

[Ejemplo de shairer con números]

(Ampliación clase de protocolos).

$$f(x) = f_0 + f_1 x + \dots + f_{k-1} x^{k-1} \quad ; \quad f_i \in \mathbb{Z}_p, \forall i$$

acciones (sharer): $u_i \leftarrow s_i = (i, f(i))$

Reconstrucción; (tenemos k sharer, supongo que son:
 $(1, y_1), \dots, (k, y_k)$)

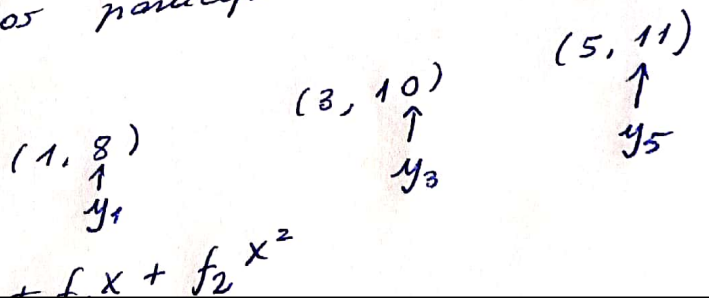
(si las sharer no son consecutivos da igual)

$$f(0) = \sum_{i=1}^k y_i \prod_{j \neq i} \frac{-j}{i-j} \pmod{p}$$

¡ Recordad! : $\frac{a}{b} \equiv a \cdot b^{-1} \pmod{p}$

Suponed, por ejemplo que en \mathbb{Z}_{17}^* nos dicen (k=3), y tenemos una coalición de los participantes

cuyas "dars" son u_1, u_3, u_5



CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
 LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
 CALL OR WHATSAPP: 689 45 44 70

Apluando la fórmula

$$f(0) = y_1 \left(\frac{-3}{1-3} \cdot \frac{-5}{1-5} \right) + y_3 \left(\frac{-1}{3-1} \cdot \frac{-5}{3-5} \right) + y_5 \left(\frac{-1}{5-1} \cdot \frac{-3}{5-3} \right)$$

$$f(0) = 8 \left(\frac{3}{2} \times \frac{5}{4} \right) + 10 \left(\frac{-1}{2} \cdot \frac{5}{2} \right) + 11 \left(\frac{-1}{4} \cdot \frac{-3}{2} \right)$$

i ojo, todo en \mathbb{Z}_{17}^* !

$$= 8 \cdot 3 \times 5 \times 8^{-1} - 10 \times 5 \times 4^{-1} + 11 \times 3 \times 8^{-1}$$

$$8^{-1} \equiv 15 \pmod{17}$$

$$4^{-1} \equiv 13 \pmod{17}$$

$$= 15 - 10 \times 5 \times 13 + 11 \times 3 \times 15$$

$$= \boxed{13} \quad \checkmark$$

i este es el secreto!

Cartagena99

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP: 689 45 44 70

Pero, ¿por qué funciona Shamir?
 La fórmula vista en teoría se justifica a través de la Teoría de Interpolación y es muy fácil de entender. Resume este razonamiento:

Si sabemos que

$$f(x) = f_0 + f_1 x + f_2 x^2$$

$$\begin{aligned} \text{y } f(1) = 8 &\Rightarrow 8 = f_0 + f_1 \cdot 1 + f_2 \cdot 1^2 \\ f(3) = 10 &\Rightarrow 10 = f_0 + f_1 \cdot 3 + f_2 \cdot 3^2 \\ f(5) = 11 &\Rightarrow 11 = f_0 + f_1 \cdot 5 + f_2 \cdot 5^2 \end{aligned}$$

(todo en \mathbb{Z}_{17}).

esto es un s.l.e (de los de ALGEBRA LINEAL)

Resolvemos el sistema;

$$\begin{aligned} e_1 \quad 8 &= f_0 + f_1 + f_2 \\ e_2 \quad 10 &= f_0 + 3f_1 + 9f_2 \\ e_3 \quad 11 &= f_0 + 5f_1 + 8f_2 \end{aligned}$$

(podemos reducir mod 17 cuando queramos)

$$e_2 - e_1 \sim 2 = 2f_1 + 8f_2$$

$$\begin{aligned} &\rightarrow 2 = 2f_1 + 8(2f_1 - 1) \\ &\rightarrow f_2 = 2f_1 - 1 \end{aligned}$$

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
 LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
 CALL OR WHATSAPP: 689 45 44 70

