Skema Pembagian Data Rahasia Berbasis Kunci Multilevel

Ahmad Hasan Albana[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]*ahmadalbana98@gmail.com,* [1]*13522041@std.stei.itb.ac.id*

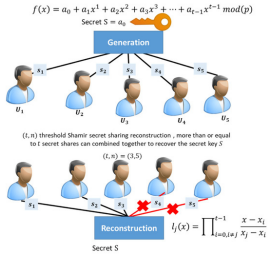
***Abstract*—Skema Shamir merupakan salah satu skema pembagian data rahasia yang memanfaatkan persoalan interpolasi polinom untuk memecah suatu data rahasia menjadi beberapa kunci yang memiliki level yang sama yang dibutuhkan untuk merekonstruksi data rahasia. Level pada kunci dapat didasarkan keharusannya untuk ada dalam rekonstruksi data rahasia sehingga data tak dapat direkonstruksi tanpa adanya kunci dengan level tertinggi. Makalah ini membahas variasi skema Shamir dengan pembangkitan kunci multilevel.**

***Index Terms*—Interpolasi Polinom, Kunci Multilevel, Pembagian Data Rahasia, Skema Shamir**

I. Pendahuluan

Skema Pembagian Data Rahasia adalah suatu protokol pemrosesan data rahasia dengan memecah data rahasia tersebut menjadi beberapa kunci berbeda untuk dibagikan kepada himpunan orang sehingga akan terdapat *subset* dari himpunan tersebut yang dapat merekonstruksi data rahasia dengan kunci yang mereka punya[1]. Skema ini sering digunakan dalam protokol kriptografi untuk menangani kasus pembagian data yang memerlukan minimal persetujuan orang, seperti misalnya mekanisme voting yang memerlukan mayoritas persetujuan kelompok.

Salah satu skema pembagian data rahasia adalah Skema Ambang Shamir. Skema ini menggunakan parameter t dan n sehingga data rahasia dibagi menjadi n buah kunci dan hanya memerlukan sembarang t buah kunci diantara n kunci untuk merekonstruksi data tersebut. Skema ini tentu saja telah memenuhi definisi dasar dari skema pembagian data rahasia. Namun, skema ini masih belum bisa menyelesaikan masalah yang memiliki tingkat otoritas dalam rekonstruksi data.



Source: https://www.mdpi.com/1424-8220/22/1/331

Fig. 1. Skema Ambang Shamir

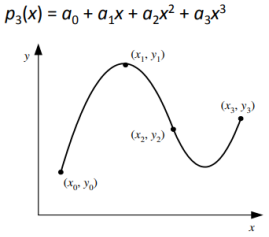
Dalam suatu perkumpulan, terkadang dibutuhkan setidaknya beberapa orang yang memiliki otoritas lebih tinggi untuk memverifikasi dan bertanggung jawab terhadap suatu proses pengambilan keputusan, atau dalam hal ini adalah proses rekonstruksi data rahasia. Oleh karena itu, diperlukan skema yang memungkinkan adanya kunci multilevel yang memerlukan minimal sejumlah kunci dengan otoritas tinggi untuk merekonstruksi data rahasia.

Makalah ini membahas tentang pengembangan skema pembagian data rahasia yang mampu menghasilkan kunci multilevel yang juga memanfaatkan persoalan interpolasi polinom dalam proses pembangkitan kunci.

II. Landasan Teori

A. Interpolasi Polinom

Persoalan interpolasi polinom adalah persoalan untuk mencari persamaan polinomial berderajat n yang menginterpolasi (melewati) $n+1$ buah titik (x,y) berbeda[2]. Interpolasi polinom pada dasarnya digunakan untuk melakukan pendekatan suatu fungsi polinom menggunakan polinom dengan derajat yang lebih kecil, namun tak membatasi untuk melakukan pembentukan polinom dengan derajat sebenarnya.



Source: [2]

Fig. 2. Interpolasi Polinom Kubik

Untuk menyelesaikan persoalan interpolasi polinom, dapat dilakukan dengan berbagai metode perdekatan, seperti metode Interpolasi Lagrange dan metode Eliminasi Gauss-Jordan untuk menyelesaikan persoalan interpolasi polinom yang telah direkonstruksi menjadi persoalan Sistem Persamaan Linear[3]. Namun, metode Interpolasi Lagrange kurang disukai akibat komputasi yang berat untuk melakukan interpolasi[2]. Sedangkan metode Eliminasi Gauss-Jordan memungkinkan fleksibilitas untuk nilai-nilai dari variabel pada polinom.

B. Eliminasi Gauss-Jordan

Eliminasi Gauss-Jordan merupakan salah satu metode untuk menyelesaikan permasalahan Sistem Persamaan Linear (SPL) berbasis operasi matriks[4]. Persoalan SPL terlebih dahulu diubah menjadi matriks *augmented* yang menggabungkan matriks koefisien dan matriks konstanta dari persamaan.

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{bmatrix} \sim \text{OBE} \sim \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & * \\ 0 & 1 & 0 & \dots & 0 & * \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \vdots & 1 & * \end{bmatrix}$$

Source: [4]

Fig. 3. Matriks Augmented menjadi Matriks Eselon Baris Tereduksi

Metode Eliminasi Gauss-Jordan dilakukan dengan cara mengubah matriks *augmented* menjadi matriks eselon baris tereduksi hanya dengan menerapkan operasi baris elementer (OBE) terhadap matriks. Adapun solusi dari SPL didapat dengan melihat nilai pada kolom matriks paling kanan.

Adapun proses penerapan OBE hingga membentuk matriks eselon bertujuan untuk melakukan reduksi variabel yang dimiliki oleh semua persamaan yang ada. Jika dimiliki dua persamaan linear PL_1 dengan himpunan variabelnya *A* dan PL_2 dengan himpunan variabelnya *B*. Maka dapat dihasilkan suatu persamaan linear baru menggunakan metode eliminasi dengan himpunan variabelnya *N*, dimana $N = (A \cup B) - \{e\}$ dengan $e \in (A \cap B)$. Sifat tersebut dapat diturunkan lebih lanjut sehingga dapat membuktikan bahwa dengan *n+1* buah persamaan linear dengan himpunan variabel yang sama, dapat dibentuk persamaan linear satu variabel untuk semua variabel atau dalam konteks polinomial dapat diketahui nilai untuk seluruh koefisien dan konstanta dari polinomial tersebut.

C. Skema Ambang Shamir

Skema Ambang Shamir (*t, n*) adalah metode kriptografi untuk membagi sebuah data rahasia (S) menjadi beberapa bagian kunci yang dibagikan kepada sejumlah *n* partisipan sedemikian sehingga sembarang himpunan bagian yang terdiri dari *t* partisipan atau lebih dapat merekonstruksi S, tetapi jika kurang dari *t* maka S tidak dapat direkonstruksi[3]. Skema Ambang Shamir didasarkan pada persoalan Interpolasi Polinomial yang menyatakan bahwa untuk merekonstruksi suatu polinomial berderajat *n*, diperlukan minimal *n+1* buah titik koordinat yang unik.

Skema Ambang Shamir diawali dengan pemilihan suatu angka prima yang lebih dari angka rahasia (S) dan banyak partisipan (*n*) yang digunakan sebagai modulus untuk membatasi operasi dalam bidang terbatas dan memastikan adanya invers untuk sembarang bilangan tidak nol. Untuk skema (*t, n*), akan dibuat suatu persamaan polinom acak berderajat *t-1* dengan S sebagai konstanta. Lalu, akan dibangkitkan *n* buah kunci yang berupa suatu titik unik pada polinom.

Proses rekonstruksi angka rahasia dilakukan dengan cara mensubstitusikan titik (kunci) pada persamaan polinom berderajat *t* dengan koefisien yang belum diketahui seperti berikut.

$$f(x) \equiv S + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \pmod{p} \quad (1)$$

Lalu akan dicari nilai dari koefisien polinom dengan menggunakan penyelesaian Sistem Persamaan Linear. Adapun angka rahasia merupakan nilai konstanta pada persamaan polinom yang telah direkonstruksi.

III. METODOLOGI

A. Model Sistem

Pada Skema Ambang Shamir, digunakan dua buah variabel publik *n* yang merepresentasikan banyaknya kunci yang dihasilkan dan variabel *t* yang merepresentasikan banyaknya kunci minimal yang dibutuhkan untuk merekonstruksi data rahasia. Akibat terdapat berbagai jenis level kunci, maka skema butuh untuk mendefinisikan jumlah minimal dari setiap kunci pada masing-masing level. Adapun level terbesar merupakan level dengan otoritas tertinggi.

Variabel yang perlu ditambahkan pada skema dengan kunci multilevel adalah banyaknya level kunci yang ada, direpresentasikan oleh huruf *l*. Diperlukan juga informasi mengenai jumlah minimum kunci yang diperlukan untuk setiap level yang dapat direpresentasikan oleh larik S_l sepanjang l ($[t_1, t_2, ..., t_l]$), dengan t_n merupakan jumlah minimum kunci yang diperlukan pada level_*n* dan $\sum_{i=1}^{l} t_i = t$. Selain itu, diperlukan juga informasi mengenai banyaknya kunci yang perlu dihasilkan pada setiap level, direpresentasikan oleh larik N_l sepanjang l ($[n_1, n_2, ..., n_l]$), dengan n_x merupakan banyaknya kunci yang perlu dihasilkan pada level_*x* dan $\sum_{i=1}^{l} n_i = n$.

Adapun suatu kunci dengan level tertentu juga dapat dianggap sebagai representasi kunci dengan level dibawahnya, namun tidak sebaliknya. Sebagai contoh untuk larik S_l [2, 2], dapat digunakan 1 buah kunci level_1 dan 3 buah kunci level_2 karena salah satu kunci level_2 dapat dianggap sebagai kunci level_1 sehingga tetap memenuhi jumlah minimum pada setiap level kunci. Namun, 3 buah kunci level_1 dan 1 buah kunci level_2 tidak dapat digunakan untuk merekonstruksi data rahasia dikarenakan kurangnya satu buah kunci level_2.

B. Pembangkitan Kunci

Skema Ambang Shamir memanfaatkan permasalahan interpolasi polinom yang memerlukan *n+1* buah titik sebagai kunci untuk merekonstruksi suatu polinom berderajat *n* yang digunakan untuk menyimpan data rahasia sebagai konstantanya. Namun, untuk membangkitkan kunci multilevel diperlukan suatu penyesuaian mekanisme pembangkitan kunci sedemikian sehingga kunci yang dihasilkan mampu memiliki tingkat yang berbeda.

1) Pembatasan Otoritas Kunci: Untuk membatasi otoritas suatu kunci dalam rekonstruksi polinom, dapat dilakukan penghilangan beberapa suku polinom untuk mereduksi jumlah variabel pada SPL sehingga akan terdapat suatu konstanta suku yang tidak dapat diketahui pada polinom utuh sebelumnya. Dikarenakan data rahasia disimpan sebagai konstanta, maka dilakukan generalisasi untuk urutan penghilangan suku dimulai dari suku dengan pangkat terendah (konstanta, koefisien x, koefisien x^2, dan seterusnya).

2) Penetapan Minimum Kunci: Adapun jumlah kunci minimum yang diperlukan untuk suatu level ditentukan berdasarkan perbedaan banyaknya suku pada polinom yang dipakai level tersebut dengan banyaknya suku pada polinom yang dipakai pada level dibawahnya. Hal ini dapat dibuktikan dengan memandang polinom yang telah digunakan pada level yang lebih rendah dijamin mampu untuk mendapatkan seluruh nilai koefisien sukunya, sehingga untuk polinom pada level yang lebih tinggi hanya perlu untuk mencari koefisien suku dan konstanta yang belum pernah muncul sebelumnya sebanyak *a+1*. Hal ini memungkinkan untuk memandang polinom pada level yang lebih tinggi untuk dianggap sebagai polinom berderajat *a* yang hanya memerlukan sebanyak *a* buah polinom untuk mendapatkan nilai koefisien dari suku yang belum diketahui.

3) Identifikasi Level Kunci: Untuk penerapan skema pada suatu sistem, diperlukan suatu aturan bagi sistem agar dapat mengetahui level dari suatu kunci yang ada sehingga sistem mampu menerapkan penanganan yang berbeda untuk level kunci yang berbeda. Kunci merupakan suatu titik yang terdiri dari nilai *x* dan *y* yang jika ditinjau akan lebih mudah untuk mengatur nilai *x* sebagai input sehingga akan dipilih sebagai patokan untuk mengetahui level kunci. Adapun mekanisme ekstraksi level kunci dari nilai *x* dapat dilakukan dengan modulus terhadap *l* dengan *l* merupakan banyaknya tingkatan level kunci.

C. Rekonstruksi Data Rahasia

Berdasarkan mekanisme pembangkitan kunci yang telah ditetapkan, dapat dilakukan rekonstruksi data rahasia untuk suatu skema multilevel $(n, t, l, [t_1, t_2, ..., t_l])$ dan beberapa kunci $k_i(x_i, y_i)$. Diawali dengan penentuan level kunci dengan rumus berikut.

$$l_i = (x_i \bmod l) + 1 \tag{2}$$

Level kunci akan digunakan untuk menentukan polinom yang digunakan dalam pembuatan kunci sebelumnya sebagai berikut.

$$0 = \sum_{i=t-1}^{q} a_i x^i, q = \sum_{i=l_i+1}^{l} t_i \tag{3}$$

Untuk setiap polinom yang didapatkan dari setiap kunci, dilakukan substitusi kunci (titik) pada polinom yang telah ditentukan sehingga akan menghasilkan suatu Sistem Persamaan Linear. Sistem Persamaan Linear akan kemudian diselesaikan menggunakan metode eliminasi Gauss-Jordan. Dari solusi Sistem Persamaan Linear tersebut, nilai variabel a_0 merupakan data rahasia yang berhasil direkonstruksi.

IV. Hasil dan Pembahasan

A. Hasil

Pengujian dilakukan dengan mengimplementasikan algoritma menggunakan bahasa pemrograman Python. Berikut adalah hasil simulasi untuk tiga skenario berbeda.

1) Skema 1-Level (Standard Shamir): Pada skema ini, semua kunci memiliki otoritas yang sama.

- Konfigurasi:
  - n: 8 (banyak kunci)
  - t: 3 (kunci minimum untuk rekonstruksi)
  - l: 1 (jumlah level)
  - S_l: [3] (syarat minimum kunci per level)
  - N_l: [8] (jumlah kunci per level)
  - p: 31337 (modulus)
- Data Rahasia (S): 1763
- Polinom: $f(x) = 29285x^2 + 14175x + 1763 \pmod{31337}$
- Kunci yang dihasilkan:
  - k_1(1, 13886)
  - k_2(2, 21905)
  - k_3(3, 25820)
  - k_4(4, 25631)
  - k_5(5, 21338)
  - k_6(6, 12941)
  - k_7(7, 440)
  - k_8(8, 15172)

Rekonstruksi menggunakan 4 kunci (k_1, k_2, k_7, dan k_8) menghasilkan matriks *augmented* dan RREF sebagai berikut:

$$\begin{bmatrix} 1 & 1 & 1 & | & 13886 \\ 4 & 2 & 1 & | & 21905 \\ 49 & 7 & 1 & | & 440 \\ 64 & 8 & 1 & | & 15172 \end{bmatrix} \xrightarrow{OBE} \begin{bmatrix} 1 & 0 & 0 & | & 29285 \\ 0 & 1 & 0 & | & 14175 \\ 0 & 0 & 1 & | & 1763 \\ 0 & 0 & 0 & | & 0 \end{bmatrix}$$

Nilai $S = 1763$ berhasil didapatkan.

Adapun jika hanya menggunakan 2 kunci (k_1 dan k_2), maka akan diperoleh matriks *augmented* dan RREF sebagai berikut:

$$\begin{bmatrix} 1 & 1 & 1| & 13886 \\ 64 & 8 & 1| & 15172 \end{bmatrix} \xrightarrow{OBE} \begin{bmatrix} 1 & 0 & 3917| & 9479 \\ 0 & 1 & 27421| & 4407 \end{bmatrix}$$

Nilai S tidak dapat ditemukan karena masih terdapat variabel yang belum tereliminasi.

2) Skema 2-Level: Pada skema ini, kunci Level 2 memiliki otoritas lebih tinggi daripada Level 1.

- Konfigurasi: $(n = 7, t = 5, l = 2, S_l = [3, 2], N_l = [4, 3], p = 31337)$
- Data Rahasia (S): 1763
- Polinom: $f(x) = 21739x^4 + 5586x^3 + 28197x^2 + 29042x + 1763 \pmod{31337}$
- Kunci:
  - k_1(2, 1081) (Level 2)
  - k_2(4, 5012) (Level 2)
  - k_3(6, 17852) (Level 2)
  - k_4(1, 24185) (Level 1)
  - k_5(3, 3201) (Level 1)
  - k_6(5, 10964) (Level 1)
  - k_7(7, 26500) (Level 1)

Jika digunakan 2 kunci Level 2 (k_1, k_3) dan 3 kunci Level 1 (k_4, k_5, k_6), maka SPL yang terbentuk sesuai Persamaan (3) adalah:

$$\left[\begin{array}{ccccc|c} 16 & 8 & 4 & 2 & 1 & 1081 \\ 1296 & 216 & 36 & 6 & 1 & 17852 \\ 1 & 1 & 1 & 0 & 0 & 24185 \\ 81 & 27 & 9 & 0 & 0 & 3201 \\ 625 & 125 & 25 & 0 & 0 & 10964 \end{array}\right]$$

$$\downarrow \text{OBE}$$

$$\left[\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 0 & 21739 \\ 0 & 1 & 0 & 0 & 0 & 5586 \\ 0 & 0 & 1 & 0 & 0 & 28197 \\ 0 & 0 & 0 & 1 & 0 & 29042 \\ 0 & 0 & 0 & 0 & 1 & 1763 \end{array}\right]$$

Nilai $S = 1763$ berhasil didapatkan.

Namun jika hanya digunakan 2 kunci Level 1 (k_4, k_5) dan 2 kunci Level 2 (k_1, k_2), maka SPL yang terbentuk adalah:

$$\left[\begin{array}{ccccc|c} 16 & 8 & 4 & 2 & 1 & 1081 \\ 256 & 64 & 16 & 4 & 1 & 5012 \\ 1 & 1 & 1 & 0 & 0 & 24185 \\ 81 & 27 & 9 & 0 & 0 & 3201 \end{array}\right]$$

$$\downarrow \text{OBE}$$

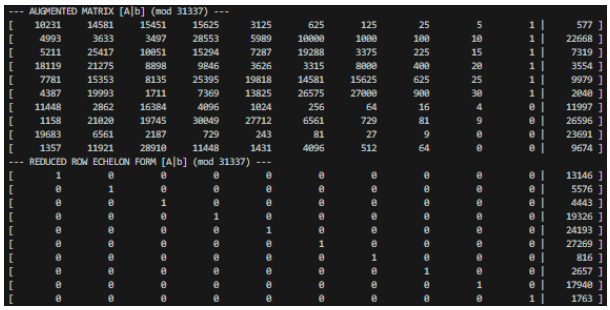
$$\left[\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 9513 & 27863 \\ 0 & 1 & 0 & 0 & 24622 & 12427 \\ 0 & 0 & 1 & 0 & 28539 & 15232 \\ 0 & 0 & 0 & 1 & 3358 & 26503 \end{array}\right]$$

Nilai S tidak dapat ditemukan karena masih terdapat variabel yang belum tereliminasi.

3) Skema Multi-Level: Skenario dengan 3 tingkatan level kunci.

- Konfigurasi: $(n = 17, t = 10, l = 5, S_l = [4, 1, 3, 1, 1], N_l = [5, 1, 3, 2, 6], p = 31337)$
- Data Rahasia (S): 1763
- Polinom: $f(x) = 13146x^9 + 5576x^8 + 4443x^7 + 19326x^6 + 24193x^5 + 27269x^4 + 816x^3 + 2657x^2 + 17940x + 1763 \pmod{31337}$
- Kunci:
  - k_1(5, 577) (Level 5)
  - k_2(10, 22668) (Level 5)
  - k_3(15, 7319) (Level 5)
  - k_4(20, 3554) (Level 5)
  - k_5(25, 9979) (Level 5)
  - k_6(30, 2040) (Level 5)
  - k_7(4, 11997) (Level 4)
  - k_8(9, 26596) (Level 4)
  - k_9(3, 23691) (Level 3)
  - k_{10}(8, 9674) (Level 3)
  - k_{11}(13, 15860) (Level 3)
  - k_{12}(2, 20698) (Level 2)
  - k_{13}(1, 11154) (Level 1)
  - k_{14}(6, 4405) (Level 1)
  - k_{15}(11, 14536) (Level 1)
  - k_{16}(16, 3500) (Level 1)
  - k_{17}(21, 10170) (Level 1)

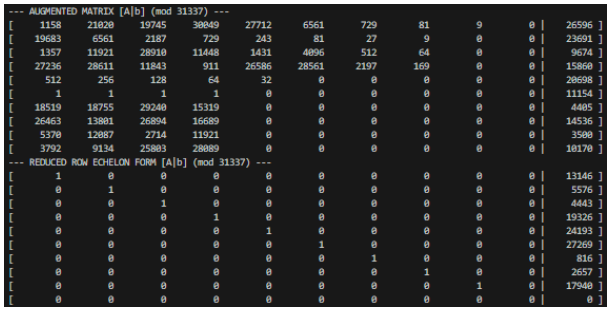
Rekonstruksi menggunakan 6 kunci Level 5, 2 kunci Level 4, 2 kunci Level 3 akan didapatkan hasil koefisien persamaan sebagai berikut:



Source: Hasil Simulasi

Fig. 4. Rekonstruksi Kunci Berhasil pada Skema Multi-Level

Namun jika hanya digunakan 1 kunci Level 4, 3 kunci Level 3, 1 kunci Level 2, dan 5 kunci Level 1 maka matriks *augmented* dan RREF yang diperoleh adalah sebagai berikut:



Source: Hasil Simulasi

Fig. 5. Rekonstruksi Kunci Gagal pada Skema Multi-Level

Nilai S tidak dapat ditemukan karena masih terdapat variabel yang belum tereliminasi.

B. Pembahasan

Berdasarkan hasil pengujian, penggunaan $x \bmod l$ sebagai penentu level kunci terbukti efektif untuk membedakan otoritas tanpa perlu menyimpan metadata tambahan pada kunci. Skema Multilevel ini juga terbukti mampu meng-*cover* permasalahan yang ada pada Skema Shamir.

Pada Skema 2-Level, terlihat bahwa kunci yang digunakan untuk rekonstruksi kurang dari syarat minimum pada setiap level dapat menyebabkan kegagalan dalam mendapatkan data rahasia. Hal ini menegaskan pentingnya pemenuhan syarat minimum kunci pada setiap level untuk menjamin keberhasilan rekonstruksi.

Pada Skema Multi-Level, terlihat bahwa kunci dengan otoritas lebih tinggi mampu untuk menggantikan peran dari kunci dengan otoritas lebih rendah dalam memenuhi syarat minimum kunci. Hal ini menunjukkan fleksibilitas yang ditawarkan oleh

skema multilevel dalam hal pemilihan kunci untuk rekonstruksi data rahasia. Namun sebaliknya, kunci dengan otoritas lebih rendah tidak dapat menggantikan peran kunci dengan otoritas lebih tinggi, yang menegaskan hierarki otoritas dalam skema ini.

V. Kesimpulan

Pengembangan skema pembagian data rahasia dengan kunci multilevel dapat dilakukan dengan memodifikasi jumlah suku polinom yang dapat diakses oleh setiap level kunci. Dengan memanfaatkan operasi modulo pada nilai x untuk identifikasi level dan metode eliminasi Gauss-Jordan untuk rekonstruksi, sistem mampu menjamin bahwa data rahasia hanya dapat dibuka jika jumlah minimum kunci pada setiap tingkatan otoritas terpenuhi. Skema ini memberikan fleksibilitas lebih baik dibandingkan Skema Shamir standar dalam organisasi yang memiliki struktur hierarki.

VI. Ucapan Terima Kasih

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa yang telah memberikan karunia, sehingga penulis dapat Makalah IF4020 Kriptografi – Sem. II Tahun 2025/2026 menyelesaikan makalah yang berjudul "Skema Pembagian Data Rahasia Berbasis Kunci Multilevel" yang dapat selesai tepat pada waktunya. Tak lupa juga penulis mengucapkan terima kasih kepada Bapak Dr. Ir. Rinaldi, M.T yang telah membimbing pada mata kuliah IF4020 Kriptografi. Terakhir, penulis mengucapkan terima kasih kepada orang tua, keluarga, dan seluruh pihak yang membantu penulis dalam menyelesaikan makalah ini.

References

[1] Amos Beimel, "Secret-Sharing Schemes for General Access Structures: An Introduction", https://eprint.iacr.org/2025/518.pdf, diakses 10 Desember 2025.

[2] Rinaldi Munir, "Interpolasi Polinom (Bagian 1)", https://informatika.stei.itb.ac.id/ rinaldi.munir/MetNum/2010-2011/Interpolasi%20Polinom.pdf, diakses 11 Desember 2025.

[3] Rinaldi Munir, "Skema Pembagian Data Rahasia (*Secret Sharing Scheme*)", https://informatika.stei.itb.ac.id/ rinaldi.munir/Kriptografi/2025-2026/37-Skema-Pembagian-Data-Rahasia-2025.pdf, diakses 11 Desember 2025.

[4] Rinaldi Munir, "Sistem Persamaan Linier (SPL) Pokok bahasan: Metode Eliminasi Gauss-Jordan", https://informatika.stei.itb.ac.id/ rinaldi.munir/AljabarGeometri/2023-2024/Algeo-05-Sistem-Persamaan-Linier-2-2023.pdf, diakses 11 Desember 2025.

Appendix

A. Repositori GitHub

Kode lengkap implementasi Skema Pembagian Data Rahasia dengan Kunci Multilevel tersedia di repositori GitHub:

GitHub Repository:
https://github.com/Bana-man/Multilevel-Keys-Scheme.git

Repository ini berisi:

- Implementasi lengkap algoritma dalam Python (`MultiLevelKeysScheme.py`)
- Modul Eliminasi Gauss-Jordan (`GaussJordanElimination.py`)
- Program utama untuk pembangkitan dan rekonstruksi kunci (`main.py`)
- Modul skema random (`random_schema.py`)
- Test case dan hasil pengujian (`testcase/`)
- Dokumentasi lengkap dalam README.md

B. Cara Menggunakan

Untuk menggunakan implementasi ini, clone repository dan jalankan:

```
git clone https://github.com/Bana-man/Multilevel-K
cd Multilevel-Keys-Scheme
python main.py
```

C. Video Penjelasan Kode Program

Berikut merupakan video penjelasan Implementasi Kode Program:

Youtube: https://youtube.com/playlist?list= PLZHjGSNAZck4eUdyjTo81FLDvgbS66_md&si= arukFjNyVxnMg6VH