

ASMUTH BLOOM'S SECRET SHARING SCHEME

noersilo@yahoo.com | www.noersilo.web.id

1. PENDAHULUAN

Suatu berita rahasia jika hanya dikendalikan oleh satu orang saja akan membahayakan keamanan berita rahasia tersebut. Salah satu cara untuk mengatasi permasalahan ini adalah dengan membagi berita rahasia tersebut menjadi beberapa bagian. Skema *Secret sharing* merupakan suatu cara atau metode untuk membagi suatu berita rahasia, menjadi beberapa bagian yang disebut *shares*, untuk dibagikan kepada sejumlah pihak yang disebut *participants*, dengan ketentuan tertentu. Aturan yang dimaksud adalah struktur akses, yaitu aturan tentang siapa saja yang mendapatkan otorisasi untuk membentuk berita rahasia itu kembali. Berita rahasia yang dimaksud lebih khusus adalah kunci hasil suatu proses enkripsi. Dalam suatu kelompok berlaku nilai ambang (*threshold value*), yaitu jumlah minimal *participants* yang dibutuhkan dalam suatu kelompok untuk membangkitkan suatu berita rahasia. Untuk menjaga keamanan kunci hasil dari sistem kriptografi agar tidak hilang, disarankan untuk membuat sejumlah kunci cadangan. Namun resiko kerahasiaan kunci akan semakin besar dengan semakin banyaknya kunci cadangan yang dibuat. Secret sharing menangani masalah ini dengan membagi kunci menjadi beberapa bagian tanpa meningkatkan resiko kerahasiaan.

Secret sharing juga menangani masalah pendistribusian kunci– kunci tersebut dengan hanya mengizinkan t dari n user dimana $t < n$ untuk melakukan pembentukan kunci awal. Ide dari secret sharing adalah dengan membagi kunci rahasia menjadi beberapa bagian yang disebut *shares*, dan membagikannya kepada beberapa orang. Hanya subset dari orang – orang tersebut yang bisa atau diijinkan untuk membentuk kunci awal kembali. Contoh kasus pengembangan metode Shamir adalah pembagian pemegang kunci menjadi 2 kelompok. Untuk membentuk kunci awal, misalnya diperlukan sedikitnya 2 *shares* dari kelompok A dan 3 *shares* dari kelompok B.

Berapapun jumlah *shares* pada kelompok A, mereka tidak dapat membentuk kunci awal tanpa minimal 2 *shares* dari kelompok A.

Pada paper ini saya akan menuliskan tentang salah satu metode secret sharing menggunakan Chinese Remainder Theorem. Skema Asmuth Bloom merupakan skema secret sharing yang menggunakan Chinese Remainder Theorem untuk merekonstruksi pesan rahasianya, dan membutuhkan generator dan bilangan bulat prima untuk menghasilkan jumlah *shares*-nya.

2. SKEMA ASMUTH BLOOM

Skema Secret Sharing Asmuth Bloom merupakan suatu metode secret sharing yang menggunakan Chinese Remainde Theorem dalam peyelesaiannya. Skema Secret Sharing Asmuth Bloom diciptakan oleh C.Asmuth dan J.Bloom pada tahun 1983, Skema ini menggunakan rangkaian bilangan bulat khusus dimana terdapat rangkaian bilangan positif prima m_0, m_1, \dots, m_k . Bilangan bulat tersebut terpenuhi dengan kondisi :

$$m_0 \cdot \prod_{i=0}^{k-2} m_{n-i} < \prod_{i=1}^k m_i .$$

Himpunan nilai n disebut juga rangkaian Asmuth Bloom. Skema tersebut bekerja dengan kondisi :

- S rahasia adalah bilangan bulat random yang terdapat pada himpunan Z/m_0Z
- Terdapat suatu generator α yang merupakan suatu bilangan bulat random sehingga,

$$(S + \alpha \cdot m_0) < m_0, m_1, \dots, m_k.$$

dan pembagiannya di tentukan dengan,

$$I_i = (S + \alpha \cdot m_0) \bmod m_i, \text{ untuk semua } 1 \leq i \leq n.$$

Selanjutnya adalah mencari nilai x menggunakan metode Chinese Remainder Theorem :

$$\begin{aligned}
 x &\equiv I_1 \pmod{m_1} \\
 x &\equiv I_2 \pmod{m_2} \\
 &\cdot \\
 &\cdot \\
 &\cdot \\
 x &\equiv I_k \pmod{m_k}
 \end{aligned}$$

Setelah itu akan ditemukan hasil X rahasia yang merupakan pesan rahasia yang dicari. X akan mudah dihitung dengan metode Chinese Remainder Theorem karena m_i adalah prima. X rahasia merupakan modulo m_0 terhadap x .

$$X \equiv x \pmod{m_0}$$

3. APLIKASI

Berikut adalah contoh aplikasi skema Asmuth Bloom pada interger prima kecil.

a. Kontruksi

Terdapat 2 sebuah pasangan parameter (k,n) yaitu $(2,3)$ dan memiliki rangkaian Asmuth Bloom

$$b. \quad m_0=5, m_1=7, m_2=11, m_3=13,$$

Kondisi nilai tersebut memenuhi, karena $5.13 < 7.11$.

Kita asumsi nilai rahasia S adalah 3 dimana $3 \in Z_5$ dan terdapat generator $\alpha = 13$, maka $(3+13.5=68) < 77$, sehingga nilai yang dibagi ke masing-masing *participant* adalah 5, 2, 3.

$$I_1=5, I_1=2, I_1=3$$

c. Rekontruksi

Proses decodingnya adalah :

$$\begin{aligned}
 x &\equiv I_1 \pmod{m_1} \\
 x &\equiv I_2 \pmod{m_2}
 \end{aligned}$$

$$\begin{aligned} & \cdot \\ & \cdot \\ & \cdot \\ x & \equiv I_k \pmod{m_k} \end{aligned}$$

Sehingga,

$$\begin{aligned} x & \equiv 5 \pmod{7} \\ x & \equiv 3 \pmod{13} \end{aligned}$$

Menggunakan Chinese Remainder Theorem maka nilai x adalah 68, sehingga nilai X rahasia yang akan dicari dapat didapatkan dari perhitungan

$$X \equiv x \pmod{m_0}$$

sehingga kongruen $68 \pmod{5}$ adalah 3. Jadi nilai X rahasia adalah 3 dimana nilainya sama dengan S .

4. DAFTAR PUSTAKA

- [1] Ulutas, M. N., Vasif. Ulutas, G. "A New Secret Image Sharing Technique Based On Asmuth Bloom's Scheme". 2009
- [2] Asmuth, C. Bloom, J. "Modular Approach to Key Safeguarding", IEEE Transactions on Information Theory, Vol.29, No.2, pp.208-210. 1983.