Secreto Compartido

Esquema Umbral (t,n)

n partes

t<n necesarias

<t no tengo info

Esquema de Shamir: $P(x)$ donde a_0 es el secreto.

t = grado $P(x)$ +1

→ Esquema umbral (grado $P(x)$ +1, n)

Ejemplo: $P(x) = a_0 + a_1x + a_2x^2 = 7 + 2x + 5x^2$ en Z_{11}

Reparto esquema (3,n)

Sombras:

- (1,3) $(7+2+5=14 \equiv 3)$
- (2,9) $(7+4+20=31 \equiv 9)$
- (3,3) $(7+6+45=58 \equiv 3)$
- (4,7) $(7+8+80=95 \equiv 7)$
- (5,10) $(7+10+125=142 \equiv 10)$
- etc

Sombras Recibidas: $x_1 = (1,3)$ $x_2 = (5,10)$ $x_3 = (2,9)$

Rearmar P(X) con Lagrange:

$P_k(X) = \sum_{i=1}^{k} L_i(X) y_i$ Donde: $L_i(X) = \prod_{\substack{j=1 \\ j \neq i}}^{k} \frac{x - x_j}{x_i - x_j}$

O sea, si k = 3: $P(x) = L_1(x).y_1 + L_2(x).y_2 + L_3(x)y_3$

Donde: $L_1(x) = (x-x_2)(x-x_3)/[(x_1-x_2)(x_1-x_3)]$

Z_{11}*	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

$$P(x) = L_1(x) * 3 + L_2(x) * 10 + L_3(x) * 9$$

Se calcula L_1, L_2, L_3

$$L_1(x) = \frac{x-5}{1-5} * \frac{x-2}{1-2} = \frac{x^2 - 7x + 10}{7 * 10} = \frac{x^2 + 4x + 10}{4} = (x^2 + 4x + 10) * 3 = (3x^2 + 1x + 8) = L_1(x)$$

$$L_2(x) = \frac{x-1}{5-1} * \frac{x-2}{5-2} = \frac{x^2 - 3x + 2}{4 * 3} = \frac{x^2 + 8x + 2}{1} = (x^2 + 8x + 2) * 1 = (x^2 + 8x + 2) = L_2(x)$$

$$L_3(x) = \frac{x-1}{2-1} * \frac{x-5}{2-5} = \frac{x^2 - 6x + 5}{1 * -3} = \frac{x^2 + 5x + 5}{8} = (x^2 + 5x + 5) * 7 = (7x^2 + 2x + 2) = L_3(x)$$

$L_1(x) = (3x^2 + 1x + 8)$ $L_2(x) = (x^2 + 8x + 2)$ $L_3(x) = (7x^2 + 2x + 2)$

Se termina de calcular P(x):

$P(x) = L_1(x) * 3 + L_2(x) * 10 + L_3(x) * 9$

$P(x) = (3x^2 + 1x + 8) * 3 + (x^2 + 8x + 2) * 10 + (7x^2 + 2x + 2)$

$P(x) = (9x^2 + 3x + 2) + (10x^2 + 3x + 9) + (8x^2 + 7x + 7)$

$$P(x) = (5x^2 + 2x + 7)$$

Z_{11}^*	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

Sombras Recibidas: $x_1 = (1,3)$ $x_2 = (5,10)$ $x_3 = (2,9)$

Rearmar P(X) con Lagrange (versión 2)

$P_k(X) = \sum_{i=1}^{k} L_i(X) y_i$ Donde: $L_i(X) = \prod_{\substack{j=1 \\ j \neq i}}^{k} \frac{x - x_j}{x_i - x_j}$

O sea, si $k = 3$: P(x) = $s_3x^2 + s_2x + s_1$ cuya versión "encajada" es: P(x) = $(s_3x + s_2)x + s_1$

Se calcula s_1

Independientemente de qué sombras se hayan recibido, $P_3(0) = s_1$.

$P_k(0) = \sum_{i=1}^{k} L_i(0) y_i$ con: $L_i(0) = \prod_{\substack{j=1 \\ j \neq i}}^{k} \frac{-x_j}{x_i - x_j}$

$$P_3(0) = L_1(0) * 3 + L_2(0) * 10 + L_3(0) * 9$$

$$P_3(0) = \frac{-5}{1-5} * \frac{-2}{1-2} * 3 + \frac{-1}{5-1} * \frac{-2}{5-2} * 10 + \frac{-1}{2-1} * \frac{-5}{2-5} * 9$$

$$P_3(0) = \frac{10}{4} * 3 + \frac{2}{1} * 10 + \frac{5}{8} * 9$$

$$P_3(0) = 10 * 3 * 3 + 9 + 5 * 7 * 9$$

$$P_3(0) = 2 + 9 + 7$$

➔ $s_1 = 7$

Sombras Recibidas: $x_1 = (1,3)$ $x_2 = (5,10)$ $x_3 = (2,9)$

$P_3(x) = s_3x^2 + s_2x + s_1$ cuya versión "encajada" es: $P_3(x) = (s_3x+s_2)x + s_1$

Ya se tiene $s_1=7$

$$y' = \frac{y - s_1}{x}$$

Por lo tanto: $P_3(x) = (s_3x+s_2)x+ 7$

Para el par (1,3) $P_3(x) = (s_3x+s_2)x+ 7=3 \rightarrow (s_3x+s_2)x=3-7 \rightarrow (s_3x+s_2)x=7 \rightarrow (s_3x+s_2)=\frac{7}{x}=\frac{7}{1} \rightarrow (s_3x+s_2)=7 = y' = P_2(1)$

Para el par (5,10) $P_3(x) = (s_3x+s_2)x+ 7=10 \rightarrow (s_3x+s_2)x=3 \rightarrow (s_3x+s_2)x=3 \rightarrow (s_3x+s_2)=\frac{3}{x}=\frac{3}{5} \rightarrow (s_3x+s_2)=5 = y' = P_2(5)$

Se calcula s_2

$P_2(x) = s_3x + s_2$

Nuevamente, haciendo $P_2(0) = s_2$

$$P_2(0) = L_1(0) * 7 + L_2(0) * 5$$

$$P_2(0) = \frac{-5}{1-5} * 7 + \frac{-1}{5-1} * 5$$

$$P_2(0) = 6 + \frac{10}{4} * 5$$

$$P_2(0) = 6 + 7$$

$$P_k(0) = \sum_{i=1}^{k} L_i(0) y_i \qquad \text{con: } L_i(0) = \prod_{\substack{j=1 \\ j \neq i}}^{k} \frac{-x_j}{x_i - x_j}$$

➔ $s_2=2$

Sombras Recibidas: $x_1 = (1,3)$ $x_2 = (5,10)$ $x_3 = (2,9)$

$P_3(x) = s_3x^2 + s_2x + s_1$ cuya versión "encajada" es: $P_3(x) = (s_3x+s_2)x + s_1$

Se calculó s_2 a partir de:

$P_2(x) = s_3x + s_2$

Con los pares (1,7) y (5,5)

Ya se tiene $s_2=2$

Por lo tanto: $P_2(x) = (s_3x+s_2)$

Para el par (1,7) $P_2(x) = s_3x+2=7 \rightarrow s_3x=7-2 \rightarrow s_3=\frac{5}{x} = 5$

$$y' = \frac{y - s_2}{x}$$

Se calcula s_3 ➔ $s_3=5$

De esta forma, cada vez se hacen menos cálculos en cada iteración.

Sombras Recibidas: $x_1 = (1,3)$ $x_2 = (5,10)$ $x_3 = (2,9)$

Rearmar P(X) con Gauss:

Rearmo sistema para obtener a_0, a_1, a_2

Si $x = 1$: $a_0 + a_1 x + a_2 x^2 = a_0 + a_1 + a_2 = 3$

Si $x = 5$: $a_0 + a_1 x + a_2 x^2 = a_0 + a_1 5 + a_2 25 = 10$

Si $x = 2$: $a_0 + a_1 x + a_2 x^2 = a_0 + a_1 2 + a_2 4 = 9$

Se resuelve el sistema:

$a_0+a_1+a_2=3$

$a_0+a_1 5+a_2 3=10$

$a_0+a_1 2+a_2 4=9$

$$\left[\begin{array}{ccc|c} 1 & 1 & 1 & 3 \\ 1 & 5 & 3 & 10 \\ 1 & 2 & 4 & 9 \end{array}\right] \left[\begin{array}{ccc|c} 1 & 1 & 1 & 3 \\ 0 & 4 & 2 & 7 \\ 0 & 1 & 3 & 6 \end{array}\right]$$

Fila 2 por inverso de 4 módulo 11 (que es 3):

$$\left[\begin{array}{ccc|c} 1 & 1 & 1 & 3 \\ 0 & 1 & 6 & 10 \\ 0 & 1 & 3 & 6 \end{array}\right] \left[\begin{array}{ccc|c} 1 & 0 & 6 & 4 \\ 0 & 1 & 6 & 10 \\ 0 & 0 & 8 & 7 \end{array}\right]$$

Fila 3 por inverso de 8 módulo 11 (que es 7):

$$\left[\begin{array}{ccc|c} 1 & 0 & 6 & 4 \\ 0 & 1 & 6 & 10 \\ 0 & 0 & 1 & 5 \end{array}\right]$$

$$\left[\begin{array}{ccc|c} 1 & 0 & 6 & 4 \\ 0 & 1 & 6 & 10 \\ 0 & 0 & 1 & 5 \end{array}\right]$$

- $a_2 = 5$
- $a_1 + 6a_2 = 10 \rightarrow a_1 + 30 = 10 \rightarrow$
  $a_1 + 8 = 10 \rightarrow a_1 = 2$
- $a_0 + a_1 2 + a_2 4 = 9 \rightarrow a_0 + 2.2 + 5.4 = 9 \rightarrow$

$a_0 + 4 + 20 = 9 \rightarrow a_0 + 4 + 9 = 9 \rightarrow$

$a_0 + 4 = 0 \rightarrow a_0 = 7$

$$P(x) = a_0 + a_1 x + a_2 x^2 = 7 + 2x + 5x^2$$