

## COMPARTICIÓN DE SECRETOS

EJ (DE JUVENTE): 4 AMIGOS COMPARTEN UNA TARJETA DE CRÉDITO PERO NO SE FÍAN EL UNO DEL OTRO Y QUIEREN ESTAFAR UN SISTEMA PARA QUE ÚNICAMENTE PUEDA SER USADA CUANDO ESTÉN DE ACUERDO LOS 4.

SOLUCIÓN "TONTA": EL PIN DE LA TARJETA TIENE 4 DÍGITOS, DECIDEN QUE CADA UNO TENGА UN DÍGITO DEL PIN.

¿ES UNA SOLUCIÓN BUENA?

- ¿CUANTAS PERSONAS SE NECESITAN  
PARA RECONSTRUIR EL PIN DE LA  
TARJETA (EL SECRETO)?

4

- ¿CUÁL ES LA SEGURIDAD DE LA  
TARJETA SI ALGUIEN DESCONOCIDO  
ROBA LA TARJETA?

$$\text{PROBABILIDAD ACERTAR PIN} = \frac{1}{10.000}$$

- ¿CUÁL ES LA SEGURIDAD DE LA TARJETA  
SI 3 AMIGOS PONEN SU INFORMACIÓN EN COMÚN?

$$\text{PROBABILIDAD ACERTAR} = \frac{1}{10}$$

- Y SI LO HACEN 2?

$$\text{PROBABILIDAD ACERTAR} = \frac{1}{100}$$

- Y SI NO LO HACE NINGUNO?

UNA PERSONA USA SU PROPIA INFORMACIÓN

$$\text{PROBABILIDAD ACERTAR} = \frac{1}{1000}$$

¿QUE HACEMOS CON UNA CLAVE?

¿COMO LA GUARDAMOS?

¿CIFRAMOS LA CLAVE USADA PARA CIFRAR?

POR EJEMPLO EN CRIPTOSISTEMAS DE CLAVE PÚBLICA ES ÚNICO PODER RECUPERAR LA CLAVE PRIVADA, POR EJEMPLO SI SE PIERDE EL DISPOSITIVO SMARTCARD DONDE SE TIENE ALMACENADA, YA NO PODRIAMOS DESCIFRAR NINGÚN MENSAJE CIFRADO.

PODRÍAMOS HACER UNA COPIA QUE LE DAREMOS A UN AMIGO, PERO POR QUESTIONES

DE SEGURIDAD, ES IMPORTANTE QUE  
LA CLAVE NO PUEDA SER RECUPERADA POR  
UNA PERSONA SÓLO PODRÍA NO SER  
TAN AMIGO...)

EN GENERAL ES MÁS SEGURO SI HAY  
UN GRUPO DE PERSONAS INVOLUCRADAS  
EN SU RECUPERACIÓN.

DATOS-VIDA REAL: PENSAD EN SERVIDO-  
RES QUE CONTIENEN INFORMACIÓN DE  
LA CLAVE. AUNQUE EVE ACCEDA A LA  
INFORMACIÓN DE VARIOS SERVIDORES, NO  
PODE RECUPERAR LA CLAVE

LOS ESQUEMAS (PROTOCOLOS) PARA COMPARTIR SECRETOS RESUELVEN EL SIGUIENTE PROBLEMA:

SEA  $U$  UN CONJUNTO FINITO DE USUARIOS,  $S$  UNA DETERMINADA INFORMACIÓN (EL SECRETO) Y  $\mathcal{G}$  UN SUBCONJUNTO DE PARDES DE  $U$ ,  $\mathcal{G} \subset P(U) \leftarrow$  CONJUNTO DE SUBCONJUNTOS DE  $U$ .

SE LLAMA ESTRUCTURA DE ACCESO (CONJUNTO DE USUARIOS AUTORIZADOS)

SE QUIERE DISTRIBUIR INFORMACIONES PARCIALES (PARTICIPACIONES) (SHARES EN INGLÉS) YI DE  $S$  ENTRE LOS USUARIOS DE  $\mathcal{G}$ , DE MANERA QUE SÓLOMENTE LA REUNIÓN DE UNA AGRUPACIÓN AUTORIZADA (POR DEFINICIÓN LOS ELEMENTOS DE  $\mathcal{G}$ ) PUEDE DESCUBRIR EL SECRETO  $S$ .

SE NECESITA UN GESTOR AJENDO (DEALER EN INGLÉS) QUE SE ENCARGA DE DISTRIBUIR LAS PARTICIPACIONES Y ES AJENDO AL CONJUNTO DE USUARIOS  $U$ . PUEDE SER UN PROGRAMA DE ORDENADOR.

$U \in G$  PUEDEN RECUPERAR EL SECRETO

$U \notin G$  NO PUEDEN RECUPERAR EL SECRETO

HAY RESTRICCIONES SOBRE LA ESTRUCTURA DE ACCESO

No PUEDE SER QUE  $A \in G$  pero  $B \supset A$  y  $B \notin G$

$\{JAVIER, CARLOS\} \in G$

$\{JAVIER, CARLOS, ALEJANDRO\} \notin G$

$\left. \begin{array}{l} \text{NO} \\ \text{PUEDE} \\ \text{SER} \end{array} \right\}$

# PARÁMETROS PRIVACIDAD Y RECONSTRUCCIÓN

$t$ : DECIMOS QUE TENEMOS PRIVACIDAD  $\Leftrightarrow$  SI NINGUN CONJUNTO DE  $t$  USUARIOS OBTIENE INFORMACIÓN ALGUNA SOBRE EL SECRETO

$r$ : DECIMOS QUE TENEMOS RECONSTRUCCIÓN  $\Leftrightarrow$  SI CUALQUIER CONJUNTO D  $\geq r$  USUARIOS ES CAPAZ DE RECONSTRUIR EL SECRETO

NORMALMENTE SE PONEN  $t$  MAYOR POSIBLE Y  $r$  EL MENOR POSIBLE DE LOS NÚMEROS QUE VERIFICAN LA DEFINICIÓN ANTERIOR. EJ "TONTO":  $t=0$  Y  $r=4$

ENTRE  $t$  Y  $r$  TENEMOS UNA "ZONA GRIS"

$$t=3 \quad r=5$$

$\Rightarrow$

4 USUARIOS

- NO SEPAN NADA
- SEPAN ALGO PERO NO PUEDA RECONSTRUIR
- PUEDAN RECONSTRUIR

## $(n, t)$ -ESQUEMAS UMbral

ES UNA ESTRUCTURA DE ACCESO SOBRE UN CONJUNTO  $U$  CON  $n$  PARTICIPANTES Y DE MANERA QUE JEG SI Y SÓLO SI  $\#U \geq t$  Y NINGUNA COALICIÓN DE FORMADA POR  $k \leq t$  PARTICIPANTES SABE NADA SOBRE EL SECRETO

CON LA NOTACIÓN DE LA TRANSPARENCIA ANTERIOR TENEMOS

$$\begin{array}{l} \text{PRIVACIDAD: } t = t \\ \text{RECONSTRUCCIÓN: } \mathcal{R} = t + 1 \end{array} \left\{ \begin{array}{l} \text{POR ESTO SE LLAMA} \\ \text{UMbral. NO HAY} \\ \text{ZONA OSCURO} \end{array} \right.$$

Nota: EN EL LIBRO DE HUFFMAN CONSIDERAN

$$\begin{aligned} t &= t - 1 \\ \mathcal{R} &= t \end{aligned}$$

# ESQUEMA DE SHAMIR (UMbral ( $n, t$ ))

EL SECRETO ES UN ENTERO  $S$

$U = \{1, \dots, n\} \leftarrow$  PERSONAS, SERVIDORES, ...

Y TOMAMOS  $P$  PRIMO,  $P > \max\{S, n\}$ .  $P$  PÚBLICO

Y SEAN  $a_1, \dots, a_t \in \mathbb{Z}_P$  ALEATORIOS

CONSTRUIMOS EL POLINOMIO

$$\begin{aligned} f(x) &= S + a_1 x + a_2 x^2 + \dots + a_t x^t \\ &= S + \sum_{i=1}^t a_i x^i \end{aligned}$$

Y LA PARTICIPACIÓN DEL USUARIO  $i$  ES SHARE

$$f(i) \bmod P$$

LOS PASOS 1, 2, Y 3, ANTERIORES LOS REDUZIÓ EL "DEALER". PUEDE SER UN PROGRAMA INFORMATICO QUE SE EJECUTA Y DESAPARECE DE LA MEMORIA DEL ORDENADOR

Nota:

$f$  ES UN POLINOMIO DE GRADO  $\leq t$  Y  $f(0) = S$ .

¡POR QUÉ SE PUEDE RECUPERAR EL SECRETO?

TEOREMA: SEAN  $m_i := (\alpha_i, y_i) \in \mathbb{Z}_p^2$ ,  $1 \leq i \leq t+1$  con  $\alpha_i \neq \alpha_j$  SIEMPRE QUE  $i \neq j$ .

EXISTE UN ÚNICO POLINOMIO  $f(x) \in \mathbb{Z}_p[x]$  DE GRADO MENOR O IGUAL QUE  $t$  DE MANERA QUE  $f(\alpha_i) = y_i \quad \forall i=1, \dots, t+1$ .

LOS VALORES  $m_i = (x_i, y_i)$  SE LLAMAN VALORES  
O PUNTOS DE INTERPOLACIÓN

EL POLINOMIO  $f(x)$  ES EL POLINOMIO INTERPOLADOR  
¿POR QUÉ  $f(x)$  ES ÚNICO?

→ PORQUE UN POLINOMIO CON COEFICIENTES EN EL  
CUERPO TIENE COMO MUCHO  $\deg(f)$  RAÍCES

ESTO NO ES CIERTO EN  $\mathbb{Z}_n[x]$  CON  $n$  NO PRIMO

¿COMO CALCULAMOS  $f$ ? → INTERPOLACIÓN DE  
LAGRANGE

# INTERPOLACIÓN DE LAGRANGE

1) PARA  $i=1, \dots, t+1$  HACEMOS

$$\begin{pmatrix} x_1 & \dots & x_n \\ \parallel & & \parallel \\ 1 & & n \end{pmatrix}$$

$$n_i(x) = \prod_{j \neq i} \frac{x - x_j}{x_i - x_j}$$

( $\deg n_i(x) = t$ )

PORQUE  $\begin{cases} n_i(x_i) = 1 \\ n_i(x_j) = 0 \quad \text{SI} \quad j \neq i \end{cases}$

2)  $f(x) := \sum_{i=1}^t y_i n_i(x)$  ( $\deg f(x) \leq t$ )

PORQUE  $f(x_i) = y_i \cdot n_i(x_i) = y_i \cdot 1 = y_i$

VNA REZ QUE SABEMOS  $f$ , PODEMOS RECU-  
PERAR EL SECRETO

$$S = f(0)$$

COMO SOLO QUEREMOS CALCULAR EL TÉRMINO  
INDEPENDIENTE DE  $f(x)$  ( $f(0)$ ) PODEMOS HACER

• CADA USUARIO  $i=1, \dots, t+1$  CALCULA

$$S_i = n_i(0) = \prod_{j \neq i} \frac{-x_j}{x_i - x_j} \bmod p$$

$$S = \sum_{i=1}^{t+1} y_i S_i \bmod p$$

# CONDICIONES NO AUTORIZADAS

SON LOS CONJUNTOS DE USUARIOS CON  $t$  O MENOS USUARIOS. (SEA  $K \leq t$ )

VEDMOS QUE NO SABEN NADA SOBRE EL SECRETO  
TOMAMOS  $\{x_1, \dots, x_k\}$  COMO CONJUNTO DE USUARIOS

- SEA  $g(x)$  EL POLINOMIO QUE INTERPOLA LOS  $k$  PARTICIPACIONES

$$\deg(g) \leq k-1 < t$$

POR TANTO

PARA  $f(x) = h(x) \prod_{j=1}^k (x - x_j) + g(x)$

CON  $h(x)$  DE GRADO  $t-k$

TENEMOS QUE

$$\begin{cases} \deg f(x) \leq t \\ f(x_i) = g(x_i) = y_i & i=1, \dots, K \end{cases}$$

$$S = f(0) = h(0) \prod (-x_j) + g(0)$$

$$= \underset{\text{↑}}{h_0} \prod (-x_j) + g(0)$$

DESCONOCEN  $h_0 \in \mathbb{Z}_p$ , PERO  
ADIVINAR  $h_0$  ES IGUAL DE DIFÍCIL  
QUE ADIVINAR  $S \in \mathbb{Z}_p$

EJ:  $n=5$ ,  $P=17$ ,  $S=3$ ,  $t=2$  (LIBRO  $t=3$ )  
 numero de participante  $\gamma = 3$

## DEALER

ESCOGE AL AZAR  $q_1=14$ ,  $q_2=15$

privacidad y reconstrucción

$$f(x) = S + q_1 x + q_2 x^2 \\ = 3 + 14 \cdot x + 15 x^2$$

montamos el polinomio acorde a la diapositiva 20

$$3 + 14 \cdot 1 + 15 \cdot 1^2$$

PARTICIPACIONES  $P_1 \leftarrow y_1 = f(1) = 15$   
 $P_2 \leftarrow y_2 = f(2) = 6$   
 $P_3 \leftarrow y_3 = f(3) = 10$   
 $P_4 \leftarrow y_4 = f(4) = 10$   
 $P_5 \leftarrow y_5 = f(5) = 6$

3 PERSONAS (P1, P2 Y P3) QUIEREN RECUPERAR EL SECRETO

$$(1, 15), (2, 6), (3, 10)$$

$$S_i = n_i(0) = \prod_{j \neq i} \frac{-x_j}{x_i - x_j} \bmod P$$

$$S = \sum_{i=1}^{t+1} y_i S_i \bmod P$$

Hallamos los S1, S2 ... tantos como participantes

$$S_1 = n_1(0) = \frac{-x_2}{x_1 - x_2} \cdot \frac{-x_3}{x_1 - x_3} = \frac{-2}{1-2} \cdot \frac{-3}{1-3} = 2 \cdot \frac{3}{2} = 3$$

$$S_2 = n_2(0) = \frac{-x_1}{x_2 - x_1} \cdot \frac{-x_3}{x_2 - x_3} = \frac{-1}{2-1} \cdot \frac{-3}{2-3} = -3 = 14$$

$$S_3 = n_3(0) = \frac{-x_1}{x_3 - x_1} \cdot \frac{-x_2}{x_3 - x_2} = \frac{-1}{3-1} \cdot \frac{-2}{3-2} = -\left(\frac{1}{2}\right)(-2) = 1$$

$$\begin{aligned}
 S &= y_1 S_1 + y_2 S_2 + y_3 S_3 = \\
 &= 15 \cdot 3 + 6 \cdot 14 + 10 \cdot 1 = \\
 &= 45 + 84 + 10 = 139 \equiv 3 \pmod{17}
 \end{aligned}$$

Y SE JUNTA N Z ?  $P_1 \times P_2$

$$S = y_1 S_1 + y_2 S_2 + y_3 S_3 =$$

$$= 15 \cdot 3 + 6 \cdot 14 + ? \cdot 1$$

NO CONOCEN  $y_3 \in \mathbb{Z}_{17}$

10 MISMO  
 DIVINAR  $y_3 \in \mathbb{Z}_{17}$   
 DIVINAR  $S \in \mathbb{Z}_{17}$

POLINOMIO QUE CONSIDERA EL DESPLAZAR PARA  
CADA NIVEL DE PRIVACIDAD Y RECONSTRUCCIÓN

$$t=1 \quad r=2 : \quad f(x) = S + Q_1 x^{\frac{1}{r}}$$

$$t=2 \quad r=3 : \quad f(x) = S + Q_1 x + Q_2 x^{\frac{2}{r}}$$

$$t=3 \quad r=4 : \quad f(x) = S + Q_1 x + Q_2 x^2 + Q_3 x^{\frac{3}{r}}$$

$$t=4 \quad r=5 : \quad f(x) = S + Q_1 x + Q_2 x^2 + Q_3 x^3 + Q_4 x^{\frac{4}{r}}$$

EJ PIN MARKET CREDITO CON  
SHADMIR

$$P = 10007 \quad t = 3 \quad r = 4$$

$$f = S + a_1 X + a_2 X^2 + a_3 X^3$$

$\uparrow$   
PIN

PARTICIPACIÓN DE LA PERSONA i:  $f(i)$

SAGE

## VARIANTEs:

- SE PUEDEN DAR MÁS PARTICIPACIONES A UN USUARIO PARA HACERLO MÁS IMPORTANTE
- SE PUEDE IMPLEMENTAR EL COMPROBAR LA IDENTIDAD DE UN USUARIO ANTES DE RECUPERAR EL SECRETO
- SE PUEDE IMPLEMENTAR EL COMPROBAR QUE UN USUARIO ESTÁ MANDANDO SU PARTICIPACIÓN REAL (NO MIENTE) SIN REVELAR SU PARTICIPACIÓN

## LINEALIDAD

EL ESQUEMA DE SHAMIR ES LINEAL  
SI LOS SECRETOS  $s_1, \dots, s_e$  SE COMPARTEN CON  
LOS VECTORES DE PARTICIPACIONES  $(y_1^i, \dots, y_n^i)$   
 $i = 1, \dots, e$ .

ENTONCES, PARA  $\lambda_1, \dots, \lambda_e \in \mathbb{Z}_p$

$$\left( \sum_{j=1}^e \lambda_j y_1^j, \dots, \sum_{j=1}^e \lambda_j y_n^j \right)$$

ES UN VECTOR DE PARTICIPACIONES PARA EL  
SECRETO  $\sum_{j=1}^e \lambda_j s_j$  EN EL MISMO ESQUEMA

$(y_1, \dots, y_n)$  PERMUTACIONES DE  $S$

$(y'_1, \dots, y'_n)$  " DE  $S'$

$(y_1 + y'_1, \dots, y_n + y'_n)$  " DE  $S + S'$

PORQUE

$$\begin{cases} f(0) = S \\ f'(0) = S' \end{cases} \Rightarrow (f + f')(0) = S + S'$$

$$f(x_i) + f'(x_i) = (f + f')(x_i)$$

# COMPUTACIÓN MULTIPARTE

n PERSONAS , QUE TIENE CADA UNA UN INPUT Si QUIERE CALCULAR  $f(s_1, \dots, s_n)$  PARA UNA CIERTA FUNCIÓN  $f$  QUE HAN ACORDADO DE MANERAS DE TAL MANERA QUE LA ÚNICA INFORMACIÓN QUE REVELAN ES EL OUTPUT DE  $f$  (NO SE REVELA SI LOS OTROS PARTICIPANTES )

INCLUSO SI:

CORRUPCIÓN PASIVA : ALGUNAS PERSONAS SIGUEN EL PROTOCOLO PERO COMPARTEN SU INFORMACIÓN

CORRUPCIÓN ACTIVA : ALGUNAS PERSONAS SE COMPORTAN DE FORMA ARBITRARIA (NO SIGUEN PROTOCOLO)

# EJ: VOTACIÓN ELECTRÓNICA (PASIVA)

$n$  PERSONAS VOTAN SI: 1 o NO: 0  $S_i = \begin{cases} 1 & \text{Si: 1} \\ 0 & \text{NO: 0} \end{cases}$

$$f(S_1, \dots, S_n) = \sum_{i=1}^n S_i = S_1 + \dots + S_n \quad P > n$$

- CONSIDERAMOS SHAMIR-T, n

- LA PERSONA  $j$  PRODUCE EL VECTOR DE PARTICIPACIONES PARA  $S_j : (y_j^1, \dots, y_j^n)$

- PERSONA  $j$  ENVÍA PARTICIPACIÓN  $y_j^i$  A PERSONA  $i$

- CADA PERSONA TIENE UN VECTOR DE PARTICIPACIONES. LA PERSONA  $j$  TIENE  $(y_j^1, \dots, y_j^n)$

- CADA PERSONA CALCULA: LA PERSONA  $j$   
CALCULA

$$d_j := y_0^1 + \dots + y_j^n = \sum_{i=1}^n y_j^i$$

- TODAS LAS PERSONAS CONSIDERAN  
 $(d_1, \dots, d_n)$  ← SE PONE EN COMÚN

Y RECUPERAN  $S = \sum_{i=1}^n S_i$  MEDIANTE

INTERPOLACIÓN DE LAGRANGE (SHAMIR)

NOTA: PODEMOS RECUPERAR  $S$  CON  $t+1$  PERSONAS  
 $1 \leq t \leq n$ .

NOTA: PODEMOS CONSIDERAR CUALQUIER FUNCIÓN  
LINEAL EN LUGAR DE  $\sum_{i=1}^n S_i$

NOTA: NO TIENE SEGURIDAD FRENTE CORRUP-  
CIÓN ACTIVA

EJ: 3 AMIGOS VOTAN SI (=1) ó NO (=0)

$$P=5, n=3$$

$t=2, r=3 \leftarrow$  LOS 3 PARA RECONSTRUIR

Alice P<sub>1</sub>

$$S_1 = 1 \text{ (SI)}$$

$$\begin{cases} f(x) = S_1 + a_1 x + a_2 x^2 \\ \text{ALICE} \\ \text{BENITO} \end{cases}$$

$$f(x) = 1 + 4x + 0x^2$$

$$(f(1), f(2), f(3))$$

$$(0, 4, 3)$$

$$\begin{matrix} \downarrow & \downarrow & \downarrow \\ A & B & C \end{matrix}$$

ENVÍA

Bob P<sub>2</sub>

$$S_2 = 1 \text{ (SI)}$$

$$\begin{cases} f(x) = S_1 + a_1 x + a_2 x^2 \\ \text{ALICE} \\ \text{BENITO} \end{cases}$$

$$f(x) = 1 + 3x + x^2$$

$$(f(1), f(2), f(3))$$

$$(0, 1, 4)$$

$$\begin{matrix} \downarrow & \downarrow & \downarrow \\ A & B & C \end{matrix}$$

ENVÍA

Carl P<sub>3</sub>

$$S_3 = 0 \text{ (NO)}$$

$$\begin{cases} f(x) = S_1 + a_1 x + a_2 x^2 \\ \text{ALICE} \\ \text{BENITO} \end{cases}$$

$$f(x) = 0 + 4x + 4x^2$$

$$(f(1), f(2), f(3))$$

$$(3, 4, 3)$$

$$\begin{matrix} \downarrow & \downarrow & \downarrow \\ A & B & C \end{matrix}$$

ENVÍA

$(0, 0, 3)$   
RECIBE

$$d_1 = 0 + 0 + 3 = 3$$

CALCULA

$(4, 1, 4)$   
RECIBE

$$d_2 = 4 + 1 + 4 = 9$$

CALCULA

$(3, 4, 3)$   
RECIBE

$$d_3 = 3 + 4 + 3 = 10$$

CALCULA

PONEN  
EN COMÚN

$$\begin{matrix} 3 & 4 & 0 \\ \underline{d_1} & \underline{d_2} & \underline{d_3} \end{matrix}$$

SHAMIR, RECONSTRUCCIÓN :  $(3, 4, 0)$

$$S'_i = n_i(0) = \prod_{j \neq i} \frac{-x_j}{x_i - x_j} \pmod{P}$$

$$S = \sum_{i=1}^{t+1} d_i S'_i \pmod{P}$$

CADA USUARIO  
SUMA UNA  
COLUMNA

$$S_1^I = N_1(0) = \frac{-x_2}{x_1 - x_2} \cdot \frac{-x_3}{x_1 - x_3} = \frac{-2}{1-2} \cdot \frac{-3}{1-3} = 2 \frac{3}{2} = 3$$

$$S_2^I = N_2(0) = \frac{-x_1}{x_2 - x_1} \cdot \frac{-x_3}{x_2 - x_3} = \frac{-1}{2-1} \cdot \frac{-3}{2-3} = -3 = 2$$

$$S_3^I = N_3(0) = \frac{-x_1}{x_3 - x_1} \cdot \frac{-x_2}{x_3 - x_2} = \frac{-1}{3-1} \cdot \frac{-2}{3-2} = \frac{-1}{2} (-2) = 1$$

↑ CONFUNDIR VOTO DE

$$S = d_1 S_1^I + d_2 S_2^I + d_3 S_3^I =$$

$$= \underline{3} \cdot \underline{3} + \underline{4} \cdot \underline{2} + \underline{0} \cdot \underline{1} =$$

$$= 9 + 8 + 0 = 17 = 2$$

↑ SE ACEPTE  
2 VOTOS △ FAVOR

NO CON CADA UNO •  
CON EL VOTO PEQUEÑO PROBLEMA,  
DE NOTACION CON LOS ESES

NOTA: SEGURIDAD POSITIVA. NO ACTIVA

SI CBR-L-P3 MIENTE Y DICE  $d_3=4$   
EN LUGAR DE  $d_3=0$ :

$$S = d_1 S_1^1 + d_2 S_2^1 + d_3 S_3^1$$

$$= 3 \cdot 3 + 4 \cdot 2 + 4 \cdot 1 =$$

$$= 9 + 8 + 4 = 21 = 1$$

↑  
1 VOTO A FAVOR  
SE DENIEGA

SE PUEDEN HACER MODIFICACIONES PARA EVITAR ESTE TIPO DE TRAMOAS

# ESQUEMA DE SHAMIR EN RÁMPA

↑  
NO ENTRÓ  
EXAMEN

- $\vec{S} = (S_0, \dots, S_{l-1}) \in \mathbb{F}_q^l$  SECRETO
- $n$  PARTICIPANTES
- RECONSTRUCCIÓN  $r = k$ , PRIVACIDAD  $t = k - l$
- SE ESCOGEN  $a_0, \dots, a_{k-1} \in \mathbb{F}_q$  ALEATORIOS  
Y SE CONSTRUYE
- $$f(x) = S_0 + S_1 x + \dots + S_{l-1} x^{l-1} + a_0 x^l + \dots + a_{k-1} x^{k-1}$$
- PARTICIPACIONES:  $f(x_1), \dots, f(x_n)$  CON  $x_i \neq x_j$   
( $x_1, \dots, x_n$  PUEDEN SER  $1, \dots, n$  SI  $q = p$ )

- ¿RECONSTRUCCION Y PRIVACIDAD?  
SE DEDUCEN DE LAS INTERPOLACIONES DE LAS ORANGE
- VENTAJA:  
EL SECRETO TIENE  $l$  BITS PERO LAS  
PARTICIPACIONES TIENEN 1 BIT  
MÁS EFICIENTE PARA FICHEROS GRANDES