KONSTRUKSI SKEMA PEMBAGIAN DATA RAHASIA MENGGUNAKAN ALGORITMA KARNIN-GREENE-HELLMAN DAN SKEMA SHAMIR

Skripsi

Disusun untuk melengkapi syarat-syarat

guna memperoleh gelar Sarjana Sains

DANIEL

3125136332

PROGRAM STUDI MATEMATIKA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS NEGERI JAKARTA

2017

LEMBAR PERSETUJUAN HASIL SIDANG SKRIPSI

KONSTRUKSI SKEMA PEMBAGIAN DATA RAHASIA MENGGUNAKAN ALGORITMA KARNIN-GREENE-HELLMAN DAN SKEMA SHAMIR

Nama : Daniel

No. Registrasi : 3125136332

	Nama	Tanda Tangan	Tanggal
Penanggung Jawab			
Dekan	: Prof. Dr. Suyono, M.Si.	.....	18-07-2017
	NIP. 19671218 199303 1 005		
Wakil Penanggung Jawab			
Wakil Dekan I	: Dr. Muktiningsih, M.Si.	.....	18-07-2017
	NIP. 19640511 198903 2 001		
Ketua	: Dr. Makmuri, M.Si.	.....	14-08-2017
	NIP. 19640715 198903 1 006		
Sekretaris	: Vera Maya Santi, M.Si.	.....	15-08-2017
	NIP. 19790531 200501 2 006		
Penguji	: Ratna Widyati, S.Si., M.Kom.	.....	14-08-2017
	NIP. 19750925 200212 2 002		
Pembimbing I	: Drs. Mulyono, M.Kom.	.....	16-08-2017
	NIP. 19660517 199403 1 003		
Pembimbing II	: Med Irzal, M.Kom.	.....	15-08-2017
	NIP. 19770615 200312 1 001		

Dinyatakan lulus ujian skripsi tanggal: 11 Agustus 2017

ABSTRACT

DANIEL, 3125136332. The Construction of Secret Sharing Scheme Based on KGH Algorithm and Lagrange Polynomial. Thesis. Faculty of Mathematics and Natural Science, Jakarta State University. 2017.

Recently, the safety of a secret is an important aspect of a life system. The process to share a secret for participants is also important to be noted. The methods that can be used to sharing a secret are KGH Algorithm and Lagrange Polynomial. The critical sets Q needs to be seacrh of the first step on a star graph that has fulfilled the edge-magic total labeling. The critical sets is rated as an agent to construct the secret. There is no specific algorithm for obtaining a critical sets, so the process solved manually. On the polynomial, it is possible to have infinite point, so the number of participants who are able to build the secret is unlimited. Meanwhile, the participants are limited, if the KGH Algorithm is used. There are both advantages and disadvantages between the methods, so the option of the method depends on the condition and the goal to be achieved.

Keywords *: secret data, star graph, edge-magic total labeling, KGH algorithm, secret sharing, Lagrange polynomial.*

ABSTRAK

DANIEL, 3125136332. Konstruksi Skema Pembagian Data Rahasia Menggunakan Algoritma KGH dan Polinomial Lagrange. Skripsi. Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Jakarta. 2017.

Dewasa ini, keamanan suatu rahasia merupakan aspek penting dalam sistem kehidupan. Proses pembagian data rahasia kepada partisipan juga merupakan proses yang penting untuk diperhatikan. Metode yang dapat digunakan untuk membagi data rahasia adalah algoritma KGH dan polinomial Lagrange. Himpunan kritis Q perlu dicari terlebih dahulu pada graf bintang yang sudah memenuhi pelabelan total sisi ajaib. Himpunan kritis ini dianggap sebagai alat untuk merekonstruksikan rahasia. Hingga saat ini belum ditemukan suatu algoritma yang khusus untuk memperoleh suatu himpunan kritis, sehingga prosesnya dilakukan secara manual. Pada polinomial, dimungkinkan untuk memiliki tak terhingga banyaknya titik sehingga jumlah partisipan yang bisa membangun data rahasia jumlahnya tak terbatas, sedangkan jika menggunakan Algoritma KGH jumlah partisipan terbatas. Terdapat kelebihan dan kekurangan diantara kedua metode tersebut, sehingga pemilihan metode tergantung dari kondisi dan tujuan yang ingin dicapai.

Kata kunci : data rahasia, graf bintang, pelabelan total sisi ajaib, Algoritma KGH, membagi data rahasia, rekonstruksi data rahasia, polinomial Lagrange.

PERSEMBAHANKU...

"*I walk slowly, but I never walk backward*"

-Abraham Lincoln

Untuk Bapak, Mama, dan Adek.

"Terima kasih atas dukungan, doa, serta kasih sayang kalian".

KATA PENGANTAR

Puji syukur kepada Tuhan YME atas pengetahuan dan kemampuan sehingga penulis dapat menyelesaikan skripsi yang berjudul "Konstruksi Skema Pembagian Data Rahasia Menggunakan Algoritma KGH dan Polinomial Lagrange" yang merupakan salah satu syarat dalam memperoleh gelar Sarjana Jurusan Matematika Universitas Negeri Jakarta.

Skripsi ini berhasil diselesaikan tidak terlepas dari adanya bantuan dari berbagai pihak. Oleh karena itu, dalam kesempatan ini penulis ingin menyampaikan terima kasih terutama kepada:

1. Bapak Drs. Mulyono, M.Kom. selaku Dosen Pembimbing I, dan Bapak Med Irzal, M.Kom. selaku Dosen Pembimbing II, yang telah meluangkan waktunya dalam memberikan bimbingan, saran, nasehat serta arahan sehingga skripsi ini dapat menjadi lebih baik dan terarah.

2. Ibu Dr. Lukita Ambarwati, S.Pd., M.Si., selaku Ketua Program Studi Matematika FMIPA UNJ yang telah banyak membantu penulis dan mengarahkan proses pengerjaan skripsi.

3. Bapak Yudi Mahatma, M.Si., selaku Pembimbing Akademik atas segala bimbingan dan kerja sama Bapak selama perkuliahan, dan seluruh Bapak/Ibu dosen atas pengajarannya yang telah diberikan, serta karyawan/karyawati FMIPA UNJ yang telah memberikan informasi yang penulis butuhkan dalam menyelesaikan skripsi.

4. Bapak, Mama, dan Adek yang selalu mendukung, memberi motivasi, semangat, dan setia mendoakan penulis dengan penuh cinta dan kasih sayang yang tulus dan tiada henti.

5. Ayunda, yang terus memberi semangat, dorongan, doa, motivasi, menemani setiap konsultasi dengan dosbim dan selalu menghibur ketika penulis mengalami kesulitan dalam penulisan skripsi ini. Semuanya tanpa lilin.

6. Teman-teman seperjuangan 2017, Hanun, Nurul, Atikah, Tias, Irena, Defy, Ita, Umam, Nisa, dan Syevie atas diskusi dan pendapatnya dalam membantu penulis menyelesaikan skripsi ini.

7. Teman-teman Matematika UNJ 2013 yang telah menjadi sahabat penulis dalam 4 tahun terakhir ini, dengan banyak ciri, sifat dan kelakuan yang membuat kita semakin beragam dan menyatu. Semoga persahabatan kita terus berlanjut hingga tua nanti.

8. Teman-teman di SD, SMP, SMA serta di UNJ yang hingga saat ini terus mengirimkan doa serta semangat untuk penulis.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Masukan dan kritikan akan sangat berarti. Semoga skripsi ini dapat bermanfaat bagi pembaca sekalian.

Jakarta, Agustus 2017

Daniel

DAFTAR ISI

DAFTAR SIMBOL

			halaman
u, v	:	simpul pada graf	5
e	:	sisi yang menghubungkan simpul u dan v	5
$V(G)$	:	himpunan simpul dari graf G	5
$E(G)$	:	himpunan sisi dari graf G	5
N_n	:	graf kosong dengan n simpul	10
$d(v)$	:	derajat dari simpul v pada graf G	10
K_n	:	graf lengkap dengan n buah simpul	13
$K_{1,n}$	:	graf bintang dengan $n+1$ simpul dan n sisi	14
L	:	pelabelan graf	14
Z^+	:	himpunan bilangan bulat positif	14
w	:	bobot pada graf	15
$L(x)$	:	pelabelan pada simpul x di graf G	15
$L(y)$	:	pelabelan pada simpul y di graf G	15
$L(xy)$	:	pelabelan pada sisi xy di graf G	15
Q_λ	:	himpunan kritis untuk pelabelan λ	19
S	:	informasi rahasia	26
P	:	himpunan partisipan	26
D	:	*dealer*	27
Z_n	:	himpunan semua kelas kongruen modulo n	30
A	:	himpunan kuasa yang dapat merekonstruksikan rahasia	32
Γ	:	struktur akses	38

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Dalam jaman yang semakin modern ini, informasi merupakan salah satu komponen terpenting dalam proses kehidupan. Ada berbagai macam jenis informasi, mulai dari yang bersifat bebas hingga yang bersifat rahasia. Informasi yang bersifat bebas biasanya bertujuan untuk kepentingan bersama dan tidak merugikan suatu individu atau kelompok. Informasi yang bersifat rahasia hanya berguna bagi suatu lembaga atau perusahaan, dan terkadang bila informasi itu diketahui orang lain yang tidak berkepentingan, dapat merugikan pemilik informasi tersebut. Berdasarkan kemungkinan tersebut, suatu lembaga atau perusahaan akan melindungi informasi rahasia tersebut agar tidak dapat dicuri oleh orang yang tidak berkepentingan.

Dewasa ini, kepercayaan antara satu orang dengan orang lainnya sangat minim dikarenakan besar kemungkinannya terjadi suatu penyalahgunaan atas peraturan dan perjanjian yang berlaku di antara kedua belah pihak. Apabila seseorang mempercayakan suatu rahasia pada satu pihak saja, ada kemungkinan pihak tersebut menyalahgunakan wewenang yang diberikan kepadanya, sehingga dapat merugikan pihak-pihak yang berkaitan dengan informasi rahasia tersebut.

Contoh nyata permasalahan diatas adalah ketika seorang direktur bank memegang informasi rahasia untuk membuka sebuah brankas uang di bank tempat ia bekerja. Ia ingin brankas uang tetap dapat dibuka walaupun ia tidak

berada di bank. Apa yang harus dilakukannya untuk mencapai tujuannya tetapi informasi penting tersebut terjamin keamanannya ?

Direktur dapat mempercayakan informasi rahasia tersebut kepada seseorang, atau memodifikasi informasi rahasisa tersebut sebelum menyerahkannya sehingga orang yang dititipkan tidak tahu informasi rahasia yang sebenarnya secara langsung, atau dengan membuat suatu kode rahasia untuk dapat membuka informasi rahasia itu. Namun menitipkan informasi kepada manusia memiliki resiko yang tinggi karena mungkin dapat terjadi hal-hal yang berakibat fatal pada informasi rahasia tersebut, seperti orang yang dititipkan informasi rahasia menghilang, terjadinya kematian kepada orang tersebut, atau ternyata orang tersebut tidak dapat dipercaya, dan hal lainnya.

Berdasarkan masalah yang telah dipaparkan, ada cara yang dapat digunakan untuk menyelesaikan masalah tersebut. Salah satu ilmu yang mempelajari cara atau teknik untuk menjaga keamanan suatu rahasia adalah Pembagian Data Rahasia, yang merupakan cabang dari ilmu kriptografi. Teknik pembagian data rahasia adalah dengan membagi rahasia tersebut kepada beberapa orang sehingga jika ingin mendapatkan kembali rahasia, orang-orang tersebut harus dikumpulkan. Gagasan dari pembagian rahasia ini adalah membagi atau memecah rahasia menjadi potongan-potongan informasi yang diberikan kepada sekelompok orang. Skema pembagian data rahasia ini dapat mempertinggi reliabilitas tanpa menambah resiko.

Adapun cara lainnya yang dapat digunakan adalah menggunakan skema ambang batas yang diperkenalkan oleh Shamir. Shamir menggunakan polinomial lagrange sebagai alat untuk membagikan dan merekonstruksikan rahasia.

Namun begitu, ada pula masalah yang berkaitan dengan penggunaan metode Pembagian Data Rahasia, yaitu bagaimana cara pembagian *shares* atau data rahasia, dan juga bagaimana cara merekonstruksikan kembali rahasia

tersebut. Guna memecahkan permasalahan tersebut, kita bisa menggunakan teori graf, salah satunya graf bintang. Penggunaan graf bintang dikarenakan model graf tersebut cocok dengan realita pembagian data rahasia yaitu hanya terdapat satu titik pusat yang dapat dianalogikan sebagai *dealer* yang hanya berjumlah satu orang. Untuk membantu penggunaan graf tersebut, dapat digunakan teori pelabelan ajaib dan teori Algoritma Karnin-Greene-Hellman (KGH). Penulis juga akan melakukan proses rekonstruksi data rahasia menggunakan Skema Shamir dengan polinomial Lagrange. Kemudian, akan dijelaskan kelebihan serta kekurangan antara dua metode tersebut.

1.2 Perumusan Masalah

Perumusan masalah yang akan dikaji adalah sebagai sebagai berikut :

1. Bagaimana mengkonstruksikan skema Pembagian Data Rahasia menggunakan pelabelan ajaib pada graf bintang dengan Algoritma KGH dan menggunakan polinomial Lagrange.

2. Membandingkan kelebihan dan kekurangan dari metode Algoritma KGH dan Skema Shamir.

1.3 Pembatasan Masalah

Pembatasan masalah dalam penulisan ini adalah sebagai berikut:

1. Graf bintang yang digunakan sudah merupakan konversi dari data rahasia.

2. Fungsi polinomial yang digunakan sudah merupakan konversi dari data rahasia.

1.4 Tujuan Penulisan

Tujuan yang ingin dicapai dalam skripsi ini adalah sebagai berikut:

1. Memaparkan proses rekonstruksi skema Pembagian Data Rahasia menggunakan pelabelan ajaib pada graf bintang dengan Algoritma KGH dan Skema Shamir.

2. Memaparkan kelebihan dan kekurangan dari metode Algoritma KGH dan Skema Shamir.

1.5 Manfaat Penulisan

Manfaat yang diharapkan dari skripsi ini adalah secara umum memperoleh penyelesaian skema Pembagian Data Rahasia sehingga dapat diaplikasikan oleh suatu kelompok atau perusahaan untuk mengamankan kunci rahasia yang dimilikinya.

1.6 Sistematika Penulisan

Skripsi ini dibagi menjadi empat bab. Bab II berisi pengertian graf, penjelasan secara umum tentang graf bintang dan pelabelan ajaib, skema Pembagian Data Rahasia serta polinomial Lagrange. Bab III berisi pembahasan mengenai skema Pembagian Data Rahasia menggunakan Algoritma KGH dan Skema Shamir. Sedangkan Bab IV merupakan kesimpulan serta saran.

BAB II

LANDASAN TEORI

Pada bab ini, akan dibahas tentang graf, bagaimana skema pembagian data rahasia, dan graf yang bisa digunakan untuk menyelesaikan permasalahan pembagian data rahasia. Sebagai awalan, akan dijelaskan mengenai definisi graf dan terminologi dasar graf.

2.1 Graf

Definisi 2.1.1. *Graf G didefinisikan sebagai pasangan himpunan (V, E), ditulis dengan notasi $G = (V, E)$, yang dalam hal ini $V(G)$ adalah himpunan tidak-kosong dari simpul-simpul (vertices atau node) dari graf G dan $E(G)$ adalah himpunan sisi (edges atau arcs) yang menghubungkan sepasang simpul dari graf G* (Munir, 2012:356).

Elemen-elemen utama suatu graf adalah simpul, sisi, dan muka. Secara geometri, suatu graf digambarkan sebagai sekumpulan titik (simpul) di dalam suatu bidang yang dihubungkan dengan sekumpulan garis (sisi). Simpul biasanya digambarkan dengan bulatan hitam, sedangkan sisi dapat disajikan dengan garis yang menghubungkan simpul-simpul pada graf. Simpul pada graf dapat diberi indeks dengan huruf, seperti $a, b, c, ..., v, w, x, ...$, dan bilangan asli $1, 2, 3, ...$, atau gabungan keduanya. Sisi yang menghubungkan simpul u dengan v dinyatakan dengan pasangan (u, v) atau dinyatakan dengan lambang e_1, e_2, dan seterusnya. Artinya, jika e adalah sisi yang menghubungkan simpul u dengan simpul v, maka e dapat ditulis sebagai $e = (u, v)$.

Graf G dikatakan memiliki sisi ganda (*multiple edges*) jika terdapat minimal dua sisi e_1, $e_2 \in E(G)$, yang keduanya menghubungkan pasangan simpul yang sama. Sedangkan sisi yang menghubungkan suatu simpul dengan dirinya sendiri dinamakan gelang (*loop*). Daerah yang dibatasi oleh sisi-sisi pada graf disebut muka ($face$).

2.2 Jenis - jenis Graf

Graf dapat dikelompokkan menjadi beberapa kategori (jenis) bergantung pada sudut pandang pengelompokannya. Pengelompokan graf dapat dibedakan berdasarkan ada tidaknya sisi ganda, berdasarkan jumlah simpul, atau berdasarkan orientasi arah pada sisi.

Berdasarkan ada tidaknya sisi ganda pada graf, secara umum graf dapat digolongkan menjadi dua jenis:

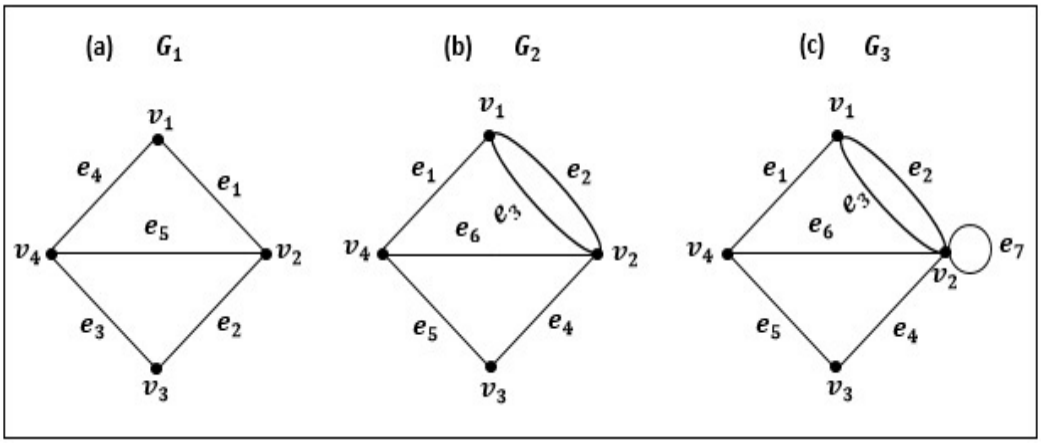
1. Graf Sederhana

   Graf sederhana merupakan graf yang tidak memiliki gelang ataupun sisi ganda. Pada graf sederhana, penulisan sisi tidak memperhatikan urutan. Jadi, penulisan sisi (u, v) sama dengan (v, u). Kita juga dapat mendefinisikan graf sederhana $G = (V, E)$ terdiri dari himpunan tak kosong simpul-simpul dan E adalah himpunan pasangan tak-terurut yang berbeda. Gambar 2.1(a) adalah contoh graf sederhana.

2. Graf Tak-Sederhana

   Merupakan graf yang memiliki sisi ganda atau gelang. Ada dua macam graf tak-sederhana, yaitu graf ganda dan graf semu. Graf ganda merupakan graf yang mengandung sisi ganda. Sisi ganda yang menghubungkan sepasang simpul bisa lebih dari dua buah. Sedangkan graf semu adalah graf yang mengandung gelang (*loop*). Gambar 2.1(b) merupakan

contoh graf tak-sederhana, dan Gambar 2.1(c) merupakan contoh graf semu.



Gambar 2.1: Tiga buah graf; (a) graf sederhana, (b) graf ganda, (c) graf semu

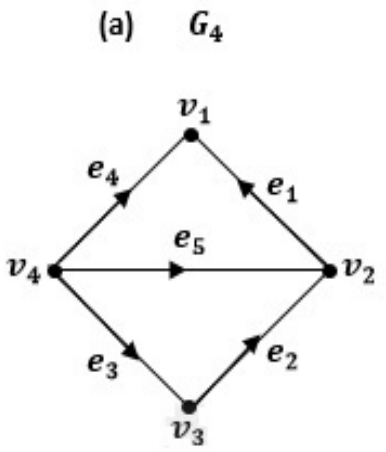
Sisi pada graf dapat mempunyai orientasi arah. Berdasarkan orientasi arah pada sisi, maka secara umum graf dibedakan menjadi 2 jenis:

1. Graf Tak-Berarah

   Graf tak-berarah merupakan graf yang sisinya tidak mempunyai orientasi arah. Pada graf tak-berarah, urutan pasangan simpul yang dihubungkan oleh sisi tidak diperhatikan. Jadi, $(u, v) = (v, u)$ adalah sisi yang sama. Tiga buah graf pada Gambar 2.1 merupakan graf tak-berarah.

2. Graf Berarah

   Graf berarah merupakan graf yang tiap sisinya diberikan orientasi arah. Pada graf berarah, (u, v) dan (v, u) menyatakan dua buah sisi yang berbeda, dengan kata lain $(u, v) \neq (v, u)$. Untuk sisi (u, v), simpul u dinamakan simpul asal, dan simpul v dinamakan simpul terminal. Pada graf berarah, gelang diperbolehkan, tetapi sisi ganda tidak. Gambar 2.2 merupakan contoh graf berarah.



Gambar 2.2: (a) Graf berarah

2.3 Terminologi Dasar Graf

Di bawah ini akan didefinisikan beberapa terminologi (istilah) yang sering digunakan pada graf.

1. **Bertetangga (*Adjacent*)**

   Definisi dari bertetangga adalah sebagai berikut.

   Definisi 2.3.1. *Dua buah simpul pada graf G dikatakan bertetangga bila keduanya terhubung langsung dengan sebuah sisi. Dengan kata lain, u bertetangga dengan v jika (u, v) adalah sebuah sisi pada graf G* (Munir, 2012:365).

   Lihat Gambar 2.3. Pada Graf G_1, simpul 1 bertetangga dengan simpul 2 dan simpul 3, sedangkan simpul 1 tidak bertetangga dengan simpul 4.

2. **Bersisian (*Incident*)**

   Definisi dari bersisian adalah sebagai berikut.

Definisi 2.3.2. *Untuk sembarang sisi $e = (u, v)$, sisi e dikatakan bersisian dengan simpul u dan simpul v* (Munir, 2012:365).

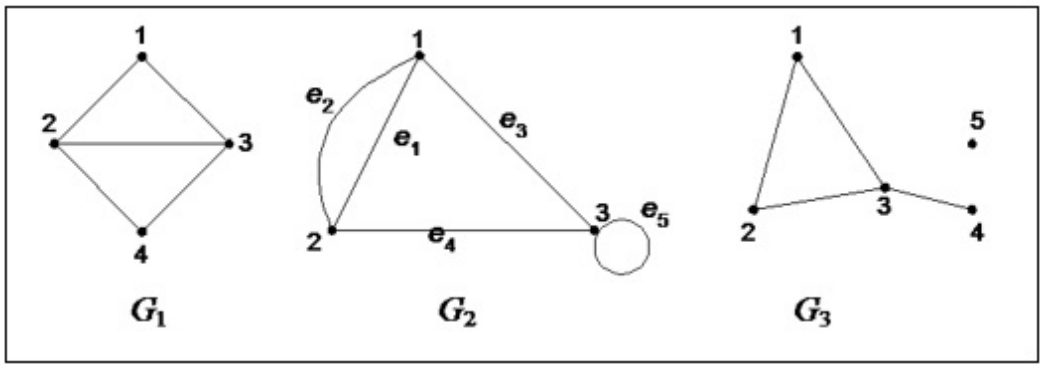
Lihat Gambar 2.3. Pada Graf G_1, sisi(2,3) bersisian dengan simpul 2 dan simpul 3, sisi(2,4) bersisian dengan simpul 2 dan simpul 4. Akan tetapi, sisi(1,2) tidak bersisian dengan simpul 4.

3. **Simpul Terpencil (*Isolated Vertex*)**

   Definisi dari simpul terpencil adalah sebagai berikut.

   Definisi 2.3.3. *Simpul terpencil merupakan simpul yang tidak mempunyai sisi yang bersisian dengannya. Dapat juga dinyatakan bahwa simpul terpencil adalah simpul yang tidak satupun bertetangga dengan simpul-simpul lainnya* (Munir, 2012:365).

   Lihat Gambar 2.3. Pada Graf G_3, simpul 5 adalah simpul terkecil.

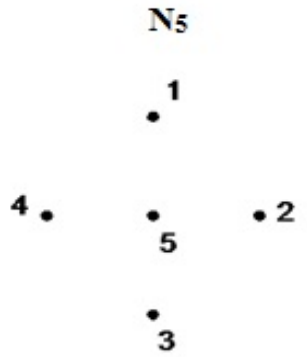


Gambar 2.3: Contoh Graf

4. **Graf kosong (*Null Graph*)**

   Definisi dari simpul terpencil adalah sebagai berikut.

Definisi 2.3.4. *Graf kosong merupakan graf yang himpunan sisinya merupakan himpunan kosong, biasa ditulis sebagai N_n, yang dalam hal ini n adalah jumlah simpul* (Munir, 2012:366).



Gambar 2.4: Graf Kosong N_5

Gambar 2.4 merupakan contoh dari graf kosong dengan 5 simpul.

5. **Derajat**

Definisi dari simpul terpencil adalah sebagai berikut.

Definisi 2.3.5. *Derajat suatu simpul pada graf tak-berarah merupakan jumlah sisi yang bersisian dengan simpul tersebut* (Munir, 2012:366).

Derajat dinotasikan dengan $d(v)$ yang menyatakan derajat simpul v. Sisi gelang dihitung berderajat dua. Alasan mengapa gelang mengkontribusikan dua untuk derajat simpulnya adalah karena gelang direpresentasikan sebagai (v, v), dan simpul v bersisian dua kali pada sisi (v, v).

Pada graf berarah, derajat suatu simpul dibedakan menjadi dua macam, yaitu untuk mencerminkan jumlah sisi dengan simpul tersebut sebagai simpul asal dan jumlah sisi dengan simpul tersebut sebagai simpul terminal. Derajat simpul v dinyatakan dengan $d_{in}(v)$ dan $d_{out}(v)$, yang dalam

hal ini,

$$\begin{aligned} d_{in}(v) &= \text{derajat-masuk } (in - degree) \\ &= \text{jumlah sisi yang masuk ke simpul } v \\ d_{out}(v) &= \text{derajat-keluar } (out - degree) \\ &= \text{jumlah sisi yang keluar dari simpul } v \end{aligned}$$

dan, $d(v) = d_{in}(v) + d_{out}(v)$

6. **Lintasan (*Path*)**

   Definisi dari lintasan adalah sebagai berikut.

   Definisi 2.3.6. *Lintasan yang panjangnya n dari simpul awal* v_0 *ke simpul tujuan* v_n *di dalam graf G ialah barisan berselang - seling simpul - simpul dan sisi - sisi yang berbentuk* v_0, e_1, v_1, e_2, v_2, ... ,$v_n - 1$, e_n, v_n *sedemikian sehingga* e_1 = (v_0, v_1), e_2 = (v_1, v_2), ... , e_n = ($v_n - 1$, v_n) *adalah sisi-sisi dari graf G* (Munir, 2012:369).

   Simpul dan sisi yang dilalui di dalam lintasan boleh berulang. Sebuah lintasan dikatakan lintasan sederhana jika semua simpulnya berbeda (setiap sisi yang dilalui hanya satu kali). Lintasan yang berawal dan berakhir pada simpul yang sama disebut lintasan tertutup *(closed path)*, sedangkan lintasan yang tidak berawal dan berakhir pada simpul yang sama disebut lintasan terbuka *(open path)*.

7. **Sirkuit**

   Definisi dari sirkuit adalah sebagai berikut.

   Definisi 2.3.7. *Lintasan yang berawal dan berakhir pada simpul yang sama disebut siklus atau sirkuit* (Munir, 2012:370).

8. **Terhubung *(Connected)***

   Dua buah simpul u dan simpul v dikatakan terhubung jika terdapat

lintasan dari u ke v. Jika dua buah simpul terhubung maka tentu simpul yang pertama dapat dicapai dari simpul yang kedua. Jika setiap pasang simpul di dalam graf dapat terhubung, maka graf tersebut dikatakan graf terhubung. Secara formal, definisi dari graf terhubung adalah sebagai berikut:

Definisi 2.3.8. *Graf tak-berarah G disebut graf terhubung (connected graph) jika untuk setiap pasang simpul u dan v di dalam himpunan V terdapat lintasan dari u ke v (yang juga harus berarti ada lintasan dari v ke u). Jika tidak,maka G disebut graf tak-terhubung (disconnected graph)* (Munir, 2012:371).

9. **Graf Berbobot**

Definisi dari graf berbobot adalah sebagai berikut.

Definisi 2.3.9. *Graf berbobot adalah graf yang setiap sisinya diberi sebuah nilai(bobot)* (Munir, 2012:376).

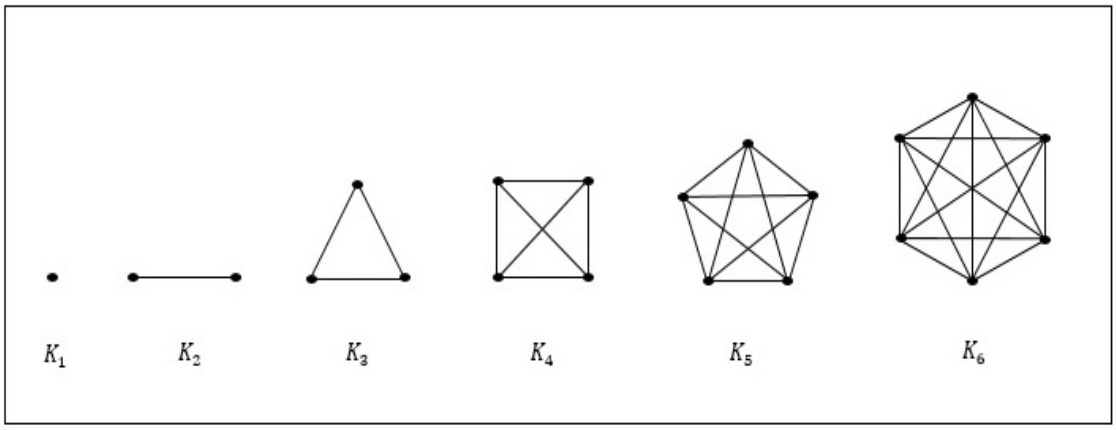
Bobot pada tiap sisi dapat berbeda - beda, bergantung pada masalah yang dimodelkan pada graf tersebut. Bobot dapat menyatakan jarak antara dua buah kota, biaya perjalanan antara dua buah kota, ongkos produksi, dan lain sebagainya. Istilah lain untuk graf berbobot adalah graf berlabel. Namun definisi dari graf berlabel sebenarnya lebih luas lagi. Label tidak hanya diberikan pada sisi, tetapi juga pada simpul. Misalnya pada graf yang memodelkan kota-kota, simpul diberi nama kota-kota, sedangkan label pada sisi menyatakan jarak antara kota-kota.

2.4 Macam-macam Graf

Graf-graf sederhana yang tergolong *well known graph* yang digunakan dalam penelitian ini adalah graf lengkap dan graf bintang. Berikut adalah penjelasan untuk masing - masing graf tersebut.

2.4.1 Graf Lengkap (*Complete Graph*)

Graf lengkap adalah graf sederhana yang setiap simpulnya mempunyai sisi ke simpul lainnya. Graf lengkap dengan n buah simpul dilambangkan dengan K_n. Setiap simpul pada K_n berderajat $n-1$. Gambar 2.5 adalah contoh graf lengkap K_n.

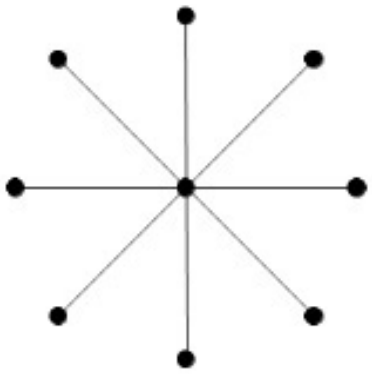


Gambar 2.5: Graf Lengkap K_n, $1 \leq n \leq 6$

Untuk 1 buah simpul terdapat $(n-1)$ buah sisi ke $(n-1)$ simpul lainnya, maka untuk n buah simpul terdapat $n(n-1)$ buah sisi. Karena setiap sisi terhitung dua kali untuk pasangan simpul yang bersisian dengannya, maka jumlah sisi seluruhnya dibagi dua, yaitu $n(n-1)/2$.

2.4.2 Graf Bintang (*Star Gtaph*)

Graf bintang $K_{1,n}$ adalah graf terhubung sederhana yang memiliki $n + 1$ simpul dan n sisi. Satu simpul pada graf bintang disebut simpul pusat berderajat n, sedangkan simpul yang berderajat satu disebut *pendant*. Gambar 2.6 adalah contoh dari graf bintang.



Gambar 2.6: Graf Bintang $K_{1,8}$

2.5 Pelabelan Graf

Pelabelan pada suatu graf adalah sebuah pemetaan atau fungsi yang memasangkan unsur-unsur graf (simpul atau sisi) dengan bilangan (biasanya bilangan positif). Jika domain dari pemetaan adalah simpul, maka pelabelan disebut pelabelan simpul (*vertex labeling*). Jika domainnya adalah sisi, maka disebut pelabelan sisi (*edge labeling*). Jika domainnya adalah simpul dan sisi, maka disebut pelabelan total (*total labeling*).

Misalkan L adalah pelabelan dan Z^+ adalah himpunan bilangan bulat positif, maka,

$L : V \to Z^+$	disebut pelabelan simpul/*vertex labeling*
$L : E \to Z^+$	disebut pelabelan sisi/*edge labeling*
$L : V \cup E \to Z^+$	disebut pelabelan total/*total labeling*

Bobot (*weight*) dari suatu graf dapat dikategorikan ke dalam dua jenis, yaitu bobot sisi (*edge weight*) dan bobot simpul (*vertex weight*). Untuk suatu pelabelan total L, bobot sisi adalah penjumlahan label dari sisi dengan dua simpul yang dihubungkan oleh sisi tersebut (bertetangga). Sedangkan bobot simpul adalah penjumlahan dari label suatu simpul dengan label dari sisi-sisi yang hadir (bersisian) di simpul tersebut.

Secara matematis, bobot simpul dan bobot sisi dapat dituliskan sebagai berikut :

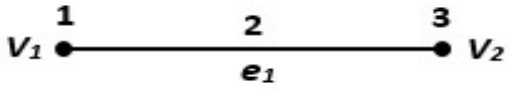
Misal w adalah bobot, L adalah suatu pelabelan total dan $x \leftrightarrow y$ menyatakan terdapat sisi diantara simpul x dan simpul y, sedangkan sisi tersebut dinyatakan dengan xy, maka bobot dari sisi $xy \in E$ adalah

$$w(xy) = L(x) + L(xy) + L(y) \tag{2.1}$$

Sedangkan bobot dari simpul $x \in V$ adalah

$$w(x) = L(x) + \sum_{y \in V : x \leftrightarrow y} L(xy) \tag{2.2}$$

Berikut ini adalah contoh dari bobot sisi :



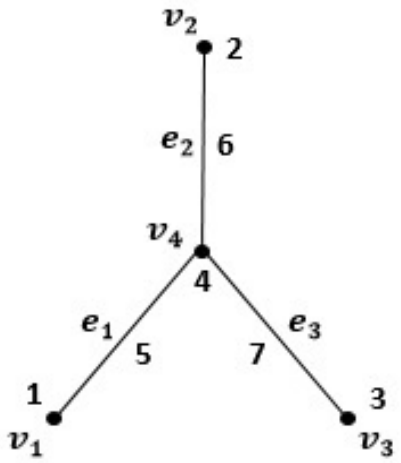
Gambar 2.7: Graf lintasan 2 (P_2)

Menurut gambar di atas, dan L merupakan pelabelan total, maka bobot

dari sisi e_1 adalah

$$w(e_1) = L(v_1) + L(e_1) + L(v_2) = 1 + 2 + 3 = 6$$

Sedangkan, berikut ini adalah contoh dari bobot simpul :



Gambar 2.8: Graf Bintang 3 (S_3)

Dengan menggunakan gambar di atas, dan L merupakan pelabelan total, maka bobot dari simpul v_2 adalah

$$w(v_2) = L(v_2) + L(e_2) = 2 + 6 = 8$$

sedangkan bobot dari simpul v_4 adalah

$$w(v_4) = L(v_4) + L(e_1) + L(e_2) + L(e_3) = 4 + 5 + 6 + 7 = 22$$

Telah dijelaskan mengenai pengertian bobot dari suatu graf. Selanjutnya akan dijelaskan mengenai pelabelan ajaib pada suatu graf.

Definisi 2.5.1. *Misalkan G adalah graf dengan himpunan titik V dan himpunan sisi E.* ***Pelabelan Ajaib*** *(magic labeling) pada graf G adalah pemetaan*

bijektif L dari E ke himpunan bilangan integer positif yang berbeda, sehingga untuk setiap titik $v \in V$, penjumlahan semua label sisi e yang bersisian terhadap titik v adalah sama.

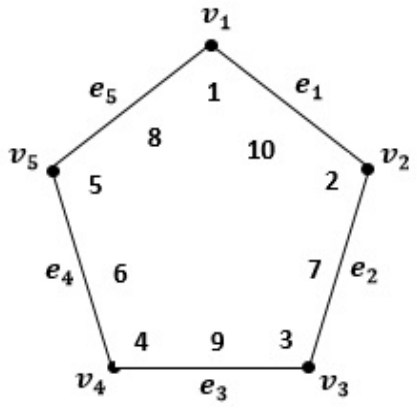
Ada beberapa jenis pelabelan graf pada suatu graf, namun hanya akan dijelaskan mengenai pelabelan total simpul ajaib dan pelabelan total sisi ajaib.

1. Misalkan G adalah graf dengan himpunan simpul V dan himpunan sisi E. Banyak simpul di G adalah v, sedangkan banyak sisi di G adalah e, dan total banyaknya simpul dan busur adalah $v + e$. Pelabelan total simpul ajaib pada graf G adalah pemetaan bijektif dari $V \cup E$, ke suatu himpunan bilangan, misalkan $\{1, 2, 3, ..., v+e\}$, sehingga untuk sebarang simpul x di G berlaku

$$L(x) + \sum_{y \in V : x \leftrightarrow y} L(xy) = k \tag{2.3}$$

Bilangan k yang demikian disebut bilangan ajaib dari graf G.

Berikut diberikan contoh pelabelan total simpul ajaib :



Gambar 2.9: Pelabelan Total Simpul Ajaib Graf K_5

Dari gambar diatas, dapat dihitung bobot dari setiap simpul adalah :

$w(v_1) = 1 + 10 + 8 = 19$ $\quad$ $w(v_4) = 4 + 9 + 6 = 19$

$w(v_2) = 2 + 10 + 7 = 19$ $\quad$ $w(v_5) = 5 + 6 + 8 = 19$

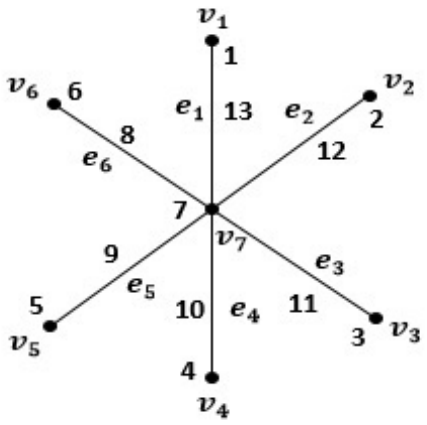
$w(v_3) = 3 + 7 + 9 = 19$

2. Misalkan G adalah graf dengan himpunan simpul V dan himpunan sisi E. Banyak simpul di G adalah v, sedangkan banyak sisi di G adalah e, dan total banyaknya simpul dan sisi adalah $v + e$. Pelabelan total sisi ajaib pada graf G adalah pemetaan bijektif dari $V \cup E$, ke suatu himpunan bilangan, misalkan $\{1, 2, 3, ..., v+e\}$, sehingga untuk sebarang sisi $e = (x, y)$ di G berlaku

$$L(x) + L(xy) + L(y) = k \tag{2.4}$$

Bilangan K yang demikian disebut bilangan ajaib dari graf G.

Berikut diberikan contoh pelabelan total sisi ajaib :



Gambar 2.10: Pelabelan Total Sisi Ajaib pada Graf Bintang 6 (S_6)

Dari gambar 2.10, dapat dihitung bobot dari setiap sisi :

$w(e_1) = 13 + 7 + 1 = 21$ $\quad$ $w(e_4) = 10 + 7 + 4 = 21$

$w(e_2) = 12 + 7 + 2 = 21$ $\quad$ $w(e_5) = 9 + 7 + 5 = 21$

$w(e_3) = 11 + 7 + 3 = 21$ $\quad$ $w(e_6) = 8 + 7 + 6 = 21$

Himpunan kritis pada pelabelan graf G adalah subhimpunan dari posisi label dan label yang bila dilengkapi akan menghasilkan pelabelan graf secara tunggal. Misal diberikan graf G dengan pelabelan λ dikenakan dalam graf tersebut. Dimisalkan pula $Q_\lambda = \{Q_1, Q_2, Q_3, ..., Q_c\}$, pada pelabelan λ, adalah himpunan $Q_i = (j, u_j)$ dengan j menunjukkan posisi dari suatu simpul atau sisi dengan label ajaib k, dan u_j menunjukkan bobot dari simpul atau sisi tersebut. $Q_\lambda(G)$ dikatakan sebuah himpunan kritis untuk pelabelan λ pada graf G jika memenuhi syarat sebagai berikut.

1. $Q_\lambda(G)$ hanya dapat membangun λ pada G.

2. Setiap subset dari $Q_\lambda(G)$ tidak memenuhi sifat (1).

Namun, menentukan himpunan kritis dari suatu pelabelan graf merupakan masalah yang tidak mudah. Hal ini dikarenakan kemungkinan dari subhimpunan label pada graf sangat banyak. Kemudian dari masing-masing subhimpunan tersebut dicari subhimpunan label yang membangun satu-satunya pelabelan dalam graf tersebut.

2.6 Pelabelan Total Sisi Ajaib pada Graf Bintang

Untuk memudahkan pembahasan pada tahap distribusi *share*, graf diberi nomor posisi. Graf ini selanjutnya dinamakan graf posisi. Penomoran posisi pada graf bintang diseragamkan dengan cara berikut ini :

Pertama, beri nomor posisi untuk setiap simpul $\{v_1, v_2, ..., v_{n+1}\}$ dengan bilangan $\{1, 2, ..., n + 1\}$. Posisi 1 diletakkan pada simpul pusat, yaitu simpul

yang bertetangga dengan setiap simpul lainnya. Kemudian, lakukan penomoran sisi sebagai berikut :

Sisi(1,2) diberi nomor posisi $n+2$

Sisi(1,3) diberi nomor posisi $n+3$

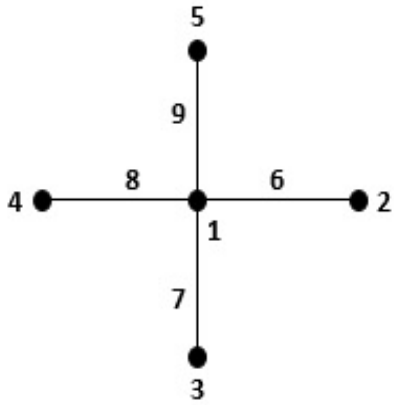
Sisi(1,4) diberi nomor posisi $n+4$

.

.

.

Sisi(1,$n+1$) diberi nomor posisi $2n+1$



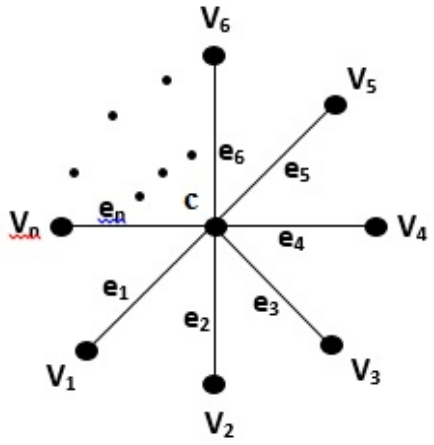
Gambar 2.11: Graf Posisi dari $K_{1,4}$

Gambar 2.11 merupakan contoh dari graf posisi.

Wallis dkk menunjukkan bahwa dalam setiap pelabelan total sisi ajaib pada graf bintang $K_{1,n}$, titik pusat akan mendapat label 1, $n+1$, atau $2n+1$. Jika graf bintang dengan label 1 pada titik pusat, maka nilai $k = 2n+4$, sedangkan jika label titik pusatnya $n+1$, maka nilai $k = 3n+3$, dan jika label titik pusatnya $2n+1$, maka nilai $k = 4n+2$.

Lemma 2.6.1. *Pada pelabelan total sisi ajaib graf bintang, label titik pusatnya adalah* 1, $n+1$, *atau* $2n+1$.

Bukti. Diberikan graf bintang $K_{1,n}$ seperti pada gambar berikut ini.



Gambar 2.12: Graf bintang $K_{1,n}$

Akan dibuktikan bahwa pada pelabelan ajaib suatu graf bintang $K_{1,n}$, label simpul pusat adalah 1, $n+1$, atau $2n+1$.

Misalkan simpul pusat dilabeli dengan x, yaitu $\lambda(c) = x$. Simpul - simpul lainnya dilabeli dengan $1, 2, 3, ..., n$. Sedangkan sisi - sisinya dilabeli dengan $(n+1), (n+2), (n+3), ..., (2n+1)$. Maka

$$kn = (x+1) + (x+2) + ... + (x+n) + (n+1) + (n+2) + ... + (2n+1) \quad (2.5)$$

Karena label simpul pusat x termasuk di antara label simpul $1, 2, 3, ..., n$, maka persamaan diatas menjadi

$$\begin{aligned} kn &= (n-1)x + 1 + 2 + ... + n + (n+1) + (n+2) + ... + (2n+1) \\ &= (n-1)x + \frac{1}{2}(2n+1)(2n+2) \\ &= (n-1)x + (n+1)(2n+1) \\ &= (nx - x) + (n+1)(2n+1) \qquad (2.6) \end{aligned}$$

Reduksi (2.6) dengan modulo n, diperoleh,

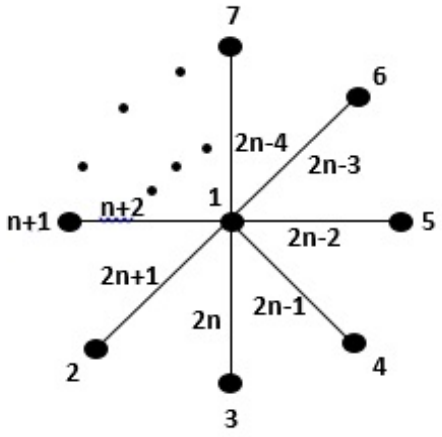
$$x \equiv (n+1)(2n+1) \equiv 1$$

Jadi diperoleh label simpul pusat adalah $1, (n+1)$, atau $(2n+1)$.

Ilustrasi untuk masing - masing label simpul pusat dapat ditunjukkan sebagai berikut.

- Simpul pusat dengan label 1

  Bila simpul pusat diberi label 1, yaitu $\lambda(c) = 1$, maka simpul - simpul lainnya diberi label $2, 3, 4, ..., n+1$. Kemudian untuk label sisi, dicari bobot sisi yang maksimum diantara sisi - sisi yang lainnya, dan sisi tersebut diberi label $n+2$. Selanjutnya dicari kembali bobot sisi yang maksimum diantara sisi - sisi lainnya yang belum diberi label, dan sisi tersebut diberi label $n+3$. Langkah ini dilakukan berulang sampai semua sisi memiliki label. Dalam hal ini, pelabelan total sisi yang dapat diperoleh untuk masing - masing sisi adalah sama, yaitu $2n+4$. Sehingga diperoleh bilangan ajaib yaitu $2n+4$. Gambar 2.13 adalah contoh graf bintang $K_{1,n}$ dengan $\lambda(c) = 1$.

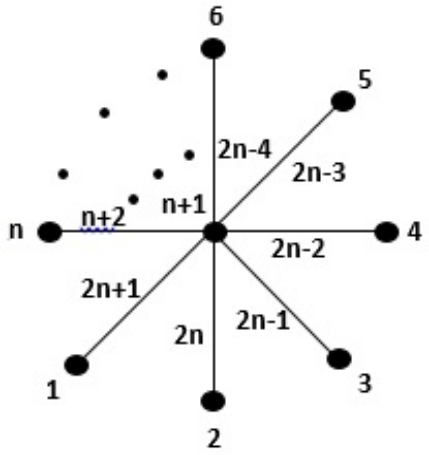


Gambar 2.13: Graf bintang $K_{1,n}$ dengan $\lambda(c) = 1$

- Simpul pusat dengan label $n+1$

  Bila simpul pusat diberi label $n+1$, yaitu $\lambda(c) = n+1$, maka simpul -

simpul lainnya diberi label $1, 2, 3, ..., n$. Kemudian untuk label sisi, dicari bobot sisi yang maksimum diantara sisi - sisi lainnya, dan sisi tersebut diberi label $n+2$. Selanjutnya dicari kembali bobot sisi yang maksimum diantara sisi - sisi lainnya yang belum diberi label, dan sisi tersebut diberi label $n+3$. Langkah ini dilakukan berulang sampai semua sisi memiliki label. Dalam hal ini, pelabelan total sisi yang diperoleh untuk masing - masing sisi adalah sama yaitu $3n+3$. Sehingga diperoleh bilangan ajaib yaitu $3n+3$. Gambar 2.14 adalah contoh graf bintang $K_{1,n}$ dengan $\lambda(c) = n+1$.

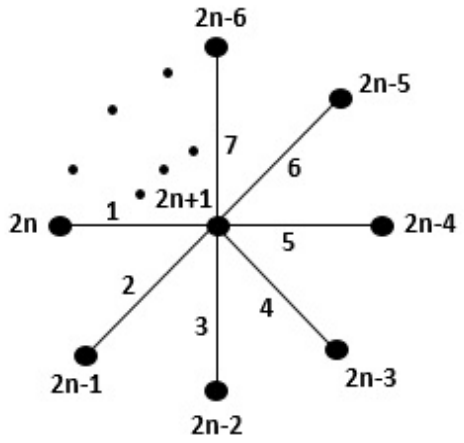


Gambar 2.14: Graf bintang $K_{1,n}$ dengan $\lambda(c) = n+1$

- Simpul pusat dengan label $2n+1$

  Bila simpul pusat diberi label $2n+1$, yaitu $\lambda(c) = 2n+1$, maka simpul - simpul lainnya diberi label $2n-1$, $2n-2$, $2n-3$,...,$2n$. Kemudian untuk label sisi, dicari bobot sisi yang minimum diantara sisi - sisi lainnya, dan sisi tersebut diberi label n. Selanjutnya dicari kembali bobot sisi yang minimum diantara sisi - sisi lainnya yang belum diberi label, dan sisi tersebut diberi label $n-1$. Langkah ini dilakukan berulang sampai semua

sisi memiliki label. Dalam hal ini, pelabelan total sisi yang diperoleh untuk masing - masing sisi adalah sama yaitu $4n+2$. Sehingga diperoleh bilangan ajaib yaitu $4n + 2$.



Gambar 2.15: Graf bintang $K_{1,n}$ dengan $\lambda(c) = 2n + 1$

Berdasarkan penjelasan diatas maka terbukti bahwa pelabelan ajaib pada gaf bintang, label titik pusatnya adalah 1, $n + 1$, dan $2n + 1$. □

2.7 Interpolasi

2.7.1 Interpolasi

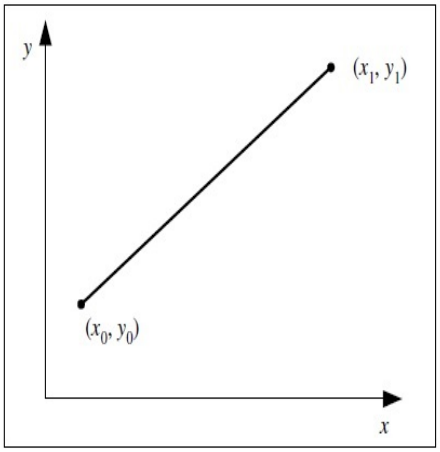
Interpolasi adalah proses pencarian dan perhitungan nilai suatu fungsi yang grafiknya melewati sekumpulan titik yang diberikan. Titik-titik tersebut mungkin merupakan hasil eksperimen dalam sebuah percobaan, atau diperoleh dari suatu fungsi yang diketahui. Fungsi interpolasi biasanya dipilih dari sekelompok fungsi tertentu, salah satunya adalah fungsi polinom. Fungsi polinom banyak digunakan karena mudah untuk dihitung nilainya, diturunkan dan diintegralkan.

2.7.2 Interpolasi Linier

Interpolasi linier adalah interpolasi antara dua buah titik dan sebuah garis lurus. Misal diberikan dua buah titik, (x_0, y_0) dan (x_1, y_1). Polinom yang menginterpolasi kedua titik itu adalah persamaan garis lurus yang berbentuk

$$p_1(x) = a_0 + a_1(x) \tag{2.7}$$

Gambar 2.16 memperlihatkan garis lurus yang menginterpolasi titik (x_0, y_0)



Gambar 2.16: Interpolasi Linier

dan (x_1, y_1).

Koefisien a_0 dan a_1 diperoleh dengan menggunakan proses substitusi dan eliminasi. Dengan mensubstitusikan (x_0, y_0) dan (x_1, y_1) ke dalam persamaan (2.7) diperoleh persamaan linier sebagai berikut.

$$y_0 = a_0 + a_1 x_0$$
$$y_1 = a_0 + a_1 x_1$$

Kedua persamaan ini kemudian dieliminasikan sehingga didapat

$$a_1 = \frac{y_1 - y_0}{x_1 - x_0} \tag{2.8}$$

dan

$$a_0 = \frac{x_1 y_0 - x_0 y_1}{x_1 - x_0} \tag{2.9}$$

Substitusikan persamaan (2.8) dan persamaan (2.9) ke dalam persamaan (2.7) sehingga diperoleh persamaan garis lurus

$$p_1(x) = \frac{x_1 y_0 - x_0 y_1}{(x_1 - x_0)} + \frac{(y_1 - y_0)x}{(x_1 - x_0)} \tag{2.10}$$

Dengan menggunakan manipulasi aljabar, persamaan (2.10) dapat disederhanakan menjadi

$$p_1(x) = y_0 + \frac{(y_1 - y_0)}{(x_1 - x_0)}(x - x_0) \tag{2.11}$$

Bukti.

$$\begin{aligned}
p_1(x) &= \frac{x_1 y_0 - x_0 y_1}{(x_1 - x_0)} + \frac{(y_1 - y_0)x}{(x_1 - x_0)} \\
p_1(x) &= \frac{x_1 y_0 - x_0 y_1 + x y_1 - x y_0}{(x_1 - x_0)} \\
p_1(x) &= \frac{x_1 y_0 - x_0 y_1 + x y_1 - x y_0 + x_0 y_0 - x_0 y_0}{(x_1 - x_0)} \\
p_1(x) &= \frac{(x_1 - x_0)y_0 + (y_1 - y_0)(x - x_0)}{(x_1 - x_0)} \\
p_1(x) &= y_0 + \frac{(y_1 - y_0)}{(x_1 - x_0)}(x - x_0)
\end{aligned}$$

□

Persamaan (2.11) adalah persamaan garis lurus yang melalui dua buah titik, (x_0, y_0) dan (x_1, y_1). Kurva polinom ini berupa garis lurus (Gambar 2.16).

2.7.3 Interpolasi Polinom Lagrange

Perhatikan kembali interpolasi linier pada persamaan (2.11) :

$$p_1(x) = y_0 + \frac{(y_1 - y_0)}{(x_1 - x_0)}(x - x_0)$$

Persamaan di atas dapat disederhanakan menjadi

$$p_1(x) = y_0\frac{(x-x_1)}{(x_0-x_1)} + y_1\frac{(x-x_0)}{(x_1-x_0)} \tag{2.12}$$

Atau dapat dinyatakan dalam bentuk

$$p_1(x) = a_0L_0(x) + a_1L_1(x) \tag{2.13}$$

yang dalam hal ini,

$$\begin{aligned} a_0 &= y_0 \quad , \qquad L_0(x) = \tfrac{(x-x_1)}{(x_0-x_1)} \\ a_1 &= y_1 \quad , \qquad L_1(x) = \tfrac{(x-x_0)}{(x_1-x_0)} \end{aligned}$$

Persamaan (2.10) disebut polinomial Lagrange berderajat 1.

Bentuk umum polinomial Lagrange dengan derajat kurang dari sama dengan n untuk $(n+1)$ titik berbeda adalah

$$p_n(x) = \sum_{i=0}^{n} a_iL_i(x) = a_0L_0(x) + a_1L_1(x) + ... + a_nL_n(x) \tag{2.14}$$

yang dalam hal ini,

$$a_i = y_i \quad , \quad i = 0, 1, 2, ..., n$$

dan,

$$L_i(x) = \prod_{\substack{j=0 \\ j\neq i}}^{n} \frac{(x-x_j)}{(x_i-x_j)} = \frac{(x-x_0)(x-x_1)...(x-x_{i-1})(x-x_{i+1})...(x-x_n)}{(x_i-x_0)(x_i-x_1)...(x_i-x_{i-1})(x_i-x_{i+1})...(x_i-x_n)} \tag{2.15}$$

Mudah dibuktikan bahwa,

$$L(x_i) = \begin{cases} 1, & \text{i } = \text{ j;} \\ 0, & \text{i } \neq \text{ j} \end{cases} \tag{2.16}$$

dan polinom interpolasi p_nx melalui setiap titik.

Bukti. Jika $i = j$, maka

$$L_i(x) = \prod_{\substack{j=0 \\ j\neq i}}^{n} \frac{(x_i - x_j)}{(x_i - x_j)} = \frac{(x_i - x_0)(x_i - x_1)...(x_i - x_{i-1})(x_i - x_{ii+1})...(x_i - x_n)}{(x_i - x_0)(x_i - x_1)...(x_i - x_{i-1})(x_i - x_{i+1})...(x_i - x_n)}$$

$$= 1 \qquad \text{(pembilang = penyebut)}$$

Jika $i \neq j$, maka

$$\begin{aligned} L_i(x_j) &= \prod_{\substack{j=0 \\ j\neq i}}^{n} \frac{(x_j - x_i)}{(x_i - x_j)} \\ &= \frac{(x_j - x_0)(x_j - x_1)...(x_j - x_j)...(x_j - x_{i-1})(x_j - x_{i+1})...(x_j - x_n)}{(x_i - x_0)(x_i - x_1)...(x_i - x_j)...(x_i - x_{i-1})(x_i - x_{i+1})...(x_i - x_n)} \\ &= \frac{0}{(x_i - x_0)(x_i - x_1)...(x_i - x_j)...(x_i - x_{i-1})(x_i - x_{i+1})...(x_i - x_n)} \\ &= 0 \end{aligned}$$

Akibatnya,

$$\begin{aligned} p_n(x_0) &= L_0(x_0)y_0 + L_1(x_0)y_1 + L_2(x_0)y_2 + ... + L_n(x_0)y_n \\ &= 1.y_0 + 0.y_1 + 0.y_2 + ... + 0.y_n \\ &= y_0 \\ &= p_n(x_1) = y_1 \\ &... \\ p_n(x_n) &= y_n \end{aligned}$$

Dengan demikian,

$$p_n(x_n) = y_i, \qquad i = 0, 1, 2, ..., n$$

Atau dengan kata lain, polinom interpolasi $p_n(x)$ melalui setiap titik data. □

2.8 Aritmatika Modulo

Aritmetika modulo memainkan peranan penting pada aplikasi ilmu kriptografi. Operator yang digunakan pada aritmetika modulo adalah mod. Opera-

tor mod memberikan sisa pembagian. Misalnya 23 dibagi 5 memberikan hasil = 4 dan sisa = 3, sehingga kita tulis 23 mod= 3. Definisi dari operator mod dinyatakan sebagai berikut.

Definisi 2.8.1. *Misalkan a adalah bilangan bulat dan m adalah bilangan bulat yang lebih besar dari* 0. *Operasi* $a \bmod m$ *(dibaca a modulo m) memberikan sisa jika a dibagi dengan m. Dengan kata lain,* $a \bmod m = r$ *sedemikian sehingga* $a = mq + r$, *dengan* $0 \leq r < m$ (Munir, 2012:191).

2.8.1 Kongruen

Misalkan a dan b adalah suatu bilangan bulat. Jika m suatu bilangan bulat positif yang lebih besar dari 1, maka a dikatakan kongruen dengan b modulo m (ditulis $a \equiv b(\mathrm{mod} m)$), jika m membagi habis $(a - b)$. Selain itu, a dikatakan kongruen dengan b modulo m, jika $(a - b)$ adalah kelipatan modulo m. Jadi, $a \equiv b(\mathrm{mod} m) \rightarrow a - b = km$

Teorema 2.8.1. Kekongruenan memiliki sifat :

1. Jika $a \equiv b(\mathrm{mod} m)$, maka $b \equiv a(\mathrm{mod} m)$
2. Jika $a \equiv b(\mathrm{mod} m)$ dan $b \equiv c(\mathrm{mod} m)$, maka $a \equiv c(\mathrm{mod} m)$
3. Jika $a \equiv b(\mathrm{mod} m)$, maka $ka \equiv kb(\mathrm{mod} m)$, untuk $k \in Z$

Bukti. 1. $a \equiv b(\mathrm{mod} m)$, berarti:

$\Leftrightarrow a = b + km$

$\Leftrightarrow a - b = km$

$\Leftrightarrow -b = -a + km$

$\Leftrightarrow b = a + (-k)m$ (kedua ruas dikalikan -1)

$\Leftrightarrow b = a + Km$

$\Leftrightarrow b \equiv a \bmod m$

2. $a \equiv b(\mathrm{mod}m) \quad \Leftrightarrow \quad a = b + k_1 m$

   $b \equiv c(\mathrm{mod}m) \quad \Leftrightarrow \quad b = c + k_2 m$

   Substitusikan, maka

   $\Leftrightarrow a = c + k_1 m + k_2 m$

   $\Leftrightarrow a = c + (k_1 + k_2)m$

   $\Leftrightarrow a = c + Km \qquad (K = k_1 + k_2)$

   $\Leftrightarrow a \equiv c(\mathrm{mod}m)$

3. $a \equiv b(\mathrm{mod}m)$

   $\Leftrightarrow a = b + k_1 m$

   $\Leftrightarrow ka = kb + kk_1 m \qquad$ (masing-masing ruas dikalikan $k, k \in Z$)

   $\Leftrightarrow ka = kb + Km \qquad (K = k + k_1)$

   $\Leftrightarrow ka \equiv kb(\mathrm{mod}m)$, untuk $k \in Z$

□

Didefinisikan Z_n sebagai himpunan semua kelas kongruen modulo n, yaitu

$$Z_n = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\}$$

Perhatikan bahwa Z_n tidaklah sama dengan Z, akan tetapi untuk setiap integer anggota Z memiliki kongruensi dengan salah satu dari $\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}$. Sebagai contoh, pada $Z_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$. $\overline{0} = \overline{4}$, karena $4(\mathrm{mod}4) = 0$, sehingga

Selanjutnya didefinisikan operasi penjumlahan pada Z_n. Untuk setiap $\overline{a}, \overline{b} \in Z_n$, $\overline{a} + \overline{b} = \overline{a+b}$.

Contoh 2.8.1. $Z_{12} = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{11}\}$.

1. $\overline{3} + \overline{7} = \overline{10}$.

2. $\overline{4} + \overline{11} = \overline{15} = \overline{3}$.

2.9 Skema Pembagian Data Rahasia

Konsep kriptografi lahir sejak jaman Mesir Kuno, kira - kira 400 tahun yang lalu, dalam bentuk hieroglyph walaupun masih dalam bentuk standar. Kriptografi kemudian berkembang hingga jaman Romawi Kuno, dimana pemimpin perang mengirimkan pesan rahasia yang bernama Scytale untuk digunakan tentara Sparta. Konsep kriptografi pun semakin berkembang seiring berjalannya waktu dan kebutuhan yang semakin kompleks. Orientasi konsep kriptografi pun berubah. Kriptografi klasik lebih menitikberatkan kekuatan pada kerahasiaan algoritma yang dipakai (apabila algoritma yang digunakan terpecahkan maka isi pesan rahasia dapat diketahui oleh siapa saja yang mengetahui algoritma tersebut). Sedangkan kriptografi modern lebih menitikberatkan pada kerahasiaan kunci (*key*) untuk membuka algoritma tersebut.

Secara umum, kriptografi terdiri dari empat komponen, yaitu *Plaintext*, *Ciphertext*, Enkripsi, dan Dekripsi. *Plaintext* merupakan pesan asli yang akan dikirimkan. *Ciphertext* merupakan pesan tersandi yang merupakan hasil enkripsi. Enkripsi merupakan proses pengubahan dari *Plaintext* ke *Ciphertext*. Sedangkan dekripsi adalah mengubah *Ciphertext* menjadi *Plaintext*.

Salah satu turunan ilmu kriptografi untuk menjaga kerahasiaan data adalah Pembagian Data Rahasia. Gagasan skema Pembagian data rahasia pertama kali diperkenalkan oleh Shamir dan Blackley secara terpisah pada tahun 1979. *Secret Sharing* merupakan suatu cara untuk membagi suatu rahasia menjadi beberapa komponen yang disebut *shares* atau data rahasia, kepada beberapa orang yang biasa disebut partisipan, dengan aturan tertentu. Aturan yang dimaksud adalah struktur akses, yaitu aturan tentang siapa saja yang mendapat otoritas untuk membentuk berita rahasia itu kembali. Berita rahasia yang dimaksud lebih khusus adalah hasil suatu proses enkripsi. Dalam setiap

kelompok berlaku terdapat nilai ambang batas minimal (*threshold value*), yaitu jumlah minimal partisipan yang dibutuhkan dalam suatu kelompok untuk merekonstruksikan suatu data rahasia .

Secara matematis, pembagian data rahasia adalah suatu metode untuk membagi sebuah rahasia S kepada anggota-anggota himpunan terhingga P, yang terdiri dari $P_1, P_2, ..., P_n$ sedemikian sehingga jika partisipan pada subhimpunan $A \subseteq P$ yang memenuhi syarat untuk mengetahui rahasia, kemudian mereka bersama-sama mengumpulkan potongan informasi rahasia yang mereka miliki, maka mereka dapat merekonstruksikan rahasia S. Sedangkan jika partisipan pada subhimpunan $B \subset P$, yang tidak memenuhi syarat untuk memenuhi rahasia, bersama-sama mengumpulkan potongan informasi rahasia, maka mereka tidak dapat merekonstruksikan rahasia S. Kunci S dipilih oleh seorang partisipan D yang disebut *dealer*, dan biasanya diasumsikan bahwa $D \notin P$. *Dealer* membagi rahasia S dengan memberi potongan informasi yang disebut *share* kepada setiap partisipan.

Sebuah struktur akses Γ adalah kumpulan dari semua subhimpunan partisipan yang dapat merekonstruksikan rahasia, atau $\Gamma = \{A|A \subseteq P\}$. Himpunan-himpunan dari P yang termasuk dalam struktur akses disebut himpunan kuasa, sedangkan yang tidak termasuk dalam struktur akses disebut bukan himpunan kuasa.

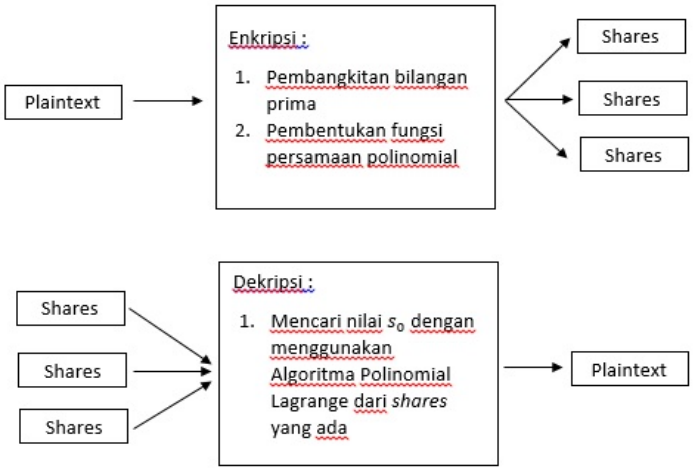
Skema pembagian data rahasia dikatakan sempurna jika untuk setiap partisipan dalam $B \subset P$, dimana B adalah bukan himpunan kuasa, bersama-sama mengumpulkan informasi rahasia yang dimilikinya, maka mereka tidak dapat merekonstruksikan rahasia tersebut. Misalkan terdapat sejumlah k $(1 < k \leq n)$ partisipan. Skema ambang batas (k, n) adalah metode membagi informasi rahasia di antara satu himpunan partisipan P, sedemikian sehingga setiap subhimpunan partisipan $k \in A \subseteq P$, dengan $A \geq t$ maka partisipan

dalam himpunan A tersebut dapat merekonstruksikan kunci, sedangkan jika $A < t$ maka partisipan tersebut tidak dapat merekonstruksikan kunci.

2.9.1 Skema Ambang Batas Shamir

Skema ambang batas Shamir ditemukan oleh Adi Shamir. Skema ambang batas digambarkan secara matematis dalam bentuk interpolasi polinomial untuk mencari bentuk kurva dari suatu fungsi polinomial dengan derajat paling tinggi $t-1$. Informasi data rahasia yang akan dicari dianalogikan sebagai fungsi polinomial tersebut, sedangkan data rahasia yang telah dibagi-bagi adalah beberapa titik kordinat dari fungsi tersebut. Dengan skema ini, n-titik kordinat tersebut dibagikan pada n orang yang berbeda sedemikian sehingga diperlukan sebanyak t orang, dimana $t < n$, untuk merekonstruksi bentuk kurva atau fungsi polinomial ini dengan menggunakan interpolasi Lagrange. Untuk selanjutnya, Skema Ambang Batas Shamir kita sebut Skema Shamir.

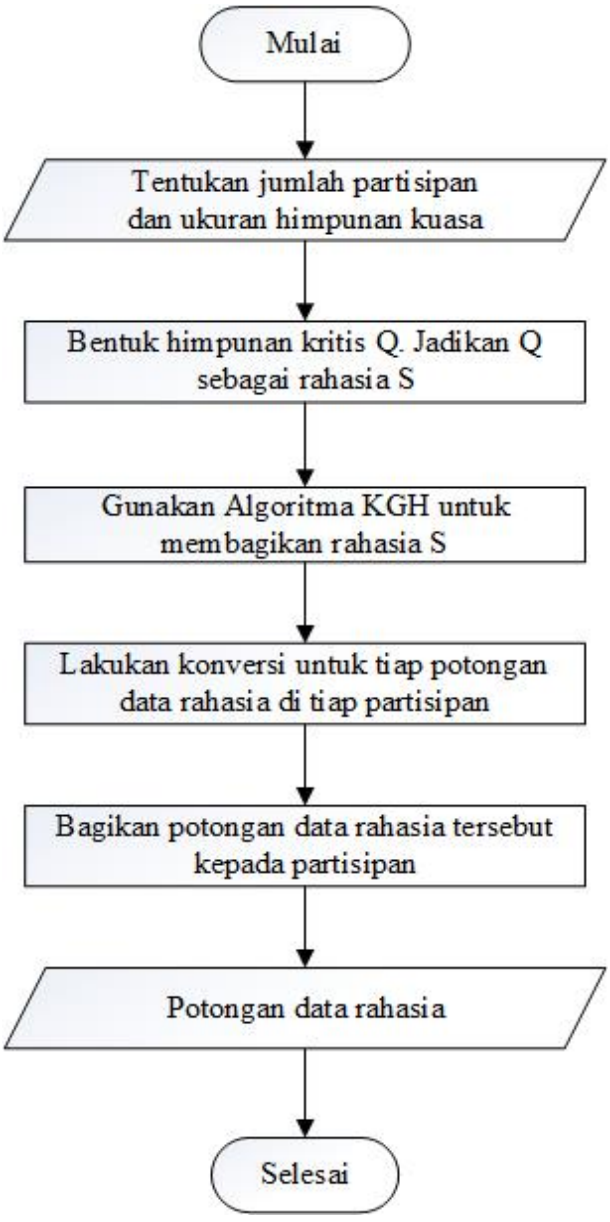
Subhimpunan-subhimpunan yang merupakan kombinasi dari t orang yang dapat merekonstruksi data rahasia tersebut disebut himpunan kuasa dan subhimpunan dari himpunan kuasa disebut struktur akses, sedangkan titik-titik kordinat yang dibagi kepada n orang yang berbeda disebut potongan data rahasia. Data rahasia, dalam hal ini fungsi polinomial, aman karena sembarang $t-1$ orang atau kurang tidak dapat merekonstruksi data rahasia tersebut.



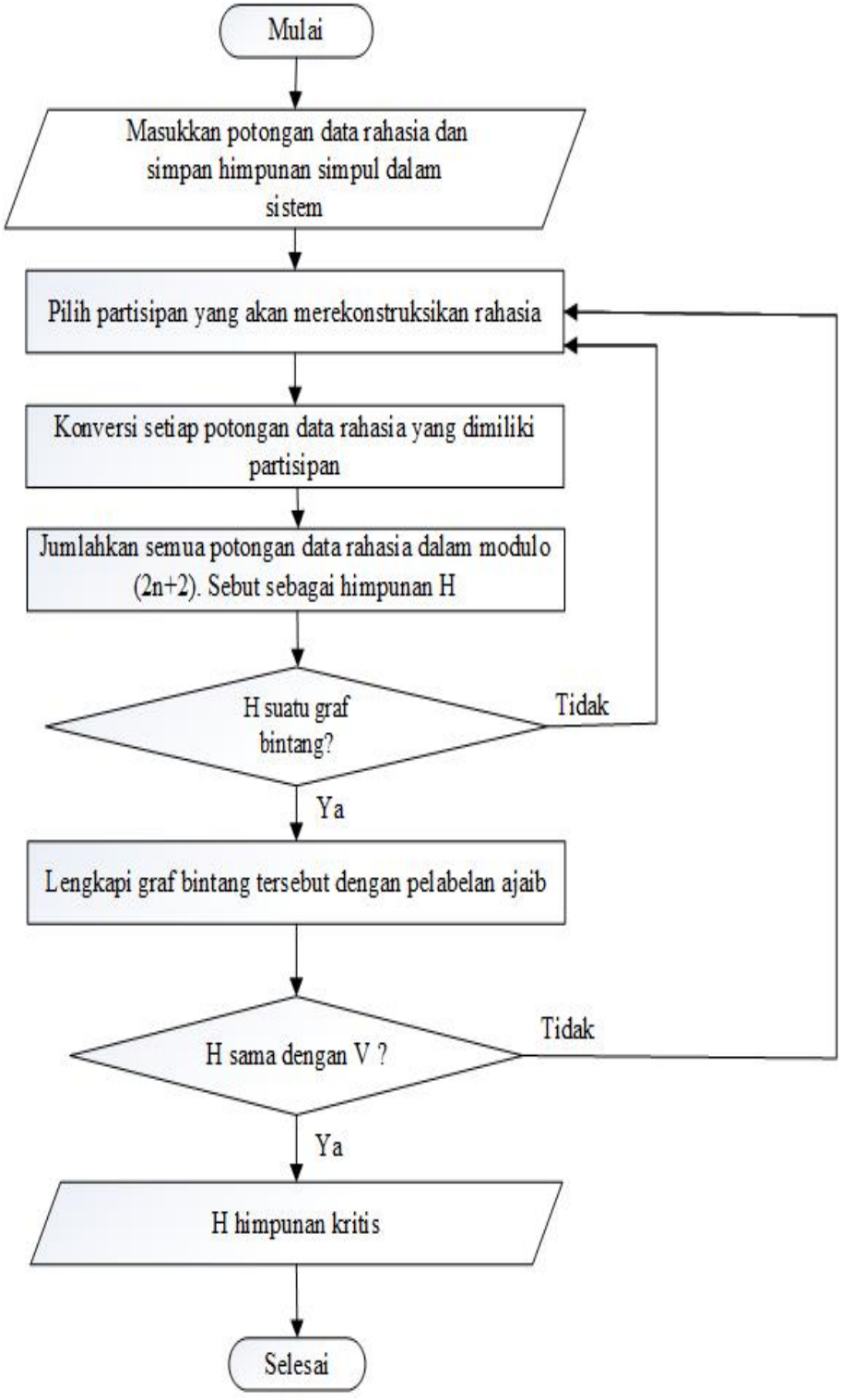
Gambar 2.17: Gambaran Umum Skema *Threshold Shamir's*

2.10 Diagram Alir

Berikut ini adalah diagram alur dari permasalah yang akan dikaji.



Gambar 2.18: Diagram Alir Membagikan Data Rahasia



Gambar 2.19: Diagram Alir Merekonstruksikan Data Rahasia

BAB III

PEMBAHASAN

Konsktruksi skema pembagian rahasia dapat dilakukan dengan menggunakan beberapa cara, yaitu polinomial, *latin square*, dan pelabelan total ajaib pada suatu graf. Pada bab ini akan dijelaskan konsktruksi skema pembagian rahasia menggunakan pelabelan total sisi ajaib pada graf bintang dan polinomial serta kelebihan dan kekurangan diantara dua metode tersebut.

3.1 Skema Pembagian Rahasia dengan Satu Pusat

Dimisalkan $P = (P_1, P_2, P_3, P_4, ..., P_n)$ adalah himpunan dari semua partisipan yang ada, yang biasa disebut dengan himpunan bagian, yaitu subhimpunan dari P dimana kombinasi t partisipan, dengan $t < n$, secara bersama-sama dengan menggunakan data rahasia masing-masing yang dimiliki dapat merekonstruksikan rahasia. Jika nilai $t = 4$, maka kombinasi $\{P_1, P_2, P_4, P_5\}$, $\{P_1, P_3, P_5, P_6\}, \{P_2, P_4, P_5, P_6\}$, dan kombinasi lainnya yang terdiri dari empat partisipan merupakan himpunan kuasa. Kumpulan dari himpunan kuasa disebut dengan struktur akses, dan dalam skripsi ini struktur akses yang digunakan adalah yang berukuran sama, yaitu dimana banyaknya elemen pada setiap himpunan kuasa adalah sama.

Suatu skema pembagian data rahasia dengan suatu pusat adalah skema pembagian data rahasia yang memiliki satu partisipan yang disebut pusat, yaitu S, sehingga $P = (S, P_1, P_2, P_3, P_4, ..., P_n)$. Contoh graf yang memiliki

pusat adalah graf bintang, graf kipas, dan graf roda. Pada sub-bab berikutnya akan dibahas mengenai skema pembagian data rahasia dengan menggunakan graf bintang.

3.2 Algoritma Karnin-Greene-Hellman (KGH)

Misalkan $P = \{P_1, P_2, ..., P_r\}$ adalah himpunan dari semua partisipan yang ada, dan $\Gamma = \{A_1, A_2, ..., A_t\}$ adalah sebuah struktur akses dengan t himpunan kuasa dari P. Dimisalkan pula $Q = \{Q_1, Q_2, ..., Q_c\}$ merupakan himpunan kritis dari pelabelan ajaib pada graf bintang dengan sisi n yang menjadi rahasia S. Untuk setiap himpunan kuasa A_j, $1 \leq j \leq t$, dengan banyaknya anggota adalah w, *dealer* menggunakan algoritma Karnin-Greene-Hellman (KGH) untuk membagikan data rahasia kepada partisipan.

Tahap Awal

1. Untuk setiap partisipan a_u, $1 \leq u \leq w-1$, seorang *dealer* memilih (secara acak dan bebas) c pasang (x_{uv},y_{uv}), $1 \leq v \leq c$, dari semua nilai yang mungkin pada (Z_{2n+2}, Z_{2n+2}).

2. *Dealer* membagikan sebuah potongan data rahasia untuk partisipan terakhir, a_w, yang saling berkorespondensi untuk setiap $Q_i = (x_i, y_i)$, $1 \leq i \leq c$, menggunakan rumus

$$(x_{wv}, y_{wv}) = (x_i, y_i) - \sum_{u=1}^{w-1} (x_{uv}, y_{uv}) \tag{3.1}$$

   Untuk setiap $1 \leq v \leq c$, dimana perhitungan tersebut memenuhi syarat Z_{2n+2}.

3. *Dealer* membagikan potongan-potongan data rahasia tersebut kepada partisipan secara rahasia.

Singkatnya, jika partisipan dari sebuah himpunan kuasa menyatukan potongan data rahasia (dengan menambahkan korespondensi data rahasia pada Z_{2n+2}), mereka dapat merekonstruksikan himpunan kritis. Dengan demikian, tahap rekonstruksi dapat dikerjakan.

3.3 Skema Algoritma KGH

Akan digunakan algoritma Karnin-Greene-Hellman (KGH) sebagai cara utama untuk membagikan data rahasia dan juga untuk merekonstruksikannya kembali. Selain itu, akan dilakukan pula modifikasi pada algoritma itu untuk meningkatkan keamanan data rahasia. Modifikasi yang penulis lakukan adalah membuat konversi dari bilangan asli ke huruf kapital untuk setiap potongan data rahasia yang dimiliki partisipan, dengan ketentuan sebagai berikut.

Metode Konversi

Untuk setiap bilangan asli yang nilainya lebih dari 9, kita melakukan konversi:

10	menjadi	A
11	menjadi	B
.	...	.
.	...	.
35	menjadi	Z

Dengan demikian, setiap potongan data rahasia memuat bilangan asli $(0, 1, ..., 9)$ dan huruf kapital.

3.3.1 Algoritma KGH untuk Pembagian Data Rahasia

Berikut ini adalah algoritma KGH untuk merekonstruksikan kembali data rahasia.

Masukan :

- r : jumlah partisipan
- w : ukuran dari himpunan kuasa

Langkah-langkah :

1. Bentuklah himpunan kritis Q, dengan memilih posisi dan labelnya (simpul atau sisi atau keduanya) secara acak. Q harus memenuhi syarat untuk sebuah himpunan kritis. Dimisalkan Q menjadi rahasia S.
2. Gunakan algoritma KGH untuk membagikan S.
   (a) Buatlah potongan data rahasia awal untuk $w-1$ partisipan, dari semua nilai yang mungkin pada Z_{36}.
   (b) Hitunglah potongan data rahasia untuk partisipan terakhir dengan menggunakan persamaan (3.1) pada modulo $(2n+2)$.
3. Lakukan konversi untuk setiap potongan data rahasia di tiap partisipan.
4. Bagikan potongan data rahasia tersebut kepada partisipan.

Hasil Akhir: Potongan data rahasia.

3.3.2 Algoritma KGH untuk Rekonstruksi Data Rahasia

Sebelumnya telah dijabarkan algoritma untuk membagikan data rahasia. Berikut ini akan dijabarkan algoritma untuk merekonstruksikan data rahasia.

Masukan :

- s_i : potongan data rahasia
- V : himpunan dari posisi dan label simpul pada graf bintang tanpa simpul pusat (*)
  Catatan : (*) berarti informasi tersebut disimpan oleh sistem.

Langkah-langkah :

1. Pilihlah partisipan yang akan merekonstruksikan rahasia tersebut. Pemilihan dilakukan secara bebas dan acak.

2. Lakukan konversi untuk setiap potongan data rahasia yang dimiliki tiap partisipan.

3. Jumlahkan semua potongan data rahasia dalam modulo $(2n+2)$, kemudian hasilnya adalah sebuah himpunan, dinamakan H.

4. Jika H tidak memenuhi kondisi yang memungkinkan dalam suatu graf maka H tidak bisa menjadi suatu rahasia, sehingga kembali ke langkah 1. Jika memenuhi syarat, maka dilanjutkan ke langkah berikutnya.

5. Selidiki apakah H dapat menjadi rahasia S atau tidak menggunakan cara berikut ini :

   (a) Cocokan H pada graf bintang S_n, lalu lengkapi menjadi pelabelan total sisi ajaib pada graf bintang dengan semua nilai label yang mungkin pada simpul pusat dan semua nilai yang mungkin untuk nilai ajaib k.

   (b) Jika H sama dengan V, maka H dapat menjadi rahasia himpunan kritis. Jika tidak , maka kembali ke langkah 1.

Hasil Akhir: Rahasia dapat dipecahkan atau tidak.

3.3.3 Contoh Kasus

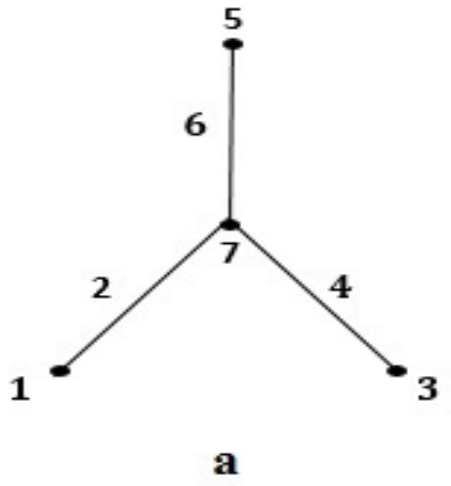
Untuk lebih memahami algoritma KGH yang telah dijabarkan, akan dijelaskan sebuah contoh kasus. Akan dilakukan dua macam pengerjaan, yaitu membagikan data rahasia dan merekonstruksikan data rahasia.

1. **Membagi data rahasia**

   Membagi data rahasia akan dikerjakan sesuai langkah-langkah pada algoritma yang sudah dijelaskan pada paparan sebelumnya.

   (a) Memilih himpunan kritis

   Carilah sebuah himpunan kritis Q, dengan cara memilih posisi dan label pada graf. Q harus memenuhi syarat untuk menjadi sebuah himpunan kritis. Kita anggap Q menjadi rahasia S. Pada kasus ini, akan dipilih himpunan kritis $Q_1 = \{(1,7),(3,3),(5,5)\}$.



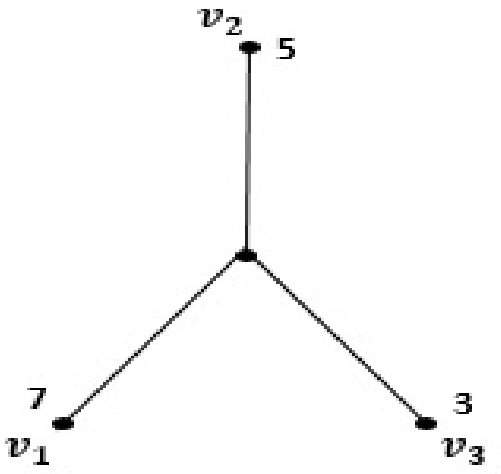
Gambar 3.1: (a) Posisi Graf Bintang

   Gambar 3.1 merupakan gambar posisi graf bintang, sedangkan Gambar 3.2 merupakan graf untuk himpunan kritis Q_1.

   (b) Algoritma KGH

   Tahap selanjutnya adalah menggunakan algoritma KGH yang sudah dijabarkan pada subbab sebelumnya.

   Langkah pertama dalam pengerjaan algoritma KGH adalah menentukan atau membagikan potongan data rahasia awal kepada $w-1$



Gambar 3.2: Himpunan Kritis Q_1

partisipan, dengan menggunakan semua nilai yang mungkin dalam Z_{36}. Perlu ditentukan terlebih dahulu, berapa partisipan yang akan mendapatkan potongan data rahasia dan berapa ambang batas minimal partisipan yang dapat mereknostruksikan rahasia. Pada contoh kasus ini, dipilih 6 orang partisipan, dengan ketentuan hanya 3 orang partisipan yang dapat merekonstruksikan kembali rahasia tersebut. Semakin banyak jumlah partisipan, maka kemungkinan untuk memecahkan kode rahasia tersebut semakin sulit, begitu pula sebaliknya.

Dikarenakan terdapat 6 orang partisipan dan hanya 3 orang partisipan yang dapat merekonstruksikan rahasia, maka banyaknya himpunan kuasa yang mungkin untuk merekonstruksikan kembali rahasia tersebut adalah kombinasi dari jumlah partisipan dan jumlah partisipan yang mungkin untuk merekonstruksikan rahasia. Oleh karena itu, terdapat 20 himpunan kuasa yang mungkin. Pemilihan anggota dari tiap himpunan kuasa dipilih secara acak dan bebas,

asalkan tidak ada pengulangan himpunan kuasa yang sama.

Misalkan dipilih secara acak himpunan kuasa, yaitu $A_4 = \{P_2, P_5, P_6\}$. Langkah selanjutnya adalah membagikan potongan data rahasia. Sebelum menentukan potongan data rahasia bagi tiap partisipan, diberikan penomeran indeks baru untuk tiap partisipan. Ini dilakukan agar tidak terjadi kekeliruan, karena belum tentu himpunan kuasa yang dipilih berisikan partisipan dengan indeks yang urut, sehingga perlu diberikan penomeran indeks yang baru. Untuk kasus ini, himpunan A_4 berisikan P_2, P_5, dan P_6. P_2 kita sebut sebagai a_1, P_5 sebagai a_2, dan P_6 sebagai a_3. Untuk partisipan lainnya, diberikan pula penomeran yang baru dimulai dari a_4 hingga a_6 secara bebas.

Setelah diberikan penomeran yang baru, maka dapat dilakukan pembagian data rahasia. Menurut algoritma KGH, bagikan potongan data rahasia secara acak untuk $w - 1$ dari partisipan yang dipilih, menggunakan aturan Z_{36}. Maka didapat

$$a_1 = \{(5, 12), (13, 25), (14, 5)\}$$
$$a_2 = \{(6, 16), (9, 7), (20, 28), \}$$

Sedangkan untuk partisipan terakhir (a_3), akan dilakukan perhitungan sesuai dengan persamaan 3.1 dengan aturan Z_{2n+2}. Hasil perhitungannya adalah sebagai berikut.

$$a_3 = \{(6, 3), (5, 3), (3, 4)\}$$

Telah diketahui potongan data rahasia untuk a_1, a_2, dan a_3. Untuk a_4, a_5, a_6, kita bagikan potongan data rahasia secara acak dan bebas, dalam Z_{36} dan Z_{2n+2}. Hal ini dimaksudnya agar semua partisipan memperoleh potongan data rahasia, sehingga tidak mudah

untuk merekonstruksikan rahasia itu dikarenakan banyaknya himpunan kuasa yang mungkin untuk merekonstruksikan kembali rahasia tersebut.

Berikut ini adalah potongan data rahasia bagi a_4, a_5, a_6 :

$$a_4 = \{(15, 31), (19, 7), (26, 8)\} = P_1$$
$$a_5 = \{(2, 5), (0, 2), (1, 6)\} = P_3$$
$$a_6 = \{(4, 1), (2, 6), (7, 2)\} = P_4$$

(c) Konversi data

Tahap berikutnya yang perlu dilakukan adalah melakukan konversi data. Konversi tersebut mengikuti aturan yang telah dijelaskan sebelumnya. Hasil konversi data tersebut adalah sebagai berikut:

$$a_1 = 5C - DP - E5$$
$$a_2 = 6G - 97 - KS$$
$$a_3 = 63 - 53 - 34$$
$$a_4 = FV - J7 - Q8$$
$$a_5 = 25 - 02 - 16$$
$$a_6 = 41 - 26 - 72$$

(d) Pendistribusian data rahasia

Setelah semua potongan data rahasia dikonversikan, maka potongan data tersebut dapat didistibusikan kepada partisipan untuk dapat disimpan.

2. **Merekonstruksikan rahasia**

Sebelumnya telah dipaparkan proses pembagian rahasia. Sekarang akan dijelaskan proses rekonstruksi rahasia menggunakan langkah-langkah yang telah dipaparkan sebelumnya. Data yang digunakan pada proses rekonstruksi rahasia ini sama dengan data dan hasil akhir pada proses pem-

bagian data rahasia yang telah dikerjakan sebelumnya.

(a) Memilih partisipan

Kita sudah menentukan bahwa bahwa banyaknya partisipan yang dapat merekonstruksikan rahasia adalah 3 orang. Pada proses pembagian data rahasia, sistem sudah menyimpan informasi bahwa partisipan yang dapat merekonstruksikan rahasia hanyalah P_2, P_5, dan P_6. Jadi apabila tepat terpilih P_2, P_5, dan P_6 untuk merekonstruksikan rahasia, maka dapat dipastikan rahasia tersebut dapat dipecahkan. Namun realitanya, ada banyak himpunan yang mungkin yang dapat digunakan merekosntruksikan rahasia. Oleh karena itu, semakin banyak himpunan tersebut, maka semakin sulit untuk menentukan satu himpunan yang mungkin untuk merekonstruksikan rahasia.

Akan ada dua kasus yang ingin dipaparkan. Untuk kasus pertama, dipilih salah satu himpunan yang tidak dapat merekonstruksikan rahasia. Sedangkan untuk kasus kedua dipilih himpunan yang bisa merekonstruksikan rahasia.

(b) Konversi data

Langkah selanjutnya adalah mengkonversi potongan data rahasia yang dimiliki tiap partisipan. Untuk kasus pertama, dipilih himpunan yang berisikan P_1, P_2 dan P_5. hasil konversinya adalah sebagai berikut :

$$s_1 = (5, 12), (13, 25), (14, 5)$$
$$s_2 = (6, 16), (9, 7), (20, 28)$$
$$s_3 = (15, 31), (19, 7), (26, 8)$$

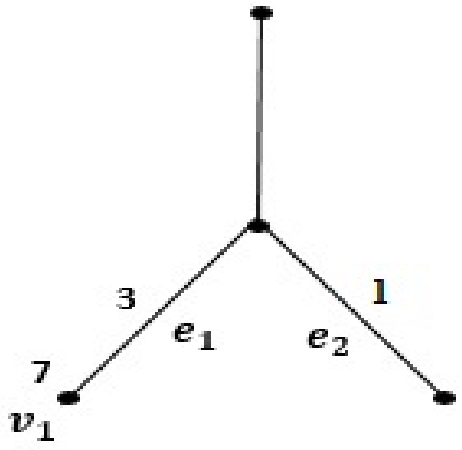
(c) Penjumlahan dalam modulo $(2n + 2)$

Setelah melakukan konversi, jumlahkan tiap potongan data rahasia dalam aturan modulo $(2n+2)$. Karena jumlah sisi pada graf bintang tersebut adalah 3, maka dilakukan penjumlahan dalam modulo 8. Hasilnya merupakan suatu himpunan, kita misalkan H. Hasilnya adalah sebagai berikut : $H = \{(2,3),(1,7),(4,1)\}$

(d) Memeriksa himpunan H

Langkah selanjutnya adalah memeriksa apakah himpunan H dapat direkonstruksikan menjadi rahasia. cocokanlah anggota himpunan H pada graf bintang. Ternyata H dapat membentuk suatu graf.

Setelah itu, lengkapilah graf bintang tersebut sesuai aturan pelabelan total sisi ajaib. Jika H sama dengan V, maka H dapat digunakan untuk merekonstruksikan rahasia. Hasil dari graf bintang tersebut adalah sebagai berikut : Bila kita mengisi titik pusat dengan label



Gambar 3.3: Himpunan H

1, dengan diketahui sebelumnya bahwa jumlah sisi pada graf tersebut adalah $n = 3$, maka bilangan k ajaib yang didapat adalah 11, yang tidak memenuhi syarat bilangan ajaib $2n + 4$. Oleh karena

itu, himpunan H ini tidak dapat merekonstruksikan rahasia.

Untuk langkah yang kedua, kita gunakan partisipan yang sama dengan partisipan yang telah dipilih terlebih dahulu untuk mendapatkan potongan data rahasia yang sebenarnya. Partisipan tersebut adalah P_2, P_5 dan P_6.

Setelah dipilih, kemudian dilakukan konversi terhadap potongan data rahasia yang dimiliki. Hasilnya adalah sebagai berikut :

$a_1 = \{(5, 12), (13, 25), (14, 5)\}$

$a_2 = \{(6, 16), (9, 7), (20, 28), \}$

$s_3 = (6, 3), (5, 3), (3, 4)$

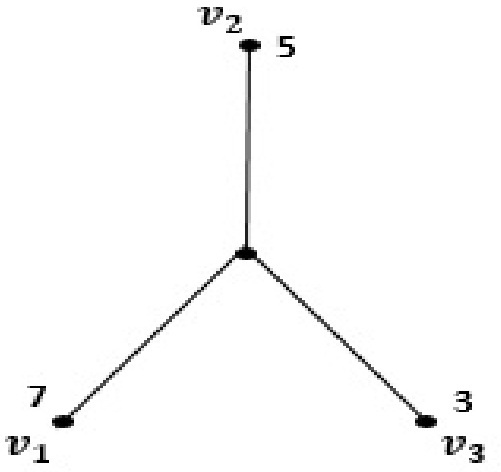
(e) Penjumlahan dalam modulo $(2n + 2)$

Setelah melakukan konversi, jumlahkan tiap potongan data rahasia dalam aturan modulo $(2n+2)$. Karena jumlah sisi pada graf bintang tersebut adalah 3, maka dilakukan penjumlahan dalam modulo 8. Hasilnya merupakan suatu himpunan, kita misalkan H. Hasilnya adalah sebagai berikut : $H = \{(1, 7), (3, 3), (5, 5)\}$

(f) Memeriksa himpunan H

Langkah selanjutnya adalah memeriksa apakah himpunan H dapat direkonstruksikan menjadi rahasia. cocokanlah anggota himpunan H pada graf bintang. Ternyata, himpunan tersebut dapat dicocokan pada graf. Setelah itu, lengkapilah graf bintang tersebut sesuai aturan pelabelan total sisi ajaib. Jika H sama dengan V, maka H dapat digunakan untuk merekonstruksikan rahasia. Hasil dari graf bintang tersebut adalah sebagai berikut :

Dikarenakan H sama dengan V, maka H dapat digunakan untuk merekonstruksikan rahasia. Apabila H tidak sama dengan V, maka



Gambar 3.4: Himpunan H pada graf bintang

ulang kembali ke langkah (a).

3.4 Polinomial Lagrange pada Skema Shamir

Setelah dijabarkaan contoh kasus untuk proses pembagian dan rekonstruksi rahasia menggunakan algoritma KGH, selanjutnya akan digunakan Skema Shamir untuk rekonstruksi rahasia. Kemudian akan dibandingkan kelebihan dan kekurangan diantara kedua metode tersebut.

Dimisalkan *dealer* ingin membagikan data rahasia kepada sekelompok orang P_1, P_2, P_3 hingga P_n, yang bisa disebut himpunan P, dengan menggunakan skema ambang batas maka *dealer* dapat membuat suatu polinomial $f(x)$ yang berderajat $t-1$ seperti berikut ini :

$$f(x) = a_0 + a_1x + a_2x^2 + ... + a_{t-1}x^{t-1}$$

Dimana $f(x)$ merupakan data rahasia.

Setelah itu, *dealer* memilih sebanyak n titik berbeda secara acak lalu membagikan membagikannya kepada P_1, P_2, P_3 hingga P_n secara rahasia, sedemi-

kian sehingga setiap P_i memiliki $S(P_i) = (x_i, f(x_i))$, untuk $i = 1, 2, 3, ..., n$, sebagai potongan data rahasianya.

Setelah potongan data rahasia dibagikan kepada (P_i), maka sebanyak t potongan data rahasia dari (P_i), untuk $i = 1, 2, 3, ..., n$ dapat digunakan untuk merekonstruksikan data rahasia $f(x)$ dengan menggunakan interpolasi lagrange sebagai berikut.

$$f(x) = \sum_{i=1}^{t} f(x_i).L(x_i) \tag{3.2}$$

Dimana,

$$L_i(x) = \frac{\prod_{i \neq j}^{t} (x - x_j)}{\prod_{i \neq j}^{t} (x_i - x_j)} \tag{3.3}$$

$L_i(x)$ adalah polinomial Lagrange.

Berikut ini adalah contoh dari penerapan Skema Shamir :

Misalkan *dealer* ingin merekonstruksikan rahasia yang berbentuk polinomial $f(x) = x^2 + 3x - 2$ dan ditetapkan nilai $t = 3$ dan $P = 6$, lalu dipilih titik-titik $x_1 = 1, x_2 = 2, x_3 = 3, x_4 = 4$. Oleh karena itu, diperoleh nilai potongan rahasia :

$$S(P_1) = (1, 2) \qquad S(P_3) = (3, 16)$$
$$S(P_2) = (2, 8) \qquad S(P_4) = (4, 26)$$

Karena telah ditentukan nilai $t = 3$, maka kombinasi himpunan yang mungkin untuk merekonstruksikan rahasia tersebut adalah $\{P_1, P_2, P_3\}, \{P_1, P_2, P_4\}$, $\{P_1, P_2, P_5\}, \{P_1, P_2, P_6\}, ..., \{P_4, P_5, P_6\}$.

Bila himpunan $\{P_1, P_2, P_4\}$ ingin merekonstruksikan $f(x)$, maka dengan menggunakan

$$S(P_1) = (1, 2); S(P_2) = (2, 8); S(P_4) = (4, 26)$$

dan interpolasi Lagrange, maka diperoleh

$$\begin{aligned} f(x) &= 2.\frac{(x-2)(x-4)}{(1-2)(1-4)} + 8.\frac{(x-1)(x-4)}{(2-1)(2-4)} + 26.\frac{(x-1)(x-2)}{(4-1)(4-2)} \\ &= 2.\frac{(x^2-6x+8)}{3} + 8.\frac{(x^2-5x+4)}{(-2)} + 26.\frac{(x^2-3x+2)}{6} \\ &= \left(\frac{2}{3}x^2 - 4x + \frac{16}{3}\right) + (-4x^2 + 20x - 16) + \left(\frac{13}{3}x^2 - 13x + \frac{26}{3}\right) \\ &= \left(\frac{2}{3}x^2 + \frac{13}{3}x^2 - 4x^2\right) + (20x - 4x - 13x) + \left(\frac{16}{3} + \frac{26}{3} - 16\right) \\ &= x^2 + 3x - 2 \end{aligned}$$

Maka didapat $f(x) = x^2 + 3x - 2$ yang merupakan data rahasia dari *dealer*.

Dengan cara yang sama kita juga dapat merekonstruksikan data rahasia menggunakan himpunan $\{P_1, P_2, P_3\}, \{P_1, P_2, P_4\}, \{P_1, P_2, P_5\}, \{P_1, P_2, P_6\}, ...,$ $\{P_4, P_5, P_6\}$. akan menghasilkan fungsi $f(x)$ yang sama, tapi untuk setiap P_1, P_2, P_3, P_4, $\{P_1, P_2\}$, $\{P_1, P_3\}$, $\{P_1, P_4\}$, $\{P_2, P_3\}$,...,$\{P_5, P_6\}$ tidak dapat merekonstruksikan $f(x)$.

3.5 Perbandingan Metode yang Digunakan

Setiap metode yang digunakan untuk meneyelesaikan suatu masalah pasti mempunyai kelebihan dan kekurangan. Begitu pula dengan metode yang kita gunakan untuk masalah pembagian data rahasia ini. Baik Algoritma KGH maupun Skema Shamir mempunyai kelebihan dan kekurangannya masing-masing. Berikut ini akan dijabarkan kelebihan dan kekurangan tiap metode.

3.5.1 Kelebihan Skema Pembagian Data Rahasia Menggunakan Algoritma KGH pada Graf Bintang

Dari penjelasan sebelumnya, diperoleh kelebihan dari skema pembagian data rahasia menggunakan algoritma KGH.

- Langkah-langkah dalam proses pengerjaannya runtun dan jelas.

  Telah diketahui bahwa proses pembagian dan rekonstruksi data rahasia menggunakan algoritma KGH dilalui dengan proses yang jelas dan runtun. Penjelasan untuk tiap langkah juga dijabarkan dengan jelas, sehingga dapat dipahami oleh pihak yang ingin menggunakannya.

- Struktur akses dapat ditentukan sendiri.

  Pada contoh kasus yang telah dijabarkan sebelumnya, struktur akses ditentukan terlebih dahulu sebelum mendistribusikan potongan data rahasia kepada semua partisipan yang ada, sehingga pada skema ini struktur akses dapat ditentukan sendiri.

3.5.2 Kekurangan Skema Pembagian Data Rahasia Menggunakan Algoritma KGH pada Graf Bintang

Dari penjelasan sebelumnya, diperoleh beberapa kekurangan dari skema pembagian data rahasia menggunakan algoritma KGH.

- Banyaknya partisipan terbatas.

  Karena jumlah dari himpunan kritis yang terdapat pada graf yang dipilih terbatas mengakibatkan banyaknya jumlah partisipan terbatas.

- Perhitungan dalam mencari himpunan kritis dan dalam memberi label pada graf masih cukup kompleks.

  Hingga waktu ini belum ditemukan cara yang efisien dan praktis untuk menentukan himpunan kritis dari sebuah graf dengan pelabelan ajaib. Cara yang sering digunakan untuk menentukan jumlah himpunan kritis adalah secara manual menghilangkan satu-persatu label pada simpul, sisi yang bertetangga dengan simpul, atau titik pusat dari suatu graf yang

diberi pelabelan ajaib. Apabila label dihilangkan, kemudian label kosong tersebut diberi nomer kembali, maka diperoleh graf awal. Namun apabila kita mengembalikan label tersebut didapat suatu graf yang berbeda dari graf awal, maka graf tersebut tidak bisa menjadi sebuah himpunan kritis. Singkatnya, himpunan kritis hanya dapat membangun sebuah graf total sisi ajaib. Apabila dapat membangun lebih dari satu graf, himpunan itu bukan himpunan kritis.

3.5.3 Kelebihan Skema Pembagian Data Rahasia Menggunakan Skema Shamir

Dari penjelasan sebelumnya, diperoleh kelebihan dari skema pembagian data rahasia menggunakan Skema Shamir.

- Banyaknya partisipan tidak terbatas.

  Setiap polinomial selalu memiliki tak-terhingga banyak titik. Dikarenakan banyak titik pada polinomial mewakili banyak potongan data rahasia yang dibagikan kepada partisipan, oleh karena itu jumlah partisipan tidak terbatas.

- Perhitungan yang sederhana.

  Dapat dilihat bahwa proses perhitungan dalam polinomial lagrange cukup sederhana dan dapat diselesaikan tanpa harus menggunakan aturan yang rumit.

- Jika lebih dari t partisipan bersama-sama merekonstruksikan rahasia, rahasia tetap dapat dipecahkan.

  Dalam mencari suatu solusi sistem persamaan linier t faktor dibutuhkan sedikit t persamaan linier, maka jika lebih dari t persamaan linear, de-

ngan lebih dari t faktor tetap dapat merekonstruksikan rahasia, karena solusinya tetap tunggal.

3.5.4 Kekurangan Skema Pembagian Data Rahasia Menggunakan Skema Shamir

Dari penjelasan sebelumnya, diperoleh kekurangan dari skema pembagian data rahasia menggunakan Skema Shamir.

- Struktur akses tidak dapat ditentukan sendiri.

  Struktur akses dalam skema ambang batas Shamir adalah sub-himpunan dari partisipan yang terdiri dari t partisipan. Jika seorang partisipan mendapatkan potongan data rahasia, maka partisipan tersebut dapat bergabung dengan himpunan struktur akses yang berjumlah $t-1$ atau lebih. Dengan kata lain, tidak ada suatu struktur akses tunggal, dimana hanya struktur akses itu yang dapat merekonstruksikan rahasia. Dengan demikian, mudah untuk dapat merekonstruksikan rahasia karena tidak ada suatu struktur akses yang khusus untuk merekonstruksikan rahasia.

BAB IV

PENUTUP

4.1 Kesimpulan

1. Suatu data rahasia haruslah dapat disembunyikan dengan aman, dan hanya orang-orang tertentu dan berkepentingan saja yang dapat mendapatkan data rahasia tersebut. Cara untuk membagikan rahasia adalah dengan menggunakan Algoritma KGH, yang langkah-langkahnya adalah sebagai berikut :

   (a) Bentuklah himpunan kritis Q. Dimisalkan Q menjadi rahasia S.

   (b) Gunakan algoritma KGH untuk membagikan S.

   (c) Lakukan konversi untuk setiap potongan data rahasia di tiap partisipan untuk meningkatkan keamanan rahasia.

   (d) Bagikan potongan data rahasia tersebut kepada partisipan.

   Sedangkan untuk merekonstruksikan rahasia menggunakan algoritma KGH, langkah-langkahnya adalah sebagai berikut :

   (a) Pilihlah partisipan yang akan merekonstruksikan rahasia tersebut.

   (b) Lakukan konversi untuk setiap potongan data rahasia yang dimiliki tiap partisipan.

   (c) Jumlahkan semua potongan data rahasia dalam modulo $(2n + 2)$, kemudian hasilnya adalah sebuah himpunan, dinamakan H.

(d) Jika H tidak memenuhi kondisi yang memungkinkan dalam suatu graf maka H tidak bisa menjadi suatu rahasia, sehingga kembali ke langkah pertama. Jika memenuhi syarat, maka dilanjutkan ke langkah berikutnya.

(e) Selidiki apakah H dapat menjadi rahasia S atau tidak. Jika H sama dengan V, maka H dapat menjadi rahasia himpunan kritis.

2. Terdapat kelebihan dan kekurangan dalam penggunaan Algoritma KGH dan Skema Shamir. Perbandingannya adalah sebagai berikut :

   - **Kelebihan Skema Pembagian Data Rahasia Menggunakan Algoritma KGH pada Graf Bintang**

     (a) Langkah-langkah dalam proses pengerjaannya runtun dan jelas.

     (b) Struktur akses dapat ditentukan sendiri.

   - **Kekurangan Skema Pembagian Data Rahasia Menggunakan Algoritma KGH pada Graf Bintang**

     (a) Banyaknya partisipan terbatas.

     (b) Komputasi dalam mencari himpunan kritis dan dalam memberi label pada graf masih cukup kompleks.

   - **Kelebihan Skema Pembagian Data Rahasia Menggunakan Skema Shamir**

     (a) Banyaknya partisipan tidak terbatas.

     (b) Jika lebih dari t partisipan bersama-sama merekonstruksikan rahasia, rahasia tetap dapat diketahui.

   - **Kekurangan Skema Pembagian Data Rahasia Menggunakan Skema Shamir**

     (a) Struktur akses tidak dapat ditentukan sendiri.

4.2 Saran

- Dapat dilakukan penelitian lebih lanjut dengan mentransformasikan suatu data rahasia menjadi suatu graf bintang dan menjadi suatu fungsi polinomial.

- Untuk penelitian selanjutnya dapat digunakan pembagian data rahasia dengan jumlah anggota pada himpunan kuasa yang berbeda, tidak harus sama untuk setiap himpunan kuasa.

DAFTAR PUSTAKA

Alfarisi, R. 2017. "Dimensi Partisi dan Dimensi Partisi Bintang Graf Hasil Operasi COMB Dua Graf Terhubung". *Tesis*. Institut Teknologi Sepuluh November, Surabaya.

Baskoro, E.T., Simanjuntak, R., Adithia, M.T., "Secret Sharing Schemes Based on Magic Labeling". *Proceeding of National Conference on Mathematics XII*, 23-27 Juli 2004, Bali.

Chatrand, Gery dan Lesniak, Linda. 1986. *Graphs and Digraphs*. Edisi ke-2. California: a Division of Wadsworth.Inc.

Damayanti, R.T., "Automorfisme Graf Bintang dan Graf Lintasan", *Jurnal CAUCHY Vol. 2, No. 1*, November 2011.

Imron, C. "Pelabelan Total Sisi Ajaib Graph Caterpillar", *Seminar Nasional Matematika Universitas Negeri Surabaya*, 28 Februari 2005.

Imron, C., Setiyono, B., Simanjuntak, R., dan Baskoro, E.T., "Critical Set of Caterpillar Graph for Secret Sharing Scheme", ITB Bandung. 2007.

Indah, M.R. dan K. Budayasa, "Pelabelan Total Sisi Ajaib Titik Terurut Pada Graph", 2011.

Karnin, E.D., Greene, J.W., dan Hellman, M.E., "On Secret Sharing Systems", *IEEE Trans. Inf. Th., Vol. IT-29, No.1: 35-41*, January 1983.

Munir, Rinaldi. 2012.*Matematika Diskrit*. Edisi Revisi ke-5. Bandung: Penerbit Informatika.

Shamir, A., "How to Share a Secret", *Communications of the ACM, Vol. 22, No. 11: 612-613*, November 1979.

Wallis, W.D., Baskoro, E.T., Miller, M., dan Slamin. "Edge-Magic Labelings". *Australasian Journal of Combinatorics 22: 177-190*, 2000.

SURAT PERNYATAAN KEASLIAN SKRIPSI

Dengan ini saya yang bertanda tangan di bawah ini, mahasiswa Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Jakarta:

Nama	:	Daniel
No. Registrasi	:	3125136332
Jurusan	:	Matematika
Program Studi	:	Matematika

Menyatakan bahwa skripsi ini yang saya buat dengan judul "**Konstruksi Skema Pembagian Data Rahasia Menggunakan Algoritma Karnin-Greene-Hellman dan Skema Shamir**" adalah :

1. Dibuat dan diselesaikan oleh saya sendiri.
2. Bukan merupakan duplikat skripsi yang pernah dibuat oleh orang lain atau jiplakan karya tulis orang lain.

Pernyataan ini dibuat dengan sesungguhnya dan saya bersedia menanggung segala akibat yang timbul jika pernyataan saya tidak benar.

Jakarta, Agustus 2017

Yang membuat pernyataan

Daniel

DAFTAR RIWAYAT HIDUP

DANIEL. Lahir di Jakarta, 24 November 1994. Anak pertama dari pasangan Bapak Rikardo Panggabean dan Ibu Lamtiur Parapat. Saat ini bertempat tinggal di Pesona Anggrek Blok F 16 no 19, Bekasi.

No. Ponsel : 082299609925

Email : monocorsivo@gmail.com

Riwayat Pendidikan : Penulis mengawali pendidikan di TK Mutiara 17 Agustus Bekasi pada tahun 2000-2001, kemudian melanjutkan pendidikan di SD Mutiara 17 Agustus Bekasi pada tahun 2001 - 2007. Setelah itu, penulis melanjutkan ke SMP Negeri 5 Bekasi hingga tahun 2010. Kemudian kembali melanjutkan ke SMA Negeri 89 Jakarta dan lulus tahun 2013. Di Tahun yang sama penulis melanjutkan pendidikan ke Universitas Negeri Jakarta (UNJ), jurusan Matematika, melalui jalur UMBPTN. Di pertengahan tahun 2017 (Jumat, 11 Agustus 2017) penulis telah memperoleh gelar Sarjana Sains, Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Jakarta.

Riwayat Pekerjaan : Penulis mulai menjadi pengajar les private matematika sejak tahun 2011. Penulis mengajar kepada siswa tingkat SD, SMP, dan SMA. Penulis juga sering menjadi guru private untuk persiapan test masuk perguruan tinggi.