Criptograf?a de curva

May 17, 2017

1 Resúmen

- No se trata de un nuevo criptosistema, sino de un nuevo enfoque.
- Se trata de usar funciones de un solo sentido en un contexto nuevo, usando una aritmética que hace los problemas más difíciles.
- Las curvas elípticas han sido muy estudiadas desde hace más de 150 años. Su uso en Criptografía fue propuesto en 1985 independientemente por Neal Koblitz(Univ. de Washington) y Victor Miller (IBM, Yorktown Heights).
- Unacurva elíptica es una curva en el plano tal que cada línea que la corta en 2 puntos, la corta además exactamente en un tercer punto.

2 Definiciones Previas:

- Cuerpo: Un cuerpo es un anillo de división conmutativo, es decir, un anillo conmutativo y unitario en el que todo elemento distinto de cero es invertible respecto del producto. Por tanto un cuerpo es un conjunto K en el que se han definido dos operaciones, + y ·, llamadas adición y multiplicación respectivamente, que la propiedades:
  - K es cerrado para la adición y la multiplicación
  - Asociatividad de la adición y la multiplicación
  - Conmutatividad de la adición y la multiplicación
  - Existencia de un elemento neutro para la adición y la multiplicación
  - Existencia de elemento opuesto y de inversos:
  - Distributividad de la multiplicación respecto de la adición
- Sea K un cuerpo y $x \in K^* = K$–0. El orden de x es el mínimo número $r > 0$ talque $x^r = 1$.
- Sea K un cuerpo. La clausura algebraica deKes el cuerpomáspequeñoque contiene a K y tal que cualquier polinomio concoeficientes enKtienetodas las raíces en este cuerpo
- La característica de un cuerpo K es el mínimo número "p" tal que para todo $x \in K$ se cumple que 1 + 1 + ... + 1(p veces)=0, donde 0 es el elemento neutro de la suma y 1 es el elemento neutro del producto en elcuerpo K. Escribiremos $char(K) = p$.
- Si para todo $n \in N$, 1 + 1 +...+ 1(p veces)=0 decimos que $char(K) = 0$.
- Grupo : (G, *) se define con una estructura basal de magma4. Queda así establecido al definir al operador "*" como interno lo que permite operar entre sí a los elementos del conjunto, obteniendo como resultado otro elemento de ese mismo conjunto, a este concepto también se le denomina clausura lineal.
  - (G, *) verifica la propiedad asociativa.
  - (G, *) posee un elemento de identidad o elemento neutro e.
  - (G, *) es un grupo si además, verifica la existencia de elemento simétrico para cada uno de sus elementos.
  - (G, *) es grupo abeliano si además, cumple la propiedad conmutativa.

3 Introducción

3.1 Criptosistema

"Un Criptosistema se define como la quíntupla (m,C,K,E,D), donde:

- m representa el conjunto de todos los mensajes sin cifrar (texto plano) que pueden ser enviados.
- C Representa el conjunto de todos los posibles mensajes cifrados, o criptogramas.
- K representa el conjunto de claves que se pueden emplear en el Criptosistema.
- E es el conjunto de transformaciones de cifrado o familia de funciones que se aplica a cada elemento de m para obtener un elemento de C. Existe una transformación diferente Ek para cada valor posible de la clave K.
- D es el conjunto de transformaciones de descifrado, análogo a E.

Todo Criptosistema cumple la condición Dk(Ek(m))=m.

Existen dos tipos fundamentales de Criptosistemas utilizados para cifrar datos e información digital y ser enviados posteriormente después por medios de transmisión libre.

- Simétricos o de clave privada: se emplea la misma clave K para cifrar y descifrar, por lo tanto el emisor y el receptor deben poseer la clave. El mayor inconveniente que presentan es que se debe contar con un canal seguro para la transmisión de dicha clave.
- Asimétricos o de llave pública:se emplea una doble clave conocidas como Kp (clave privada) y KP (clave Pública). Una de ellas es utilizada para la transformación E de cifrado y la otra para el descifrado D. En muchos de los sistemas existentes estas clave son intercambiables, es decir que si empleamos una para cifrar se utiliza la otra para descifrar y viceversa.

3.2 Criptografía de Curva Elíptica(CCE)

En los sistemas de criptografía asimétrica se utiliza 2 tipos de claves, las cuales son: la clave pública y la clave privada. En la cual mediante conceptos matemáticos podemos tener la certeza que conseguir la clave privada en cada unas de la partes(cifrado y descifrado) no sean faciles de calcular conociéndose la clave pública.

Este tipo de sistemas nos ayudan a encontrar solución a ciertos problemas matemáticos, como puede ser la realización de tests de primalidad, la factorización de números enteros, la demostración del último teorema de Fermat o el logaritmo discreto, donde g e y son elementos de un grupo cíclico finito G, y x la solución a la ecuación gˆx = y <=> x = logy, este puede ser un problema de complejidad exponencial para ciertos grupos finitos de gran tamaño, sin embargo el problema inverso, puede ser resuelto mediante exponenciación discreta.

Un criptosistema basado en curva elíptica puede lograr: * menores longitudes de las claves * mayor rapidez de calculo * menos memoria y ahorro en transferencia de los datos * con seguridad equivalente * cuando se compara con criptosistemas clásicos, como el RSA

3.2.1 Curva elíptica

Una curva elíptica sobre un cuerpo $\underline{K}$ es una curva algebraica sin puntos singulares que viene dada por una ecuación del tipo:

$$y^2 + a_1xy + a_3y = x^3 + a_4x + a_6$$

denominada ecuación general de Weierstrass.

Una curva elíptica E(K) es: * el conjunto de puntos que satisfacen la ecuación * mas un punto O en el infinito

Según la característica del cuerpo K, usamos transformaciones lineales para simplificar la ecuación, sin embargo la curva elíptica es una curva plana definida por una ecuación de la forma:

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

Con el conjunto de puntos G que forman la curva (i.e., todas las soluciones de la ecuación más un punto O, llamado punto en el infinito) más una operación aditiva +, se forma un grupo abeliano. Si las coordenadas x e y se escogen desde un cuerpo finito, entonces estamos en presencia de un grupo abeliano finito. El problema del logaritmo discreto sobre este conjunto de puntos (PLDCE) se cree que es más difícil de resolver que el correspondiente a los cuerpos finitos (PLD). De esta manera, las longitudes de claves en criptografía de curva elíptica pueden ser más cortas con un nivel de seguridad comparable.

3.3 Aritmétrica Geométrica

- El opuesto (negativo) de un punto P= (x, y) es su simétrico respecto al eje x : -P= (x, -y).

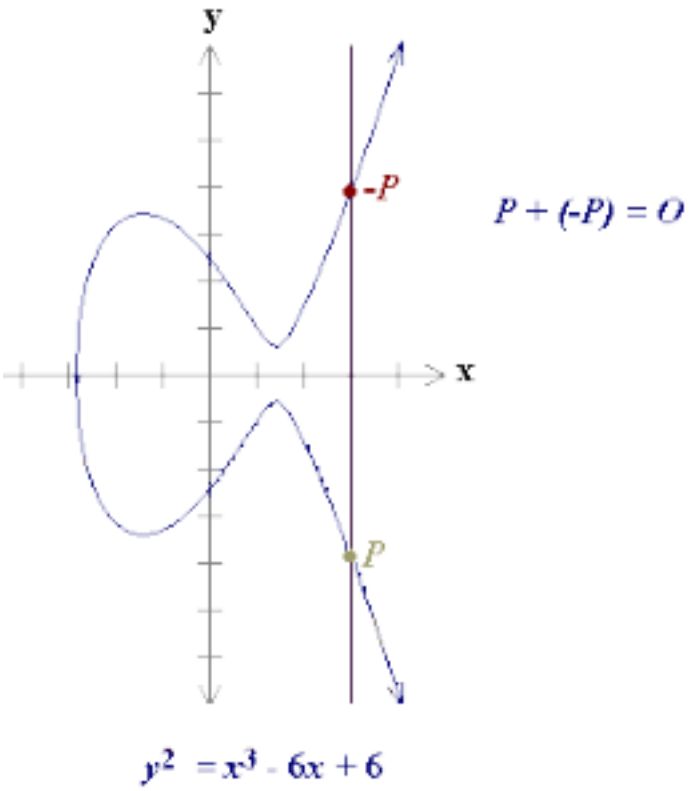

Figure 1:

Para sumar P y -P lo anterior no funciona ya que la línea que los une no corta a la curva en otro punto. Para evitar este problema se añade un punto del infinito que se designa por O, y por definición se dice que P+(-P)=O (y por tanto P + O = P).

- Para sumar dos puntos P, Q (con P!=-Q) se traza una línea que los une, que corta a la curva en otro punto R; entonces P+Q = -R.

- Para sumar P consigo mismo se traza la tangente en P, que corta a la curva en otro punto -R; entonces 2P = P + P = R.

Caso especial: Si P= (x, 0) entonces la tangente es vertical y no corta de nuevo a la curva. Entonces se establece que 2P = O.

NOTA: Debemos evitar las curvas con singularidades (tangente no es posible cuando discriminante = 0)

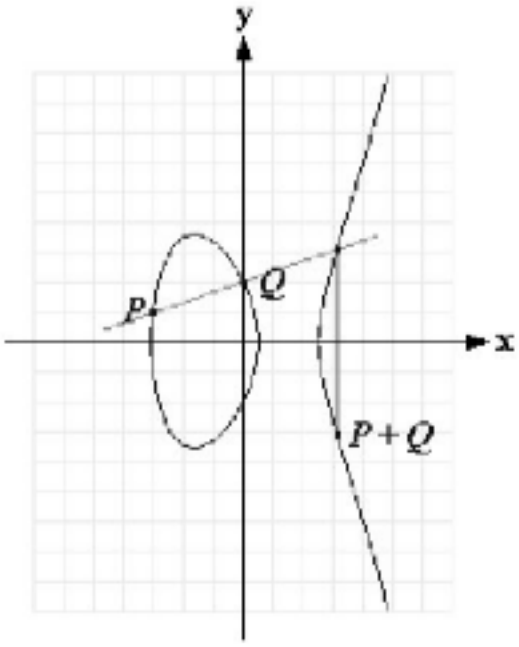

Figure 2:

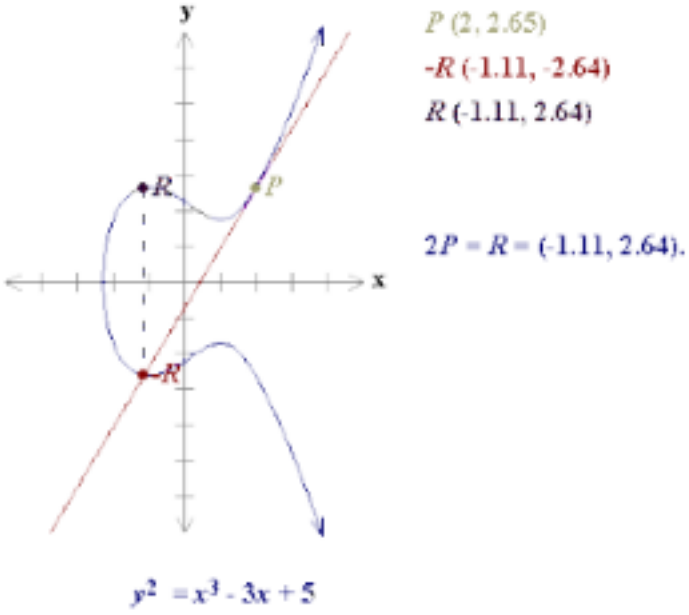

Figure 3:

3.3.1 El cálculo de la suma:

- es posible deducir fórmulas para calcular la suma
- ellas dependerán de la característica del cuerpo K.

Por ejemplo:

- Si y^2 = (x^3+ ax + b), con 4a^3+ 27b^2 != 0 mod p

$$\text{Sea } P = (x_1, y_1) \text{ y } Q = (x_2, y_2)$$
$$\text{Se define } P + Q = (x_3, y_3) \text{ por:}$$

$$x_3 = t^2 - x_1 - x_2$$
$$y_3 = t(x_1 - x_3) - y_1, \text{ donde:}$$

$$t = \begin{cases} \left(\frac{y_2 - y_1}{x_2 - x_1}\right) & \text{si} \quad P \neq Q \\ \left(\frac{3x_1^2 + a}{2y_1}\right) & \text{si} \quad P = Q \end{cases}$$

Figure 4:

- Si y^2+cy= (x^3 + ax + b), con c != 0 mod 2^m

$$x_3 = \begin{cases} \left(\frac{y_1 + y_2}{x_1 + x_2}\right)^2 + x_1 + x_2 & \text{si} \quad P \neq Q \\ \frac{x_1^4 + a^2}{c^2} & \text{si} \quad P = Q \end{cases}$$

$$y_3 = \begin{cases} \left(\frac{y_1 + y_2}{x_1 + x_2}\right)(x_1 + x_3) + y_1 + c & \text{si} \quad P \neq Q \\ \left(\frac{x_1^2 + a}{c}\right)(x_1 + x_3) + y_1 + c & \text{si} \quad P = Q \end{cases}$$

Figure 5:

3.4 Elliptic curve Diffie–Hellman (ECDH)

3.4.1 Parámetros del dominio:

Nuestros algoritmos de curva elíptica funcionarán en un subgrupo cíclico de una curva elíptica sobre un campo finito. Por lo tanto, nuestros algoritmos necesitarán los siguientes parámetros:

- El primo p que especifica el tamaño del campo finito.

- Los coeficientes a y De la ecuación de la curva elíptica.
- El punto base G que genera nuestro subgrupo.
- La orden n del subgrupo.
- El cofactor h del subgrupo.

En conclusión, los parámetros de dominio para nuestros algoritmos son el sextuplo (p, a, b, G, n, h) .

3.4.2 Algoritmo:

Diffie-Hellman: protocolo para intercambio de claves.

Sea E una curva elíptica con G un generador de un subgrupo cíclico de orden prima p.

- La clave privada es un entero aleatorio X elegido de {1, . . . , n-1} (donde n es el orden del subgrupo).
- La clave pública es el punto Y = X.G (Donde G es el punto base del subgrupo).

Si sabemos **Y** y **G** (junto con los otros parámetros del dominio), encontrar Y es "fácil". Pero si conocemos Y y G, encontrar la clave privada X es "difícil", porque nos obliga a resolver el problema del logaritmo discreto.

- Alice elige un entero secreto XA ; Bob elige XB
- Las claves públicas correspondientes son
- YA = xA · G
- YB = xB · G
- La clave compartida es
- K = xA · xB · G
- Alice calcula K = xA · YB
- Bob calcula K = xB · YA

3.4.3 Ejemplo:

Si tenemos la curva:

y^2 = x^3 +x - 1, sobre Z7,con G=(1,1)

- Alice elige xA = 4; calcula YA = 4 · G = (4,5)
- Bob elige xB = 9; calcula YB = 9 · G = (2,3)
- Alice calcula K = xA · YB = 4 · (2,3) = (6,5)
- Bob calcula K = xB · YA = 9 · (4,5) = (6,5)
- K = xA · xB · G = 4 · 9 · G = (36 mod 11) · G =
- K = 3 · G = (6,5) = (KENC,)

3.4.4 Key encrypion y key MAC

El cifrado proporciona confidencialidad, un MAC proporciona integridad. El uso de cifrado solo hace que sus mensajes sean vulnerables a un ataque de texto cifrado.

- Confidencialidad: Es la protección de datos y de información intercambiada entre un emisor y uno o más destinatarios frente a terceros. Esto debe hacerse independientemente de la seguridad del sistema de comunicación utilizado, de hecho un asunto de interés es el problema de garantizar la Confidencialidad de la comunicación utilizada cuando el sistema es inseguro.

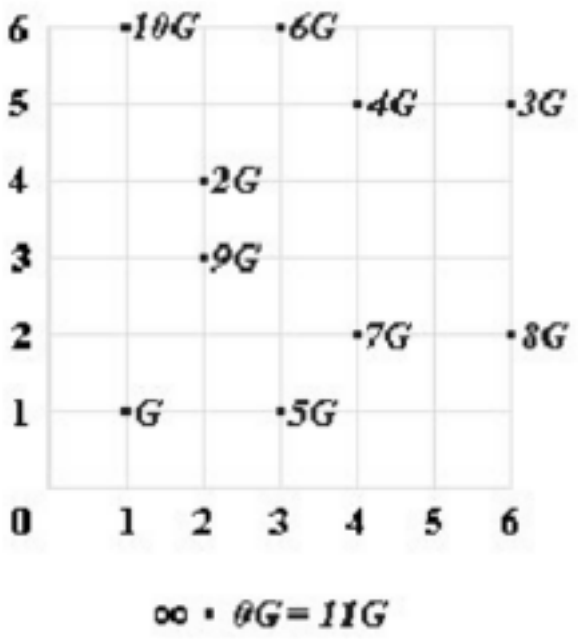

Figure 6:

- Integridad: Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. La violación de la Integridad se presenta cuando un empleado, programa o proceso por accidente o con mala intención, modifica o borra los datos importantes que son parte de la información, así mismo hace que su contenido permanezca inalterado a menos que sea modificado por el personal autorizado; y esta modificación será registrada, asegurando su precisión y confiabilidad.

  El problema de Diffie-Hellman para las curvas elípticas se supone que es un problema "duro". Se cree que es tan "difícil" como el problema del logaritmo discreto, aunque no hay pruebas matemáticas disponibles. Lo que podemos afirmar con seguridad es que no puede ser "más difícil", porque resolver el problema del logaritmo es una forma de resolver el problema de Diffie-Hellman.