

Chia sẻ thông tin mật (Secret sharing)



KHOA CÔNG NGHỆ THÔNG TIN
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

Nội dung môn học

- ☐ Ẩn dữ liệu (data/information hiding)
 - ☒ Steganography ✓
 - ☒ Watermarking ✓
- ☐ Chia sẻ thông tin mật (secret sharing) ← Buổi này

Bài toán chia sẻ thông tin mật

- Giả sử ta muốn chia sẻ một thông tin mật S cho n người
 - ▣ Ta muốn phải có ít nhất là k người ($k \leq n$) thì mới tái tạo được S
 - ▣ Còn nếu có ít hơn k người thì sẽ không tái tạo được S (cũng không biết gì về S)
- **Bài toán chia sẻ thông tin mật:** chia thông tin mật S thành n phần S_1, S_2, \dots, S_n sao cho:
 - ▣ Với ít nhất là k phần bất kỳ ($k \leq n$) thì sẽ tái tạo được S
 - ▣ Với ít hơn k phần thì sẽ không biết gì về S

Phương pháp chia sẻ thông tin mật của Shamir

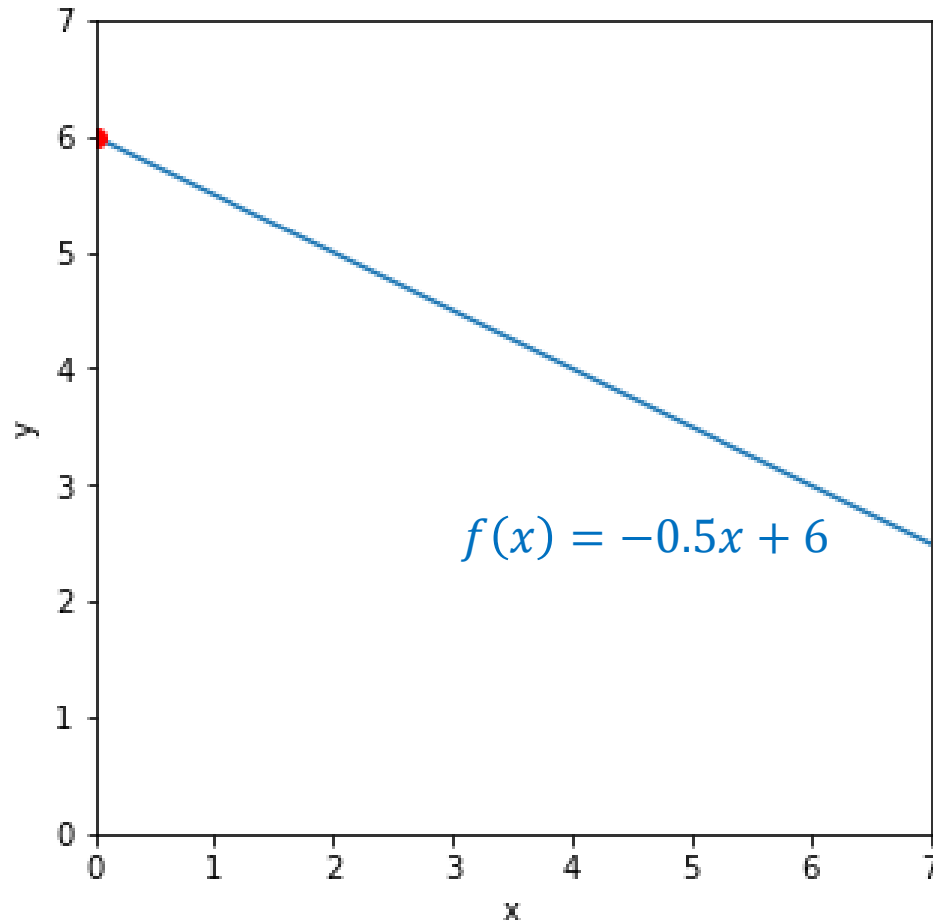
Trong phương pháp của Shamir, dữ liệu mật S là một con số

Phương pháp chia sẻ thông tin mật của Shamir

Ví dụ 1: $S = 6, n = 3, k = 2$

Phương pháp Shamir làm như thế nào?

- Bước 1: tạo hàm f là một đa thức bậc nhất sao cho $f(0) = S$
ví dụ, $f(x) = -0.5x + 6$

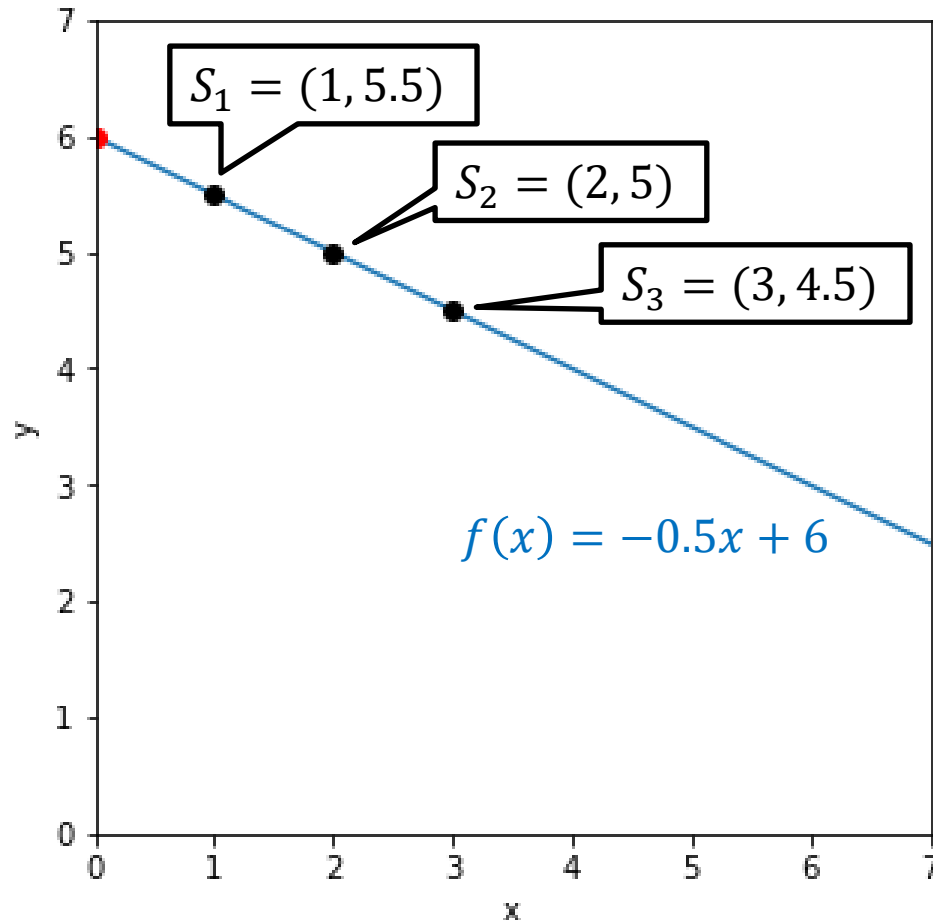


Phương pháp chia sẻ thông tin mật của Shamir

Ví dụ 1: $S = 6, n = 3, k = 2$

Phương pháp Shamir làm như thế nào?

□ Bước 2: $S_1 = (1, f(1)), S_2 = (2, f(2)), S_3 = (3, f(3))$

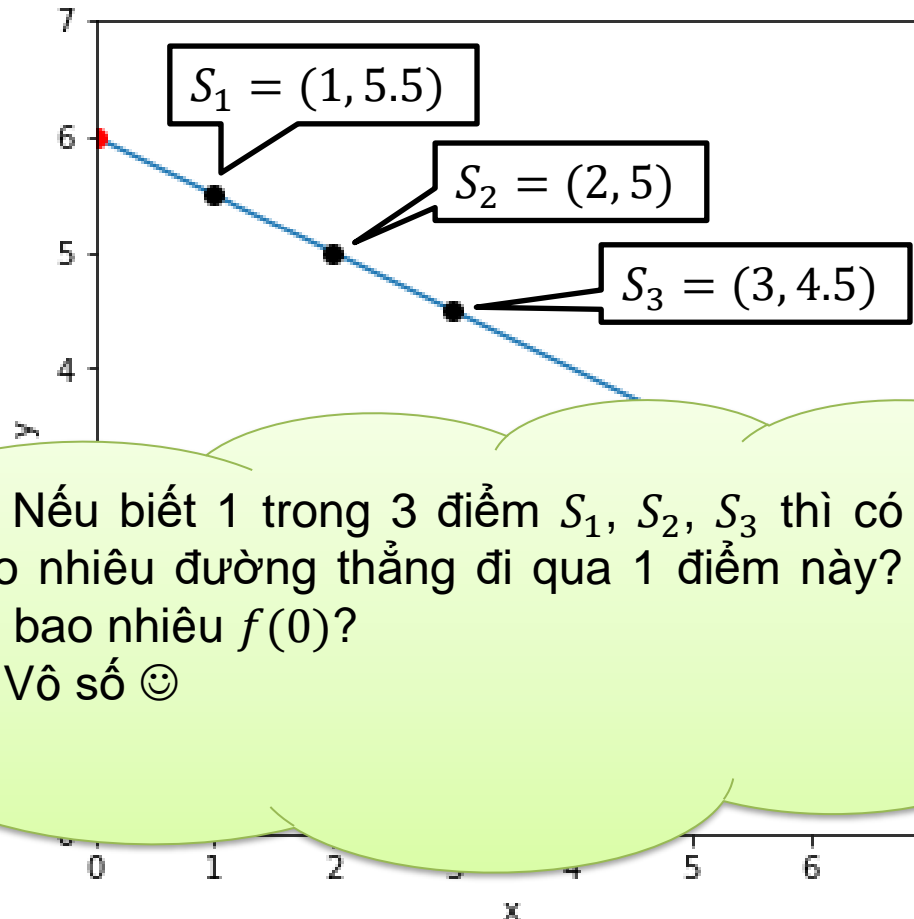


Phương pháp chia sẻ thông tin mật của Shamir

Ví dụ 1: $S = 6, n = 3, k = 2$

Phương pháp Shamir làm như thế nào?

□ Bước 2: $S_1 = (1, f(1)), S_2 = (2, f(2)), S_3 = (3, f(3))$

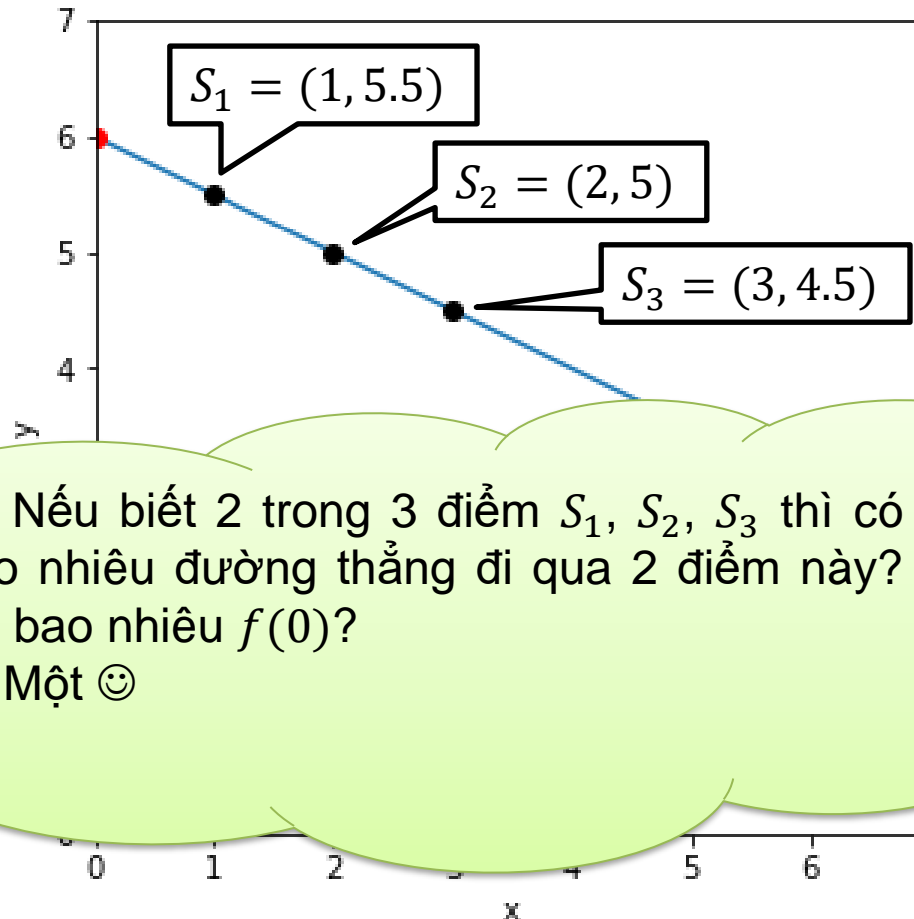


Phương pháp chia sẻ thông tin mật của Shamir

Ví dụ 1: $S = 6, n = 3, k = 2$

Phương pháp Shamir làm như thế nào?

□ Bước 2: $S_1 = (1, f(1)), S_2 = (2, f(2)), S_3 = (3, f(3))$



Q: Nếu biết 2 trong 3 điểm S_1, S_2, S_3 thì có bao nhiêu đường thẳng đi qua 2 điểm này?
Có bao nhiêu $f(0)$?

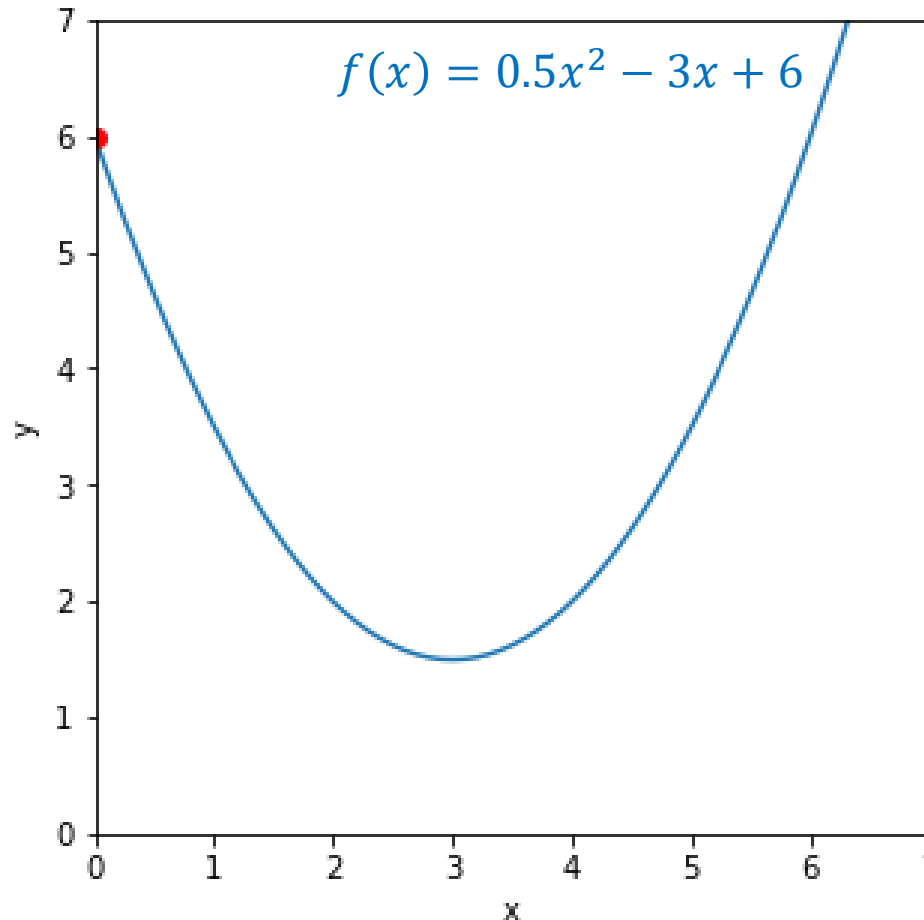
A: Một 😊

Phương pháp chia sẻ thông tin mật của Shamir

Ví dụ 2: $S = 6, n = 5, k = 3$

Phương pháp Shamir làm như thế nào?

- Bước 1: tạo hàm f là một đa thức bậc **hai** sao cho $f(0) = S$
ví dụ, $f(x) = 0.5x^2 - 3x + 6$

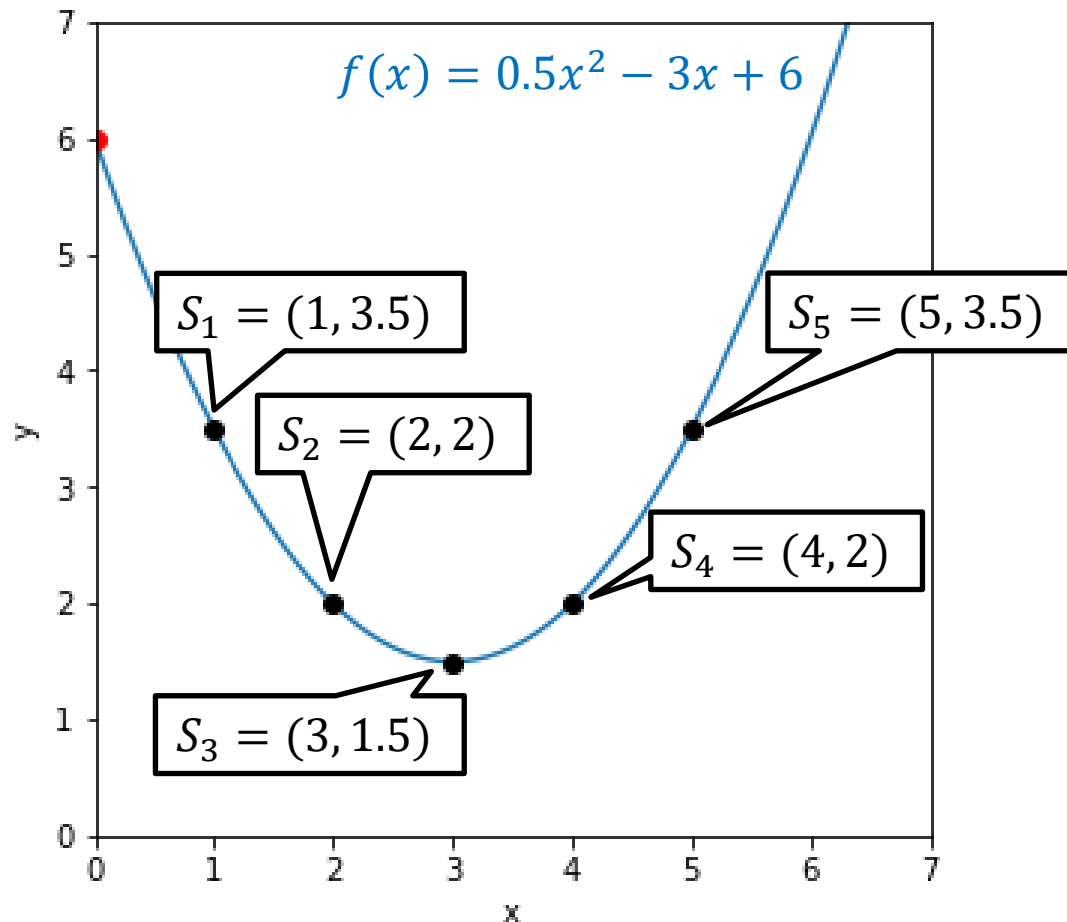


Phương pháp chia sẻ thông tin mật của Shamir

Ví dụ 2: $S = 6, n = 5, k = 3$

Phương pháp Shamir làm như thế nào?

□ Bước 2: $S_1 = (1, f(1)), S_2 = (2, f(2)), S_3 = (3, f(3)), \dots$



Phương pháp chia sẻ thông tin mật của Shamir

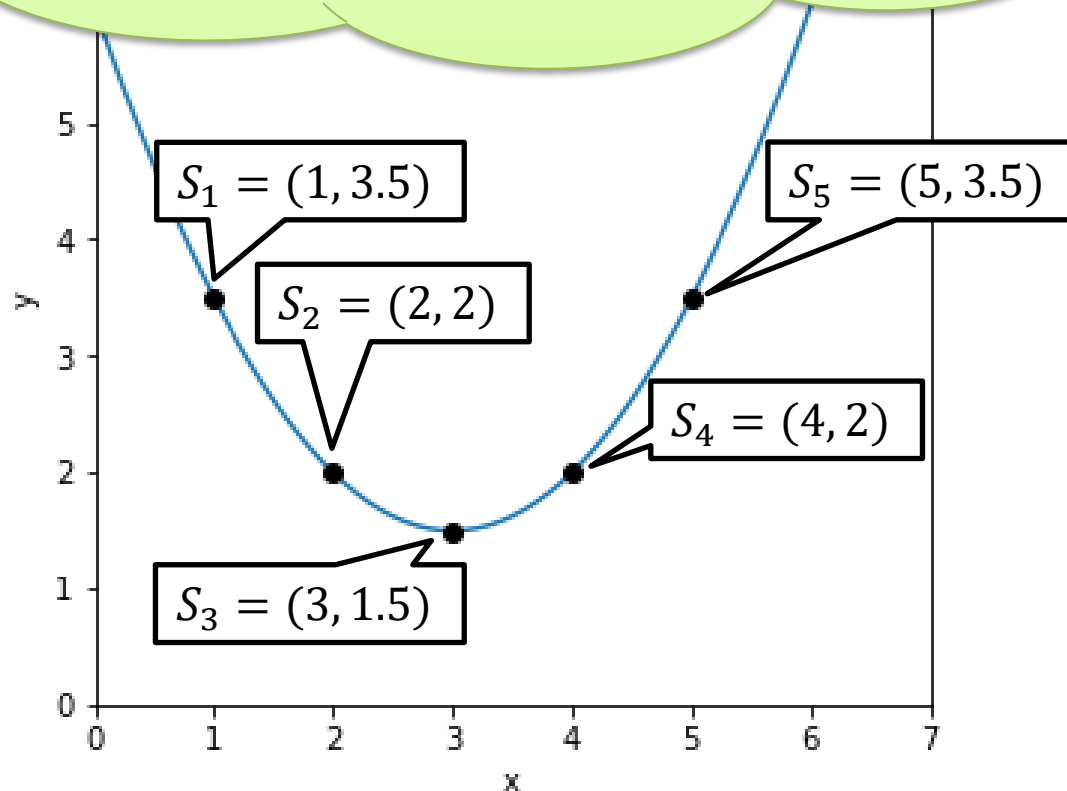
Ví dụ 2: $S = 6$

Phương pháp



Q: Nếu biết 2 trong 5 điểm S_1, S_2, S_3, S_4, S_5 thì có bao nhiêu đường cong bậc hai đi qua 2 điểm này? Có bao nhiêu $f(0)$?

A: Vô số ☺



Phương pháp chia sẻ thông tin mật của Shamir

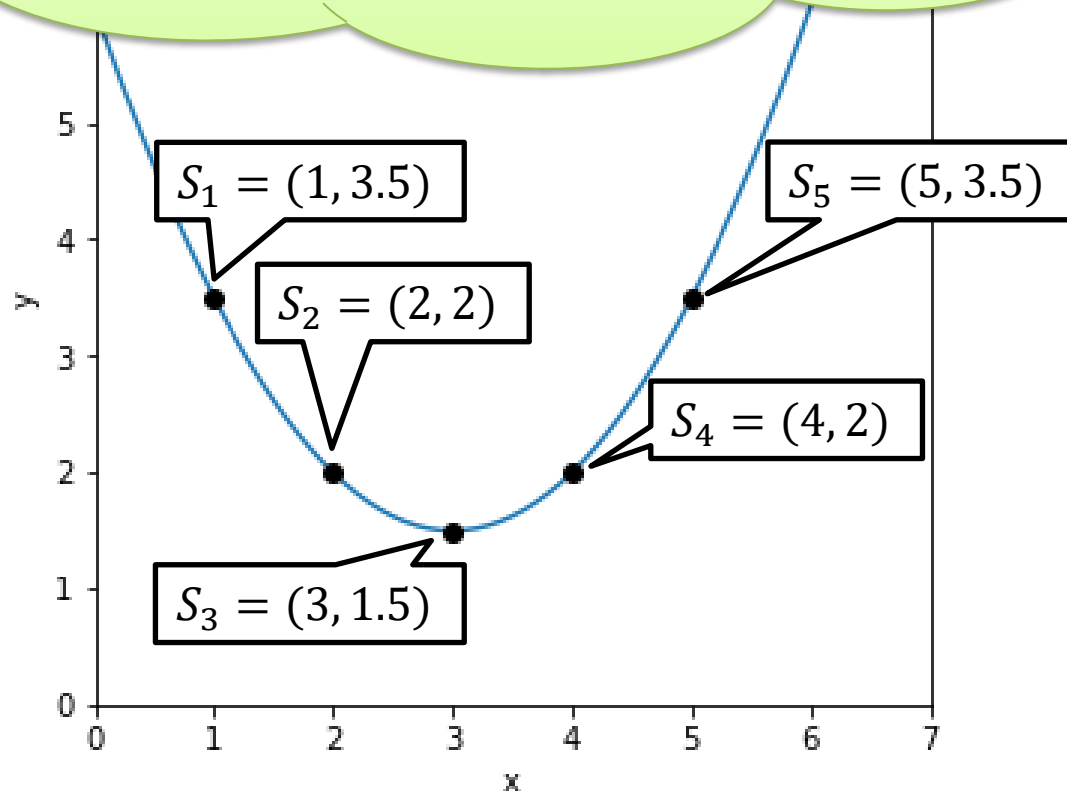
Ví dụ 2: $S = 6$

Phương pháp



Q: Nếu biết 3 trong 5 điểm S_1, S_2, S_3, S_4, S_5 thì có bao nhiêu đường cong bậc hai đi qua 3 điểm này? Có bao nhiêu $f(0)$?

A: Một 😊



Phương pháp chia sẻ thông tin mật của Shamir

Phân chia thông tin mật

☐ Input

- ☐ Thông tin mật S (một con số)
- ☐ Số phần cần chia n
- ☐ Ngưỡng k

☐ Quá trình thực hiện

- ☐ Tạo hàm f là một đa thức bậc $k - 1$ sao cho $f(0) = S$
- ☐ $S_1 = (1, f(1)), S_2 = (2, f(2)), S_3 = (3, f(3)), \dots$

Phương pháp chia sẻ thông tin mật của Shamir

Tái tạo thông tin mật

☐ Input

- ☐ Ngưỡng k

- ☐ n' phần của thông tin mật ($n' \geq k$)

☐ Quá trình thực hiện

- ☐ Tái tạo hàm f (đa thức bậc $k - 1$) từ k phần trong n' phần

- ☐ $S = f(0)$

Tái tạo hàm f (đa thức bậc $k - 1$) từ k phần của thông tin mật như thế nào?

Tìm hàm đa thức bậc $k - 1$

[có dạng: $f(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \dots + a_0$]

từ k điểm $(x_1, y_1), \dots, (x_k, y_k)$ với $y_i = f(x_i)$

→ k phương trình, k ẩn:

$$\square a_{k-1}x_1^{k-1} + a_{k-2}x_1^{k-2} + \dots + a_0 = y_1$$

$$\square a_{k-1}x_2^{k-1} + a_{k-2}x_2^{k-2} + \dots + a_0 = y_2$$

$$\square \dots$$

$$\square a_{k-1}x_k^{k-1} + a_{k-2}x_k^{k-2} + \dots + a_0 = y_k$$

Giải sao?

□ Một cách giải hiệu quả là dùng nội suy Lagrange

Nội suy Lagrange

Ví dụ, tìm hàm f (hàm đa thức bậc 3) biết:

- ☐ $f(5) = 3$
- ☐ $f(7) = 2$
- ☐ $f(12) = 6$
- ☐ $f(30) = 15$

Ta chỉ cần tìm một hàm: (i) bậc 3, và (ii) đi qua 4 điểm ở trên

$$f(x) = 3\delta_5(x) + 2\delta_7(x) + 6\delta_{12}(x) + 15\delta_{30}(x)$$

với $\delta_i(x)$ là một hàm bậc 3

$$\text{và } \delta_i(x) = \begin{cases} 1 & \text{nếu } x = i \\ 0 & \text{nếu } x \in \{5, 7, 12, 30\} - \{i\} \\ \text{"sao cũng được"} & \text{trong những trường hợp khác} \end{cases}$$

Hàm f này thỏa
(i) và (ii) không?

Nội suy Lagrange

Ví dụ, tìm hàm f (hàm đa thức bậc 3) biết:

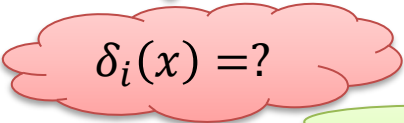
- ☐ $f(5) = 3$
- ☐ $f(7) = 2$
- ☐ $f(12) = 6$
- ☐ $f(30) = 15$

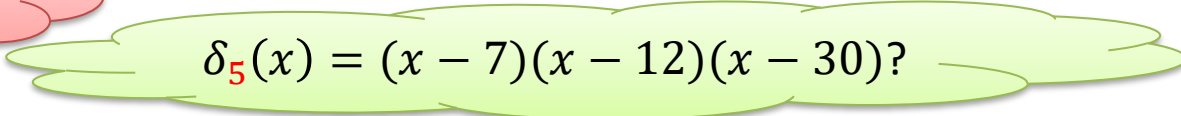
Ta chỉ cần tìm một hàm: (i) bậc 3, và (ii) đi qua 4 điểm ở trên

$$f(x) = 3\delta_5(x) + 2\delta_7(x) + 6\delta_{12}(x) + 15\delta_{30}(x)$$

với $\delta_i(x)$ là một hàm bậc 3

$$\text{và } \delta_i(x) = \begin{cases} 1 \text{ nếu } x = i \\ 0 \text{ nếu } x \in \{5, 7, 12, 30\} - \{i\} \\ \text{"sao cũng được" trong những trường hợp khác} \end{cases}$$


$$\delta_i(x) = ?$$


$$\delta_5(x) = (x - 7)(x - 12)(x - 30)?$$

Nội suy Lagrange

Ví dụ, tìm hàm f (hàm đa thức bậc 3) biết:

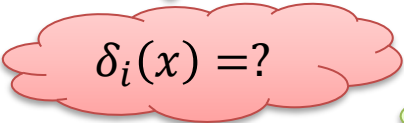
- ☐ $f(5) = 3$
- ☐ $f(7) = 2$
- ☐ $f(12) = 6$
- ☐ $f(30) = 15$

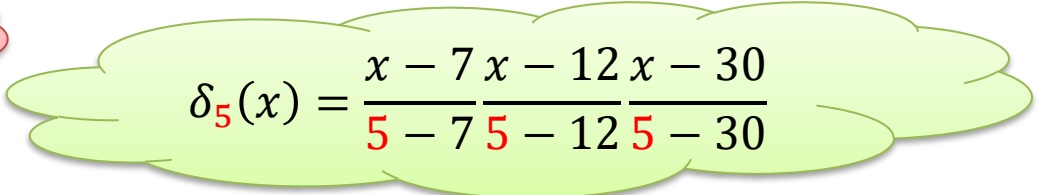
Ta chỉ cần tìm một hàm: (i) bậc 3, và (ii) đi qua 4 điểm ở trên

$$f(x) = 3\delta_5(x) + 2\delta_7(x) + 6\delta_{12}(x) + 15\delta_{30}(x)$$

với $\delta_i(x)$ là một hàm bậc 3

$$\text{và } \delta_i(x) = \begin{cases} 1 \text{ nếu } x = i \\ 0 \text{ nếu } x \in \{5, 7, 12, 30\} - \{i\} \\ \text{"sao cũng được" trong những trường hợp khác} \end{cases}$$


$$\delta_i(x) = ?$$


$$\delta_5(x) = \frac{x-7}{5-7} \frac{x-12}{5-12} \frac{x-30}{5-30}$$

Nội suy Lagrange

Ví dụ, tìm hàm f (hàm đa thức bậc 3) biết:

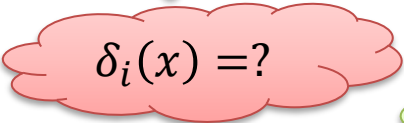
- ☐ $f(5) = 3$
- ☐ $f(7) = 2$
- ☐ $f(12) = 6$
- ☐ $f(30) = 15$

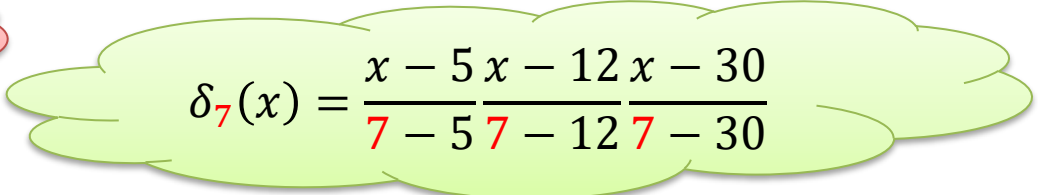
Ta chỉ cần tìm một hàm: (i) bậc 3, và (ii) đi qua 4 điểm ở trên

$$f(x) = 3\delta_5(x) + 2\delta_7(x) + 6\delta_{12}(x) + 15\delta_{30}(x)$$

với $\delta_i(x)$ là một hàm bậc 3

$$\text{và } \delta_i(x) = \begin{cases} 1 \text{ nếu } x = i \\ 0 \text{ nếu } x \in \{5, 7, 12, 30\} - \{i\} \\ \text{"sao cũng được" trong những trường hợp khác} \end{cases}$$


$$\delta_i(x) = ?$$


$$\delta_7(x) = \frac{x-5}{7-5} \frac{x-12}{7-12} \frac{x-30}{7-30}$$

Nội suy Lagrange

Ví dụ, tìm hàm f (hàm đa thức bậc 3) biết:

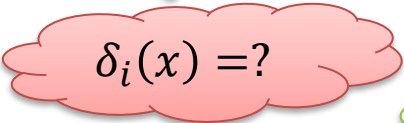
- ☐ $f(5) = 3$
- ☐ $f(7) = 2$
- ☐ $f(12) = 6$
- ☐ $f(30) = 15$

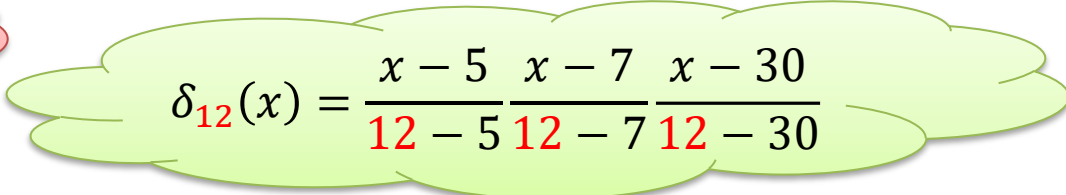
Ta chỉ cần tìm một hàm: (i) bậc 3, và (ii) đi qua 4 điểm ở trên

$$f(x) = 3\delta_5(x) + 2\delta_7(x) + 6\delta_{12}(x) + 15\delta_{30}(x)$$

với $\delta_i(x)$ là một hàm bậc 3

$$\text{và } \delta_i(x) = \begin{cases} 1 \text{ nếu } x = i \\ 0 \text{ nếu } x \in \{5, 7, 12, 30\} - \{i\} \\ \text{"sao cũng được" trong những trường hợp khác} \end{cases}$$


$$\delta_i(x) = ?$$


$$\delta_{12}(x) = \frac{x-5}{12-5} \frac{x-7}{12-7} \frac{x-30}{12-30}$$

Nội suy Lagrange

Ví dụ, tìm hàm f (hàm đa thức bậc 3) biết:

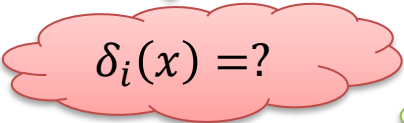
- ☐ $f(5) = 3$
- ☐ $f(7) = 2$
- ☐ $f(12) = 6$
- ☐ $f(30) = 15$

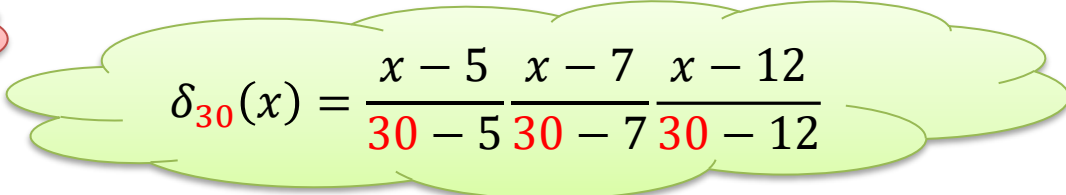
Ta chỉ cần tìm một hàm: (i) bậc 3, và (ii) đi qua 4 điểm ở trên

$$f(x) = 3\delta_5(x) + 2\delta_7(x) + 6\delta_{12}(x) + 15\delta_{30}(x)$$

với $\delta_i(x)$ là một hàm bậc 3

$$\text{và } \delta_i(x) = \begin{cases} 1 \text{ nếu } x = i \\ 0 \text{ nếu } x \in \{5, 7, 12, 30\} - \{i\} \\ \text{"sao cũng được" trong những trường hợp khác} \end{cases}$$


$$\delta_i(x) = ?$$


$$\delta_{30}(x) = \frac{x-5}{30-5} \frac{x-7}{30-7} \frac{x-12}{30-12}$$

Demo ...

Mở rộng phương pháp Shamir cho thông tin mật gồm nhiều con số (vd, ảnh)

Cách đơn giản nhất là áp dụng phương pháp Shamir cho từng con số của thông tin mật