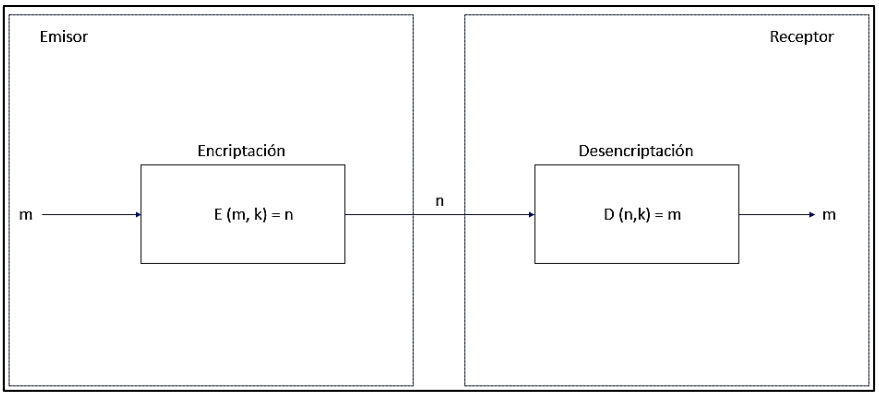


Ilustración 4: Encriptación Simétrica

Como vemos, hay una simetría en el protocolo y se caracterizan por ser altamente seguros y rápidos.

Clave Pública/Asimétrica

Para los protocolos de clave pública, tenemos el mismo esquema, con la dificultad de que los usuarios no pueden acordar cual es la clave que se utilizará. Sin embargo, en la década de los 70, se obtuvo la solución: el cifrado asimétrico. Ambos usuarios tendrán dos pares de claves diferentes: usuario A tiene clave privada A y la clave pública; mientras que el usuario B tiene la clave privada B y la clave pública. La clave pública permite encriptar el mensaje, pero solo mediante una de las dos privadas, se puede desencriptar el mensaje. Por tanto, el emisor cifrará con la clave pública y el receptor descifrará con su clave privada.

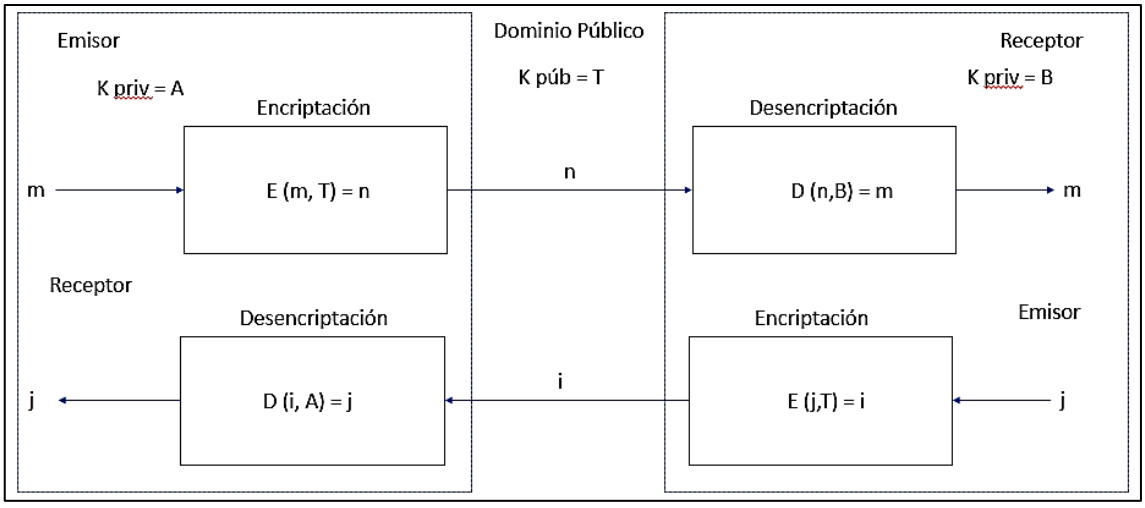


Ilustración 5: Encriptación Asimétrica

El espacio central es el dominio púbico y es accesible a cualquiera de la red. Por este motivo es importante asegurar que este esquema se repite sin alteraciones de terceras personas. Por ello, se utilizarán certificados de usuario, de clave de seguridad y de mensaje; habiendo entidades que los subministran.

Por último, los protocolos asimétricos requieren un intercambio de claves, lo cual será el objeto de estudio en esta monografía. Estos intercambios de clave son una Función Hash:

- La función tiene una inversa ineficiente para la computación (única dirección)
- Dos valores de entrada no pueden dar un mismo resultado (fenómeno conocido como colisión)

Es básico que se cumplan estas condiciones para propiciar una buena comunicación.

Puntos Singulares: Nodos y Cúspides

Una de las principales propiedades estudiadas en una curva es la presencia de puntos singulares.

> **Definición *(*Punto Singular)** *(Román)**: Sea P un punto de EC tal que sus derivadas sean igual a 0.***
>
> $$\begin{cases} \frac{\partial f}{\partial x} = 0 \\ \frac{\partial f}{\partial y} = 0 \end{cases}$$
>
> *Dentro de los Puntos Singulares, se distinguen entre dos tipos:*
>
> - ***Cúspides:** punto singular donde se pueden trazar infinitas tangentes al punto.*
> - ***Nodo:** punto singular donde se pueden trazar 2 tangentes en direcciones diferentes.*

En nuestro caso, como la ecuación de EC (2) se presenta con car($\mathbb{K}$) ≠ 2, 3, esto implica que no haber puntos singulares siempre que el discriminante no sea igual a 0

Ejemplos de EC usadas en la actualidad

Debido a que el ECDH no puede funcionar con su máxima sin ayuda de otros sistemas, por lo que los principales servidores de Internet, así como el NIST, utilizan combinación de varios sistemas:

- Google (Langley): ECDHE_RSA_AES128_GCM_SHA256_P256, con ECDHE (sistema real utilizado ya los números de Kpriv da utilizados son efímeros y cambian constantemente) para el intercambio, RSA certificado de claves, AES128 para encriptar, GCM para certificar la encriptación y SHA256 como generador de números aleatorios y P256 siendo la EC utilizada.
- Microsoft (Windows 10) (Chiper Suites in TLS/SSL (Schannel SSP)): TLS_ECDHE_ECDSA_AES_256_GCM_-SHA384_P384. Pudiendo hacer el mismo análisis.

Anexo 2: Archivos/Documentos

Documento 1: Transformación de la ecuación de Weiertrass a simplificada

Demostración realizada por: (García)

Definición 2.1.2. Sean K un cuerpo y $a_1, a_2, a_3, a_4, a_6 \in K$. Una curva elíptica E sobre K es una curva proyectiva no singular, admitiendo una ecuación definida sobre K, denominada **ecuación de Weierstrass generalizada**

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.1}$$

junto con un punto O que se denomina **punto del infinito**.

Proposición 2.1.3. *Sea K un cuerpo con $char(K) \neq 2, 3$. Entonces la ecuación (2.1) es equivalente a*

$$y^2 = x^3 + Ax + B, \tag{2.2}$$

con $A, B \in K$. Esta ecuación se denomina ***ecuación de Weierstrass simplificada****.*

Demostración. Partiendo de la ecuación generalizada (2.1) podemos dividir entre 2 y completar cuadrados:

$$\left(y + \frac{a_1x}{2} + \frac{a_3x}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{2}\right)x + \left(a_6 + \frac{a_3^2}{4}\right).$$

Haciendo un cambio de variable

$$y_1 = y + \frac{a_1x}{2} + \frac{a_3x}{2}$$

y poniendo

$$a_2' = a_2 + \frac{a_1^2}{4},$$

$$a_4' = a_4 + \frac{a_1a_3}{2},$$

$$a_6' = a_6 + \frac{a_3^2}{4},$$

obtenemos

$$y_1^2 = x^3 + a_2'x^2 + a_4'x + a_6'.$$

Como $char(K) \neq 3$ podemos completar cubos tomando $x_1 = x + \frac{a_2'}{3}$ obteniendo:

$$y_1^2 = x_1^3 + Ax_1 + B,$$

que es lo que queríamos.

□

Documento 2: Algoritmo Extendido de Euclides

El Algoritmo Extendido de Euclides propuesto por el Profesor Christof Paar en su libro *Introduction to Cryptography* es:

Extended Euclidean Algorithm (EEA)
Input: positive integers r_0 and r_1 with $r_0 > r_1$
Output: $\gcd(r_0, r_1)$, as well as s and t such that $\gcd(r_0, r_1) = s \cdot r_0 + t \cdot r_1$.
Initialization:
$s_0 = 1 \quad t_0 = 0$
$s_1 = 0 \quad t_1 = 1$
$i = 1$
Algorithm:

1 DO
1.1 $i = i + 1$
1.2 $r_i = r_{i-2} \bmod r_{i-1}$
1.3 $q_{i-1} = (r_{i-2} - r_i)/r_{i-1}$
1.4 $s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$
1.5 $t_i = t_{i-2} - q_{i-1} \cdot t_{i-1}$
WHILE $r_i \neq 0$
2 RETURN
$\gcd(r_0, r_1) = r_{i-1}$
$s = s_{i-1}$
$t = t_{i-1}$

Aplicado de forma manual:

$$12 \cdot x \equiv 1 \, mod \, (53)$$

Algoritmo de Euclides:

$$53 = 4 \cdot 12 + 5$$

$$12 = 2 \cdot 5 + 2$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 2 \cdot 1$$

Algoritmo Extendido de Euclides

$$1 = 5 - 2 \cdot 2$$

$$1 = 5 - 2 \cdot (12 - 2 \cdot 5) = 5 - 2 \cdot 12 + 4 \cdot 5 = -2 \cdot 12 + 5 \cdot 5$$

$$1 = -2 \cdot 12 + 5 \cdot (53 - 4 \cdot 12)$$

$$= -2 \cdot 12 + 5 \cdot 53 + 5 \cdot 5 - 20 \cdot 12$$

Seleccionando solo los números que nos interesan (12, 53):

$$1 = -22 \cdot 12 + 5 \cdot 53 \equiv 31 \cdot 12 + 5 \cdot 0 \, mod(53) = 1$$

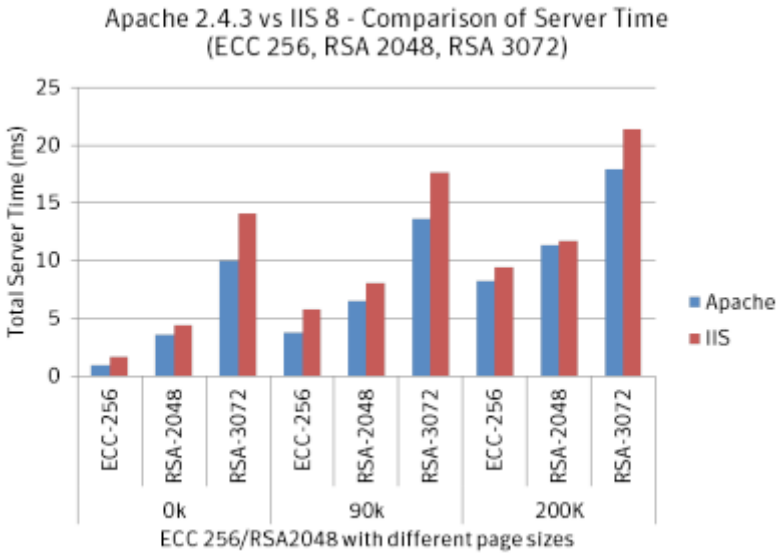
Por tanto, el inverso modular de 12 es 31 y viceversa. De este modo si tenemos la siguiente operación se realizará de la siguiente forma:

$$\frac{12}{12} \, mod(53) = 12 \cdot (12)^{-1} mod(53) = 12 \cdot 31 mod \, (53) \equiv 1 \, mod \, (53)$$

$$\frac{48}{12} \, mod(53) = 48 \cdot (12)^{-1} mod(53) = 48 \cdot 31 \, mod \, (53) \equiv 40 \, mod \, (53)$$

Documento 3: Gráfico comparativo del Tiempo de computación

Según el informe realizado por White Paper en su informe: *"Elliptic Curve Cryptography (ECC) Certificates Performance Analysis"*, el tiempo de computación varía del siguiente modo:



Documento 4: Definiciones

Según el trabajo de Manuel Palacios (2002), definimos a los distintos conjuntos como:

> **"Anillo:** Sean A un conjunto dotado de dos operaciones (leyes de composición), que denotaremos + y · , respectivamente. Diremos que (A,+, ·) es un anillo (o que A posee estructura de anillo con y·) si se cumplen los siguientes axiomas:
>
> o) + es operación interna: ∀a, b ∈ A, a + b ∈ A
>
> 1) propiedad asociativa: ∀a, b, c ∈ A, a + (b + c)=(a + b) + c
>
> 2) existencia de elemento neutro (cero): ∃ 0 ∈ A tal que 0 + a = a +ANexo0= a, ∀a ∈ A
>
> 3) existencia de elemento simétrico (opuesto): ∀a ∈ A ∃ − a ∈ A tal que a + (−a) = −a + a = 0
>
> 4) propiedad conmutativa: ∀a, b ∈ A, a + b = b + a (es decir, A es grupo abeliano respecto de +) o') · es operación interna: ∀a, b ∈ A, a · b ∈ A
>
> 5) propiedad asociativa: ∀a, b, c ∈ A, a · (b · c)=(a · b) · c 6) propiedad distributiva de · respecto de + : ∀a, b, c ∈ A, a·(b+c) = a·b+a·c (a+b).·c = a · c + b · c