Reducción del algoritmo de Lagrange

Allan y Jhon

April 24, 2016

1 Lagrange

Para ejemplificar el método de Lagrange se usara el mismo ejercicio que en el método de Shamir.

Se selccionó un anillo $Z_p = 11$ con $w = 5$ incógnitas de las que se resuelven $t = 2$. Se seleccionó como llave $k = 8$

Se seleccionan los $t - 1$ elementos del anillo Z_p
$a_0 = 5$

Del anillo Z_p se seleccionan los w elementos x
$x_1 = 2$ $x_2 = 7$ $x_3 = 9$ $x_4 = 10$ $x_5 = 3$

Se calcula el conjunto de elementos y por medio de la ecuación

$$y_n = k + \sum_{j=1}^{t-1} a_j x_j^j mod p \tag{1}$$

$y_1 = 8 + 5(2) mod 11 = 7$ $y_2 = 8 + 5(7) mod 11 = 10$
$y_3 = 8 + 5(9) mod 11 = 9$ $y_4 = 8 + 5(10) mod 11 = 3$
$y_5 = 8 + 5(3) mod 11 = 1$

Se tienen los pares $A_n(x_n, y_n)$
$A_1(2, 7)$ $A_2(7, 10)$ $A_3(9, 9)$ $A_4(10, 3)$ $A_5(3, 1)$

Para recuperar la llave k es necesario seleccionar 2 pares del conjunto A_n, los seleccionados son:
$A_2(7, 10)$ $A_4(10, 3)$

Con estos pares podemos calcular un sistema de ecuaciones resolviendo el polinomio caracteristico para $t = 2$
$a_0 + a_1 x = y$ donde $a_0 = k$
De lo que resulta el siguiente sistema de ecuaciones al sustituir los pares A_2 y A_4 en el polinomio
$a_0 + 7a_1 = 10$
$a_0 + 10a_1 = 3$

Podemos resolver el sistema de ecuaciones para obtener los valores de a_0 y a_1 o usar otro método, como es la ecuación de Lagrange como se muestra a continuación:

$$k = \sum_{j=1}^{t} y_j \prod \frac{x - x_j}{x_i - x_j} mod \quad p \tag{2}$$

Al sustituir los valores de las ecuaciones anteriores reconstruimos el polinomio original pero a nosostros solo nos interesa obtener el valor de a_0 por que esta es k. Para conseguir esto en el calculo de l_i quitamos la variable x quedando la de la siguiente forma

$$l_i = \prod \frac{-x_j}{x_i - x_j} \tag{3}$$

Ahora sustituiremos en la ecuacion (4) los pares seleccionados para recuperar el secreto $A_2(7, 10)$ y $A_4(10, 3)$ quedando las siguientes ecuaciones.

$l_2 = \frac{-x_4}{x_2 - x_4}$

Reduciendo la expresión nos queda
$l_2 = \frac{-10}{7-10} = \frac{-10}{-3} mod 11 = \frac{1}{8}$

$l_4 = \frac{-x_2}{x_4 - x_2}$

Reduciendo la expresión nos queda
$l_4 = \frac{-7}{10-7} = \frac{-7}{3} mod 11 = \frac{4}{3}$

Por ultimo para calcular el valor del secreto que estamos buscando tenemos que obtener los correspondientes coeficientes a_0 y a_1 usaremos las siguientes expresiones.

$a_0 = (y_2)(l_2)$

$a_0 = 10(\frac{1}{8}) = \frac{10}{8} = (10)(7) = 70 mod 11 = 4$

$a_1 = (y_4)(l_4)$

$a_1 = 3(\frac{4}{3}) = 4$

$k = a + b = 4 + 4 = 8$ y podemos notar que el secreto k se recupero exitosamente.