Penerapan Algoritma "LaGrange Interpolating Polynomial" pada Secret Sharing

Lisa Chandra[1], Yohana Dewi Lulu W, S.Si, M.T. [2], Memen Akbar, S.Si[3]
Politeknik Caltex Riau
Jl. Umban Sari No. 1 Rumbai Pekanbaru, Telp : 0761-53939, Fax : 0761-554224
e-mail: pcr@pcr.ac.id

Abstrak

PIN (Personal Identification Number) merupakan salah satu data yang bersifat rahasia dan penting. Untuk itu, dibutuhkan suatu teknik menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Teknik tersebut disebut dengan kriptografi. Salah satu teknik kriptografi yang dapat dilakukan adalah dengan secret sharing.Jurnal ini membahas penerapan algoritma Interpolasi Polinomial LaGrange dalam secret sharing. Data berupa PIN akan dienkripsi menjadi beberapa shares (hasil pembagian secret) untuk dibagikan kepada sejumlah pihak yang disebut participants, yang dianggap memiliki hak untuk memegang rahasia tersebut. Shares akan digabungkan kembali untuk membentuk pesan rahasia dengan menerapkan algoritma tersebut. Dengan adanya aplikasi ini, PIN dapat disebarkan dengan sistem kerja yang cepat karena diproses secara komputasi. Selain itu, PIN juga lebih aman di dalam proses distribusi karena shares tunggal yang dibentuk oleh aplikasi tidak mengandung informasi yang berkaitan dengan PIN. Dari hasil pengujian dan perbandingan, dapat dilihat bahwa aplikasi yang telah dibuat telah sesuai dengan konsep dasar secret sharing, dimana terdapat nilai ambang minimal yang dibutuhkan untuk menggabungkan kembali PIN, sehingga apabila jumlah shares yang diinputkan kurang dari nilai ambang, maka PIN tidak dapat didekripsi menjadi PIN awal.

***Kata kunci** : Secret sharing, Shares, Interpolasi Polinomial LaGrange, Kriptografi.*

Abstract

PIN (Personal Identification Number) is one of the data that is secrecy and important. Therefore, it is needed technic for keep the secrecy of the data by convert the data from a readable state to apparent nonsense. This technic is called cryptography. One of the cryptography methods is secret sharing. This paper will explain how LaGrange Interpolation Polynomial Scheme works on secret sharing. This method share a secret data, become some parts that call share (fraction of the secret data) to be shared to people that call participants which being believed to have a right to keep that part of secret. Shares will being bundle again to create the secret data by using certain methods. By using this application, PIN can be share securely by an expeditious system. Besides, PIN also more secure in the distribution process because the single shares that made by this application does not contain the PIN information itself. From the research and comparable, the application that made is appropriate with the base concept of secret sharing, which there is a threshold that needed to bundle the PIN and if input shares is less than the definite threshold, the PIN can't be decrypted.

***Keywords**: Secret sharing, Shares*, *LaGrange Interpolation Polynomial*, *Cryptography*.

1. Pendahuluan

1.1 Latar Belakang

Dewasa ini, teknologi informasi sudah berkembang dengan sangat pesat. Data dan informasi menjadi bagian yang tidak terpisahkan dari perkembangan teknologi saat sekarang. Infomasi-informasi yang ada sangat mudah menyebar dan penyebarannya pun cepat. Kerahasiaan data adalah hal yang sangat penting. Agar kerahasiaan data dapat terjaga dengan baik, maka sebisa mungkin data dan informasi tersebut harus dijaga dengan menggunakan metode penyimpan rahasia yang baik[4].

Salah satu metode yang dapat digunakan adalah metode *secret sharing*. Metode *secret sharing* merupakan bagian dari kriptografi. Metode ini membagi suatu pesan rahasia, menjadi beberapa bagian yang disebut *shares* (hasil pembagian *secret*), untuk dibagikan kepada sejumlah pihak yang disebut *participants*, yang dianggap memiliki hak untuk memegang rahasia tersebut [5]. Salah satu algoritma yang dapat diterapkan untuk *secret sharing* adalah algoritma Interpolasi Polinomial LaGrange. Dengan Interpolasi LaGrange, pesan-pesan rahasia yang telah dipecahkan dapat dibentuk kembali menjadi pesan rahasia semula dimana algoritma ini dapat menemukan nilai titik dengan teknik yang sederhana namun

akurat. Selain itu, Interpolasi Polynomial LaGrange terbukti dapat mengkonstruksi koefisien dari polinomial jika diketahui nilai dari titik-titik yang bersangkutan[7].

1.2 Tujuan

Tujuan dari penulisan jurnal ini antara lain :

1. Membuat aplikasi untuk menjaga keamanan data sehingga data yang disebar kepada lebih dari satu pihak dapat terjaga kerahasiaannya.
2. Mengimplementasikan algoritma Interpolasi Polinomial LaGrange pada secret sharing.

1.3 Perumusan Masalah

Dalam pembuatan jurnal ini terdapat beberapa perumusan masalah antara lain :

1. Bagaimana membangun aplikasi *secret sharing* dengan tingkat akurasi yang baik, dimana sebuah *secret* dapat di *share* dalam sebuah himpunan *participants* sedemikian sehingga hanya himpunan bagian tertentu saja dari himpunan *participants* tersebut yang bisa membentuk kembali *secret* tersebut, sementara himpunan bagian lainnya tidak akan mampu untuk membentuk kembali *secret* tersebut[6].
2. Bagaimana menerapkan Algoritma Interpolasi Polynomial LaGrange pada secret sharing

1.4 Ruang Lingkup

Adapun ruang lingkup pada proyek akhir ini adalah :

1. Nilai t (jumlah *share* yang diperlukan untuk memperoleh pesan kembali) dan n (total jumlah *share*) dibatasi minimum 2 dan maksimal 10, dimana $t \leq n$.
2. Panjang pesan rahasia berupa PIN 6 digit angka.
3. Tidak menangani permasalahan mengenai cara penyebaran pada *participants*.
4. Aplikasi program dibuat dengan bahasa pemograman Java dengan *tools* Netbeans.
5. Tidak adanya pengulangan penginputan kunci apabila terjadi kesalahan penginputan.
6. Tidak menangani masalah yang terjadi apabila terdapat *participant* yang kehilangan kuncinya.

1.5 Manfaat

Manfaat dari penulisan jurnal ini antara lain :

1. Mengamankan informasi yang disebar kepada lebih dari satu pihak sehingga tidak terjadi kebocoran rahasia pada saat penyebaran pesan rahasia.
2. Meningkatkan kesadaran pentingnya kriptografi dalam menjaga kerahasiaan data.

2. Tinjauan Pustaka

2.1 Kriptografi

Kriptografi (cryptography) berasal dari Bahasa Yunani: "*cryptós*" artinya rahasia, sedangkan *gráphein* artinya tulisan. Jadi, kriptografi berarti tulisan rahasia. Ada beberapa definisi kriptografi yang telah dikemukakan di dalam berbagai literatur. Definisi yang dipakai di dalam buku-buku yang lama (sebelum tahun 1980-an) menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Namun saat ini kriptografi lebih dari sekadar *privacy*, tetapi juga untuk tujuan keutuhan data(*data integrity)*, keabsahan data(*authentication)*, dan keabsahan bukti yang tidak dapat disangkal(*non-repudiation)*. Fungsi-fungsi yang mendasar dalam kriptografi adalah enkripsi dan dekripsi. Enkripsi adalah proses mengubah suatu pesan asli yang disebut *plaintext,* menjadi suatu pesan dalam bahasa sandi yang disebut dengan *ciphertext*.

2.2 Secret Sharing

Secret sharing ditemukan oleh Adi Shamir yang merupakan seorang kriptografer dari Israel dan George Blaker, seorang kriptografer dari Amerika Serikat secara masing-masing pada tahun 1979. Dalam metode *secret sharing* ada seorang pembagi dan n pemegang bagian (*shares*) yang disebut *participants*. Pembagi memberikan rahasia kepada pemegang bagian jika suatu syarat tertentu terpenuhi. Syarat yang dimaksud adalah struktur akses, yaitu aturan tentang siapa saja yang mendapat otorisasi untuk membentuk berita rahasia itu kembali. Dalam suatu kelompok berlaku nilai ambang(*threshold value*), yaitu jumlah minimal *participants* yang dibutuhkan dalam suatu kelompok untuk membangkitkan suatu berita rahasia [4].

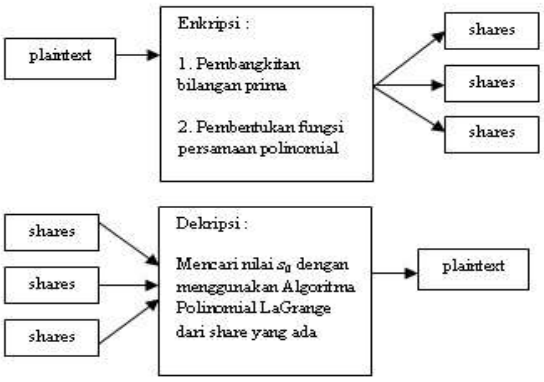
Metode ini tercipta disebabkan karena, untuk menjaga keamanan kunci hasil dari sistem kriptografi agar tidak hilang, disarankan untuk membuat sejumlah kunci cadangan. Namun, resiko kerahasiaan kunci akan semakin besar dengan semakin banyaknya kunci cadangan yang dibuat. *Secret sharing* menangani masalah ini dengan membagi kunci menjadi beberapa bagian tanpa meningkatkan resiko kerahasiaan, karena pesan rahasia dipecahkan menjadi bagian-bagian yang tidak memiliki arti jika berdiri sendiri. Sehingga dapat dikatakan, skema *secret sharing* mempertinggi reliabilitas tanpa menambah resiko [5].

Metode *secret sharing* di zaman ini diterapkan pada bidang-bidang aplikasi yang beragam, misalnya kontrol akses, peluncuran senjata atau proyektil, membuka kotak deposito atau *safety box*, dan lain-lain.

Ada beberapa istilah yang digunakan pada metode ini :

1. *Secret*
   Secret adalah informasi rahasia atau *plaintext* yang direpresentasikan sebagai sebuah integer dan pada penerapan dalam aplikasi ini disebut sebagai PIN.
2. *Share*
   Share merupakan hasil pembagian secret yang disebut sebagai *ciphertext*
3. *Dealer*
   Dealer adalah pihak yang melakukan pembagian *secret* menjadi sejumlah *share*.
4. *Participant*
   Participant adalah n pihak yang memperoleh *share* yang berbeda satu sama lain [1].

Gambaran umum Skema *Threshold Shamir's* [Gambar 1]:



Gambar 1. Gambaran Umum Skema Threshold Shamir's

2.3 Interpolasi Polinomial LaGrange

Interpolasi Lagrange diterapkan untuk mendapatkan fungsi polinomial $P(x)$ berderajat tertentu yang melewati sejumlah titik data. Misalnya, akan dicari fungsi polinomial berderajat satu yang melewati dua buah titik yaitu (x_0, Y_0) dan (x_1, Y_1). Interpolasi polinomial Lagrange dapat diturunkan dari persamaan Newton.

Bentuk umum interpolasi polinomial Lagrange order *n* adalah:

$$f_n(x) = \sum_{i=0}^{n} L_i(x)\, f(x_i) \tag{6}$$

dengan

$$L_i(x) = \prod_{\substack{j=0 \\ j \neq i}}^{n} \frac{x - x_j}{x_i - x_j} \tag{7}$$

Simbol Π merupakan perkalian.
Sehingga bentuk interpolasi Lagrange order 2 adalah:

$$f_2(x) = \left(\frac{x-x_1}{x_0-x_1}\right)\left(\frac{x-x_2}{x_0-x_2}\right) f(x_0) + \left(\frac{x-x_0}{x_1-x_0}\right)\left(\frac{x-x_2}{x_1-x_2}\right) f(x_1) + \left(\frac{x-x_0}{x_2-x_0}\right)\left(\frac{x-x_1}{x_2-x_1}\right) f(x_2) \tag{8}$$

3. Hasil dan Analisa

3.1 Implementasi Metode dan Algoritma LaGrange Interpolating Polynomial

Penerapan Algoritma LaGrange Interpolating Polynomial pada Secret Sharing:

a. Pilih suatu bilangan prima p yang harus lebih besar dari semua kemungkinan nilai secret (*plaintext*) M dan juga lebih besar dari jumlah n *participants*. p ini akan dijadikan modulus

untuk semua perhitungan. p harus bilangan prima untuk memastikan tiap bilangan memiliki *invers*.

b. Selanjutnya, pilih t – 1 buah bilangan bulat dalam modulus p secara acak, misalkan $s_1, s_2, s_3, \ldots, s_{t-1}$ dan bentuk suatu polinomial:
$$f_x \equiv M + s_1 x + s_2 x^2 + \cdots + s_{t-1} x^{t-1} (mod\ p)$$
sedemikian sehingga s(0) ≡ M (mod p). f_x dapat disebut juga sebagai fungsi ambang.

c. Untuk n *participants*, tentukan n bilangan bulat berbeda dalam modulus p, misal x_1 , x_2 , …x_n (mod p) dan setiap orang memperoleh *share* (x_i, y_i) di mana $y_i \equiv f_i(x_i)\ (mod\ p)$

d. Misalkan t orang *participants* akan merekonstruksi M, dengan share masing-masing (x_1, y_1), (x_2, y_2) …, (x_t, y_t). Substitusikan setiap (x_k, y_k) ke dalam polinomial $f(x)$, yang berarti:
$$y_k \equiv M + s_1 {x_k}^1 + \cdots + s_{t-1} {x_k}^{t-1} (mod\ p), 1 \leq k \leq t$$
dimana jumlah share minimum adalah 2 buah.

e. Selesaikan system persamaan di atas untuk memperoleh s_0= M dengan menggunakan LaGrange.

Dalam implementasi skema di atas, nilai prima p tidak perlu rahasia, tetapi polinom $f(x)$ harus dirahasiakan.

Dengan adanya algoritma ini, maka *shares* yang dibagikan kepada setiap *participants* akan aman karena *shares* tunggal tidak mengandung informasi mengenai *secret*.

3.2 Aplikasi

Aplikasi ini merupakan aplikasi kriptografi dimana terdapat form yang digunakan untuk enkripsi dan form yang digunakan untuk dekripsi. Selain itu, juga terdapat fitur untuk cara penggunaan, dan fitur mengenai teori Interpolasi Polinomial LaGrange dan juga Aritmetika Modulo. Adapun tampilan awal dari aplikasi adalah sebagai berikut [Gambar 2]:

Gambar 2 Halaman Awal Aplikasi

Pada form enkripsi [Gambar 3], user yang disebut dealer akan melakukan enkripsi dengan cara menginputkan PIN rahasia berupa 6 digit angka. Setelah itu, dealer harus menginputkan jumlah pemegang kunci yang akan memegang kunci rahasia tersebut. Nilai ambang merupakan jumlah minimum yang dibutuhkan untuk membentuk kembali kunci yang telah dipecah menjadi sejumlah kunci. *Share* atau *ciphertext* dapat didapatkan dengan dua cara, yakni langsung ditampilkan pada form enkripsi, atau dapat juga disimpan dalam file yang berekstensi *.out yang disimpan dalam suatu folder tertentu.

Gambar 3 Hasil Enkripsi dengan menampilkan langsung dan menyimpan data

Untuk melakukan dekripsi [Gambar 4], terdapat pilihan pada form awal, maupun terdapat pada pilihan menu yang tersedia pada setiap form. Pada proses dekripsi, dealer akan menginputkan data berupa kunci publik dan *share* yang telah diberikan kepada setiap *participants*. Kunci publik dapat diinputkan secara manual oleh dealer, maupun menginputkan file yang telah dibuat pada saat proses enkripsi.

Gambar 4 Form Dekripsi

Penginputan secara manual dapat dilakukan dengan menginputkan data pada *text field* masukkan data, dan menekan button *add(+).*

3.3 Analisa dan Pengujian

3.3.1 Pengujian berulang dengan inputan yang sama.

Pengujian berulang dengan inputan yang sama bertujuan untuk mengetahui konsistensi dari hasil dekripsi, apakah akan menghasilkan data yang tetap. Pengujian dilakukan dengan menginputkan data berupa :
PIN: 654321, Jumlah participants: 5, Nilai ambang : 3, Jumlah share yang diinputkan : 4

Tabel 2 Tabel Pengujian berulang terhadap aplikasi

No	Kunci Dealer	Share-1	Share-2	Share-3	Share-4	Share-5	Hasil Dekripsi
1	767857	1-250149	2-757963	3-642049	4-670264	5-74751	654321
2	799333	1-656876	2-553887	3-345359	4-31277	5-410989	654321
3	831023	1-581830	2-272098	3-556148	4-602957	5-412525	654321
4	684347	1-89795	2-102266	3-7387	4-489505	5-179926	654321
5	763913	1-75428	2-134103	3-66433	4-636331	5-315971	654321

Dari hasil pengujian *Tabel 1* dapat dilihat bahwa enkripsi dengan PIN yang sama, akan menghasilkan kunci publik yang bervariasi dan nilai share yang bervariasi. Namun ketika di dekripsi kembali, kunci akan membentuk nilai PIN yang sama dan tepat.

3.3.2 Pengujian terhadap jumlah *shares* yang diinputkan

Pengujian dilakukan dengan menggunakan data yang ada, untuk melihat hasil dekripsi yang sesuai dengan ketentuan nilai ambang yang telah ditentukan.
Pengujian dilakukan dengan data:
PIN: 264573 Jumlah Participants : 10 Nilai ambang : 4

Tabel 3 Tabel Pengujian terhadap jumlah shares

No	Kunci Publik Dealer	Jumlah share yang diinputkan	Hasil Dekripsi
1	322669	6	264573
2	322669	5	264573
3	322669	4	264573
4	322669	3	320263
5	322669	2	101423

Dari hasil pengujian *Tabel 2*, didapatkan bahwa hasil dekripsi akan sesuai dengan PIN yang dimasukkan, jika jumlah *shares* yang diinputkan lebih besar atau sama dengan jumlah nilai ambang yang dimasukkan pada saat enkripsi. Jika jumlah *shares* yang diinputkan lebih kecil dari nilai ambang, maka hasil dekripsi akan tidak sesuai. Dengan demikian, aplikasi dapat dikatakan memenuhi ketentuan awal dari *secret sharing*.

4. Kesimpulan

Setelah menerapkan Algoritma Interpolasi Polinomial LaGrange pada secret sharing, dapat disimpulkan bahwa :

1. Aplikasi yang dibangun telah memenuhi Threshold's Shamir dimana sebuah *secret* dapat di *share* dalam sebuah himpunan *participants* sedemikian sehingga hanya himpunan bagian tertentu saja yang bisa membentuk kembali *secret* tersebut.
2. Algoritma Interpolasi Polinomial LaGrange merupakan algoritma yang dapat diterapkan pada Secret Sharing karena mampu membentuk pesan-pesan yang tidak berkaitan satu sama lain, dan mampu menggabungkan kembali kunci tersebut dengan himpunan bagian tertentu.
3. Dengan adanya pembatasan terhadap type data dan jumlah digit angka, maka sistem hanya dapat bergerak pada ruang lingkup yang terbatas, sehingga tidak semua informasi dapat dienkripsi.

Daftar Pustaka

[1] Handaka, Michell Setyawati. Studi dan Analisis Skema Benaloh untuk Pembagian Rahasia dengan Verifikasi beserta Studi dan Implementasi Skema Ambang Shamir. Sekolah Teknik Elektro dan Informatika ITB; 2011
[2] Kristanto, Yoseph. Studi dan Implementasi Protokol Secret Sharing dengan Algoritma Multiple Threshold Changeable: Miskroskil Medan.2010
[3] Munir, Rinaldi. *Skema Pembagian Data Rahasia*. Teknik Informatika ITB; (t,t)
[4] Saputra, Dimas Gilang. *Aplikasi Chinese Remainder Theorem dalam Secret Sharing*. Institut Teknologi Bandung;2010
[5] Syahroni, Zainul Gufron, dkk. *Secret Sharing Schemes*. Universitas Jember;2011
[6] Theodore, Robertus. Implementasi Pembagian Rahasia dengan Menggunakan Teorema Chinese Remainder. Teknik Informatika ITB. 2011
[7] Zhenjun, Ye. Design and realization of threshold secret sharing scheme with random weights. Journal of Systems Engineering and Electornics. 2009