



GRADO DE MATEMÁTICAS

Curso Académico 2019/2020

Trabajo Fin de Grado

Criptografía sobre curvas elípticas. Cifrado basado en
identidades.

Autor : José Francisco Rodríguez Peña

Tutor : Ángel Luis Pérez del Pozo

Objetivo

El objetivo de este trabajo es tener un primer contacto con el estudio de la criptografía, haciendo énfasis en la criptografía de clave pública y la teoría necesaria para definir la criptografía sobre curva elíptica. Finalmente se estudiará un esquema de cifrado basado en identidades sobre curvas elípticas.

Índice general

1. Introducción	7
1.1. Estructura del trabajo	9
2. Herramientas matemáticas	11
2.1. Grupo	11
2.2. Grupo cíclico	12
2.3. Logaritmo discreto	12
2.4. Exponenciación binaria	13
2.5. Algoritmo Baby-step/Giant-step	13
3. Curvas elípticas	15
3.1. Definiciones	15
3.1.1. Plano proyectivo	15
3.1.2. Curva elíptica	16
3.2. Paso al plano afín	16
3.3. Ley de grupo	17
3.4. Curvas elípticas sobre cuerpos finitos	18
3.5. Compresión de punto	19
4. Clave pública	21
4.1. Intercambio de claves Diffie-Hellman	21
4.2. Funciones Hash	23
4.3. Cifrado de clave pública	23
4.3.1. Ejemplo: Cifrado RSA	24
4.4. Firma digital	26

4.4.1. Ejemplo: Firma digital con RSA	26
5. Cifrado basado en identidad	29
5.1. Emparejamiento	30
5.2. Esquema basado en emparejamiento	30
5.2.1. Preparación	31
5.2.2. Obtención de clave privada	31
5.2.3. Cifrado	32
5.2.4. Descifrado	32
5.3. Consideraciones sobre el esquema	33
6. Conclusiones	35
Bibliografía	37
7. Anexo: Representación de curvas elípticas	39

Capítulo 1

Introducción

La criptografía es el estudio y las técnicas para tratar la información de manera segura en presencia de adversarios. Para conseguir ese objetivo podemos tener en cuenta cuatro puntos fundamentales para tratamiento de la información:

- Confidencialidad: La información no puede ser accedida por miembros externos al grupo destinado a tratar la información.
- Integridad: La información no puede ser modificada en ningún punto de su ciclo de vida.
- Autenticidad: El origen de la información debe ser contrastable.
- No repudio: El origen de la información no puede negar que la información fue originada por él.

Dentro de este marco, vamos a centrarnos en el cifrado de datos. Para esto se hace uso de alguna transformación del mensaje de forma que no pueda ser recuperada ninguna información útil y que solo los receptores legítimos del mensaje puedan volver a transformarlo en el mensaje original, estas transformaciones son llamadas *cifrado* y *descifrado* respectivamente.

Las primeras técnicas para cifrar mensajes consistían en sustituir todas las letras del mensaje mediante alguna tabla o relación, en concreto en el cifrado César se alternaban por su correspondiente en el alfabeto desplazada un número de posiciones, este número era la clave del cifrado y para descifrar bastaba con realizar el mismo desplazamiento en sentido inverso, dada la poca cantidad de claves posibles para este cifrado es muy fácil de romper por fuerza bruta, sin embargo una de las formas más ingeniosas para romperlo consiste en analizar la distribución de letras

en el idioma del mensaje y, si este es suficientemente largo, se puede detectar el desplazamiento en esa distribución.

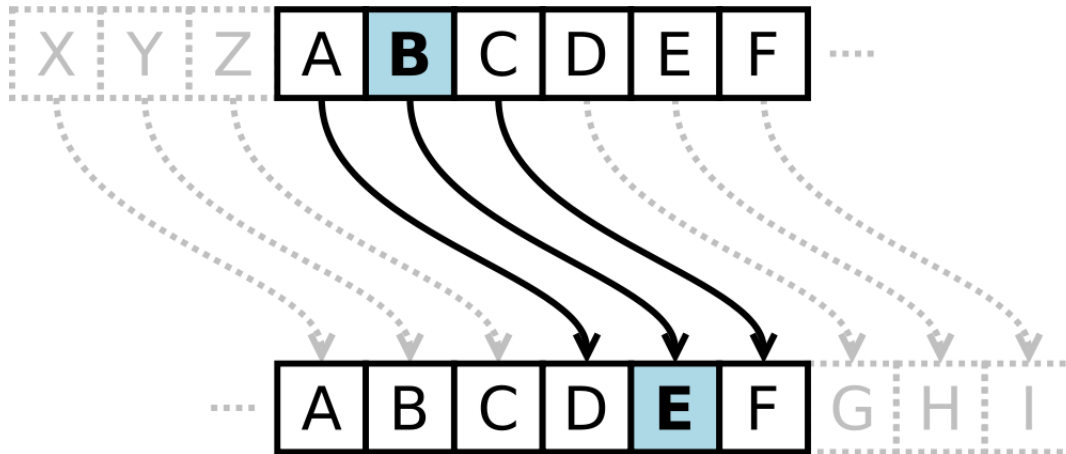


Figura 1.1: Cifrado César

En el siglo XV aparece el cifrado Vigènere que consistía en una palabra clave que se usaba para desplazar las letras del mensaje, por ejemplo si la clave es 'ABC' los desplazamientos serían 1, 2 y 3 posiciones respectivamente, y se repetía esta clave hasta acabar por completo el mensaje.

La criptografía estuvo ligada fuertemente al uso militar y durante los siglos XIX y XX tuvo una importancia fundamental con la máquina Enigma, en este periodo de tiempo se invirtió un gran esfuerzo en desarrollar este área dando lugar a grandes avances.

Posteriormente a la Segunda Guerra Mundial se realizaron muchos estudios teóricos y en los años 70 se crearon algunos estándares de algoritmos de cifrado, a partir de entonces, con la evolución de la informática existe una actualización constante de algoritmos cada vez mas seguros ya que la capacidad de cómputo es mayor.

Es habitual agrupar los algoritmos según la naturaleza de las claves que son necesarias al cifrar y descifrar:

- **Criptografía simétrica:** Estos métodos utilizan la misma clave para cifrar y descifrar mensajes, las distintas partes que intercambian información deben conocer esta clave de antemano, existen distintos algoritmos que ponen esto en practica, uno de los mas conocidos

entre los métodos recientes es DES (Data Encryption Standard), diseñado en los años 70 y reemplazado a día de hoy por AES (Advanced Encryption Standard).

- Criptografía asimétrica: También conocida como criptografía de clave pública, se basa en un par de claves, una pública que se debe dejar a disposición de cualquiera y una privada que se debe mantener en secreto. Este tipo de métodos son utilizados, entre otras cosas, para el cifrado basado en identidad y el cifrado basado en certificados.

1.1. Estructura del trabajo

Para realizar este estudio se empieza mostrando las herramientas matemáticas necesarias para desarrollar algunos de los esquemas fundamentales de clave pública, esto se verá en el capítulo 2.

Posteriormente se trata en más detalle las curvas elípticas en el capítulo 3, que se usarán junto con las herramientas anteriores. En este apartado se hace uso del código proporcionado en el anexo para generar la figura que representa la operación fundamental que se usa en las curvas elípticas.

Una vez presentados los conocimientos básicos con los que se trabaja, se pasa a mostrar los esquemas de clave pública así como algún ejemplo de los mismos en el capítulo 4.

Finalmente en el capítulo 5 se usa la mayoría de conceptos anteriores para plantear un esquema de clave pública sobre curvas elípticas, el cifrado basado en identidad.

Tras ello se encuentra el apartado de conclusiones donde muestro algunas de las ideas generales que me ha transmitido este estudio y que he aprendido al realizarlo.

Capítulo 2

Herramientas matemáticas

En este apartado se presentan una serie de conceptos y algoritmos necesarios para poder entender el origen de la seguridad de los diferentes esquemas, así como su implementación.

2.1. Grupo

Dado un conjunto no vacío de elementos G y una operación \cdot que combina un par de elementos en un tercero, se define grupo al par (G, \cdot) donde se cumplen las siguientes propiedades:

- Clausura: $\forall a, b \in G$ se tiene que $a \cdot b \in G$.
- Asociatividad: $\forall a, b, c \in G$ se tiene que $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- Elemento neutro: $\exists e \in G$ tal que $\forall a \in G$ se cumple $a \cdot e = e \cdot a = a$. Cuando la operación es la multiplicación se denota este elemento como 1 y cuando es la suma se denota como 0.
- Elemento inverso: $\forall a \in G, \exists a^{-1} \in G$ elemento inverso de a tal que $a \cdot a^{-1} = e$. Cuando la operación es la suma $+$ se suele denotar al elemento inverso como $-a$.

Se denomina grupo abeliano si además de esto se cumple la propiedad conmutativa:

$\forall a, b \in G$ se cumple que $a \cdot b = b \cdot a$.

Es habitual que los grupos abelianos usen notación aditiva $+$.

2.2. Grupo cíclico

Sea G un grupo, se dice que G es un *grupo cíclico* si existe un elemento del grupo $g \in G$ de forma que $G = \langle g \rangle$, es decir, cualquier elemento del grupo puede expresarse como g^n (o ng si es un grupo aditivo) para algún $n \in \mathbb{Z}$, llamamos entonces a g *generador* de G . Un ejemplo habitual de grupo cíclico es el grupo aditivo de los números enteros módulo n , denotado habitualmente como $\mathbb{Z}/n\mathbb{Z}$, tomando como generador el 1.

Lema: Cada grupo cíclico finito de orden n es isomorfo al grupo $\mathbb{Z}/n\mathbb{Z}$.

Demostración:

Sea G un grupo cíclico finito generado por g , puesto que G es finito se tiene que $g^n = e$ para algún $n > 0$. Asumimos que n sea el menor posible (el orden de g).

Se puede escribir G como $\{e, g, \dots, g^{n-1}\}$ donde todos los elementos son distintos, es decir, que si $m_1, m_2 \in \{0, 1, \dots, n-1\}$ tal que $m_1 > m_2$, entonces $g^{m_1} \neq g^{m_2}$, de no ser así se tendría que $g^{m_1-m_2} = e$ que contradice que n sea el orden de g .

Usando el algoritmo de la división se puede escribir cualquier entero m como $m = nq + r$, donde $r = m \bmod n$. Por tanto $g^m = (g^n)^q g^r = g^r = g^{m \bmod n}$. Definimos $f : \mathbb{Z}_n \rightarrow G$ donde $f(m) = g^m$, esta función corresponde cada elemento uno a uno. Finalmente se puede comprobar que además es un isomorfismo ya que

$$f(m_1)f(m_2) = g^{m_1}g^{m_2} = g^{m_1+m_2} = g^{(m_1+m_2) \bmod n} = f(m_1 \oplus m_2)$$

2.3. Logaritmo discreto

Para algunos algoritmos de criptografía necesitamos una función que sea fácil de aplicar pero difícil de invertir a nivel de tiempo de cómputo, por ello vamos a ver el caso del logaritmo discreto.

Dado un grupo cíclico finito G con base g , definimos el logaritmo discreto como:

$$y = g^x \iff x = \log_g(y)$$

Por un lado tenemos la *exponenciación discreta*, es decir, g^x cuando x es conocido, esta operación se puede calcular con el algoritmo recursivo de exponenciación binaria, con complejidad $\mathcal{O}(\log x)$.

No obstante el problema de calcular $x = \log_g(y)$ es más difícil, el algoritmo Baby-step/Giant-step tiene complejidad $\mathcal{O}(\sqrt{p})$, asumiendo que el grupo tiene orden primo p .

2.4. Exponenciación binaria

Para calcular g^x , tenemos que hacer la operación recursiva F definida de la siguiente forma:

$$F(g^x) = \begin{cases} g & \text{si } n = 1 \\ (F(g^{\frac{x}{2}}))^2 & \text{si } x \text{ es par} \\ F(g^{(x-1)}) \cdot g & \text{si } x \text{ es impar} \end{cases}$$

Puesto que en cada operación reducimos el exponente x a la mitad, tenemos que realizar $\lceil \log_2(x) \rceil$ operaciones, por tanto este problema se puede resolver en $\mathcal{O}(\log x)$.

2.5. Algoritmo Baby-step/Giant-step

Queremos conocer x en la ecuación $h = g^x$, sea p el orden del grupo G .

Descompondremos nuestra solución en:

$$x = x_0 + x_1 \lceil \sqrt{p} \rceil$$

Puesto que $x < p$, entonces $0 \leq x_0, x_1 < \lceil \sqrt{p} \rceil$.

En primer lugar calcularemos los *baby-step*, esto es:

$$g_i = g^i \text{ t.q. } 0 \leq i < \lceil \sqrt{p} \rceil$$

Tras ello calcularemos los *giant-step*, esto es:

$$h_j = hg^{-j \lceil \sqrt{p} \rceil} \text{ t.q. } 0 < j < \lceil \sqrt{p} \rceil$$

Una forma eficiente de almacenar estos resultados es con una tabla hash almacenando los pares (i, g_i) y (h_j, j) respectivamente.

Ahora intentamos encontrar una coincidencia tal que $g_i = h_j$, si esto ocurre tenemos que:

$$x_0 = i, x_1 = j$$

Ya que

$$g^i = hg^{-j \lceil \sqrt{p} \rceil} \Rightarrow g^{i+j \lceil \sqrt{p} \rceil} = h$$

Dado que para calcular los *baby-step* y los *giant-step* son necesarias como mucho $2 \lceil \sqrt{p} \rceil$ operaciones, y para buscar una coincidencia solo es necesario tener almacenados los pares (clave, valor) de forma (i, g_i) y (h_j, j) para ver si existe la clave g_i en el segundo hash map, por tanto encontrando una coincidencia, puesto que comprobar una clave es $\mathcal{O}(1)$ y se recorren únicamente los g_i tenemos de nuevo $\lceil \sqrt{p} \rceil$ operaciones, por lo que este algoritmo es de complejidad $\mathcal{O}(\sqrt{p})$.

Capítulo 3

Curvas elípticas

En este capítulo se presenta la base de la criptografía sobre curvas elípticas, como hemos visto el problema en el que se va a basar la seguridad de los algoritmos es el logaritmo discreto, este requiere de un grupo cíclico, para ello vamos a utilizar el grupo formado por las curvas elípticas con su operación de suma de puntos que veremos a continuación.

3.1. Definiciones

3.1.1. Plano proyectivo

Sea K un cuerpo, *el plano proyectivo* $\mathbb{P}^2(K)$ definido sobre K son la tripletas:

$$(X, Y, Z) \text{ t.q. } X, Y, Z \in K$$

donde X, Y, Z no son simultáneamente 0 y definimos la relación de equivalencia:

$$Eq : (X, Y, Z) \equiv (X', Y', Z') \iff \exists \lambda \in K \text{ t.q. } X = \lambda X', Y = \lambda Y', Z = \lambda Z'$$

Se define *el plano proyectivo* sobre el cuerpo K como:

$$\mathbb{P}^2(K) = \frac{K^3 \setminus (0, 0, 0)}{Eq}$$

3.1.2. Curva elíptica

Una *curva elíptica* se define sobre el conjunto de soluciones de la ecuación Weierstrass homogénea de la forma:

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \quad (3.1)$$

donde $a_1, a_2, a_3, a_4, a_6 \in K$, esta notación es conocida como forma larga Weierstrass. Dicha curva debe ser no singular, es decir, si la escribimos de la forma $F(X, Y, Z) = 0$, las derivadas parciales no deben ser cero simultáneamente en ningún punto de la curva. El conjunto de los *puntos K -racionales* en E son la solución de la ecuación 3.1 y lo denotaremos $E(K)$. Destacar que la curva tiene exactamente un punto racional con coordenada Z igual a cero, el $(0, 1, 0)$, este es el punto en el infinito y lo denotaremos como \mathcal{O} .

Nota:

Esta representación de la curva permite realizar operaciones de forma eficiente, esto puede verse en [3, pag. 31-32].

3.2. Paso al plano afín

Si tomamos la ecuación 3.1 y definimos el cambio de forma que:

- El punto \mathcal{O} se toma como el infinito en cualquier dirección en K^2 .
- Un punto en el plano proyectivo con $Z \neq 0$ como $\left(\frac{X}{Z}, \frac{Y}{Z}\right)$ en K^2 .
- Para volver al plano proyectivo se toma cualquier $Z \in K$ y se calcula $(X \cdot Z, Y \cdot Z, Z)$.

Con este cambio la curva queda definida por:

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \quad (3.2)$$

con $a_1, a_2, a_3, a_4, a_6 \in K$

Es posible demostrar (se demuestra en [3, pag. 25-26]) que dada cualquier curva de la forma 3.2, existe un isomorfismo a la curva que llamaremos *forma corta Weierstrass*:

$$E : Y^2 = X^3 + aX + b \quad (3.3)$$

donde $a, b \in K$

3.3. Ley de grupo

Definimos la *suma de puntos*, sea $P, Q \in E$, entonces:

- Se toma la recta que une P y Q .
- Se calcula el punto de corte de la recta y la curva E al que llamaremos R .
- $P + Q$ se define como el simétrico de R respecto al eje x .

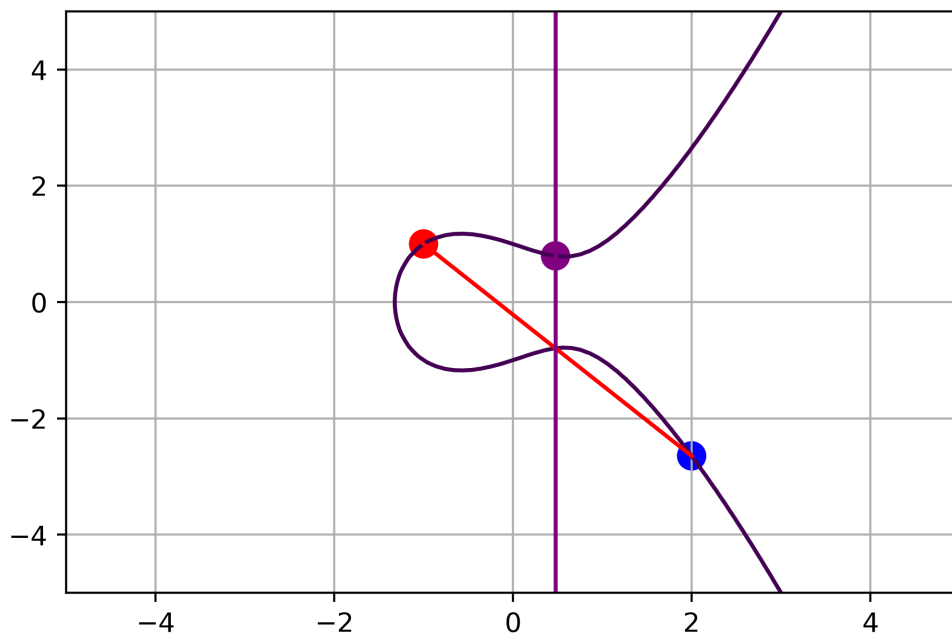


Figura 3.1: Suma de puntos

Observación:

[2] $P = P + P$ se calcula usando la recta tangente a la curva en el punto P , por lo que si la tangente es una recta vertical se considera que $P + P = \mathcal{O}$.

De manera algebraica definimos la *suma de puntos* como:

Sea la curva de la forma

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

y los puntos de la curva $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$. Entonces $-P_1 = (x_1, -y_1 - a_1x_1 - a_3)$.

Tomamos λ, μ :

$$\begin{cases} x_1 \neq x_2 & \begin{cases} \lambda = \frac{y_2 - y_1}{x_2 - x_1} \\ \mu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1} \end{cases} \\ x_1 = x_2, P_2 \neq P_1 & \begin{cases} \lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} \\ \mu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} \end{cases} \end{cases}$$

Entonces si $P_3 = (x_3, y_3) = P_1 + P_2 \neq \mathcal{O}$ se puede calcular x_3 e y_3 como:

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$

$$y_3 = -(\lambda + a_1)x_3 - \mu - a_3$$

Nota:

Para un entero positivo m tenemos que $[m]$ denota la aplicación de la *multiplicación-por-m* de la curva en si misma. Esta aplicación lleva un punto P a $\underbrace{P + P + \dots + P}_{m \text{ veces}}$.

Esta aplicación será la base de la criptografía sobre curvas elípticas ya que se considera fácil de computar pero difícil de invertir como hemos visto en el capítulo 2.3.

3.4. Curvas elípticas sobre cuerpos finitos

Sobre un cuerpo finito \mathbb{F}_q el número de puntos racionales de la curva es finito y queda determinado por:

$$\#E(\mathbb{F}_q) = q + 1 - t$$

Donde t se conoce como la traza de Frobenius.

Teorema de Hasse: t cumple que $|t| < 2\sqrt{q}$.

La aplicación q^{th} -potencia de Frobenius de la curva E definida sobre \mathbb{F}_q es:

$$\varphi \begin{cases} E(\overline{\mathbb{F}_q}) \rightarrow E(\overline{\mathbb{F}_q}) \\ (x, y) \rightarrow (x^q, y^q) \\ \mathcal{O} \rightarrow \mathcal{O} \end{cases}$$

Esta aplicación es un endomorfismo que respeta la operación de la ley de grupo $\varphi(P + Q) =$

$$\varphi(P) + \varphi(Q)$$

3.5. Compresión de punto

Para transmitir la información de un punto en una curva elíptica en el plano afín se podría enviar las coordenadas x e y del punto, pero esto puede mejorarse si nos damos cuenta que para cada coordenada x solo hay dos posibles valores en la curva de la coordenada y , por lo que solo es necesario indicar cual debemos tomar, reduciendo nuestra representación a la mitad más un bit del tamaño original.

Demostración:

Para una curva elíptica sobre un cuerpo finito \mathbb{F}_p^* con p un número primo grande, tomamos $\alpha \in \mathbb{F}_p^*$.

Ahora bien, siendo $\pm\beta$ las raíces cuadradas de α , estas tienen distinta paridad, ya que $-\beta = p - \beta$. Por tanto podemos reconstruir cualquier punto de la curva indicando con un bit b la paridad de y .

Computamos $\beta = \sqrt{x^3 + ax + b} \pmod{p}$. Si la paridad de β y b coinciden asignamos $y = \beta$, en caso contrario asignamos $y = p - \beta$. Si $\beta = 0$ asignamos $y = 0$ sin importar b .

Capítulo 4

Clave pública

Los esquemas de clave pública se basan en una pareja de claves (clave pública, clave privada), estas claves a diferencia de la criptografía simétrica requieren de su pareja para realizar la operación inversa.

Existen dos usos fundamentales de este tipo de esquemas, el primero donde dos extremos quieren intercambiar información, el emisor usará la clave pública del receptor para cifrar el mensaje y enviarlo, el receptor al ser el único conocedor de su clave privada puede recuperar el mensaje original, el segundo caso donde el emisor hace uso de su clave privada y el mensaje para que cualquier receptor pueda validar la identidad del emisor y la integridad del mensaje haciendo uso de la clave pública del emisor, este caso es el que se conoce como *firma digital*.

4.1. Intercambio de claves Diffie-Hellman

En algunos algoritmos es necesario que partes no autenticadas lleguen a intercambiar claves por un canal no seguro, esto supuso un problema que solventaron Whitfield Diffie y Martin Hellman con su protocolo, se utiliza para acordar claves simétricas en una sesión y esto posteriormente permite los protocolos de comunicación autenticada. Su seguridad tiene origen en el problema del logaritmo discreto ya que, como hemos visto antes en el capítulo 2.3, es fácil de computar y difícil de invertir.

Supongamos que tenemos dos usuarios finales que quieren comunicarse entre sí, sean estos Alice y Bob, el protocolo Diffie-Hellman en una versión simple sigue los siguientes pasos:

- Fijar un primo p y un generador del grupo $g \in \mathbb{Z}_p^*$. Estos valores son conocidos para

cualquiera que tenga acceso al canal donde se intercambian.

- Alice elige un $a \in \mathbb{Z}_{p-1}$, computa $A = g^a \bmod p$ y lo envía a Bob.
- Bob elige un $b \in \mathbb{Z}_{p-1}$, computa $B = g^b \bmod p$ y lo envía a Alice.

Con esta información ambos extremos son capaces de computar $K = (g)^{ab} \bmod p$, ya que Alice puede calcular $K = B^a \bmod p$ y Bob $K = A^b \bmod p$. Se utilizará K como la clave compartida.

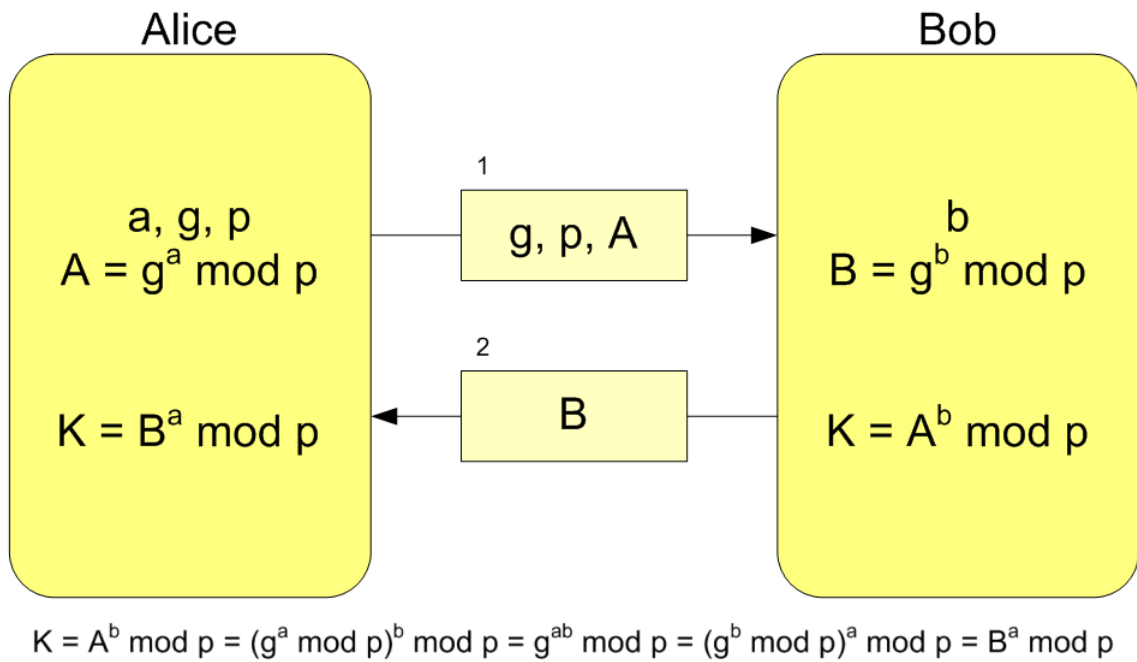


Figura 4.1: Intercambio de claves Diffie-Hellman

No obstante cualquier atacante que quiera conocer la clave K en el canal solo tiene acceso a g, p, A y B , por lo que para computar la clave tiene que calcular $a = \log_p(A)$ y $b = \log_p(B)$ siendo este el logaritmo discreto.

Existen ataques a este protocolo que no están basados en resolver el logaritmo discreto sino en aprovechar que las partes no están autenticadas y por tanto hacer creer a ambos que él es el otro extremo, esto es conocido como *Man-in-the-middle*.

De la misma forma que se aplica este protocolo en su versión original es posible aplicarla sobre el grupo aditivo de las curvas elípticas, este protocolo es conocido como EC-DH y una de las ventajas que nos proporciona es que utilizando la compresión de punto se puede reducir la

cantidad de información necesaria para realizar el protocolo con la misma seguridad, reduciendo el ancho de banda y mejorando el rendimiento. Curve25519 es una curva elíptica conocida por ofrecer buen rendimiento.

4.2. Funciones Hash

Hasta este punto hemos visto como se puede mantener la confidencialidad de un mensaje para que cualquier atacante no pueda obtener la información aún teniendo acceso al canal por el que se transmite, no obstante debemos tener en cuenta el escenario donde el atacante manipula el mensaje, por tanto debemos preocuparnos de la integridad, para comprobar que un mensaje no ha sido modificado es habitual hacer uso de *funciones hash*.

Una *funcion hash* es una aplicación que lleva una cadena de bits de cualquier longitud a una cadena de bits de longitud fija. Estas funciones tienen una serie de propiedades deseables, si tenemos la función hash $h(x) = y$, sus propiedades deberían ser:

- Resistencia a la preimagen: debe ser difícil a efectos prácticos que conociendo y se pueda calcular x .
- Resistencia a colisiones: debe ser difícil encontrar dos valores x y x' tal que $h(x) = h(x')$ pero $x \neq x'$.
- Resistencia a la segunda preimagen: dado un x debe ser difícil encontrar otro x' tal que $h(x) = h(x')$ pero $x \neq x'$.

Más adelante veremos como estas funciones son necesarias a la hora de comprobar la integridad de la información, ya que cualquier pequeña modificación en el mensaje se reflejaría al calcular el hash del mismo.

4.3. Cifrado de clave pública

Para poder realizar el cifrado de clave pública se deben llevar a cabo varias etapas con la que se pueden definir los distintos algoritmos:

- Generación de claves: En primer lugar se debe acometer la tarea de generar las claves necesarias para el cifrado, estas están basadas en algún problema matemático complejo

de invertir, el resultado de esta etapa debe ser la clave privada, que debe ser conocida únicamente por el receptor del mensaje, y la clave pública que debe dejarse a disposición de cualquiera ya que esto no debe comprometer la seguridad del sistema.

- **Cifrado:** Una vez un emisor desea enviar un mensaje, debe hacer uso de la clave pública del receptor para transformar el mensaje como indique el esquema correspondiente para posteriormente enviarlo.
- **Descifrado:** Cuando un receptor ha recibido un mensaje debe hacer uso de su clave privada, que es conocida únicamente por él, para recuperar el mensaje original por medio de las transformaciones que requiera el esquema correspondiente sin que nadie haya podido modificarlo ni leerlo.

Esto a priori no garantiza la autenticidad del emisor, no obstante veremos como se solventa este problema en el siguiente apartado.

Se denomina *corrección* de un esquema a la propiedad de poder recuperar el mensaje original aplicando el descifrado sobre el mensaje cifrado sin intervención del adversario.

4.3.1. Ejemplo: Cifrado RSA

Como ejemplo de esquema de clave pública vamos a analizar RSA, nombrado así por sus creadores Rivest, Shamir y Adleman, ya que es uno de los primeros ,originado en 1979, y además es uno de los algoritmos más usados tanto para cifrar como para firmar digitalmente.

En primer lugar analicemos en que consiste el algoritmo aplicado al cifrado de mensajes entre extremos.

Supongamos dos usuarios finales Alice y Bob. Bob quiere enviar un mensaje a Alice y para ello se va a usar el algoritmo RSA, este consiste en:

- **Generación de claves:**
 - Alice elige dos números primos grandes p y q y calcula $N = p \cdot q$.
 - Alice elige un exponente e de forma que $\text{mcd}(e, (p - 1) \cdot (q - 1)) = 1$.

- En el calculo del exponente para descifrar, Alice usa el algoritmo de Euclides extendido para conocer d en la ecuación:

$$e \cdot d \equiv 1 \pmod{(p-1)(q-1)} \quad (4.1)$$

En este punto la clave pública de Alice es el par (N, e) y su clave privada es la tripleta (d, p, q) . Por tanto para intercambiar el mensaje se realizan los siguientes pasos:

■ Cifrado:

- Bob quiere mandar su mensaje m , por lo que cifra el mensaje para obtener c calculando $c = m^e \pmod N$.

■ Descifrado:

- Alice recibe c por lo que para poder leer el mensaje tiene que calcular m de la forma $m = c^d \pmod N$.

Teorema: El cifrado RSA presentado es correcto.

Demostración: Corrección del esquema

Queremos demostrar que $m = c^d \pmod N$.

El orden del grupo $(\mathbb{Z}/N\mathbb{Z})^*$ viene dado por $\phi(N) = (q-1)(p-1)$, por tanto:

$$\forall x \in (\mathbb{Z}/N\mathbb{Z})^* : x^{(q-1)(p-1)} \equiv 1 \pmod N \quad (4.2)$$

Ahora bien, para algún entero s se tiene que $ed - s(q-1)(p-1) = 1$ puesto que se cumple la ecuación 4.1. Por tanto:

$$\begin{aligned} c^d &= m^{ed} \pmod N \\ &= m^{1+s(q-1)(p-1)} \pmod N \\ &= m \cdot m^{s(q-1)(p-1)} \pmod N \\ &= m \pmod N \end{aligned}$$

Como queríamos demostrar.

Nota: La seguridad de este algoritmo reside en el problema de factorización, ya que si logramos factorizar N como $p \cdot q$ entonces podremos calcular d , no obstante este problema se considera complejo a nivel de cómputo.

4.4. Firma digital

La firma digital es un mecanismo que se usa para verificar el origen de un mensaje, es decir, asegura la autenticación del emisor y el no repudio, además permite también verificar la integridad del mensaje.

Para lograr este objetivo se llevan a cabo diferentes etapas que definen los diferentes esquemas, estas son:

- **Generación de claves:** Al igual que en el cifrado, se debe acometer la tarea de generar las claves necesarias para la firma digital, estas están basadas en algún problema matemático complejo de invertir, el resultado de esta etapa debe ser la clave privada, que debe ser conocida únicamente por el receptor del mensaje, y la clave pública que debe dejarse a disposición de cualquiera ya que esto no debe comprometer la seguridad del sistema.
- **Firma:** Cuando un emisor desea firmar un mensaje, debe hacer uso de la clave privada de la forma que indique el algoritmo para dejar una información a la que llamamos *firma* y que enviaremos junto al mensaje.
- **Verificación:** Haciendo uso del mensaje recibido, la firma y la clave pública del emisor, el receptor puede verificar la autenticidad, integridad y no repudio del mensaje mediante los pasos que se detallan en el algoritmo.

4.4.1. Ejemplo: Firma digital con RSA

Existen varias implementaciones diferentes de este mecanismo, pero en este caso nos vamos a centrar en la firma con RSA.

Supongamos dos usuarios finales Alice y Bob, Alice quiere enviar un mensaje a Bob, pero Bob tiene que poder asegurarse que el mensaje procede de Alice y nadie lo ha modificado, para ello van a usar la firma digital:

- **Generación de claves:** De la misma forma que se genera en la sección 4.3.1, Alice genera su clave privada (N, e) y su clave pública (d, p, q) .
- **Firma:**

- Alice aplica una función hash h al mensaje m , quedandose con $r_s = h(m)$.
 - Alice usa su clave privada (d, p, q) para cifrar r_s , esta será la firma del mensaje $S = r_s^d \bmod p \cdot q$.
 - Alice envía el mensaje, que no tiene porque estar cifrado, junto con la firma a Bob.
- Verificación:
- Bob recibe el mensaje y la firma de Alice y usa la firma para calcular $r_s = S^e \bmod N$ con la clave pública de Alice (e, N) .
 - Bob aplica la misma función hash que Alice al mensaje $r_m = h(m)$.
 - Si $r_s = r_m$ entonces el mensaje queda verificado.

Dado que Alice tuvo que usar su clave privada para cifrar la firma, no es posible modificar la firma S sin que invalide la verificación, de la misma forma que ocurre en el mensaje ya que no podrías cifrar el nuevo hash.

Capítulo 5

Cifrado basado en identidad

El cifrado basado en identidad es un esquema de clave pública donde la clave de un usuario se obtiene a partir de una información que lo identifique, ya sea su email, número de teléfono, etc...

Este esquema necesita de un generador de claves privadas (PKG), este provee a los usuarios de su clave privada y les da la forma de conocer la clave pública de los demás usuarios a partir de su identidad, el proceso que realiza un usuario final para conocer su clave privada y la clave pública de los demás solo se necesita aplicar una vez.

Si dos usuarios finales quieren intercambiar un mensaje, por ejemplo Alice quiere enviar un mensaje a Bob, entonces Alice usa la clave pública maestra con la identidad de Bob para cifrar el mensaje y lo envía, luego Bob usará su clave privada para descifrar el mensaje, como queda representado en el siguiente diagrama.

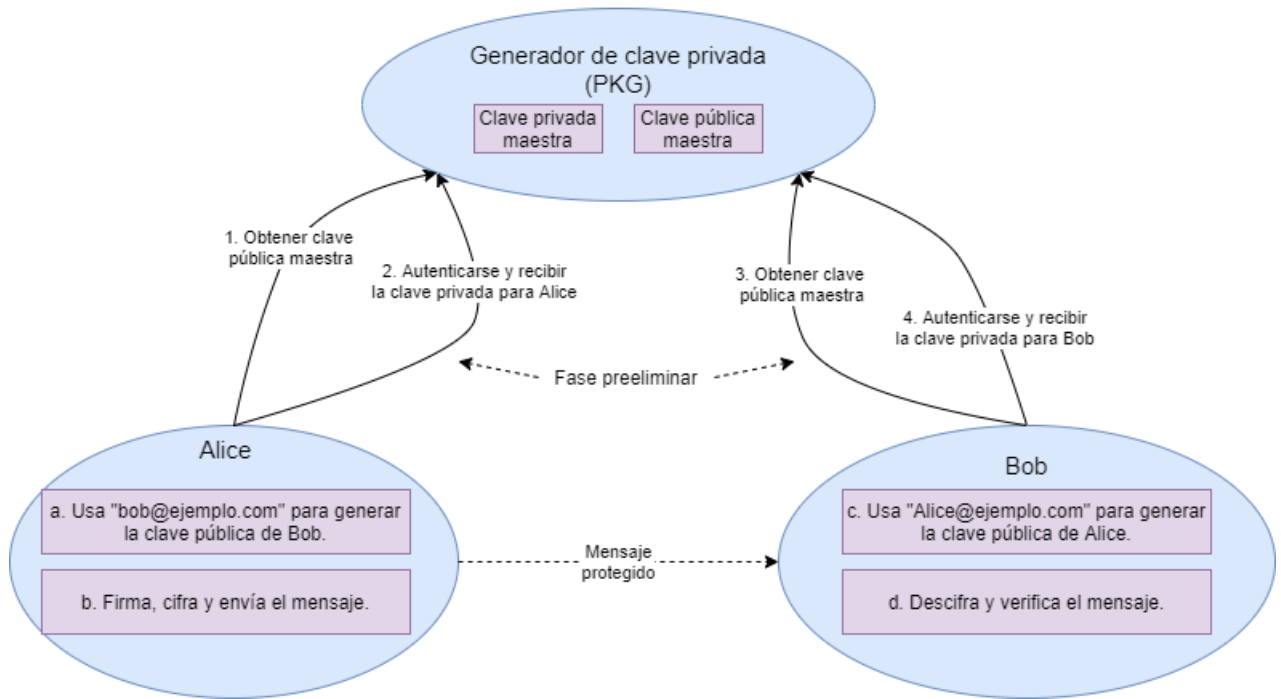


Figura 5.1: Cifrado basado en identidad

5.1. Emparejamiento

Dados dos grupos cíclicos aditivos G_1, G_2 de orden primo p y un grupo cíclico G_T escrito multiplicativamente, un *emparejamiento* es una aplicación $e : G_1 \times G_2 \rightarrow G_T$ que cumple:

- Bilinealidad:

$$\forall a, b \in F_p^*, \forall P \in G_1, \forall Q \in G_2 : e(aP, bQ) = e(P, Q)^{ab}$$

- No degenerado:

$$\forall P \in G_1 \ P \neq 0, \exists Q \in G_2 \text{ t.q. } e(P, Q) \neq 1$$

$$\forall Q \in G_2 \ Q \neq 0, \exists P \in G_1 \text{ t.q. } e(P, Q) \neq 1$$

- Computable: existe un algoritmo eficiente para computar e .

5.2. Esquema basado en emparejamiento

En este punto tenemos los conceptos necesarios para plantear el esquema propuesto en el artículo original de Dan Boneh y Matthew Franklin sobre cifrado basado en identidad usando

Weil pairing [1].

5.2.1. Preparación

Para poder tener los elementos necesarios del cifrado basado en identidad, necesitamos un paso previo de selección de parámetros para el algoritmo. Sea \mathcal{G} un generador de parámetros para el problema Diffie-Hellman Bilineal [1, pag. 7-9].

Dado un parámetro de seguridad $k \in \mathbb{Z}^+$, se realizan los siguientes pasos:

- Paso 1: Ejecutar \mathcal{G} con el parámetro k para obtener un primo q , dos grupos G_1 y G_2 de orden q y un emparejamiento válido $e : G_1 \times G_1 \rightarrow G_2$. Elegir al azar un generador $P \in G_1$.

Nota: G_1 es elegido como un subgrupo de $E(\mathbb{F}_p)$, en concreto el subgrupo generado por $P \in E(\mathbb{F}_p)$ de orden q . Por otro lado G_2 es el subgrupo de $\mathbb{F}_{p^2}^*$ de orden q .

- Paso 2: Elegir al azar $s \in \mathbb{Z}_q^*$ y tomar $P_{pub} = sP$. La clave maestra será s .
- Paso 3: Elegir las funciones criptográficas:

$$H_1 : \{0, 1\}^* \rightarrow G_1^*$$

$$H_2 : G_2^* \rightarrow \{0, 1\}^n$$

El espacio de mensajes es $\mathcal{M} = \{0, 1\}^n$, el espacio de texto cifrado es $\mathcal{C} = G_1^* \times \{0, 1\}^n$.

Los parámetros para el sistema son $\langle q, G_1, G_2, e, n, P, P_{pub}, H_1, H_2 \rangle$, junto con la clave maestra s .

5.2.2. Obtención de clave privada

Cuando un usuario del sistema quiere solicitar su clave privada, se realiza el siguiente computo.

Dada su $ID \in \{0, 1\}^*$ calculamos $Q_{ID} = H_1(ID) \in G_1^*$ y tomamos d_{ID} como la clave privada de la forma $d_{ID} = sQ_{ID}$.

5.2.3. Cifrado

Sea el mensaje $M \in \mathcal{M}$, para poder cifrarlo en primer lugar se calcula la clave pública del destinatario, para ello se computa $Q_{ID} = H_1(ID) \in G_1^*$, se elige al azar $r \in \mathbb{Z}_q^*$, el texto cifrado sería:

$$C = \langle rP, M \oplus H_2(g_{ID}^r) \rangle$$

donde $g_{ID}^r = e(Q_{ID}, P_{pub}) \in G_2$

5.2.4. Descifrado

Sea el mensaje cifrado $C = \langle U, V \rangle \in \mathcal{C}$ que ha sido computado con la clave pública usando la identidad ID . Para descifrar el mensaje usando la clave privada $d_{ID} \in G_1^*$ y obtener el mensaje original M tenemos que computar:

$$M = V \oplus H_2(e(d_{ID}, U))$$

Teorema: El cifrado basado en identidad presentado es correcto.

Demostración: Corrección del esquema.

Se quiere demostrar que $M = V \oplus H_2(e(d_{ID}, U))$.

Para demostrar que el mecanismo de cifrar y descifrar efectivamente es correcto, hay que probar que el mensaje original puede obtenerse descifrando el mensaje cifrado. Para ello se debe usar la propiedad de bilinearidad del emparejamiento.

$$\begin{aligned} V \oplus H_2(e(d_{ID}, U)) &= V \oplus H_2(e(sQ_{ID}, rP)) \\ &= V \oplus H_2(e(Q_{ID}, P)^{rs}) \\ &= V \oplus H_2(e(Q_{ID}, sP)^r) \\ &= V \oplus H_2(e(Q_{ID}, P_{pub})^r) \\ &= V \oplus H_2(g_{ID}^r) \\ &= M \oplus H_2(g_{ID}^r) \oplus H_2(g_{ID}^r) \\ &= M \end{aligned}$$

5.3. Consideraciones sobre el esquema

- La clave maestra es un punto crítico del sistema, ya que si alguien es capaz de conseguirla podrá obtener todas las claves privadas de los usuarios del sistema.
- Si se rompe una clave privada se podrían descifrar todos los mensajes anteriores cifrados con la clave publica correspondiente.
- Para una clave privada comprometida es imposible generar una nueva asociada a esa ID.
- Si se conoce desde el principio el número de participantes del sistema se puede eliminar el generador de claves privadas (PKG) una vez todos los usuarios conozcan la suya, eliminando unos de los posibles puntos de ataque.

Capítulo 6

Conclusiones

En las últimas décadas los mecanismos criptográficos se han basado en dos problemas fundamentalmente, el logaritmo discreto que se ha tratado en este estudio y el problema de la factorización de números enteros. Aunque se consideren problemas difíciles en tiempo de cómputo y se haya planteado el algoritmo Baby-step/Giant-step de complejidad $\mathcal{O}(\sqrt{p})$, esto no significa que no haya algoritmos mejores y que puedan comprometer en un futuro la seguridad de los sistemas basados en estos dos problemas. De hecho existen algoritmos en el paradigma de la computación cuántica capaces de resolver estos problemas con una menor complejidad como el algoritmo de Shor.

La seguridad de los sistemas una vez se implementan crean puntos de ataque que no están contemplados originalmente en el algoritmo, ya sea por la elección de los números primos, ataques de canal lateral o por las funciones hash elegidas. Por lo que un esquema que de forma teórica tiene buenos mecanismos de seguridad puede ser vulnerable cuando se lleva a la práctica.

Este trabajo me ha aportado los fundamentos necesarios para entender el razonamiento detrás de algunos esquemas de cifrado y firma digital, permitiéndome llevar los conceptos teóricos desarrollados en el grado hacia una utilidad real de las matemáticas, además de esto me ha permitido comprender los problemas que enfrentan fuera del ámbito académico los matemáticos que en el caso de este estudio lograron combinar las ramas de álgebra y geometría de una manera ingeniosa para dar lugar a un grupo que no es nada obvio.

Bibliografía

- [1] D. Boneh and M. K. Franklin. *Identity-Based Encryption from the Weil Pairing Advances in Cryptology*. Springer-Verlag, 2001.
- [2] N. Koblitz. *A Course in Number Theory and Cryptography*. Springer-Verlag, 1991.
- [3] N. Smart. *Cryptography: An Introduction (3rd Edition)*. McGraw-Hill College, 2003.
- [4] L. C. Washington. *Elliptic Curves: Number Theory And Cryptography (2n Edition)*. Chapman and Hall/CRC, 2008.

Capítulo 7

Anexo: Representación de curvas elípticas

Durante mi estudio quería comprender y verificar que las fórmulas que se plantean para la ley de grupo de las curvas elípticas se contrastaban con la idea geométrica de la suma de puntos, por lo que desarrollé el siguiente código que permite representar una curva en el plano afín partiendo de los parámetros a y b de la forma corta de Weierstrass de la curva, así como incorporar puntos a partir de la coordenada x y el signo del punto, para posteriormente poder computar la suma y representarlo como se puede ver en la figura 3.1

```
import numpy as np
import math
import matplotlib.pyplot as plt
# Siempre en la forma corta de Weierstrass
class curva:
    a = -1
    b = 1
    #lista de diccionarios {nombre,x,signo,[color]}
    puntos = []
    def __init__(self,a,b):
        self.a=a
        self.b=b
    def dibuja(self):
        y, x = np.ogrid[-5:5:100j, -5:5:100j]
        plt.contour(x.ravel(), y.ravel(), pow(y, 2) - pow(x, 3)\
```

```

        - x * self.a - self.b, [0])
plt.grid()

def figura(self):
    plt.show()

def limpiar_p(self):
    self.puntos=[]
def add_p(self,punto):
    self.puntos.append(punto)
def dibuja_p(self):
    X=[punto['x'] for punto in self.puntos]
    Y=[self.calcula_y(punto) for punto in self.puntos]
    colors=[punto['color'] if 'color' in punto.keys()\
            else 'purple' for punto in self.puntos]
    plt.scatter(X,Y,c=colors,s=100)

def calcula_y(self,punto):
    return punto['signo']*math.sqrt(pow(punto['x'], 3)\
        + punto['x'] * self.a + self.b)

def suma_p(self,nombre1,nombre2):
    A=next(item for item in self.puntos\
        if item["nombre"] == nombre1)
    B=next(item for item in self.puntos\
        if item["nombre"] == nombre2)
    A_x=A['x']
    A_y=self.calcula_y(A)
    B_x=B['x']
    B_y=self.calcula_y(B)
    if A_x != B_x:

```



```

        lamda=(B_y-A_y)/(B_x-A_x)
        mu=(A_y*B_x-B_y*A_x)/(B_x-A_x)
    elif A_x == B_x and A_y != B_y:
        lamda=(3*pow(A_x,2)+self.a)/(2*A_y)
        mu=(-pow(A_x,3)+self.a*A_x+2*self.b)/(2*A_y)
    else:
        return {'nombre':'inf'}
P_x=pow(lamda,2)-A_x-B_x
P_y=-lamda*P_x-mu
punto = {'nombre':'%s + %s'%(nombre1,nombre2),'x':P_x,\
        'signo':1 if P_y>=0 else -1}
return punto

#El primer punto debe tener menor x
def dibuja_suma_p(self,nombre1,nombre2):
    A=next(item for item in self.puntos\
        if item["nombre"] == nombre1)
    B=next(item for item in self.puntos\
        if item["nombre"] == nombre2)
    suma=self.suma_p(nombre1,nombre2)
    y_init=self.calcula_y(A) if min(A['x'],suma['x'])==A['x']\
        else -self.calcula_y(suma)
    y_fin=self.calcula_y(B) if max(B['x'],suma['x'])==B['x']\
        else -self.calcula_y(suma)
    plt.plot([min(A['x'],suma['x']),\
        max(B['x'],suma['x'])], [y_init,y_fin], 'r-')
    plt.axvline(x=suma['x'],c='purple')

def guarda_plot(directorio="",nombre="Curva",extension="png"):
    plt.savefig("%s%s.%s"%(directorio+"/"if directorio!=""\
        else "",nombre,extension),dpi=400)

```