BAB III

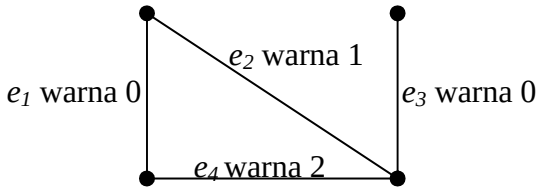
APLIKASI SKEMA PEMBAGIAN RAHASIA

PADA GRAF

3.1 Pengkodean Matriks Ketetanggaan Sisi

Graf dapat direpresentasikan dalam tiga cara yang berlainan, yaitu dengan menggunakan himpunan pasangan berurut, diagram, dan matriks. Sebuah graf yang dinyatakan dalam bentuk diagram, dapat dinyatakan dalam bentuk matriks atau himpunan pasangan berurut, dan sebaliknya.

Matriks ajasensi sisi $A(G)$ adalah matriks simetri sehingga, dengan memilih semua pada elemen-elemen di bawah diagonal utama dan elemen-elemen diagonal utama, akan didapat gambaran matriks secara keseluruhan. Sehingga dapat ditulis suatu barisan bilangan $a_{21}, a_{31}, a_{32}, a_{41}, a_{42}, ..., a_{m(m-1)}, a_{11}, a_{22}, ..., a_{mm}$ di mana bagian pertama ($a_{21}, a_{31}, a_{32}, a_{41}, a_{42}, ..., a_{m(m-1)}$) berkorespondensi pada semua elemen di bawah diagonal utama, dan bagian selanjutnya ($a_{11}, a_{22}, ..., a_{mm}$) berkorespondensi dengan diagonal utama. Sebagai contoh perhatikan graf *G* dan pewarnaannya pada Gambar 3.1.



Gambar 3.1 Gambar Graf *G*

Didapat pengkodean matriks dari graf *G*

$m = a_{21}, a_{31}, a_{32}, a_{41}, a_{42}, a_{43}, a_{11}, a_{22}, a_{33}, a_{44}$ = 1,0,1,1,1,1,0,1,0,2.

3.2 Pengelompokkan Jenis-jenis Graf Sisi Terwarnai

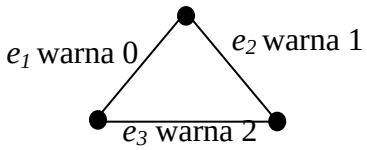
Pada umumnya, pewarnaan sisi suatu graf G sama dengan mempartisi sisi-sisi pada graf G menjadi n himpunan, sedemikian sehingga setiap sisi di satu himpunan menjadi tidak terhubung.

Definisi 3.1

Derajat kebebasan sisi pada graf G adalah jumlah warna maksimal yang dapat digunakan pada pewarnaan minimal untuk mewarnai sisi graf G tersebut sehingga tidak ada dua sisi yang bertetangga menggunakan warna yang sama (Kluesza, K. dan Kotulski, Z., 2003:3).

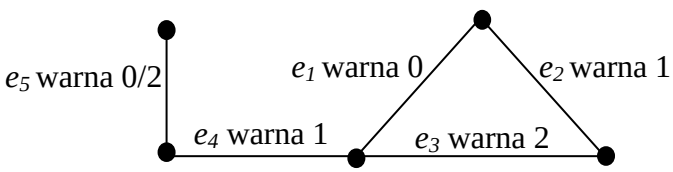
Setiap sisi-sisi pada graf G dengan $\chi'(G) = n$ dapat dikelompokkan ke dalam jenis berikut ini :

1. Sisi jenis pertama yaitu sisi-sisi pada graf yang memiliki derajat kebebasan sisi sama dengan 1 pada setiap kemungkinan pewarnaan sisi. Sebagai contoh yaitu sisi-sisi pada graf lengkap K_3.



Gambar 3.2 Gambar Graf Lengkap K_3

2. Sisi jenis kedua yaitu sisi-sisi pada graf yang memiliki derajat kebebasan sisi sama dengan y, di mana $1 < y < n ; y \in$ pada setiap pewarnaan graf tersebut.



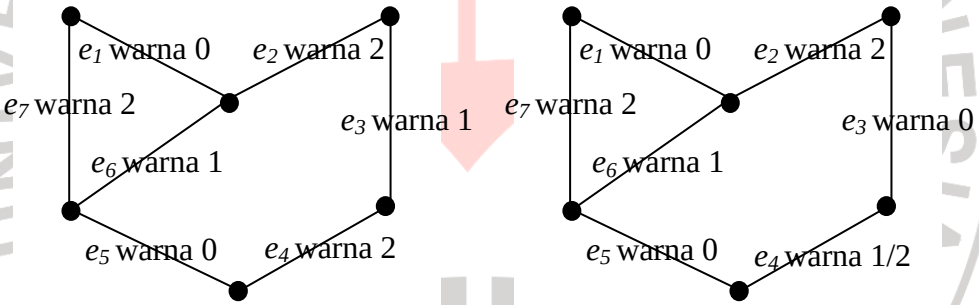
Gambar 3.3 Gambar Graf G

Graf G pada Gambar 3.3 di atas adalah sisi jenis kedua, yaitu e_5 dengan derajat kebebasan 2.

Karena itu, matriks ketetanggaan sisi spesial $A^*(G)$ di atas adalah

	e_1	e_2	e_3	e_4	e_5
e_1	0	1	1	1	0
e_2	1	1	1	1	0
e_3	1	1	2	0	1
e_4	1	1	0	2	0
e_5	0	0	1	0	0/1

3. Sisi jenis ketiga yaitu sisi-sisi pada graf yang memiliki derajat kebebasan sisi berubah-ubah, sesuai dengan pola pewarnaan yang diberikan.



Gambar 3.4 Gambar Graf Sisi Jenis Ketiga

Karena sisi e_4 memiliki derajat kebebasan sisi berubah sesuai dengan pola pewarnaan yang diberikan maka graf di atas termasuk sisi jenis ketiga. Pada Gambar 3.4 (a) derajat kebebasan sisi e_4 adalah 1, sedangkan pada gambar 3.4 (b) derajat kebebasan sisi e_4 adalah 2.

Matriks ketetanggaan sisi spesial $A^*(G)$ diatas adalah

	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	0	1	0	0	0	1	1
e_2	1	2	1	0	0	1	0
e_3	0	1	1	1	0	0	0
e_4	0	0	1	2	1	0	0
e_5	0	0	0	1	0	1	1
e_6	1	1	0	0	1	1	1
e_7	1	0	0	0	1	1	2

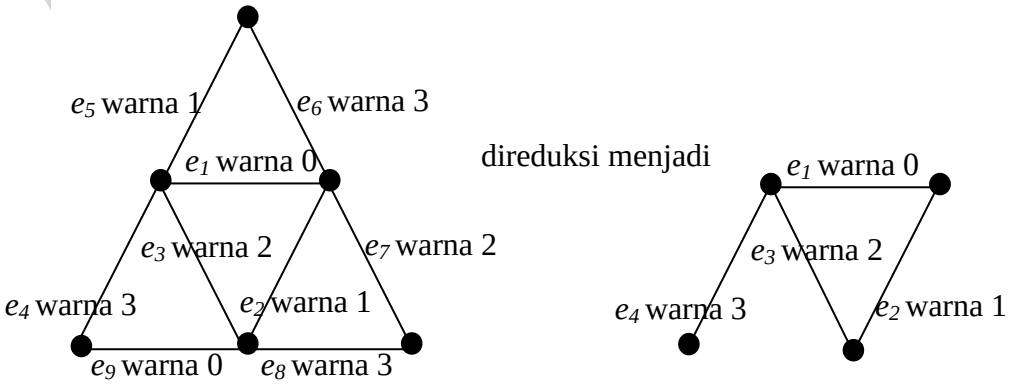
(a)

	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	0	1	0	0	0	1	1
e_2	1	2	1	0	0	1	0
e_3	0	1	0	1	0	0	0
e_4	0	0	1	1/2	1	0	0
e_5	0	0	0	1	0	1	1
e_6	1	1	0	0	1	1	1
e_7	1	0	0	0	1	1	2

(b)

3.3 Pereduksian Graf

Setiap graf dapat direduksi menjadi subgraf yang hanya terdiri dari sisi-sisi jenis pertama saja. Untuk setiap subgraf, dapat diperoleh himpunan sisi minimal yang menentukan sisi terwarnai dari subgraf tersebut. Oleh karena itu, sisi-sisi ini dapat direduksi lagi sehingga menjadi himpunan yang lebih kecil. Struktur atau bagian dari graf yang tereduksi merupakan sebuah himpunan sisi jenis pertama minimal yang menentukan pewarnaan pada graf terhubung yang dibentuk oleh sisi-sisi jenis pertama.



Gambar 3.5 Gambar Pereduksian Graf

3.4 Proses Enkripsi Pola Pewarnaan Graf

Graf yang akan digunakan dalam aplikasi skema pembagian rahasia yang diinginkan adalah graf yang terdiri atas sisi jenis pertama dan kedua. Dengan terlebih dahulu diketahui suatu pewarnaan sisi dari graf tersebut

Terdapat dua bagian terpisah dari rahasia yang dapat dibagi, yaitu bagian yang dibentuk oleh sisi-sisi jenis pertama dan bagian yang dibentuk oleh sisi-sisi jenis kedua. Jika hanya satu bagian yang diketahui, maka sisanya masih tetap merupakan suatu rahasia, dan peluang untuk memecahkan rahasia tersebut akan semakin besar.

3.4.1 Enkripsi sisi-sisi jenis pertama

Berikut ini adalah algorima yang dipakai untuk menentukan enkripsi pada graf yang memiliki sisi-sisi jenis pertama :

Algoritma 1:

1. Diketahui pewarnaan sisi dari graf *G,* dan *k* warna yang dapat digunakan;
2. Selanjutnya menentukan bagian tereduksi sehingga menghasilkan sisi-sisi jenis pertama minimal dari graf *G*;
3. Masing-masing sisi $e_i, i = 1,2,...,n$ dari bagian tereduksi dipetakan dengan warna *s* di mana $s \in \square_n$, $n = \chi'(G)$ atau kombinasi dari $\binom{k}{n}$ warna. Dengan demikian, diperoleh pemetaan dari $\square_k$ ke $\square_n$;
4. Selesai.

3.4.2 Enkripsi sisi-sisi jenis kedua

Jika pola pewarnaan sisi-sisi jenis kedua sudah diketahui, maka pola pewarnaan sisi-sisi jenis pertama bukan lagi menjadi suatu rahasia. Oleh karena itu, sisi-sisi jenis kedua harus dipetakan ke sesuatu di $\Box_n$. Sehingga diperlukan variabel tertentu untuk sisi-sisi jenis kedua, yaitu :

1. n_i adalah jumlah warna yang tidak boleh digunakan oleh sisi tertentu e_i dengan memeriksa sisi-sisi jenis pertama yang bertetangga dengan e_i. Oleh karena itu, setiap warna yang digunakan untuk menandai setiap sisi yang bertetangga dengan e_i tidak terdapat pada daftar warna yang tersedia;
2. l_i adalah banyaknya warna yang tersedia untuk mewarnai sisi-sisi e_i, $l_i = n - n_i$;
3. $\Box_{l_i} = \{0,1,2,...,l_i - 1\}$;
4. C_i adalah himpunan l_i warna dari $\Box_n$ yang tersedia untuk sisi e_i;
5. w adalah banyaknya sisi-sisi jenis kedua di graf G.

Graf G adalah graf sisi terwarnai dengan menggunakan warna-warna di $\Box_n$, maka masing-masing sisi e_i telah diwarnai oleh salah satu warna dari C_i, sehingga $|C_i| = |\Box_{l_i}|$ yang membuktikan pemetaan satu-satu antara $\Box_{l_i}$ dan C_i dapat didefinisikan.

Berikut ini adalah algorima yang dipakai untuk menentukan enkripsi pada graf yang memiliki sisi-sisi jenis kedua :

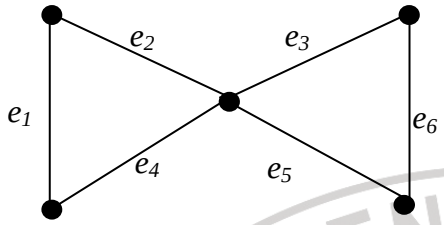
Algoritma 2:

Untuk setiap sisi-sisi jenis kedua e_i dilakukan :

1. Menyusun elemen dari Φ_{l_i} dan C_i secara monoton naik sesuai dengan bilangan asli Φ ;
2. Setelah elemen di Φ_{l_i} dan C_i disusun, lalu diberi label. Ini dilakukan dengan diawali dari elemen terkecil di C_i dan menggunakan bilangan berurutan dari $\{0,1,2,...,l_i-1\}$ untuk menyusun elemen C_i secara berurutan;
3. Dengan melakukan langkah 2, pemetaan antara C_i dan $\{0,1,2,...,l_i-1\}$ diketahui, sehingga pemetaan antara C_i dan Φ_{l_i} juga diketahui. Kemudian masing-masing sisi e_i dapat diwarnai oleh warna-warna dari Φ_{l_i} ;
4. Selesai.

Perhatikan bahwa warna yang digunakan untuk mewarnai sisi-sisi jenis kedua tertentu e_i, dapat dikodekan dengan sebarang bilangan dari Φ_{l_i}. Sehingga, sisi jenis kedua yang diwarnai menggunakan Φ_{l_i} tidak memberikan informasi tentang pengkodean Φ_n untuk graf *G*.

Untuk lebih jelasnya, berikut ini contoh mengenkripsi pola pewarnaan sisi dari suatu graf *G* dengan warna-warna yang digunakan berasal dari $\mathbb{Z}_{10}$.



Gambar 3.5 Gambar Graf *G*

	e_1	e_2	e_3	e_4	e_5	e_6
e_1	8	1	0	1	0	0
e_2	1	7	1	1	1	0
e_3	0	1	6	1	1	1
e_4	1	1	1	4	1	0
e_5	0	1	1	1	8	1
e_6	0	0	1	0	1	4

Matriks $A^*(G)$ memberikan barisan 1,0,1,1,1,1,0,1,1,1,0,0,1,0,1,8,7,6,4,8,4.

Langkah 1.

Sisi-sisi jenis pertama : e_2, e_3, e_4, e_5 memberikan bentuk tereduksi e_2, e_3, e_4, e_5, pemetaan $\mathbb{Z}_{10}$ pada $\mathbb{Z}_4$ didefinisikan sebagai $e_2 = 0,\ e_3 = 1,\ e_4 = 2,\ e_5 = 3$ (semuanya dari $\mathbb{Z}_4$), mengakibatkan $7 \to 0,\ 6 \to 1,\ 4 \to 2,\ 8 \to 3$. Sehingga pengkodean $\mathbb{Z}_4$ untuk graf *G* adalah $e_2, e_3, e_4, e_5 \to 0,1,2,3$.

Langkah 2.

Sisi-sisi jenis kedua : e_1, e_6 penempatan warna dari $\mathbb{Z}_{10}$ ke $\mathbb{Z}_4$ adalah $e_1 = 8 \to 3, e_6 = 4 \to 2$.

Karena itu, e_1, e_6 berkorespondensi dengan 3,2 di pengkodean $\mathbb{Z}_4$.

Himpunan bilangan anggota $\mathbb{Z}_4$ yang tidak boleh digunakan oleh masing-masing sisi jenis kedua adalah $e_1\{0,2\}$, $e_6\{1,3\}$. Himpunan bilangan $\mathbb{Z}_4$ yang dapat digunakan oleh masing-masing sisi jenis kedua adalah $e_1 \in C_1 = \{1,3\}$, $e_6 \in C_6 = \{0,2\}$. Jadi $l_i = 2$ untuk masing-masing e_1, e_6, sehingga $\mathbb{Z}_{l_i} = \mathbb{Z}_2$.

Langkah 3.

Pemetaan $\square_4 \rightarrow \square_2$ untuk e_1 mendefinisikan $\{1,3\} \rightarrow \{0,1\}$ sehingga $1 \rightarrow 0,\ 3 \rightarrow 1,$

Pemetaan $\square_4 \rightarrow \square_2$ untuk e_6 mendefinisikan $\{0,2\} \rightarrow \{0,1\}$ sehingga $0 \rightarrow 0,\ 2 \rightarrow 1,$

Akhirnya, e_1, e_6 berkorespondensi dengan 1,1 dalam pengkodean $\square_2$.

Oleh karena itu, untuk graf *G* yang diketahui diatas, rahasia yang akan dibagi adalah 1,1,7,6,4,8 dengan 1,1 berkorespondensi dengan sisi-sisi jenis kedua dan 7,6,4,8 berkorespondensi dengan sisi-sisi jenis pertama.

3.5 Penerapan Skema Pembagian Rahasia

Sebagaimana yang telah disampaikan pada bab sebelumnya, skema pembagian rahasia yang akan digunakan adalah skema pembagian rahasia KGH (*Karnin-Greene-Hellman).* Rahasia yang akan dibagi dengan menggunakan skema pembagian rahasia KGH adalah pola pewarnaan sisi dari graf yang telah dienkripsi sebelumnya yaitu *K*= 1,1,7,6,4,8.

Berdasarkan proses enkripsi yang telah dilakukan sebelumnya, vektor rahasia yang akan dibagi diperoleh dari sisi-sisi jenis kedua dan sisi-sisi jenis pertama pada bagian tereduksi dari graf. Panjang vektor rahasia η, merupakan jumlah sisi-sisi jenis kedua dan sisi-sisi tereduksi tersebut. *Share* yang akan dibagikan kepada partisipan adalah vektor dengan panjang yang sama dengan vektor rahasia di mana elemen-elemennya merupakan anggota himpunan $\square_r$

dengan *r* merupakan bilangan yang lebih besar dari elemen terbesar pada vektor rahasia.

Misalkan banyaknya partisipan yang akan memperoleh *share* adalah *t*. Untuk *t*-1 buah *share* dapat diperoleh dengan membentuk vektor panjang η yang elemen-elemennya anggota $\mathbb{Z}_r$ secara acak. Sedangkan untuk *share* yang ke *t* dapat diperoleh dengan mengurangi vektor rahasia dengan jumlah *t*-1 buah *share* yang telah ada dalam modulo *r*.

Untuk contoh yang dibahas sebelumnya, vektor rahasia yang diperoleh adalah $S=(1,1,7,6,4,8)$. Dapat dipilih nilai $r=9>max(1,1,7,6,4,8)$. Misalkan banyaknya partisipan yang akan memperoleh share adalah t = 5, maka $S^1=(1,2,6,2,1,3)$, $S^2=(3,0,4,0,7,0)$, $S^3=(2,8,3,6,2,6)$, $S^4=(7,6,2,1,2,4)$, $S^5=(6,3,1,6,1,4)$ dapat menjadi salah satu skema pembagian rahasia KGH, kerena jumlah dari semua vektor tersebut dalam $\mathbb{Z}_9$ adalah $S=(1,1,7,6,4,8)$.

3.6 Proses Memecahkan Rahasia (Dekripsi)

Berikut ini adalah algorima yang dipakai untuk proses dekripsi atau proses memecahkan rahasia :

Algoritma 3 :

1. Partisipan yang berhak mengetahui rahasia mengumpulkan *share* mereka, sehingga rahasia yang dibagi dari graf *G* diketahui;

2. Rahasia digunakan untuk :
   a. Menetapkan warna-warna dari $\square_k$ untuk bagian tereduksi. Ini juga dapat memberikan pola pewarnaan dengan menggunakan $\square_n$ (ingat bahwa kedua himpunan berurutan sesuai bilangan asli);
   b. Setelah pola pewarnaan bagian tereduksi diketahui, pola pewarnaan semua sisi jenis pertama diketahui;
   c. Tetapkan warna-warna dari $\square_{l_i}$ untuk sisi-sisi jenis kedua.
3. Dengan menggunakan pola pewarnaan pada sisi jenis pertama, C_i untuk setiap sisi jenis kedua dapat diketahui;
4. Untuk masing-masing sisi jenis kedua, tentukan warna $\square_n$nya, dengan menggunakan $\square_{l_i}$ dan C_i. Ingat bahwa keduanya terurut sesuai dengan bilangan asli;
5. Untuk setiap sisi jenis kedua, periksa pemetaan $\square_k \rightarrow \square_n$ dan warna-warna yang digunakan yang berasal dari $\square_k$;
6. Selesai.

Dengan menjalani prosedur secara lengkap, rahasia dapat diketahui. Dari contoh di atas akan dilakukan proses dekripsi, langkah-langkahnya sebagai berikut :

Langkah 1.

Dari pembahasan sebelumnya langkah 1 telah jelas.

Langkah 2.

Dari graf *G* yang diketahui, dilakukan pereduksian sehingga sisi-sisi tereduksi dapat diketahui yaitu e_2, e_3, e_4, e_5. Dari langkah 1 dengan mudah diketahui pengkodean $e_2, e_3, e_4, e_5 \to 7, 6, 4, 8$, sehingga $\square_n$ dapat diketahui yaitu $n = 4$ diperoleh pemetaan $0, 1, 2, 3 \to 7, 6, 4, 8$. Jadi pola pewarnaan sisi-sisi jenis pertama telah diketahui.

Langkah 3.

Dari pereduksian diketahui sisi-sisi jenis kedua yaitu e_1, e_6. Himpunan bilangan $\square_4$ yang dapat digunakan oleh masing-masing sisi jenis kedua adalah $e_1 \in C_1 = \{1, 3\}$, $e_6 \in C_6 = \{0, 2\}$. Jadi $l_i = 2$ untuk masing-masing e_1, e_6, sehingga $\square_{l_i} = \square_2$.

Langkah 4.

Pemetaan $\square_2 \to \square_4$ untuk e_1 mendefinisikan $\{0,1\} \to \{1,3\}$ sehingga $0 \to 1, 1 \to 3$.

Pemetaan $\square_2 \to \square_4$ untuk e_6 mendefinisikan $\{0,1\} \to \{0,2\}$ sehingga $0 \to 0, 1 \to 2$.

Dari langkah 1 dapat diketahui $e_1 \to 1 \to 3$ dan $e_6 \to 1 \to 2$

Lankah 5.

Dari langkah 4 dan langkah 2 dapat diketahui $e_1 \to 3 \to 8$ dan $e_6 \to 2 \to 4$

Jadi pola pewarnaan graf yang dirahasiakan dapat diketahui yaitu $e_1, e_2, e_3, e_4, e_5, e_6 \to 8, 7, 6, 4, 8, 4$.