SERTIFIKAT

3.9.5/UN32.3/DT/2015

Diberikan Kepada

KHOLIFATUR ROSYIDAH

Universitas Negeri Jember

Atas partisipasinya sebagai

PEMAKALAH

Dalam Seminar Nasional Matematika dan Pembelajarannya
dengan Tema Peranan Matematika dalam Menumbuhkembangkan Daya Saing dan Karakter Bangsa
yang diselenggarakan oleh Jurusan Matematika Fakultas MIPA Universitas Negeri Malang Tanggal 5 September 2015

Judul Makalah

Super (a,d)-S3 Antimagic Total Dekomposisi Graf Helm Untuk Pengembangan Ciphertext

Malang, 5 September 2015

Dekan FMIPA Universitas Negeri Malang	Ketua Pelaksana
Dr. Markus Diantoro, M.Si	Dr. Eny Hidayanto, M.Si
NIP. 196612211991031001	NIP. 196609061992031004

Super (a,d)-S_3 Antimagic Total Dekomposisi Graf Helm dan untuk Pengembangan Ciphertext

(Super (a,d)-S_3 Antimagic Total Decomposition Helm Graph and its Aplication for a Criptosystem)

K. Rosyidah[1], Dafik[1,2], S. Setiawani[1]

[1]Department of Mathematics Education- University of Jember
[2]CGANT- University of Jember
ifa_kholifatur10077@yahoo.co.id; d.dafik@unej.ac.id; setiawanisusi@gmail.com

Abstract

A graph $G(V,E)$ has a H-Covering if every edge in E belongs to a subgraph of G isomorphic to H. The $(a,d)-H$ antimagic covering on the G graph is a biijective functin of $f: V(G) \cup E(G) \to \{1,2,...,|V(G)|+|E(G)|\}$ till all of the H' subgraphs that isomorphic to H have weight $w(H) = \sum_{v \epsilon V(H')} f(v) + \sum_{e \epsilon E(H')} f(e)$ from an arithmatic sequence $\{a, a+d, a+2d, ..., a+(t-1)d\}$, where a and d is the positive integres and t is the number of all subgraphs H' isomorphic to H. Such a labeling is called super if $f: V(G) \to \{1,2,...,|V(G)|\}$. This research aims to determine the super $(a,d)-S_3$ antimagic total decomposition of Helm graph and also we will use it to develop *chipertext* from a secret message.

Keywords: Super $(a,d)-S_3$, Decomposition, Helm Graph, and *ciphertext*.

Pendahuluan

Ilmu pengetahuan dan teknologi akan selalu berkembang seiring dengan kebutuhan manusia di era globalisasi. Salah satu ilmu pengetahuan yang selalu berkembang adalah teori graf. Teori Graf merupakan ilmu matematika yang pertama kali diperkenalkan oleh L. Euler, matematikawan asal Swiss pada tahun 1736. Idenya muncul sebagai upaya dalam menyelesaikan masalah jembatan Konigsberg menggunakan graf. Ide inilah yang mengundang banyak ilmuan mengembangkan Teori Graf untuk memecahkan berbagai masalah yang muncul dalam kehidupan sehari-hari. Salah satu masalah yang berkaitan dengan graf yang telah dikaji adalah dekomposisi graf. Penerapan dekomposisi graf sudah banyak digunakan dalam beberapa disiplin ilmu.

Jika selimut$-H$ dari graf G memiliki sifat yaitu sisi G termuat dalam tepat satu graf H_i untuk suatu $i \in 1,2,...,k$, maka selimut-H disebut dekomposisi-H. G dikatakan memuat dekomposisi$-H$ atau G terdekomposisi atas H [1]. Super (a,d)-H total dekomposisi diperoleh dengan melabeli titik sebuah graf, mencari bobot sisi super (a,d)-H [10], melebeli sisi graf H [7] [12], dan kemudian mencari bobot total sisi super (a, d)-H antimagic total dekomposisi graf H. Graf yang digunakan dalam artikel ini adalah graf Helm. Graf Helm H_n adalah graf yang didapatkan dari sebuah graf roda W_n dengan menambahkan sisi anting-anting pada setiap titik pada sikel. [8]

Teori pelabelan dekomposisi graf sangat bermanfaat untuk sektor transportasi, navigasi, sistem komunikasi, pengkodean dan lain-lain. Ilmu pengkodean sangat dibutuhkan untuk merahasiakan suatu pesan. Teknik untuk membuat pesan rahasia ini dikenal dengan kriptosistem. Kriptosistem merupakan suatu teknik menjaga keamanan data dan informasi agar tidak diketahui dan dibaca oleh pihak yang tidak berwenang. *Ciphertext* diperlukan karena semakin tingginya tingkat kriminalitas pengacakan kode rahasia. Oleh karena itu, penelitian ini akan membuat suatu *ciphertext* yang didasari pada pelabelan dekomposisi graf Helm H_n. Kalimat yang akan di ubah yaitu kalimat yang mengandung huruf saja. Jika terdapat kalimat yang mengandung angka maka angka tersebut akan di ubah ke dalam bentuk alfabet. Hasil penelitian terkait ini terdapat pada [5, 6, 4].

Artikel ini akan menjelaskan tentang dekomposisi dari graf Helm. Akan ditentukan kardinalitas dan teorema-teorema tentang super antimagic total dekomposisi, kemudian akan dikembangkan ke dalam pembuatan *ciphertext*. Dari uraian tersebut maka penulis menulis judul artikel "Super (a, d)-S_3 Antimagic Total Dekomposisi Graf Helm untuk Pengembangan *Ciphertext*".

Lemma yang Digunakan

Misalkan H_n= $(V(H_n), E(H_n))$ adalah graf berhingga dengan $|V(H_n)| = p_G$ dan $E(H_n) = q_G$. Pelabelan pada H_n didefinisikan sebagai suatu fungsi yang memetakan elemen-elemen H_n ke suatu subhimpunan bilangan bulat positif. Daerah definisi dari fungsi ini dapat berupa himpunan titik, himpunan sisi, atau gabungan himpunan titik. Pelabelan tersebut berturut-turut disebut pelabelan titik, pelabelan sisi, atau pelabelan total. Selanjutnya, jumlah semua label yang berkaitan dengan satu elemen pada suatu graf dikatakan bobot dari elemen tersebut. [11], [16], [9], dan [5]

Berdasarkan uraian diatas, Graf helm adalah graf yang memiliki $V(H_n) = \{P\} \cup \{x_i, y_i, 1 \le i \le n\}$, $E(H_n) = \{Px_i, x_ix_{i+1}, x_iy_i, 1 \le i \le n\} \cup \{x_nx_1\}$, $p_G = |V|$=$2n+1$, $q_G = |E|$=$3n$, $p_{H_n} = 4$, dan $q_{H_n} = 3$.

Lemma 1 *[6] Jika graf $H_n(V, E)$ adalah super $(a, d) - S_3$ antimagic total dekomposisi maka*

$$d \le \frac{(p_G - p_H)p_H + (q_G - q_H)q_H}{s - 1}$$

untuk $s = |H_i|$, $p_G = |V|$, $q_G = |E|$, $p_H = |V'|$, $q_H = |E'|$

Bukti.
$(s-1)d \le p_Hp_G - \frac{p_H-1}{2}p_H + q_Hp_G + q_Hq_G - \frac{q_H-1}{2}q_H - a$

$(s-1)d \leq p_H p_G - \frac{p_H-1}{2}p_H + q_H p_G + q_H q_G - \frac{q_H-1}{2}q_H - (\frac{p_H}{2} + \frac{p_H^2}{2} + q_H p_G + \frac{q_H}{2} + \frac{q_H^2}{2})$
$(s-1)d = p_H p_G - \frac{p_H^2}{2} + \frac{p_H}{2} + q_H q_G - \frac{q_H^2}{2} + \frac{q_H}{2} - (\frac{p_H}{2} + \frac{p_H^2}{2} + \frac{q_H}{2} + \frac{q_H^2}{2})$
$(s-1)d = p_H p_G + q_H q_G - p_H^2 - q_H^2$
$(s-1)d = p_H p_G - p_H^2 + q_H q_G - q_H^2$
$(s-1)d = (p_G - p_H)p_H + (q_G - q_H)q_H$
$d \leq \frac{(p_G-p_H)p_H+(q_G-q_H)q_H}{s-1}$
Jadi, untuk $s = |H_i|$, $p_G = |V|$, $q_G = |E|$, $p_H = |V'|$, $q_H = |E'|$ terbukti bahwa $d \leq \frac{(p_G-p_H)p_H+(q_G-q_H)q_H}{s-1}$

Hasil Penelitian

Dekomposisi

Metode penelitian yang digunakan yaitu menentukan kardinalitas dari garf Helm, menentukan d untuk dekomposisi dari S_3, menentukan fungsi titik, fungsi bobot dekomposisi, fungsi sisi, fungsi bobot total dekomposisi, dan pembuatan *ciphertext* untuk suatu pesan rahasia. Berikut akan diuraikan hasil dari penelitian berupa teorema beserta pembuktiannya terkait dekomposisi graf untuk graf Helm dan juga suatu *ciphertext* yang didasari atas teorema tersebut.

Theorem 1 *Graf helm H_n memiliki super $(\frac{31n+15}{2}, 5)$-S_3 antimagic total dekomposisi untuk $n \geq 3$.*

Bukti. Labeli titik graf Helm H_n dengan fungsi f_1 yang didefinikan sebagai berikut:

$$f_1(P) = 1$$

$$f_1(x_i) = \begin{cases} \frac{n+i+2}{2}; & 1 \leq i \leq n, \text{untuk}\, i \in ganjil \\ \frac{i+1}{2}; & 1 \leq i \leq n, \text{untuk}\, i \in genap \end{cases}$$

$$f_1(y_i) = n + i + 1; 1 \leq i \leq n$$

Dengan mudah dapat dipahami bahwa f_1 adalah merupakan fungsi bijektif yang memetakan $f_1 : V(H_n) \to \{1, 2, \ldots, 2n+1\}$. Misal w_{f_1} adalah bobot sisi super $(\frac{31n+15}{2}, 5)$-S_3 antimagic total dekomposisi graf helm H_n untuk $n \geq 3$, maka dapat diturunkan sebagai berikut:

$$w_{f_1} = \frac{3n + 4i + 9}{2}; 1 \leq i \leq n$$

Kemudian labeli sisi graf Helm H_n dengan fungsi f yang didefinikan sebagai berikut:

$$f_1(Px_i) = 2n + i + 1; 1 \leq i \leq n$$

$$f_1(x_i x_{i+1}) = 3n + i + 11 \leq i \leq n$$

$$f_1(x_n x_1) = 4n + 1$$

dan

$$f_1(x_iy_i) = 4n + i + 1; 1 \le i \le n$$

Misal W_{f_1} adalah bobot total sisi super $(\frac{31n+15}{2}, 5)$-S_3 antimagic total dekomposisi graf helm H_n untuk $n \ge 3$, maka dapat diturunkan sebagai berikut:

$$W_{f_1} = \frac{21n + 10i + 15}{2}; 1 \le i \le n$$

Dengan mudah dapat diuraikan untuk masing-masing i pada inerval $1 \le i \le n$ adalah $W_{f_1} = \{\frac{21n+25}{2}, \frac{21n+35}{2}, \ldots, \frac{31n+15}{2}\}$ Sehingga terbukti bahwa Graf helm H_n memiliki super $(\frac{31n+15}{2}, 5)$-S_3 antimagic total dekomposisi untuk $n \ge 3$.

Theorem 2 *Graf helm H_n memiliki super $(\frac{19n+27}{2}, 7)$-S_3 antimagic total dekomposisi untuk $n \ge 3$.*

Bukti. Labeli titik graf Helm H_n dengan fungsi f_2 yang didefinikan sebagai berikut:

$$f_2(P) = 1$$

$$f_2(x_i) = \begin{cases} \frac{n+i+2}{2}; & 1 \le i \le n, \text{untuk}\, i \in ganjil \\ \frac{i+1}{2}; & 1 \le i \le n, \text{untuk}\, i \in genap \end{cases}$$

$$f_2(y_i) = n + i + 1; 1 \le i \le n$$

Dengan mudah dapat dipahami bahwa f_2 adalah merupakan fungsi bijektif yang memetakan $f_2 : V(H_n) \rightarrow \{1, 2, \ldots, 2n + 1\}$. Misal w_{f_2} adalah bobot sisi super $(\frac{19n+27}{2}, 7)$-S_3 antimagic total dekomposisi graf helm H_n untuk $n \ge 3$, maka dapat diturunkan sebagai berikut:

$$w_{f_2} = \frac{3n + 4i + 9}{2}; 1 \le i \le n$$

Kemudian labeli sisi graf Helm H_n dengan fungsi f_2 yang didefinikan sebagai berikut:

$$f_2(Px_i) = 5n - 3i + 2; 1 \le i \le n$$

$$f_2(x_ix_{i+1}) = 5n - 3i + 3; 1 \le i \le n$$

$$f_2(x_nx_1) = 2n + 3$$

dan

$$f_2(x_iy_i) = 5n - 3i + 4; 1 \le i \le n$$

Misal W_{f_2} adalah bobot total sisi super $(\frac{19n+27}{2}, 7)$-S_3 antimagic total dekomposisi graf helm H_n untuk $n \ge 3$, maka dapat diturunkan sebagai berikut:

$$W_{f_2} = \frac{33n - 14i + 27}{2}; 1 \le i \le n$$

Dengan mudah dapat diuraikan untuk masing-masing i pada inerval $1 \le i \le n$ adalah $W_{f_2} = \{\frac{33n+13}{2}, \frac{33n-1}{2}, \ldots, \frac{19n+27}{2}\}$ Sehingga terbukti bahwa Graf helm H_n memiliki super $(\frac{19n+27}{2}, 7)$-S_3 antimagic total dekomposisi untuk $n \ge 3$.

Theorem 3 *Graf helm H_n memiliki super $(\frac{37n+9}{2}, 11)$-S_3 antimagic total dekomposisi untuk $n \geq 3$.*

Bukti. Labeli titik graf Helm H_n dengan fungsi f_3 yang didefinikan sebagai berikut:

$$f_3(P) = 1$$

$$f_3(x_i) = \begin{cases} \frac{n+i+2}{2}; & 1 \leq i \leq n, \text{untuk}\, i \in ganjil \\ \frac{i+1}{2}; & 1 \leq i \leq n, \text{untuk}\, i \in genap \end{cases}$$

$$f_3(y_i) = n + i + 1; 1 \leq i \leq n$$

Dengan mudah dapat dipahami bahwa f_3 adalah merupakan fungsi bijektif yang memetakan $f_3 : V(H_n) \rightarrow \{1, 2, \ldots, 2n + 1\}$. Misal w_{f_3} adalah bobot sisi super $(\frac{37n+9}{2}, 11)$-S_3 antimagic total dekomposisi graf helm H_n untuk $n \geq 3$, maka dapat diturunkan sebagai berikut:

$$w_{f_3} = \frac{3n + 4i + 9}{2}; 1 \leq i \leq n$$

Kemudian labeli sisi graf Helm H_n dengan fungsi f_3 yang didefinikan sebagai berikut:

$$f_3(Px_i) = 2n + 3i - 1; 1 \leq i \leq n$$

$$f_3(x_i x_{i+1}) = 2n + 3i; 1 \leq i \leq n$$

$$f_3(x_n x_1) = 5n$$

dan

$$f_3(x_i y_i) = 2n + 3i + 1; 1 \leq i \leq n$$

Misal W_{f_3} adalah bobot total sisi super $(\frac{37n+9}{2}, 11)$-S_3 antimagic total dekomposisi graf helm H_n untuk $n \geq 3$, maka dapat diturunkan sebagai berikut:

$$W_{f_3} = \frac{15n + 22i + 9}{2}; 1 \leq i \leq n$$

Dengan mudah dapat diuraikan untuk masing-masing i pada inerval $1 \leq i \leq n$ adalah $W_{f_3} = \{\frac{15n+31}{2}, \frac{15n+3}{2}, \ldots, \frac{37n+9}{2}\}$ Sehingga terbukti bahwa Graf helm H_n memiliki super $(\frac{37n+9}{2}, 11)$-S_3 antimagic total dekomposisi untuk $n \geq 3$.

Aplikasi

Tingkat kriminalitas pengacakan kode yang semakin meningkat membuat para pemilik pesan rahasia harus lebih waspada. Permasalahan ini adalah termasuk bagian aplikasi total dekomposisi dalam *cryptography*. *Cryptography* adalah sebuah teknik merubah dari *plaintext* (kalimat pesan) ke dalam ciphertext (kalimat rahasia yang akan dikembangkan)[15]. Ciphertext merupakan bentuk pesan yang tersandi ke bentuk lain yang tidak dapat dipahami [13] [14]. Misalnya pesan rahasia yang akan dikirim adalah "20127 adalah PIN kartu kredit anda". Pelabelan yang digunakan untuk mengubah pesan tersebut yaitu pelabelan total dekomposisi pada graf Helm H_9 dengan $d = 7$ (sesuai teorema 2).

Setelah melabeli graf Helm, dilanjutkan dengan mendata huruf dan angka yang digunakan dalam pesan dengan mengabaikan spasi dan tanda baca. Angka yang digunakan dalam pesan di ubah dalam bentuk alphabet yaitu menjadi "dua nol satu dua tujuh adalah PIN kartu kredit anda". Huruf yang digunakan adalah a, d, e, h, i, j, k, l, n, o, p, r, s, t, dan u. Langkah awal untuk merubah huruf tersebut yaitu dengan diagram pohon yang berakar di label 1. Cabang dari label 1 disesuaikan dengan cabang di graf Helm (H_9). Cabang tersebut diberi nama layer pertama. Layer kedua dimulai dari sebelah kiri cabang dari layer pertama. Jumlah cabang disesuaikan dengan jumlah huruf yang digunakan dalam pesan rahasia. Label sisi diletakkan di garis penghubung 2 titik (sesuai dengan label sisi pada graf Helm (H_9)).

Letakkan huruf-huruf yang digunakan dalam pesan sesuai dengan abjad (abjad awal diletakkan di cabang kiri), dan urutkan label sisinya. Kemudian pesan rahasia dipecahkan dengan menerapkan teknik kriptosistem modulo 26 terhadap masing-masing hurufnya sehingga menjadi $a = mod(4145, 26) = 11$, $d = mod(4142, 26) = 8$, $e = mod(4143, 26) = 9$, $h = mod(3539, 26) = 3$, $i = mod(3536, 26) = 0$, $j = mod(3537, 26) = 1$, $k = mod(2933, 26) = 21$, $l = mod(2930, 26) = 18$, $n = mod(2931, 26) = 19$, $o = mod(23, 26) = 23$, $p = mod(44, 26) = 18$, $r = mod(38, 26) = 12$, $s = mod(32, 26) = 6$, $t = mod(26, 26) = 0$, dan $u = mod(20, 26) = 20$.

Kemudian hasil modulo tersebut dikombinasikan dengan label titik terakhir untuk menghindari terjadinya kesamaan bilangan diantara *ciphertext*. Dituliskan sebagai berikut $a = mod(611, 26) = 13$, $d = mod(78, 26) = 0$, $e = mod(129, 26) = 25$, $h = mod(73, 26) = 21$, $i = mod(80, 26) = 2$, $j = mod(141, 26) = 11$, $k = mod(821, 26) = 15$, $l = mod(918, 26) = 8$, $n = mod(1619, 26) = 7$, $o = mod(523, 26) = 3$, $p = mod(618, 26) = 20$, $r = mod(712, 26) = 10$, $s = mod(86, 26) = 8$, $t = mod(90, 26) = 12$, $u = mod(1020, 26) = 6$. Kombinasi titik dan sisi tersebut di ubah dalam bentuk modulo 26, sehingga diperoleh *ciphertext* yaitu a=n, d=a, e=z, h=v, i=c, j=l, k=p, l=i, n=h, o=d, p=u, r=k, s=i, t=m, dan u=g. Oleh karena itu, dengan menggunakan proses substitusi pesan kedalam *ciphertext* tanpa spasi dan tanda baca, maka *ciphertext* dari pesan "duanolsatuduatujuhadalahpinkartukreditanda" adalah "agnhdiinmgagnmglgvnaninvuchpnkmgpkzacmnhan".

Kesimpulan

Berdasarkan hasil penelitian diatas, maka kita dapat menyimpulkan bahwa:

- Graf helm H_n memiliki super $(\frac{31n+15}{2}, 5)$-S_3 antimagic total dekomposisi untuk $n \geq 3$.
- Graf helm H_n memiliki super $(\frac{19n+27}{2}, 7)$-S_3 antimagic total dekomposisi untuk $n \geq 3$.

- Graf helm H_n memiliki super $(\frac{37n+9}{2}, 11)$-S_3 antimagic total dekomposisi untuk $n \geq 3$.
- *Ciphertext* untuk pelabelan dekomposisi graf Helm dengan $d = 7$ dari pesan "duanolsatuduatujuhadalahpinkartukreditanda" adalah "agnhdiinmgagnmglgvnaninvuchpnkmgpkzacmnhan"

References

[1] A.E. Hader,A. N. M Salman, An A_M-Supermagic Decomposition Of The Cartesian Product Of a Path and Sun, Artikel, 2013.

[2] AK Purnapraja, R Hidayat, Cycle-Super Antimagicness of Connected and Disconnected Tensor Product of Graphs, *Procedia Computer Science*, **74**, (2015), 9399

[3] Dafik, M. Miller, J. Ryan and M. Bača, Antimagic labeling of the union of stars, *Australasian Journal of Combinatorics*, **42** (2008), 4909-4915.

[4] Dafik Dafik, A.I. Kristiana, S. Setiawani, K.M.F. Azizah, Generalized Shackled of Fans is a Super (a, d)-edge-antimagic Total Graph, **Journal of Graph Labeling**, **Vol. 2, Issue 1**, (2016), 59-68

[5] Dafik, M. Miller, J.Ryan and M.Baca, On super (a,d)-edge antimagic total labeling of disconnected graphs, Discrite Math, (To appear).

[6] Dafik, Structural Properties and Labeling of Graphs, University of Ballarat, 2007.

[7] Erni Novianti, Dekomposisi Cyclic dari Graf Lengkap, Graf Graceful, dan Aplikasinya dalam Telecommand Codes, Artikel, 2012.

[8] Gallian, J.A. 2007. "dynamic Survey DS6: Graph Labeling" Electronic J. Combinatorics. DS6. (online): http://mathword.wolfram.com/www.combinatorics.-org/surveys/ds6.pdf. Diakses tanggal 27 Juni 2015.

[9] Joseph A. Gallian, A Dynamic Survey of Graph Labeling, University of Minnesota, 1997.

[10] M. Baca, Y. Lin, M. Miller and M.Z. Youssef, Edge-antimagic graphs, Discrete Math, 2007.

[11] Nur Inayah, Pelabelan $(a, d) - H$-Anti Ajaib Pada Beberapa Kelas Graf, Disertasi, Not Publicated, Institut Teknologi Bandung, 2013.

[12] Nur Rahmawati, Dekomposisi graf sikel, graf roda, graf gir dan graf persahabatan, Skripsi, Not Publicated, Universitas Negeri Surabaya, 2014.

[13] Ongko, Erianto. 2013. *Aplikasi Pembelajaran Kriptografi Klasik dengan Visual Basic .NET*. Medan: STMIK IBBI.

[14] Palupi, Retno. 2008. *Kriptosistem Kunci Asimetrik Menggunakan Algoritma Genetika Pada Data Citra.* (Vol 1 No 1)

[15] Pearson, E. 2006. *Introduction To Cryptography With Coding Theory.* America: United States of America

[16] W.D. Wallis, E.T. Baskoro, M. Miller and Slamin, Edge-magic total labelings, Austral, J. Combin., 2000.