Penggunaan Secret Sharing untuk Berbagi Password

Abraham Sri Paskah Ageng Wahono – 2012730072

1 Data Skripsi

Pembimbing utama/tunggal: **Mariskha Tri Adithia**
Pembimbing pendamping: **-**
Kode Topik : **MTA4201***
Topik ini sudah dikerjakan selama : **1** semester
Pengambilan pertama kali topik ini pada : Semester **42 - Genap 16/17**
Pengambilan pertama kali topik ini di kuliah : **Skripsi 1**
Tipe Laporan : **B** - Dokumen untuk reviewer pada presentasi dan **review Skripsi 1**

2 Detail Perkembangan Pengerjaan Skripsi

Detail bagian pekerjaan skripsi sesuai dengan rencana kerja/laporan perkembangan terakhir :

1. **Melakukan studi literatur mengenai dasar-dasar kriptografi.**
   Status : Ada sejak rencana kerja skripsi.
   Hasil : Studi literatur yang dilakukan mencakup dasar-dasar kriptografi, otentikasi entitas, dan *password*. Berikut adalah hasil studi literatur yang sudah dilakukan.

   - Kriptografi
     Kriptografi berasal dari bahasa Yunani "*kryptós*" yang artinya adalah rahasia dan "*graphein*" yang berarti tulisan. Jadi, kriptografi berarti "tulisan rahasia". Definisi kriptografi yang umum dipakai di masa lalu adalah : ilmu dan seni untuk menjaga kerahasiaan pesan. Namun, kriptografi modern saat ini membahas lebih dari sekedar kerahasiaan saja. Pada saat ini kriptografi merupakan ilmu yang mempelajari teknik matematis yang bertujuan memberikan layanan (aspek-aspek) keamanan. Aspek-aspek keamanan dari kriptografi tersebut adalah sebagai berikut :
     (a) Kerahasiaan (*confidentiality*) : layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak.
     (b) Integritas data (*data integrity*) : layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman.
     (c) Otentikasi (*authentication*) : layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*entity authentication*) maupun mengidentifikasi kebenaran sumber pesan (*data origin authentication*).
     (d) Nirpenyangkalan (*non-repudiation*) : layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

     Pada kriptografi, aspek keamanan yang berkaitan dengan kerahasiaan (*confidentiality*) dapat dicapai dengan melakukan dua proses dasar yaitu proses enkripsi dan proses dekripsi. Proses enkripsi adalah proses mengubah/menyandikan pesan asli yang disebut dengan plainteks menjadi bentuk lain yang tidak dapat dipahami dengan menggunakan algoritma kriptografi. Pesan yang sudah tersandi tersebut disebut juga sebagai cipherteks. Proses dekripsi adalah proses mengubah

kembali cipherteks menjadi plainteks. Bila proses enkripsi dinotasikan sebagai E, proses dekripsi sebagai D, plainteks sebagai P, dan cipherteks sebagai C, maka proses enkripsi dan dekripsi dapat dinyatakan secara matematis seperti pada rumus 1 dan rumus 2 secara berturut-turut.

$$E(P) = C \tag{1}$$

$$D(C) = P \tag{2}$$

Pada awalnya, tingkat keamanan algoritma kriptografi ditentukan oleh tingkat kerahasiaan algoritmanya. Namun cara tersebut tidak selalu aman karena jika algoritmanya diketahui maka pesan rahasia mudah untuk dipecahkan. Masalah ini diatasi dengan menggunakan kunci sebagai parameter untuk transformasi proses enkripsi dan proses dekripsi. Dengan menggunakan kunci, algoritma tidak perlu lagi dijaga kerahasiaannya namun kunci harus tetap dirahasiakan. Kunci biasanya berupa *string* (deretan huruf) atau deretan bilangan. Dengan menggunakan kunci K, maka proses enkripsi dan proses dekripsi dapat dinyatakan secara matematis seperti pada rumus 3 dan 4 secara berturut-turut.

$$E_K(P) = C \tag{3}$$

$$D_K(C) = P \tag{4}$$

Sehingga memenuhi persamaan 5 seperti berikut :

$$D_K(E_K(P)) = P \tag{5}$$

- Otentikasi Entitas

  Dalam kriptografi, otentikasi entitas adalah teknik otentikasi yang dirancang untuk memungkinkan suatu pihak membuktikan kebenaran identitas dari pihak lain. Entitas dalam hal ini bisa berupa manusia, proses, *client*, atau *server*. Entitas yang identitasnya ingin dibuktikan kebenarannya disebut sebagai *claimant*, dan pihak yang mencoba untuk membuktikan kebenaran identitas dari *claimant* disebut sebagai *verifier*. Terdapat beberapa perbedaan antara otentikasi pesan (*message authentication*) dengan otentikasi entitas (*entity authentication*). Perbedaan kedua teknik otentikasi tersebut adalah :

  – Otentikasi entitas berjalan secara *real time* sementara otentikasi pesan tidak.
  – Otentikasi pesan hanya dapat melakukan otentikasi terhadap satu pesan saja; proses otentikasi perlu diulang untuk setiap pesan baru. Sementara pada otentikasi entitas hanya dilakukan satu kali otentikasi dalam satu sesi pertukaran informasi.

  Dalam otentikasi entitas, pihak *claimant* harus mengidentifikasikan dirinya kepada pihak *verifier*. Pihak *claimant* perlu memberikan suatu bukti kepada pihak *verifier* untuk membuktikan kebenaran identitasnya. Bukti tersebut dapat berupa sesuatu yang diketahui (*something known*) oleh *claimant*, sesuatu yang dimiliki (*something possessed*) oleh *claimant*, atau sesuatu yang melekat (*something inherent*) pada *claimant*.

  (a) Sesuatu yang diketahui (*something known*) : adalah rahasia yang hanya diketahui oleh pihak *claimant*, yang dapat dibuktikan kebenarannya oleh pihak *verifier*. Contohnya adalah *password* dan PIN.
  (b) Sesuatu yang dimiliki (*something possessed*) : adalah sesuatu yang dapat membuktikan kebenaran identitas dari *claimant*. Contohnya adalah paspor, SIM, KTP, dan kartu kredit.
  (c) Sesuatu yang melekat (*something inherent*) : adalah sesuatu yang merupakan ciri khas dari *claimant*. Contohnya adalah tanda tangan, sidik jari, retina mata, dan bentuk wajah.

- Password

  Otentikasi menggunakan *password* adalah salah satu metode otentikasi entitas yang paling sederhana dan paling lama digunakan. *Password* digunakan ketika pengguna (*user*) ingin mengakses suatu sistem untuk menggunakan sumber daya atau mengakses informasi yang tersedia pada sistem tersebut. Otentikasi menggunakan *password* dibagi menjadi dua kelompok yaitu :

  (a) *Fixed password* : adalah *password* tetap yang dapat digunakan berkali-kali untuk setiap kali akses.

  (b) *One-time password* : adalah *password* yang hanya berlaku untuk satu kali akses.

2. **Mempelajari metode-metode *secret sharing* seperti metode *secret sharing* Shamir dan *secret sharing* Blakley.**
   Status : Ada sejak rencana kerja skripsi.
   Hasil : Berikut adalah hasil pembelajaran metode *secret sharing* Shamir dan *secret sharing* Blakley.

   - Secret Sharing

     Secret Sharing adalah metode untuk merahasiakan pesan dengan cara membagikan pesan rahasia ke sejumlah partisipan. Skema *secret sharing* dibuat untuk mengatasi masalah yang dimiliki oleh teknik enkripsi- dekripsi menggunakan kunci. Teknik enkripsi-dekripsi menggunakan kunci masih memiliki banyak kekurangan. Kunci rahasia rentan mengalami kerusakan atau hilang apabila kunci hanya disimpan di satu tempat. Namun kunci rahasia juga rawan untuk diperoleh oleh pihak yang tidak bertanggung jawab apabila kunci tersebut diduplikasi dan disimpan di beberapa tempat. Apabila kunci mengalami kerusakan atau hilang, proses enkripsi dan dekripsi akan mengalami hambatan karena harus membuat kunci baru, dan hal ini membutuhkan waktu yang cukup lama. Selain itu, teknik enkripsi-dekripsi dengan menggunakan kunci juga memiliki tingkat kompleksitas yang cukup tinggi. Dengan menggunakan skema *secret sharing*, tingkat keamanan pesan rahasia akan semakin terjaga dengan baik karena pesan rahasia dipecah dan dibagikan ke sejumlah partisipan di mana setiap partisipan tidak memiliki informasi apapun mengenai pesan rahasia tersebut.

     Pada skema *threshold secret sharing* (k, n) pesan rahasia dibagikan ke n banyak partisipan. Setiap partisipan memperoleh bagian dari pesan rahasia yang disebut dengan *share*, dan *share* yang diperoleh setiap partisipan akan berbeda dengan partisipan-partisipan lainnya. Pesan rahasia hanya dapat dibangun kembali (direkonstruksi) dengan mengumpulkan k buah share atau lebih.

   - Metode Secret Sharing Shamir

     Pada metode *secret sharing* Shamir, pesan rahasia terletak pada suatu fungsi polinomial yang unik dengan derajat $(k-1)$. Pesan rahasia terletak pada fungsi $f(0)$ dan fungsi polinomial tersebut dapat diperoleh dengan memperoleh k buah titik pada polinomial. Pada metode ini, pesan rahasia dibagikan ke n buah partisipan dengan menggunakan polinomial seperti pada rumus 6 di bawah ini :

     $$f(x) = \sum_{i=0}^{k} a_i \cdot x^i \tag{6}$$

     Di mana x adalah partisipan ke-n sehingga masing-masing partisipan akan memiliki fungsi yang tidak sama dan masing-masing partisipan memperoleh *share* yang berupa fungsi $f(x) = (x, y)$ seperti berikut :

     $$f(i) = (i, f(i)\ mod\ p) \tag{7}$$

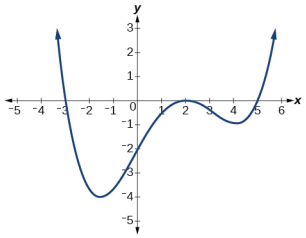
Pada metode *secret sharing* Shamir ini, bilangan prima p ditentukan secara acak dan digunakan untuk meningkatkan keamanan pesan rahasia agar tidak rawan terhadap serangan *brute force*. *Share* yang dimiliki setiap partisipan merepresentasikan suatu titik yang terletak pada fungsi polinomial. Setiap partisipan hanya memiliki informasi mengenai *share* yang mereka miliki, mereka tidak memiliki informasi sama sekali mengenai pesan rahasia yang terletak pada fungsi $f(0)$. Pesan rahasia dapat dibangun kembali dengan melakukan interpolasi di mana diperlukan k buah titik pada fungsi polinomial untuk memperoleh fungsi polinomial yang mengandung pesan rahasia. Metode *secret sharing* Shamir menggunakan interpolasi Lagrange untuk memperoleh kembali fungsi polinomial unik yang mengandung pesan rahasia tersebut. Interpolasi Lagrange dinyatakan secara matematis pada rumus 8 berikut :

$$f(x) = \sum_{i=1}^{k} y_i \left(\prod_{j=1, j \neq i}^{k} \frac{x_j}{x_j - x_i} \right) \tag{8}$$

Sehingga fungsi polinomial $f(0)$ diperoleh dengan rumus 9 seperti berikut :

$$f(0) = \sum_{i=1}^{k} y_i \left(\prod_{j=1, j \neq i}^{k} \frac{x_j}{x_j - x_i} \right) \ mod\ p \tag{9}$$

Fungsi polinomial $f(0)$ yang berhasil dibangun kembali akan mengembalikan pesan rahasia.



Gambar 1: Contoh grafik fungsi polinomial berderajat 4 dengan nilai $f(0) = -2$

- Metode Secret Sharing Blakley

  Metode *secret sharing* Blakley menggunakan pendekatan geometri untuk membagikan pesan rahasia kepada n buah partisipan. Pada metode *secret sharing* Blakley ini, pesan rahasia terletak pada suatu titik di bidang k dimensi di mana k buah *hyperplane* beririsan. *Hyperplane* adalah bidang $k-1$ dimensi yang terletak di dalam bidang bidang utama k dimensi yang merepresentasikan *share* yang dimiliki setiap partisipan.

Gambar 2: Representasi bidang 3 dimensi dengan *hyperplane* 2 dimensi

Pada skema *secret sharing* Blakley $(3, n)$, pesan rahasia dinotasikan dengan fungsi $Q(x, y, z)$ yang merepresentasikan koordinat letak pesan rahasia di bidang k dimensi. *Hyperplane* untuk setiap partisipan pada *secret sharing* Blakley skema $(3, n)$ direpresentasikan dalam notasi matematika

seperti berikut :

$$z \equiv a_i x + b_i y + c_i \tag{10}$$

di mana nilai a dan b untuk masing-masing partisipan ditentukan secara acak, dan nilai c untuk masing-masing partisipan diperoleh dengan menggunakan persamaan 11 berikut :

$$c_i \equiv (z_i - a_i x - b_i y) \ mod \ p \tag{11}$$

Sama dengan metode *secret sharing* Shamir, pada metode *secret sharing* Blakley ini bilangan prima p digunakan untuk meningkatkan keamanan pesan rahasia. Dengan menggunakan kedua persamaan yang telah disebutkan di atas, masing-masing partisipan akan memperoleh *share* yang berupa bidang 2 dimensi. Pesan rahasia dapat dibangun kembali dengan menggunakan persamaan 12 di bawah ini :

$$a_i x + b_i y - z \equiv -c_i \ (mod \ p) \tag{12}$$

Persamaan tersebut kemudian direpresentasikan ke dalam bentuk matriks seperti berikut :

$$\begin{pmatrix} a_1 & b_1 & -1 \\ a_2 & b_2 & -1 \\ a_3 & b_3 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -c_1 \\ -c_2 \\ -c_3 \end{pmatrix} \ mod \ p \tag{13}$$

Nilai x, y, dan z akan diperoleh dengan melakukan operasi baris elementer. Masing-masing nilai x, y, dan z akan di-*mod* dengan bilangan prima p untuk memperoleh pesan rahasia.

3. **Mengaplikasikan metode *secret sharing* Shamir dan *secret sharing* Blakley secara manual.**
   Status : Ada sejak rencana kerja skripsi.
   Hasil : Pada bagian ini akan dipaparkan masalah yang melatarbelakangi penggunaan metode *secret sharing* untuk berbagi *password* beserta contoh implementasi metode *secret sharing* Shamir dan metode *secret sharing* Blakley secara manual.

   Password adalah salah satu proses otentikasi yang umum digunakan untuk meningkatkan keamanan suatu sistem. Namun pada penggunaannya, seringkali ditemukan kelemahan-kelemahan pada proses otentikasi yang menggunakan *password*. Beberapa kelemahan tersebut antara lain adalah pembobolan *password* menggunakan *brute force*, dan dilupakannya atau hilangnya *password*.

   Dibutuhkan suatu cara untuk meningkatkan keamanan *password* sehingga kelemahan-kelemahan teknik otentikasi menggunakan *password* dapat diatasi. Cara yang dapat digunakan adalah dengan menggunakan metode *secret sharing*. Metode ini digunakan untuk mendistribusikan *password* ke beberapa orang partisipan sehingga meningkatkan tingkat keamanan *password*. Pada skripsi ini akan dibuat perangkat lunak yang dapat mengimplementasikan penggunaan metode *secret sharing* untuk membagikan *password* tanpa mengubah teknik otentikasi dari *password*. Perangkat lunak yang akan dibuat akan mengimplementasikan metode *secret sharing* Shamir dan *secret sharing* Blakley.

   Berikut adalah hasil perhitungan manual dari metode *secret sharing* Shamir dan metode *secret sharing* Blakley :

   - Metode Secret Sharing Shamir
     Perhitungan manual untuk metode *secret sharing* Shamir ini menggunakan skema (3,5) di mana terdapat 5 buah partisipan dan untuk membangun kembali pesan rahasia, dikumpulkan minimal 3 buah *share*. Pada contoh perhitungan manual ini, input *password*-nya adalah : "A". Dimisalkan

representasi numerik dari *password* "A" sesuai dengan format ASCII (*American Standard Code for Information Interchange*) adalah 17. Maka untuk contoh perhitungan ini diperoleh pesan rahasia $S = 17$ dan diberikan bilangan prima acak $p = 19$.

Pembentukan *share* untuk masing-masing partisipan menggunakan rumus 14 di bawah ini :

$$f(x) = \sum_{i=0}^{k} a_i \cdot x^i \tag{14}$$

Pembentukan *share* untuk masing-masing partisipan :

$$\begin{aligned}
f(1) &= 17 + (1.1) + (2.1^2) = 17 + 1 + 2 = 20 \\
f(2) &= 17 + (1.2) + (2.2^2) = 17 + 2 + 8 = 27 \\
f(3) &= 17 + (1.3) + (2.3^2) = 17 + 3 + 18 = 38 \\
f(4) &= 17 + (1.4) + (2.4^2) = 17 + 4 + 32 = 53 \\
f(5) &= 17 + (1.5) + (2.5^2) = 17 + 5 + 50 = 72
\end{aligned}$$

Sehingga masing-masing partisipan memperoleh *share* seperti berikut :

$$\begin{aligned}
S_i &= (i, f(i) \ mod \ p) \\
S_1 &= (1, 20 \ mod \ 19) = (1, 1) \\
S_2 &= (2, 27 \ mod \ 19) = (2, 8) \\
S_3 &= (3, 38 \ mod \ 19) = (3, 0) \\
S_4 &= (4, 53 \ mod \ 19) = (4, 5) \\
S_5 &= (5, 72 \ mod \ 19) = (5, 15)
\end{aligned}$$

Rekonstruksi pesan rahasia S menggunakan interpolasi Lagrange seperti pada rumus 15 di bawah ini :

$$f(x) = \sum_{i=1}^{k} y_i \left(\prod_{j=1, j \neq i}^{k} \frac{x_j}{x_j - x_i} \right) \ mod \ p \tag{15}$$

Share yang dikumpulkan adalah : $S_1,\ S_3$, dan S_5.
Sehingga perhitungan fungsi $f(0)$ yang mengandung pesan rahasia S adalah seperti berikut :

$$\begin{aligned}
f(0) &= \left(y_1 \left(\tfrac{x_3}{x_3 - x_1} \cdot \tfrac{x_5}{x_5 - x_1} \right) + y_3 \left(\tfrac{x_1}{x_1 - x_3} \cdot \tfrac{x_5}{x_5 - x_3} \right) + y_5 \left(\tfrac{x_3}{x_3 - x_5} \cdot \tfrac{x_1}{x_1 - x_5} \right) \right) \ mod \ p \\
&= \left(1 \left(\tfrac{3}{3-1} \cdot \tfrac{5}{5-1} \right) + 0 \left(\tfrac{1}{1-3} \cdot \tfrac{5}{5-3} \right) + 15 \left(\tfrac{3}{3-5} \cdot \tfrac{1}{1-5} \right) \right) \ mod \ 19 \\
&= \left(1\tfrac{15}{8} + 0\tfrac{5}{-4} + 15\tfrac{3}{8} \right) \ mod \ 19 \\
&= \tfrac{60}{8} \ mod \ 19 \\
&= 60 \ . \ 8^{-1} \ mod \ 19 \\
&= \left((60 \ . \ mod \ 19) \ . \ \left(8^{-1} \ mod \ 19 \right) \right) \ mod \ 19 \\
&= 3 \ . \ 12 \ mod \ 19 \\
&= 36 \ mod \ 19 \\
&= 17
\end{aligned}$$

Pesan rahasia S yang telah diperoleh kembali tersebut kemudian diubah ke bentuk awal sesuai dengan format ASCII. Sehingga bila pesan rahasia 17 diubah kembali ke bentuk alfabet, *password* yang diperoleh adalah "A".

- Metode Secret Sharing Blakley

  Perhitungan manual untuk metode *secret sharing* Blakley ini menggunakan skema (3,5) di mana terdapat 5 buah partisipan dan untuk membangun kembali pesan rahasia, perlu dikumpulkan 3 buah *share*. Pesan rahasia terletak di bidang 3 dimensi yang dipetakan dalam fungsi $Q(x, y, z)$. Pada contoh perhitungan manual metode *secret sharing* Blakley ini, diberikan input *password* berupa : "tif". Dimisalkan representasi numerik untuk setiap karakter dari *password* "tif" sesuai dengan format ASCII (*American Standard Code for Information Interchange*) adalah 21, 37, dan 45. Maka untuk contoh perhitungan manual *secret sharing* Blakley ini diperoleh pesan rahasia $x = 21,\ y = 37,\ z = 45$, dan bilangan prima acak $p = 51$.

  Masing-masing partisipan i akan memperoleh nilai z yang merepresentasikan bidang 2 dimensi, dinyatakan secara matematis pada persamaan 16 di bawah ini :

$$z \equiv a_i x + b_i y + c_i \tag{16}$$

  di mana nilai a dan b untuk masing-masing partisipan ditentukan secara acak, dan nilai c untuk masing-masing partisipan diperoleh dengan menggunakan persamaan 17 berikut ini :

$$c_i \equiv (z_i - a_i x - b_i y)\ mod\ p \tag{17}$$

  Pembentukan *share* untuk masing-masing partisipan :
  Secret Share 1 :
  $a_1 = 1$
  $b_1 = 2$
  $c_1 = (z - a_1 x - b_1 y)\ mod\ p = (45 - 21 - 74)\ mod\ 51 = -50\ mod\ 51 = 1$

  Secret Share 2 :
  $a_2 = 2$
  $b_2 = 3$
  $c_2 = (z - a_2 x - b_2 y)\ mod\ p = (45 - 42 - 111)\ mod\ 51 = -108\ mod\ 51 = 45$

  Secret Share 3 :
  $a_3 = 5$
  $b_3 = 7$
  $c_3 = (z - a_3 x - b_3 y)\ mod\ p = (45 - 105 - 209)\ mod\ 51 = -319\ mod\ 51 = 38$

  Secret Share 4 :
  $a_4 = 1$
  $b_4 = 3$
  $c_4 = (z - a_4 x - b_4 y)\ mod\ p = (45 - 21 - 111)\ mod\ 51 = -87\ mod\ 51 = 15$

Secret Share 5 :

$a_5 = 2$

$b_5 = 7$

$c_5 = (z - a_5x - b_5y) \ mod \ p = (45 - 42 - 209) \ mod \ 51 = -206 \ mod \ 51 = 49$

Sehingga untuk masing-masing partisipan diperoleh *share* seperti berikut :

$$S_i : z = a_ix + b_iy + c_i$$
$$S_1 : z = x + 2y + 1$$
$$S_2 : z = 2x + 3y + 45$$
$$S_3 : z = 5x + 7y + 38$$
$$S_4 : z = x + 3y + 15$$
$$S_5 : z = 2x + 7y + 49$$

Pesan rahasia direkonstruksi dengan menggunakan persamaan 18 :

$$a_ix + b_iy - z \equiv -c_i \ (mod \ p) \tag{18}$$

Sehingga menghasilkan persamaan matriks di bawah ini :

$$\begin{pmatrix} a_1 & b_1 & -1 \\ a_2 & b_2 & -1 \\ a_3 & b_3 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -c_1 \\ -c_2 \\ -c_3 \end{pmatrix} \ mod \ p \tag{19}$$

Share yang dikumpulkan adalah : $S_1, \ S_2$, dan S_3

Sehingga matriks yang diperoleh adalah :

$$\begin{pmatrix} 1 & 2 & -1 \\ 2 & 3 & -1 \\ 5 & 7 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -1 \\ -45 \\ -38 \end{pmatrix} \ mod \ p$$

Dilakukan operasi baris elementer untuk memperoleh nilai $x, \ y$, dan z :

Operasi 1 :

$$R2 + (-2R1) \rightarrow R2 \quad \left(\begin{array}{ccc|c} 1 & 2 & -1 & -1 \\ 0 & -1 & 1 & -43 \\ 5 & 7 & -1 & -38 \end{array}\right)$$

Operasi 2 :

$$R3 + (-5R1) \rightarrow R3 \quad \left(\begin{array}{ccc|c} 1 & 2 & -1 & -1 \\ 0 & -1 & 1 & -43 \\ 0 & -3 & 4 & -33 \end{array}\right)$$

Operasi 3 :

$$-1R2 \rightarrow R2 \quad \left(\begin{array}{ccc|c} 1 & 2 & -1 & -1 \\ 0 & 1 & -1 & 43 \\ 0 & -3 & 4 & -33 \end{array}\right)$$

Operasi 4 :

$$R3 + 3R2 \rightarrow R3 \quad \left(\begin{array}{ccc|c} 1 & 2 & -1 & -1 \\ 0 & 1 & -1 & 43 \\ 0 & 0 & 1 & 96 \end{array}\right)$$

Dari operasi yang sudah dilakukan diperoleh persamaan berikut :

$$x + 2y - z = -1$$
$$0 + y - z = 43$$
$$0 + 0 + z = 96$$

Maka nilai x, y, dan z adalah :
$z = 96$
$y = 43 + z = 43 + 96 = 139$
$x = -1 - 2y + z = -1 - (2.139) + 96 = -1 - 278 + 96 = -183$

Rekonstruksi pesan rahasia :

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -183 \\ 139 \\ 96 \end{pmatrix} \bmod 51 = \begin{pmatrix} 21 \\ 37 \\ 45 \end{pmatrix}$$

Pesan rahasia x, y, dan z yang telah diperoleh kemudian diubah kembali ke bentuk awal sesuai dengan tabel ASCII. Sehingga bila angka 21, 37, dan 45 diubah kembali ke bentuk alfabet, diperoleh kembali *password* : "tif".

4. **Melakukan analisis kebutuhan dan perancangan perangkat lunak.**
   Status : Ada sejak rencana kerja skripsi.
   Hasil : Pada skripsi 1, yang dikerjakan pada bagian ini adalah alur penyelesaian masalah yang diilustrasikan menggunakan *flowchart* dan perancangan diagram kelas awal.

   - Flowchart Proses Penyelesaian Masalah

     Berikut adalah ilustrasi langkah-langkah penyelesaian masalah penggunaan metode *secret sharing* untuk berbagi *password* disertai penjelasan untuk setiap langkahnya.

Gambar 3: *Flowchart* proses penyelesaian masalah untuk perangkat lunak yang akan dibuat

Deskripsi langkah-langkah :

(a) Memasukkan input berupa *password*
Pada tahap ini pengguna dapat memasukkan input *password*. *Password* yang diinginkan oleh pengguna dapat berupa kombinasi *string* (deretan alfabet), deretan angka, dan simbol-simbol.

(b) Memilih metode *secret sharing*
Pada tahap ini pengguna dapat memilih metode *secret sharing* yang ingin digunakan. Perangkat lunak yang dibuat menyediakan dua buah metode *secret sharing* yang dapat digunakan untuk mengimplementasikan penggunaan *secret sharing* untuk berbagi *password*. Metode-metode tersebut adalah metode *secret sharing* Shamir dan metode *secret sharing* Blakley.

(c) Menentukan banyak *threshold* dan partisipan
Pada tahap ini pengguna dapat memilih banyak *threshold* dan partisipan yang diinginkan.

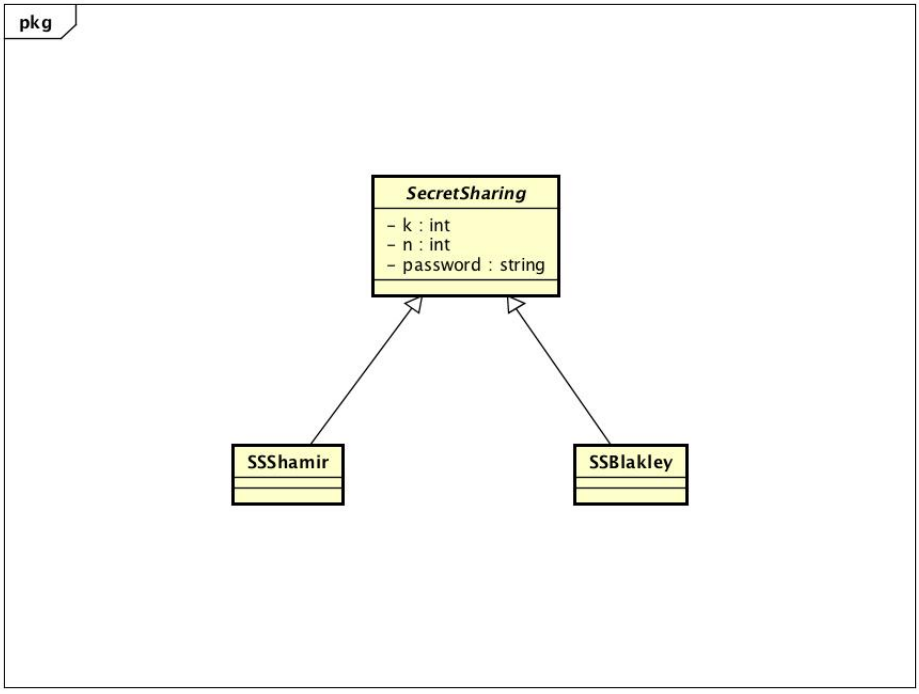
Untuk metode *secret sharing* Blakley, perangkat lunak yang dibuat hanya dapat mengimplementasikan metode *secret sharing* Blakley dengan skema $(3, n)$, yang artinya banyak *threshold* yang dapat digunakan pada metode ini adalah 3.

(d) Mengubah *password* ke format ASCII
Pada tahap ini perangkat lunak akan mengubah format *password* yang sebelumnya berupa kombinasi deretan alfabet, deretan angka, dan simbol, menjadi format ASCII (*American Standard Code for Information Interchange*) yang merupakan representasi numerik dari karakter alfabetis dan simbol.

(e) Mendistribusikan *password* ke n buah partisipan
Pada tahap ini perangkat lunak akan mendistribusikan *password* ke n buah partisipan menggunakan metode *secret sharing* Shamir atau metode *secret sharing* Blakley.

(f) Merekonstruksi *password*
Pada tahap ini perangkat lunak akan membangun kembali *password* dengan algoritma yang digunakan pada metode *secret sharing* Shamir dan metode *secret sharing* Blakley. *Password* yang sudah direkonstruksi akan ditampilkan oleh perangkat lunak sebagai keluaran/*output*.

- Diagram Kelas Awal
  Pada Gambar 4 dilampirkan rancangan diagram kelas awal dari perangkat lunak yang akan dibuat.



Gambar 4: Diagram kelas awal

Deskripsi kelas :

(a) Kelas SecretSharing
Kelas SecretSharing adalah kelas utama perangkat lunak yang bertipe abstrak dan menjadi kelas *parent* dari kelas SSShamir dan kelas SSBlakley. Kelas SecretSharing memiliki tiga buah atribut yaitu :

- Atribut k : Atribut k merepresentasikan banyaknya *share* yang dibutuhkan untuk merekonstruksi *password*.
- Atribut n : Atribut n merepresentasikan banyak partisipan.
- Atribut password : Atribut password merepresentasikan *password*/pesan rahasia.

(b) Kelas SSShamir
Kelas SSShamir adalah turunan dari kelas SecretSharing yang akan membagi *password* menjadi n banyak bagian dan merekonstruksi *password* menggunakan metode *secret sharing* Shamir.

(c) Kelas SSBlakley
Kelas SSBlakley adalah turunan dari kelas SecretSharing yang akan membagi *password* menjadi n banyak bagian dan merekonstruksi *password* menggunakan metode *secret sharing* Blakley.

5. **Mengimplementasikan penggunaan skema *secret sharing* untuk pembagian *password*.**
   Status : Ada sejak rencana kerja skripsi.
   Hasil :

6. **Melakukan pengujian metode-metode *secret sharing* yang telah diimplementasikan.**
   Status : Ada sejak rencana kerja skripsi.
   Hasil :

7. **Melakukan analisis hasil pengujian.**
   Status : Ada sejak rencana kerja skripsi.
   Hasil :

8. **Menulis dokumen skripsi.**
   Status : Ada sejak rencana kerja skripsi.
   Hasil :

3 Pencapaian Rencana Kerja

Persentase penyelesaian skripsi sampai dengan dokumen ini dibuat dapat dilihat pada tabel berikut :

1*	2*(%)	3*(%)	4*(%)	5*	6*(%)
1	5	5			5
2	20	20			20
3	5	5			5
4	10	5	5	*Flowchart* penyelesaian masalah dan diagram kelas awal dikerjakan di S1	5
5	20		20		
6	10		10		
7	10		10		
8	20	5	15	Pendahuluan, dasar teori, dan sebagian analisis dikerjakan di S1	5
Total	100	40	60		40

Keterangan (*)
1 : Bagian pengerjaan Skripsi (nomor disesuaikan dengan detail pengerjaan di bagian 5)

2 : Persentase total
3 : Persentase yang akan diselesaikan di Skripsi 1
4 : Persentase yang akan diselesaikan di Skripsi 2
5 : Penjelasan singkat apa yang dilakukan di S1 (Skripsi 1) atau S2 (skripsi 2)
6 : Persentase yang sudah diselesaikan sampai saat ini

Bandung, 08/05/2017

Abraham Sri Paskah Ageng Wahono

Menyetujui,

Nama: Mariskha Tri Adithia
Pembimbing Tunggal