Secreto Compartido de shamir

Allan y Jhon

March 31, 2016

1 Secreto Compartido

El secreto compartido, es un metodo diseñado para compartir un objeto entre un grupo de participantes. Este metodo fue propuesto por Adi Shamir en 1997.

El objetivo de este metodo es el de dividir un secreto K en n partes,que son dadas a n participantes. Para recuperar el secreto es necesario tener almenos u elementos de las w partes siendo $u \leq w$. Y no es posible recuperar el secreto si se tienen menos que u partes.

Para construir el esquema del secreto compartido primero es necesario seleccionar un $p \geq w + 1$ el cual define el anillo Z_p.

El procedimiento para dividir un secreto K en w partes es el siguiente:

1. Se seleccionan w elementos distintos de cero del anillo Z_p denotados como x_i donde $1 \leq i \leq w$.
2. Se seleccionan $u - 1$ elementos aleatorios de Z_p denotados como $a_1, ..., a_i$.
3. Sea
$$y_n = k + \sum_{j=1}^{t-1} a_j x^j mod p \tag{1}$$
4. La salida es el conjunto $S = \{(x_1, y_1), ..., (x_w, y_w)\}$.

Para recuperar el secreto solo tenemos que resolver un sistema de ecuaciones que es definido por el polinomio caracteristico $a(x) = a_0 + a_1 x + ... + a_{u-1} x^{u-1}$.

Posteriormente se seleccionan u pares de elementos (x_w, y_w) con los que obtendremos nuestro sistema de ecuaciones a resolver. El elemento que nos interesa obtener del sistema de ecuaciones es a_0 ya que este es el valor de nuestro secreto K.

2 Ejemplo

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

Se selecciona los $u-1$ elementos del anillo Z_p
$a_1 = 5$

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

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

$$y_i = k + \sum_{j=1}^{u-1} a_j x_i^j mod p \tag{2}$$

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

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 u pares del conjunto S, 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 $u = 2$
$a_0 + a_1 x = y$ 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
$a_0 + 7a_1 = 10$
$a_0 + 10a_1 = 3$

Para resolver este polinomio lo podemos resolver por cualquiera de los metodos comunes que se usan en algebra, solo que repetando el anillo $Z_p == 1$, en este caso se resolvera por el metodo suma y res.

$$a_0 + 7a_1 = 10 \tag{3}$$
$$a_0 + 10a_1 = 3 \tag{4}$$

Multiplicamos la equacion (3) por -1 y obtenemos el siguiente sistema:

$$-a_0 - 7a_1 = -10 \tag{5}$$
$$a_0 + 10a_1 = 3 \tag{6}$$

sumamos la equacion (5) + (6) dandonos como resultado:

$$3a_1 = 4 \tag{7}$$

De la equacion (7) despejamos $a1$

$$a_1 = \frac{4}{3} \tag{8}$$

Siendo 4 el inverso multiplicativo de 3 la equacion (8) queda de la siguiente forma

$$a_1 = (4)(4) = 16mod11 = 5 \tag{9}$$

Sustituimos a_1 en la equacion (4)

$$a_0 + 10(5) = 3 \tag{10}$$

Simplificamos y despejamos a_0

$$a_0 + (50mod11) = 3 \tag{11}$$

$$a_0 + 6 = 3 \tag{12}$$

$$a_0 = 3 - 6 \tag{13}$$

$$a_0 = -3mod11 = 8 \tag{14}$$

Como $a_0 = 8$ podemos ver que esto es verdad por que $a_0 = K$ y el K que seleccionamos es $K = 8$ con lo que recuperamos K exitosamente.