


Esquema de compartición de secretos de Shamir

Integrantes: Daniel Valencia Cordero
Jorge M. Benavides Castro

Biografía de Shamir




- Adi Shamir
- Nació en 1952 en Tel Aviv, Israel
- Estudios en licenciatura en matemáticas, con máster y doctorado en Ciencias de la computación
- Gran Medalla de la Academia de Ciencias de Francia en 2012, por sus trabajos en criptografía.
- En 2017 , Premio Fundación BBVA Fronteras del Conocimiento, en la categoría de Tecnologías de la Información y la Comunicación.

A. S. A. Shamir, 2009 Nombre Adi Shamir Nacimiento 1952 Israel, T. A. N. israelí O. matemático, criptógrafo, y informática P. P. T. en 2002, « Adi Shamir», *Los diccionarios y las enciclopedias sobre el Académico*. [En línea]. Disponible en: <https://esacademic.com/dic.nsf/eswiki/37779>. [Accedido: 20-oct-2019].

¿En qué consiste un esquema de compartición de secretos?

Problema: Que una persona no posea todo el secreto.

Solución: Dividir el mensaje entre varias personas para que así solo una no posea todo el mensaje y que se necesite un número mínimo de estas para poder recuperar el mensaje.

« Esquema de Shamir», *Los diccionarios y las enciclopedias sobre el Académico*. [En línea]. Disponible en:
<https://esacademic.com/dic.nsf/eswiki/447965>. [Accedido: 20-oct-2019].



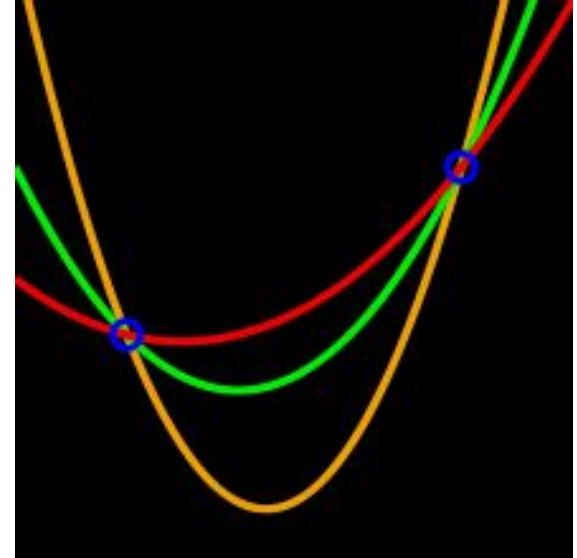
Criptografía con umbral

Tiene como objetivo distribuir alguna funcionalidad criptográfica entre muchos usuarios de tal forma que

- Cualquier conjunto con t usuarios pueda colectivamente calcular la funcionalidad
- Ningún conjunto con solo $t-1$ usuarios pueda realizar la funcionalidad.

Secreto de Shamir

- Es un algoritmo criptográfico de umbral.
- Consiste en dividir un secreto en N partes un mensaje y se da a cada participante una parte de este.
- Todas o parte de ellas son necesarias para reconstruir el secreto.



M. A. Acedo Arias, M. A. Molina Vilchis, R. Silva Otigoza, M. Marciano Melchor, y E. A. Portilla Flores, «Análisis de los secretos compartidos para la autenticación de nodos en las Wireless Sensor Networks mediante el algoritmo de Shamir», Cienc. E Ing. Neogranadina, vol. 18, n. o 2, pp. 101-116, dic. 2008.

Secreto de Shamir

Ej: Supongamos que nos interesa hacer un esquema (6,3). Eso quiere decir que hay 6 participantes y que solo al juntar al menos a 3 de ellos es posible recuperar el secreto. La clave es $S=1234$.

Se arma un polinomio de grado $3 - 1$: $P(x) = s + a_1 x + a_2 x^2$

Se le pide al usuario que de los valores de las constantes a_1 y a_2 :

$$\begin{aligned} a_1 &= 166 \\ a_2 &= 94 \end{aligned}$$

Se arma el polinomio con las constantes dadas:

$$P(x) = s + a_1 x + a_2 x^2 = 1234 + 166x + 94x^2$$

Secreto de Shamir

Se calculan 6 puntos distintos del polinomio:

(1, 1494), (3, 2578), (4, 3402), (6, 5614), (8, 8578), (11, 14434).
y se les reparte en cualquier orden a cada integrante.

Para decodificar, se resuelve el siguiente sistema de ecuaciones, suponiendo que se hayan reunido los siguientes puntos (3, 2578) (8, 8578), (11, 14434).

$$\left. \begin{array}{l} s + 3a_1 + 9a_2 = 2578 \\ s + 8a_1 + 64a_2 = 8578 \\ s + 11a_1 + 121a_2 = 14434 \end{array} \right\}$$

Esquema de Shamir modificado

Alfabeto de 31 caracteres

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Q	R	S	T	U	V	W	X	Y	Z	.	¿	?	*
17	18	19	20	21	22	23	24	25	26	27	28	29	30

Muchas gracias

