

Contoh Soal-Pembahasan
Threshold-Scheme Secret Sharing
Oleh : Rudi Cahyo Budiyo [11-10-2008]
E-mail: rudibudiyono@gmail.com
http://rudibudiyono.blogspot.com

1. Skema Secret Sharing

Dunia teknologi berkembang begitu cepat. Data dan informasi menjadi bagian yang tidak terpisahkan dari laju perkembangan teknologi saat ini. Pada kasus tertentu, kerahasiaan data adalah hal yang sangat penting. Oleh karena itu berbagai upaya dilakukan agar data hanya dapat diakses oleh mereka yang memiliki hak akses.

Salah satu contoh metode menjaga kerahasiaan data adalah dengan menggunakan metode **Secret Sharing (SS)**. *Secret Sharing* ini merupakan bagian dari kriptografi. Ide dasar SS adalah membagi informasi menjadi beberapa bagian, dan kemudian dengan subset tertentu dari bagian-bagian informasi tersebut dapat digunakan untuk *me-recover* informasi awal. Proses *recovery* menggunakan **interpolasi Lagrange**. Dan yang akan kita bahas kali ini adalah sebatas pada **Threshold-Scheme Secret Sharing**.

Mengenai teori matematika yang melandasi *Threshold-Scheme SS*, pembaca dapat merujuk pada buku-buku referensi yang disertakan. Pada *paper* sederhana ini hanya akan dibahas sekilas tentang penerapan *Threshold-Scheme SS* dalam kehidupan sehari-hari.

2. Contoh Aplikasi Threshold-Scheme SS

Baiklah, gambaran sekilas mengenai *Threshold-Scheme SS* dapat diikuti dari cerita berikut:

“Pada suatu negara, ada rencana peluncuran roket. Insinyur roket ini mendesain eksekusi peluncuran sedemikian rupa sehingga hanya dapat diluncurkan apabila ada tiga orang pemegang kunci yang menyetujui peluncuran tersebut dan mengumpulkan kunci mereka. Insinyur ini kemudian membagi kunci peluncuran menjadi empat bagian. Masing-masing bagian kunci diberikan kepada:

presiden, perdana menteri, menteri pertahanan, dan kepala kepolisian negara.

Tiga orang dari empat orang pemegang kunci dapat melakukan eksekusi peluncuran roket. Tiga orang tersebut bisa presiden, perdana menteri, dan menteri pertahanan. Atau bisa juga dilakukan oleh presiden, menteri pertahanan, dan kepala kepolisian negara. Atau bisa juga kombinasi lainnya.

Namun demikian, apabila kurang dari tiga orang peluncuran tidak dapat dilaksanakan.

Kemudian insinyur, memilih 2 angka acak yakni $a_1=2$ dan $a_2=5$. Kemudian insinyur juga sepakat membuat sistem pembagian kunci ini berjalan pada bilangan modulo 31.

Dalam kasus ini, akhirnya presiden, perdana menteri, dan menteri pertahanan dapat menghadiri dan menyaksikan peluncuran roket.

Mereka sebelumnya masing-masing mendapat sebuah bagian kunci, yakni:

- presiden (1,3);
- perdana menteri (2,20),
- menteri pertahanan (3,16).

Dari ketiga kombinasi bagian kunci tersebut, setelah melalui proses perhitungan tertentu akan didapatkan kunci tunggal yang dapat mengeksekusi peluncuran roket.”

Dalam cerita di atas, kita peroleh beberapa keterangan:

$$\begin{array}{ll} t = 3; & n = 4; \\ p = 31; & a_1 = 2; \\ a_2 = 5; & s_1 = (1,3); \\ s_2 = (2,20); & s_3 = (3,16); \end{array}$$

Karena $t = 3$; dan $n = 4$; maka $(t,n) = (3,4)$.

Dan karena terbatas pada *Threshold-Scheme*, maka cerita di atas dapat ditulis sebagai persoalan **(3,4) Threshold-Scheme SS**.

Pertanyaan:

Carilah kunci tunggal S berdasarkan informasi di atas!

Pembahasan:

Akan dicari kunci tunggal S .
Semua hitungan bekerja pada modulo 31.
Dari soal diketahui, nilai $a_1 = 2$ dan $a_2 = 5$;
maka dapat dibentuk fungsi :

$$f(x) = S + 2x + 5x^2 \dots\dots\dots (1)$$

Dalam *Threshold-Scheme SS*, pencarian kunci tunggal S dilakukan menggunakan **interpolasi Lagrange**.

Interpolasi Lagrange:

$$f(x) = \sum_{i=1}^t y_i \prod_{\substack{1 \leq i \leq t \\ i \neq j}} \frac{x - x_j}{x_i - x_j} \dots\dots\dots (2)$$

Nilai S dalam (1) dapat diketahui jika semua nilai x dalam $f(x)$ adalah 0.

Maka untuk mencari S ,

$$f(0) = S$$

Sedangkan dari Interpolasi Lagrange, jika nilai $x = 0$, maka diperoleh:

$$f(0) = \sum_{i=1}^t y_i \prod_{\substack{1 \leq i \leq t \\ i \neq j}} \frac{x_j}{x_j - x_i}$$

dengan demikian untuk $x = 0$, dari (1) dan (2) dapat diperoleh:

$$f(0) = S = \sum_{i=1}^t y_i \prod_{\substack{1 \leq i \leq t \\ i \neq j}} \frac{x_j}{x_j - x_i}$$

Dengan diketahui nilai-nilai:

- $s_1 = (1,3)$;
- $s_2 = (2,20)$;
- $s_3 = (3,16)$;

dan

$$S = \sum_{i=1}^t y_i \prod_{\substack{1 \leq i \leq t \\ i \neq j}} \frac{x_j}{x_j - x_i}$$

Maka dapat dihitung nilai S :

$$\begin{aligned} S &= \left(3 \cdot \frac{2 \cdot 3}{(2-1)(3-1)} + 20 \cdot \frac{1 \cdot 3}{(1-2)(3-2)} \right. \\ &\quad \left. + 16 \cdot \frac{1 \cdot 2}{(1-3)(2-3)} \right) \text{ mod } 31 \\ &= \left(3 \cdot \frac{3}{1} + 20 \cdot \frac{3}{(-1)} + 16 \cdot \frac{1}{1} \right) \text{ mod } 31 \\ &= (9 - 60 + 16) \text{ mod } 31 \\ &= (-35) \text{ mod } 31 \\ &= 27 \end{aligned}$$

Jadi, diperoleh kunci tunggal = $S = 27$

Soal Latihan :

1. Diketahui nilai-nilai untuk $(3,5)$ *Threshold-Scheme SS* sebagai berikut :
 $p = 19$; $s_1 = (1,12)$;
 $s_4 = (4,11)$; $s_5 = (5,2)$;

Carilah kunci tunggal dari soal tersebut!!

Jawab: $S = 10$

(Petunjuk: Untuk menghitung invers pergandaan modulo, bisa menggunakan metode Algoritma Euclide Diperluas)

Referensi :

- [1.] Menezes, A.J., Oorschot, P.C dan Vanstone, S.A., 1997, "*Handbook of Applied Cryptography*", CRC Press, Inc. USA.
- [2.] Stinson, D.R., 1995, "*Cryptography Theory and Practice*", CRC Press, Inc., Boca Raton, Florida.

☺☺☺ Terima kasih ☺☺☺