

Bahan kuliah IF4020 Kriptografi

# Skema Pembagian Data Rahasia

*(Secret Sharing Scheme)*

**Oleh: Rinaldi Munir**

Program Studi Informatika  
Sekolah Teknik Elektro dan Informatika  
ITB - 2024

- Misalkan anda memiliki PIN kartu ATM tabungan anda di sebuah bank. PIN tersebut tentu saja rahasia. Tabungan itu akan diwariskan kepada anak-anak anda.
- Sebelum meninggal dunia, Anda ingin membagi (*sharing*) PIN itu kepada enam orang anak anda menjadi enam bagian.
- Namun Anda mensyaratkan untuk merekonstruksi enam bagian menjadi PIN semula dibutuhkan *sedikitnya* tiga orang anak untuk merangkai bagian-bagiannya menjadi PIN yang utuh.
- Bagaimana cara melakukan pembagian ini?

→ *Secret sharing schemes!!!*

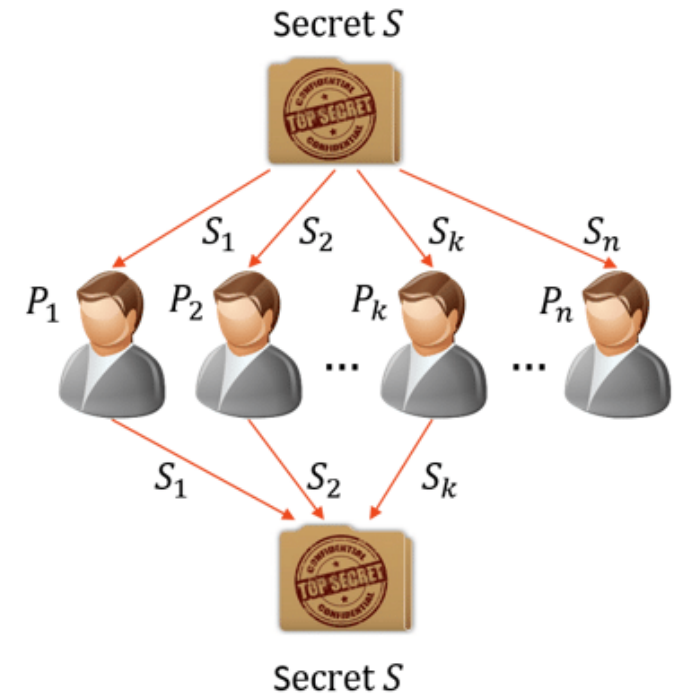


Download from  
Dreamstime.com  
The subscription covers usage for generating purposes only.

1620193  
Sandra Van Der Steen | Dreamstime.com

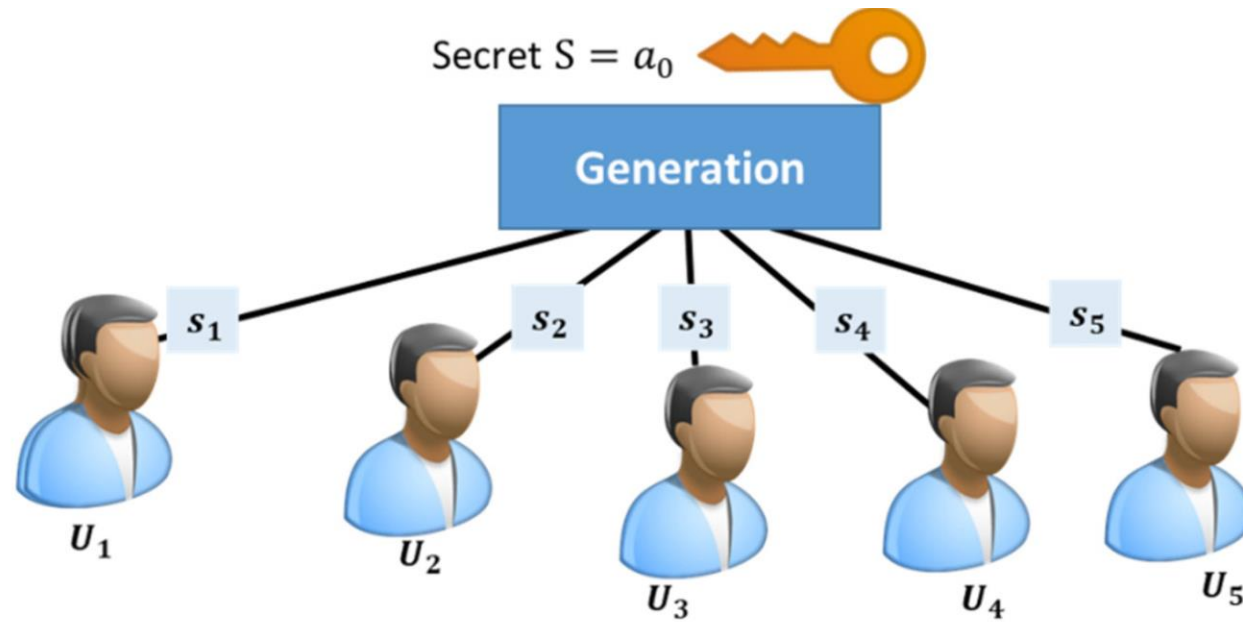
# Terminologi

- *Secret*: data/informasi rahasia (*password*, kunci, PIN, pesan, file, dsb).
- *Secret* direpresentasikan sebagai sebuah *integer S*.  
Contoh: 'abcd' dinyatakan sebagai 102030405  
(A = 01, B = 02, C = 03, dst)
- *Share*: hasil pembagian *secret* ( $S_1, S_2, \dots, S_n$ )
- *Dealer*: pihak yang melakukan pembagian *secret*
- Partisipan: orang yang memperoleh *share* ( $P_1, P_2, \dots, P_n$ )

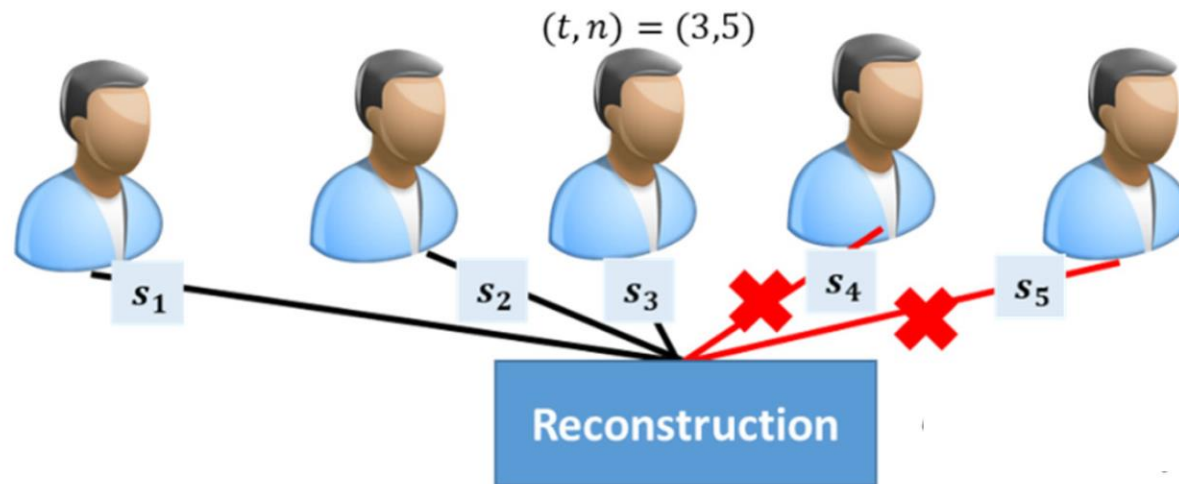


# Skema Ambang (*threshold schemes*)

- Misalkan  $t, n$  adalah bilangan bulat positif dengan  $t \leq n$ .
- Skema ambang  $(t, n)$  adalah metode pembagian *secret*  $S$  kepada  $n$  partisipan sedemikian sehingga sembarang himpunan bagian yang terdiri dari  $t$  partisipan dapat merekonstruksi  $S$ , tetapi jika kurang dari  $t$  maka  $S$  tidak dapat direkonstruksi.
- Ditemukan oleh Shamir (1979), dikenal sebagai skema ambang Shamir (*Shamir threshold scheme*).



$(t, n)$  threshold Shamir secret sharing reconstruction, more than or equal to  $t$  secret shares can be combined together to recover the secret key  $S$





Adi Shamir

Programming  
Techniques

R. Rivest  
Editor

---

## How to Share a Secret

Adi Shamir  
Massachusetts Institute of Technology

---

**In this paper we show how to divide data  $D$  into  $n$  pieces in such a way that  $D$  is easily reconstructable from any  $k$  pieces, but even complete knowledge of  $k - 1$  pieces reveals absolutely no information about  $D$ . This technique enables the construction of robust key management schemes for cryptographic systems that can function securely and reliably even when misfortunes destroy half the pieces and security breaches expose all but one of the remaining pieces.**

**Key Words and Phrases:** cryptography, key management, interpolation

**CR Categories:** 5:39, 5.6

tion) and in which nonmechanical solutions (which manipulate this data) are also allowed. Our goal is to divide  $D$  into  $n$  pieces  $D_1, \dots, D_n$  in such a way that:

- (1) knowledge of any  $k$  or more  $D_i$  pieces makes  $D$  easily computable;
- (2) knowledge of any  $k - 1$  or fewer  $D_i$  pieces leaves  $D$  completely undetermined (in the sense that all its possible values are equally likely).

Such a scheme is called a  $(k, n)$  *threshold scheme*.

Efficient threshold schemes can be very helpful in the management of cryptographic keys. In order to protect data we can encrypt it, but in order to protect the encryption key we need a different method (further encryptions change the problem rather than solve it). The most secure key management scheme keeps the key in a single, well-guarded location (a computer, a human brain, or a safe). This scheme is highly unreliable since a single misfortune (a computer breakdown, sudden death, or sabotage) can make the information inaccessible. An obvious solution is to store multiple copies of the key at different locations, but this increases the danger of security breaches (computer penetration, betrayal, or human errors). By using a  $(k, n)$  threshold scheme with  $n = 2k - 1$  we get a very robust key management scheme: We can recover the original key even when  $\lfloor n/2 \rfloor = k - 1$  of the  $n$

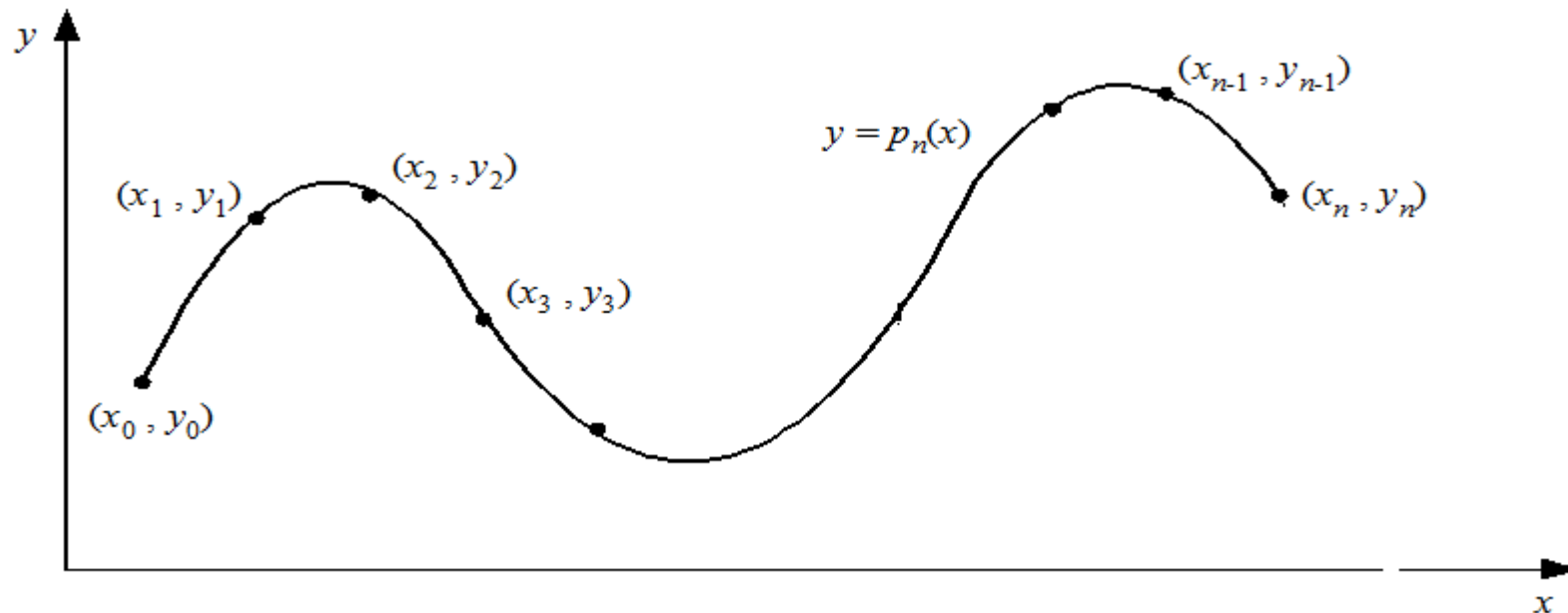
# Skema Shamir

- Idenya dari persoalan interpolasi:
  - Untuk membentuk persamaan linier  $y = a_0 + a_1x$  diperlukan 2 buah titik:  $(x_1, y_1), (x_2, y_2)$
  - Untuk membentuk persamaan kuadratik  $y = a_0 + a_1x + a_2x^2$  diperlukan 3 buah titik  $(x_1, y_1), (x_2, y_2), (x_3, y_3)$
  - dst
  - Untuk membentuk polinomial  $y = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$  diperlukan  $n + 1$  titik.

# Interpolasi

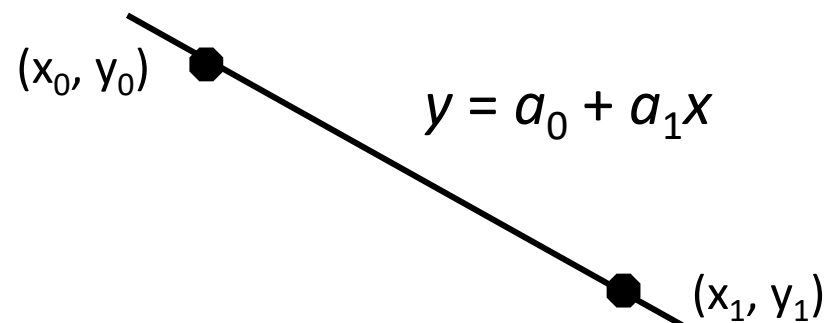
- Polinom interpolasi derajat  $n$  yang menginterpolasi titik-titik  $(x_0, y_0), (x_1, y_1), \dots, (x_n, y_n)$  adalah

$$y = p_n(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$$





## Contoh: Interpolasi linier



Substitusikan  $(x_0, y_0)$  dan  $(x_1, y_1)$  ke dalam  $y = a_0 + a_1x$ , diperoleh SPL:

$$y_0 = a_0 + a_1x_0$$

$$y_1 = a_0 + a_1x_1$$

SPL dapat dipecahkan dengan metode eliminasi untuk menentukan  $a_0$  dan  $a_1$

- Untuk polinom interpolasi berderajat  $n$ :

$$y = p_n(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$$

dibutuhkan  $(n+1)$  buah titik data.

- Dengan menyulihkan  $(x_0, y_0), (x_1, y_1), \dots, (x_n, y_n)$  ke dalam  $y = p_n(x)$ , diperoleh  $n$  buah sistem persamaan linier dalam  $a_0, a_1, a_2, \dots, a_n$ ,

$$\begin{aligned} a_0 + a_1x_0 + a_2x_0^2 + \dots + a_nx_0^n &= y_0 \\ a_0 + a_1x_1 + a_2x_1^2 + \dots + a_nx_1^n &= y_1 \\ a_0 + a_1x_2 + a_2x_2^2 + \dots + a_nx_2^n &= y_2 \\ \dots & \dots \\ a_0 + a_1x_n + a_2x_n^2 + \dots + a_nx_n^n &= y_n \end{aligned}$$

- Solusi sistem persamaan linier ini diperoleh dengan menggunakan metode eliminasi Gauss yang sudah anda pelajari.

# Skema $(t, n)$

Algoritma:

1. Pilih bilangan prima  $p$ , yang harus lebih besar dari semua kemungkinan nilai *secret*  $S$  dan juga lebih besar dari jumlah  $n$  partisipan. Semua komputasi dilakukan dalam modulus  $p$ .
2. Pilih  $t - 1$  buah bilangan bulat acak dalam modulus  $p$ , misalkan  $a_1, a_2, \dots, a_{t-1}$ , dan nyatakan polinomial:

$$f(x) \equiv S + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1} \pmod{p}$$

sedemikian sehingga  $f(0) \equiv S \pmod{p}$ .

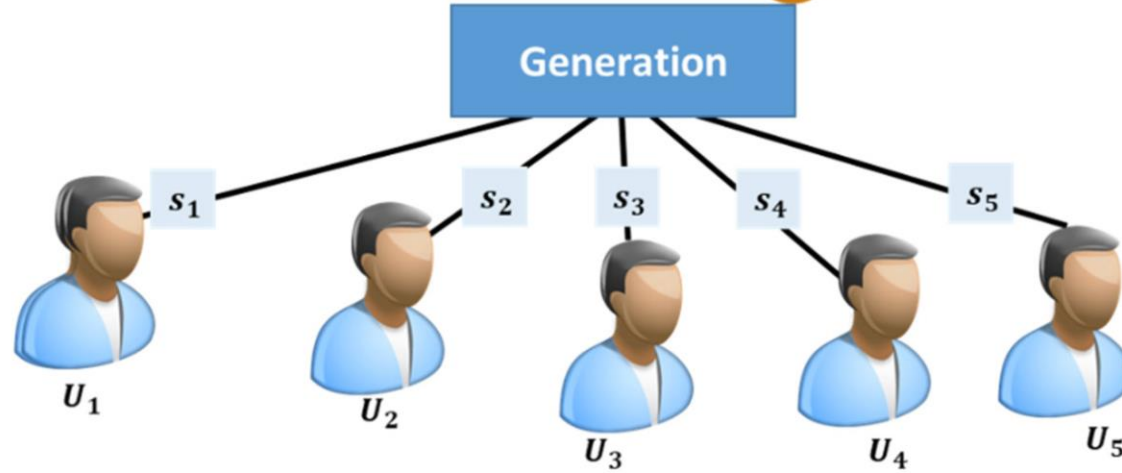
3. Untuk  $n$  partisipan, kita pilih *integer* berbeda,  $x_1, x_2, \dots, x_n \pmod{p}$  dan setiap orang memperoleh *share*  $(x_i, y_i)$  yang dalam hal ini

$$y_i \equiv f(x_i) \pmod{p}.$$

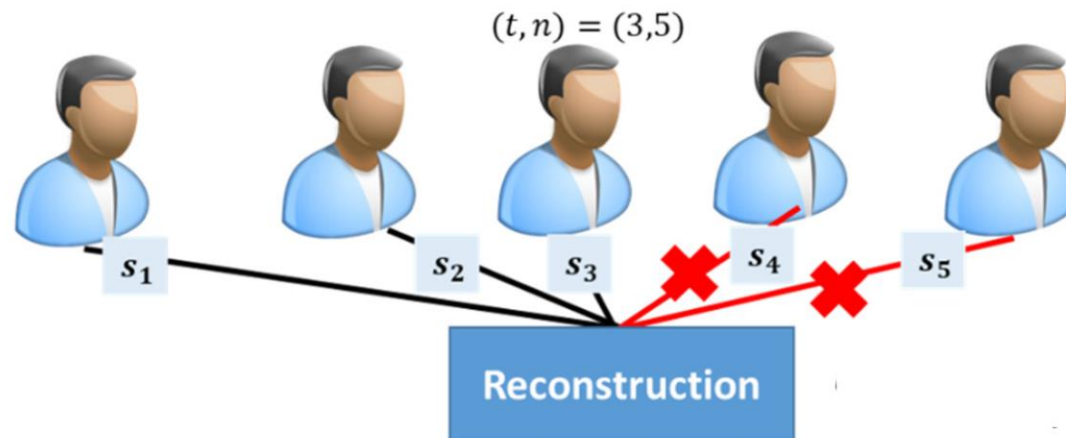
Misalnya, untuk  $n$  orang kita memilih  $x_1 = 1, x_2 = 2, \dots, x_n = n$ .

$$f(x) = a_0 + a_1x^1 + a_2x^2 + a_3x^3 + \dots + a_{t-1}x^{t-1} \text{ mod}(p)$$

Secret  $S = a_0$  



$(t, n)$  threshold Shamir secret sharing reconstruction, more than or equal to  $t$  secret shares can be combined together to recover the secret key  $S$



# Contoh 1: Skema Shamir (4, 3)

- Artinya: secret  $S$  dibagi kepada  $n = 4$  partisipan, dan untuk melakukan rekonstruksi  $S$  diperlukan  $t = 3$  partisipan  $S$ .
- Misalkan  $S = 1954$  (*secret*)
- Misalkan  $p = 1973$  (prima) ( $p > S$ )
- Pilih  $3 - 1 = 2$  buah bilangan acak,  $a_1 = 43$ ,  $a_2 = 12$  untuk membentuk polinom:

$$f(x) \equiv S + a_1x + a_2x^2 \pmod{p}$$

$$f(x) \equiv 1954 + 43x + 12x^2 \pmod{1973}$$

Polinom  $f(x)$  harus dirahasiakan!

- Tiap partisipan memperoleh  $(x, f(x))$ . Misakan  $x_1 = 1, x_2 = 2, x_3 = 3, x_4 = 4$ , maka, setiap orang memperoleh *share* sebagai berikut:

$$f(x) \equiv 1954 + 43x + 12x^2 \pmod{1973}$$

$$x = 1 \rightarrow f(1) \equiv 1954 + 43*1 + 12*1^2 \pmod{1973} \equiv 2009 \pmod{1973} = 36 \rightarrow (1, 36)$$

$$x = 2 \rightarrow f(2) \equiv 1954 + 43*2 + 12*2^2 \pmod{1973} \equiv 2088 \pmod{1973} = 115 \rightarrow (2, 115)$$

$$x = 3 \rightarrow f(3) \equiv 1954 + 43*3 + 12*3^2 \pmod{1973} \equiv 2191 \pmod{1973} = 224 \rightarrow (3, 224)$$

$$x = 4 \rightarrow f(4) \equiv 1954 + 43*4 + 12*4^2 \pmod{1973} \equiv 2318 \pmod{1973} = 345 \rightarrow (4, 345)$$

Jadi,

$$\text{share 1} = (1, 36), \text{share 2} = (2, 115), \text{share 3} = (3, 224), \text{share 4} = (4, 345)$$

Misalkan  $t$  orang partisipan akan merekonstruksi  $S$ , dengan *share* masing-masing:

$$(x_1, y_1), (x_2, y_2) \dots, (x_t, y_t).$$

Substitusikan setiap  $(x_k, y_k)$  ke dalam polinomial:

$$f(x) \equiv S + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1} \pmod{p}$$

Ini berarti:

$$y_k \equiv f(x_k) \equiv S + a_1x_k + a_2x_k^2 \dots + a_{t-1}x_k^{t-1} \pmod{p}, \quad 1 \leq k \leq t$$



Diperoleh sistem persamaan linier sebagai berikut:

$$\begin{pmatrix} 1 & x_1 & \cdots & x_1^{t-1} \\ 1 & x_2 & \cdots & x_2^{t-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_t & \cdots & x_t^{t-1} \end{pmatrix} \begin{pmatrix} S \\ a_1 \\ \vdots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_t \end{pmatrix} \pmod{p}$$

Selesaikan sistem persamaan linier di atas, misalnya dengan metode eliminasi Gauss-Jordan, untuk memperoleh  $M$ .

Catatan:  $p$  tidak perlu rahasia, tetapi polinom  $f(x)$  dirahasiakan.

- Misalkan  $t = 3$  partisipan yaitu partisipan 1, 2, dan 4 ingin merekonstruksi  $S$ :  
*Share* mereka:  $s_1 = (1, 36)$ ,  $s_2 = (2, 115)$ ,  $s_4 = (4, 345)$
- Substitusikan setiap *share* ke dalam polinom:

$$f(x) \equiv S + a_1x + a_2x^2 \pmod{p}$$

$$s_1 = (1, 36) \rightarrow S + a_1 + a_2 = 36$$

$$s_2 = (2, 115) \rightarrow S + 2a_1 + 4a_2 = 115$$

$$s_4 = (4, 345) \rightarrow S + 4a_1 + 16a_2 = 345$$

- Lalu pecahkan sistem persamaan linier:

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 4 & 16 \end{pmatrix} \begin{pmatrix} S \\ a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} 36 \\ 115 \\ 345 \end{pmatrix} \pmod{1973}$$

yang menghasilkan solusi

$$(S, a_1, a_2) = (1954, 43, 12)$$

*Secret* yang dicari adalah 1954

- Apa yang terjadi jika 2 orang partisipan mencoba merekonstruksi  $S$ ?
- Tidak mungkin 2 buah titik bisa membentuk polinom derajat 2:

$$f(x) \equiv S + a_1x + a_2x^2 \pmod{p}$$

Diperlukan setidaknya 3 buah titik!

- Misalkan dicoba menggunakan titik ketiga  $(0, c)$ ,  $c$  adalah sembarang *secret*, maka polinom tetap mengandung sebuah nilai yang tidak diketahui ( $S$ ).
- Apa yang terjadi jika  $> 3$  orang partisipan mencoba merekonstruksi  $M$ ?
- SPL tetap bisa diselesaikan!

## Contoh 2: Skema Shamir (3, 8)

- Artinya: secret  $S$  dibagi kepada  $n = 8$  partisipan, dan untuk melakukan rekonstruksi  $S$  diperlukan  $t = 3$  partisipan  $S$ .
- Misalkan  $S = \text{"TFDSFU"}$   $\rightarrow$  ubah ke integer  $S = 190503180520$  (*secret*)

A = 00, B = 01, C = 02, D = 03, E = 04, F = 05, G = 06, H = 07, I = 08, J = 09, K = 10, L = 11, M = 12, N = 13,  
O = 14, P = 15, Q = 16, R = 17, S = 18, T = 19, U = 20, V = 21, W = 22, X = 23, Y = 24, Z = 25

- Misalkan  $p = 1234567890133$  (prima) ( $p > S$ )
- Pilih 3 – 1 = 2 buah bilangan acak,  $a_1 = 482943028839$ ,  $a_2 = 1206749628665$  untuk membentuk polinom:

$$f(x) \equiv S + a_1x + a_2x^2 \pmod{p}$$

$$f(x) \equiv 190503180520 + 482943028839x + 1206749628665x^2 \pmod{1234567890133}$$

Polinom  $f(x)$  harus dirahasiakan!

- Tiap partisipan memperoleh  $(x, f(x))$ . Misakan  $x_1 = 1, x_2 = 2, \dots, x_8 = 8$ , maka, setiap orang memperoleh *share*:

$$f(x) \equiv 190503180520 + 482943028839x + 1206749628665x^2 \pmod{1234567890133}$$

$$x = 1 \rightarrow f(1) = 645627947891, \text{ diperoleh } \textit{share 1} = (1, 645627947891)$$

$$x = 2 \rightarrow f(2) = 1045116192326, \text{ diperoleh } \textit{share 2} = (2, 1045116192326)$$

...dst untuk  $x = 3, 4, 5, 6, 7, 8$  diperoleh:

$$\textit{share 3} = (3, 154400023692)$$

$$\textit{share 4} = (4, 442615222255)$$

$$\textit{share 5} = (5, 675193897882)$$

$$\textit{share 6} = (6, 852136050573)$$

$$\textit{share 7} = (7, 973441680328)$$

$$\textit{share 8} = (8, 1039110787147)$$

- Misalkan  $t = 3$  partisipan yaitu partisipan 2, 3, dan 7 ingin merekonstruksi  $S$ :  
*Share* mereka:  $s_1 = (2, 1045116192326)$ ,  $s_2 = (3, 154400023692)$ ,  $s_3 = (7, 973441680328)$
- Substitusikan setiap *share* ke dalam:

$$y_k \equiv f(x_k) \equiv S + a_1x_k + a_2x_k^2 \dots + a_{t-1}x_k^{t-1} \pmod{p}, \quad 1 \leq k \leq t$$

$$s_1 = (2, 1045116192326) \rightarrow S + 2a_1 + 4a_2 = 1045116192326$$

$$s_2 = (3, 154400023692) \rightarrow S + 3a_1 + 9a_2 = 154400023692$$

$$s_3 = (7, 973441680328) \rightarrow S + 7a_1 + 49a_2 = 973441680328$$

- Lalu pecahkan sistem persamaan linier:

$$\begin{pmatrix} 1 & 2 & 4 \\ 1 & 3 & 9 \\ 1 & 7 & 49 \end{pmatrix} \begin{pmatrix} S \\ a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} 1045116192326 \\ 154400023692 \\ 973441680328 \end{pmatrix} \pmod{1234567890133}$$

yang menghasilkan solusi


$$(S, a_1, a_2) = (190503180520, 482943028839, 1206749628665)$$

*Secret* yang dicari adalah 190503180520




# Demo Shamir secret sharing online: <https://asecuritysite.com/shares/shamir>

→ ↻ <https://asecuritysite.com/shares/shamir> 📄 ☆ 🛡️ ⬇️ 👤



## Shamir Secret Sharing

[\[Secret Shares Home\]](#) [\[Home\]](#)

Secret Shares   
@asecuritysite.com

Shamir's secret sharing method generates a number of shares, of which a threshold defines the number of shares which can be used to re-build the message. [\[Decoder\]](#) [\[Theory\]](#)

Secret message:	<input type="text" value="HelloWorld"/>
No of shares (1-10):	<input type="text" value="8"/>
Threshold (2-10):	<input type="text" value="3"/>

[Determine](#)


The results are then:

Shares	<pre>0008ydb4ms02K/xhQtv 001Dg9vR7uscfhMW1EZ 0029w4aV+PL20tNIg0+ 003CEYu8jNPcbzw/VnI</pre>
Reconstructed	<pre>HelloWorld</pre>

# Rekonstruksi secret:

→ ↻ [https://asecuritysite.com/encryption/shamir\\_decode](https://asecuritysite.com/encryption/shamir_decode) 📄 ☆ 🛡

## Shamir Secret Sharing (Rebuild)

[\[Encryption Home\]](#)[\[Home\]](#) 

Shamir's secret sharing method generates a number of shares, of which a threshold defines the number of shares which can be used to rebuild the message. [\[Encoder\]](#)[\[Theory\]](#)

Secret shares (new line for each one): <input type="button" value="Determine"/>	0008ydb4mso2K/xhQtv 001Dg9vR7uscfhMW1EZ 0029w4aV+PL2OtNIgO+
The results are then:	
Reconstructed	<pre>Trying a share of 1: ó' [âk(øñ...o Trying a share of 2: tq³èöçfæ'd Trying a share of 3: HelloWorld</pre>

# Metode Interpolasi Lagrange

- Alternatif lain: menggunakan metode interpolasi Lagrange
- Diberikan  $t$  buah titik:  $(x_1, y_1), (x_2, y_2), \dots, (x_t, y_t)$ .
- Polinom Lagrange (mod  $p$ ) yang melalui  $t$  titik adalah polinom derajat  $t - 1$ :

$$p(x) \equiv y_1L_1(x_1) + y_2L_2(x_2) + \dots + y_tL_t(x_t) \pmod{p}$$

yang dalam hal ini:  $L_k(x) = \prod_{\substack{i=1 \\ i \neq k}}^t \frac{x - x_i}{x_k - x_i} \quad k = 1, 2, \dots, t$

Untuk memperoleh  $S$ , hitung  $p(x)$  pada  $x = 0$ .

Contoh: Jika partisipan 2, 3, dan 7 menggunakan tiga buah share sebagai berikut:

$$(x_1, y_1) = (2, 1045116192326)$$

$$(x_2, y_2) = (3, 154400023692)$$

$$(x_3, y_3) = (7, 973441680328)$$

Hitung:  $p(x) \equiv y_1L_1(x_1) + y_2L_2(x_2) + y_3L_3(x_3) \pmod{p}$

$$L_k(x) = \prod_{\substack{i=1 \\ i \neq k}}^t \frac{x - x_i}{x_k - x_i}$$

$$p(x) \equiv y_1 \frac{(x-x_2)(x-x_3)}{(x_1-x_2)(x_1-x_3)} + y_2 \frac{(x-x_1)(x-x_3)}{(x_2-x_1)(x_2-x_3)} + y_3 \frac{(x-x_1)(x-x_2)}{(x_3-x_1)(x_3-x_2)} \pmod{p}$$

$$\begin{aligned} p(x) &\equiv 1045116192326 (x-3)(x-7)/(2-3)(2-7) \\ &\quad + 154400023692 (x-2)(x-7)/(3-2)(3-7) \\ &\quad + 973441680328 (x-2)(x-3)/(7-2)(7-3) \pmod{1234567890133} \end{aligned}$$

$$\begin{aligned} &\equiv 1045116192326/5 (x-3)(x-7) - 38600005923 (x-2)(x-7) + \\ &\quad 973441680328/5 (x-2)(x-3) \pmod{1234567890133} \end{aligned}$$

Karena kita bekerja dalam modulus  $p$  dan mengingat:

$$1/5 = 5^{-1} \pmod{1234567890133} = 740740734080$$

Ganti  $1/5$  dengan 740740734080, sehingga diperoleh polinom:

$$\begin{aligned}
p(x) &\equiv 1045116192326/5 (x - 3)(x - 7) - 38600005923 (x - 2)(x - 7) + \\
&\quad 973441680328/5 (x - 2)(x - 3) \pmod{1234567890133} \\
&\equiv (1045116192326)(740740734080)(x - 3)(x - 7) - 38600005923 (x - 2)(x - 7) + \\
&\quad 973441680328 )(740740734080) (x - 2)(x - 3) \pmod{1234567890133}
\end{aligned}$$

Untuk memperoleh  $S$ , hitung  $p(0)$ , diperoleh

$$\begin{aligned}
p(0) &\equiv (1045116192326)(740740734080)(0 - 3)(0 - 7) - 38600005923 (0 - 2)(0 - 7) + \\
&\quad 973441680328 )(740740734080) (0 - 2)(0 - 3) \pmod{1234567890133} \\
&= \mathbf{190503180520} = S.
\end{aligned}$$

# Referensi

- Trappe, W., Washington, L., *Introduction to Cryptography with Coding Theory*, 2<sup>nd</sup> edition, Pearson-Prentice Hall, 2006