Pengembangan Kriptosistem Polyalphabetic Cipher dengan Pelabelan Edges Antimagic Total pada Graf Tribun

Muhlisatul Mahmudah, S. Pd., M. Si
Maxlisa742@gmail.com
Universitas Islam Jember

Abstrak

Sebuah graf G yang memiliki jumlah titik p dan jumlah sisi q jika terdapat fungsi bijektif $f{:}(V(G)E(G)) \rightarrow \{1,2,...,p+q\}$ dimana bobot sisinya $w(uv) = f(u)+f(v)+f(uv)$; ; $uv,(G)$ dari barisan aritmatika dengan nilai awal a dan beda d. Maka graf G disebut super jika pelabelan terkecil terletak pada titik. Pada artikel ini dikaji mengenai pelabelan total super (a,d)-sisi antimagic pada graf Tribun dan aplikasi dalam pengembangan polyalphabetic cipher. Dalam peneltian ini, dihasilkan pelabelan total super (a,d)-sisi antimagic pada graf Tribun tunggal untuk d=0,1,2 dan dapat digunakan untuk pengembangan polyalphabetic cipher.

Kata Kunci: ***Pelabelan total super (a,d)-sisi antmagic, graf Tribun, polyalhabetic cipher.***

Abstrack

A graph G of order p and size q is an called an (a,d)-edge antimagic total if there exist a bijection $f{:}(V(G)E(G)) \rightarrow \{1,2,...,p+q\}$ such that the edge-weights, $w(uv) = f(u)+f(v)+f(uv)$; ; $uv,(G)$ form an arithmetic sequence with ¯first term a and common diference d. Such a graph G is called *super* if the smallest possible labels appear on the vertices. In this paper we will study a super edge-antimagic total Tribun Graph and the application of developing of polyalphabetic cryptosystem. The result shows that connected Tribun Graph admits a super ($a;$ d)-edge antimagic total labeling for d = 0,1,2, and it can be used to develop a secure polyalphabetic cryptosystem.

Keywords: ***Super (a; d)-edge-antimagic total labeling, Tribun graph polyalphabetic cryptosystem***.

PENDAHULUAN

A. Latar Belakang

Sebuah graf didefinisikan sebagai pasangan terurut himpunan (V,E) dimana V adalah sebuah himpunan tidak kosong yang berhingga yang anggota-anggotanya dinamakan simpul (*vertex*). E adalah sebuah himpunan sisi (*edge*) yang menghubungkan sepasang simpul. Graf dilambangkan dengan $G = (V,E)$. Dimana V tidak boleh kosong, sedangkan E boleh kosong. Jadi, sebuah graf dimungkinkan tidak mempunyai sisi satu buah pun, tetapi Vertexnya harus ada minimal satu. Bila (V,E) adalah himpunan berhingga maka graf yang demikian disebut dengan graf berhingga (*finite graph*).

Suatu graf dengan p buah vertexs dan q buah sisi ditulis dengan $G(p,q)$. Secara umum graf dapat digambarkan dengan suatu diagram dimana vertexs yang ditunjukkan sebagai titik yang dinotasikan dengan v_i i = $1,2,3, \ldots$ dan sisi yang digambarkan dengan sebuah garis lurus atau dengan garis lengkung yang menghubungkan dua vertexs v_i, v_j dan dinotasikan e_k, k = 1, 2, 3, …., q disebut dengan titik-titik dari e_k.

Teori pelabelan graf ini 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. Penelitian ini akan membuat suatu ciphertext yang didasari pada pelabelan graf bersisi genap yang dimisalkan dengan graf H. Dikarenakan graf ini mudah dilabeli titik dan sisinya.

Penggunaan internet sangat luas seperti pada bisnis, perdagangan, bank, industri dan pemerintahan yang umumnya mengandung informasi yang bersifat rahasia maka keamanan in formasi menjadi faktor utama yang harus dipenuhi. Salah satu metode yang digunakan untuk memenuhi masalah tersebut yaitu aplikasi dari pelabelan graf yang dinamakan kriptografi. [8]menyatakan kriptografi merupakan studi tentang teknik-teknik matematika yang berhubungan dengan aspek-aspek pengamanan informasi seperti kerahasiaan (*confidentiality*), keutuhan data (*data integrity*), otentikasi entitas (*enity authentication*) dan otentikasi asal data (on *data origin authenrication*). Dalam artikel kami meneliti tentang pengembangan kriptosistem polyalphabetic cipher pada graf tribun yang dinotasikan dengan $\Im_n$.

B. Rumusan Masalah

1. Bagaimana pelabelan total super (a,d)-sisi antimagic yang tunggal untuk graf Tribun?
2. Bagaimana aplikasi pengembangan kriptosistem polyalphabetic cipher terhadap pelabelan total super (a,d)-sisi antimagic pada graf tribun?

C. Tujuan

1. Dapat mengetahui elabelan total super (a,d)-sisi antimagic yang tunggal untuk graf Tribun
2. Mengetahui aplikasi pengembangan kriptosistem polyalphabetic cipher terhadap pelabelan total super (a,d)-sisi antimagic pada graf tribun

TELAAH LITERATUR

Penggunaan graf dilakukan pertama kali untuk memecahkan masalah yang terkenal dengan nama Masalah Jembatan Konigsberg, yang dilakukan pada tahun 1736. Orang yang pertama kali mempunyai ide untuk memecahkan masalah jembatan ini adalah L. Euler, matematikawan asal Swiss, ketika mencoba membuktikan kemungkinan untuk melewati empat daerah yang terhubung dengan tujuh jembatan di atas sungai Pregel di Konigsberg, Jerman hanya dalam sekali waktu atau tidak boleh diulang lalu kembali ke tempat semula (tanpa berenang melalui sungai). Dua bagian yang penting dalam representasi graf adalah simpul (*vertex*) dan ruas (*edge*). Sehingga graf bisa dikatakan sebagai himpunan dari simpul dan ruas.

Metode pengaplikasiannya pun tidak sesederhana teori. Karena variabel di dunia nyata bukan sekedar jarak saja, ada banyak aspek-aspek lain baik berupa aspek sosial, ekonomi, maupun aspek yang bersifat matematis lainnya yang tidak dapat diabaikan. Dan salah manfaat daari teori graf yaitu pengkodean. 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. Penelitian ini akan membuat suatu ciphertext yang didasari pada pelabelan graf bersisi genap yang dimisalkan dengan graf H. Dikarenakan graf ini mudah dilabeli titik dan sisinya Penggunaan internet yang sangat luas seperti pada bisnis, perdagangan,bank, industri dan pemerintahan yang umumnya mengandung informasi yang bersifat rahasia maka keamanan informasi menjadi faktor utama yang harus dipenuhi. Salah satu cara yang digunakan adalah dengan menyandikan isi \ informasi menjadi suatu kode-kode yang tidak dimengerti sehingga apabila disadap, maka akan kesulitan untuk mengetahui isi informasi yang sebenarnya. Salah satu alat yang digunakan untuk mengamankan data dan informasi adalah Kriptografi.

(Menezes dkk,1996) menyatakan Kriptografi merupakan studi tentang teknik-teknik matematika yang berhubungan dengan aspek-aspek pengamanan informasi seperti kerahasiaan (contendentiality), keutuhan data (data integrity), otentikasi entitas (entity authentication) dan otentikasi asal data (data origin authentication).

METODE PENELITIAN

Untuk mencari batas atas nilai beda *d* pelabelan total super (*a*,*d*)-sisi antimagic dapat di tentukan dengan teorema berikut (Dafik, 2007):

Teorema 1 *Jika sebuah graf* (*p*, *q*) *adalah pelabelan total super* (*a; d*)*-sisi antimagic maka* $d \leq \frac{2p+q-5}{q-1}$

(M. Bacaa, 2014) menjelaskan bahwa hubungan antara EAVL dengan SEATL yaitu pada proporsisi 1, dan dimotivasi dari (KA Sugeng, 2005) maka diperoleh teorema 3

Proporsisi 1 *Jika sebuah graf G memiliki pelabelan titik (a, d)-sisi antimagic maka graf G memiliki pelabelan total super* (*a*+|*V* |+1,*d*+1)*-sisi antimagic dan pelabelan total super* (*a* + |*V* | + |*E*|, *d-1*)*-sisi antimagic*.

Lemma 1 *Misalkan γ adalah barsan ψ = {c,c+1, c+2, …, c+k}, k genap. Maka ada permutasi π (γ) dari anggota ψ seperti ψ + π (ψ)* $=2c+\frac{k}{2}$, $2c+\frac{k}{2}+1, 2c+\frac{k}{2}+2, \ldots, 2c+\frac{3k}{2}-1, 2c+\frac{3k}{2}$.

Untuk mencari batas atas dari bilangan kromatik dapat ditentukan dengan menggunakan teorema seperti berikut:

Teorema 3 *Jika G adalah sebuah graf khusus dengan p titik dan q sisi dan G mempunyai bilangan kromatik* χ *maka hubungannya* $(\chi\text{-}1)p \leq 2q$.

HASIL DAN PEMBAHASAN

Graf Tribun merupakan sebuah graf yang dinotasikan dengan $\Im_n$ dengan himpunan vertex $V = \{B, x_i, z_j, y_i \;; 1 \leq i \leq n; 1 \leq j \leq 2n+1 \; n \in N\}$ dan himpunan edge $E\Im_n$=

$\{Bz_1, Bz_2, Bz_3 \cup z_j z_{j+1} \;; 1 \leq j \leq n \cup x_i x_{2i}; 1 \leq i \leq n \cup x_i x_{2i+3}; 1 \leq i \leq n \cup y_i z_{2i+1}; 1 \leq i \leq n \cup y_i z_{2i-1}; 1 \leq i \leq n\}$
, $p = 4n+2$ dan $q = 8n+1$

nilai n adalah banyaknya titik pada graf Tribun.

Teorema yang pertama adalah teorema yang berkaitan dengan pelabelan titik (a,1)-sisi antimagic yang disajikan dalam teorema berikut.

Teorema 3. Ada pelabelan titik (3,1)-sisi antimagic pada graf Tribun jika $n \geq 1$.

Bukti. Labeli titik graf Tribun dengan fungsi bijektif f_1 yang definisikan sebagai pelabelan f_1: $V\Im_n \rightarrow \{1,2,3,\ldots,4n+2\}$maka pelabelan f_1 dapat dituliskan sebagai berikut:

$f_1(B) = 1$

$f_1(x_i) = 4i+1, untuk\ 1 \leq i \leq n$

$f_1(z_j) = 2j, untuk\ 1 \leq j \leq 2n+1$ untuk $j \in$bilangan ganjil

$f_1(z_j) = 2j-1, untuk\ 1 \leq j \leq 2n+1$ untuk $j \in$bilangan genap

$f_1(y_i) = 4i, untuk\ 1 \leq i \leq n$

Untuk pelabelan titik pada f_1 adalah fungsi bijektif yang memetakan $\Im_n$ ke himpunan bilangan bulat f_1: $V\Im_n \rightarrow \{1,2,3,\ldots,4n+2\}$. Jika wf_1 didefinisikan bobot sisi pelabelan titik f_1 dimana bobot sisi pelabelan titik diperoleh dari penjumlahan 2 buah label titik yang bersisian, fungsi bijektif wf_1 dapat ditentukan melalui pengamatan pola dan penggunaan konsep barisan aritmatika berikut:

$w_{f_1}(Bz_1) = 3$

$w_{f_1}(Bz_2) = 4$

$w_{f_1}(Bz_3) = 7$

$w_{f_1}(z_j z_{j+1}) = 4j + 1 \; untuk \; 1 \leq j \leq 2n$

$w_{f_1}(x_i x_{2i+2}) = 8i + 4 \; untuk \; 1 \leq i \leq n - 1$

$w_{f_1}(x_i x_{2i}) = 8i \; untuk \; 1 \leq i \leq n$

$w_{f_1}(x_i x_{2i+1}) = 8i + 3 \; untuk \; 1 \leq i \leq n$

$w_{f_1}(x_i x_{2i+3}) = 8i + 7 \; untuk \; 1 \leq i \leq n - 1$

$w_{f_1}(y_i z_{2i+1}) = 8i + 2 \; untuk \; 1 \leq i \leq n$

$w_{f_1}(x_i x_{2i-1}) = 8i - 2 \; untuk \; 1 \leq i \leq n$

Berdasarkan bobot sisi EAV ini didapatkan nilai nilai berurutan yang akan membentuk himpunan $w_{f_1} \rightarrow$ {3, 4, 5, ...,8n+3} Dengan demikian f_1 adalah suatu pelabelan titik (3,1). Selanjutnya setelah ditemukan rumus EAV untuk d = 1 maka akan ditentukan rumus SEATL untuk d = 0,2. Menurut Proporsisi 1 didapat:

Teorema 4. Ada pelabelan total super (12n+6,0)-sisi antimagic dan (4n +6, 2)-sisi antimagic pada graf Tribun untuk n ≥ 1.

Bukti. Untuk d=0, dengan menggunakan proporsisi 1 didapat pelabelan $p + 1, p + 2, \dots, p + q$ sehingga terdapat pelabelan f_2 untuk pelabelan total super (a, 0)-sisi antimagic, sehingga a = 3 + p + q = 3 + 4n + 2+ 8n +1 = 12n + 6. Jika w_{f_2} didefinisikan sebagai bobot sisi pelabelan total graf tribun berdasarkan penjumlahan bobot sisi dengan label sisinya maka w_{f_1} sehingga didapat himpunan bobot sisi untuk w_{f_2} dapat ditulis w_{f_1} = {12n + 6, 12n + 6, ... , 12n + 6}. Untuk d=2, dengan menggunakan proporsisi 1 didapat pelabelan p+1,p+2, …, p+q sehingga terdapat pelabelan f_3 untuk pelabelan total super (a, 2)-sisi antimagic, sehingga a = 3 + p + 1 = 3 + 4n + 2+ 1 = 4n + 6. Jika w_{f_3} didefinisikan sebagai bobot sisi pelabelan total graf tribun berdasarkan penjumlahan bobot sisi dengan label sisinya maka w_{f_3} sehingga didapat himpunan bobot sisi untuk w_{f_3} dapat ditulis w_{f_3} = {4n + 6, 4n + 8., ... , 20n + 6. }.

Kemudian d yang akan diteliti adalah d = 1 untuk super edge antimagic total labeling. Dari **teorema 3** dan **lemma 1** maka didapat **teorema 5** sebagai berikut:

Teorema 5. Ada pelabelan total super (8n+6,1)-sisi antimagic pada graf Tribun untuk n ≥ 1.

Bukti. Misalkan c = 3 dan k = q -1 = 8n+1-1=8n, sesuai pada lemma 1 yang mana ψ + [π (ψ)-c+p+1] labeli graf Tribun dengan f_4 untuk pelabelan total super(a,d)-sisi antimagic pada graf Tribun sehingga didapat $a = c + \frac{k}{2} + p + 1 = 3 + \frac{8n}{2} + 4n + 2 + 1 = 8n + 6$

Sedangkan untuk aplikasinya yaitu mengenai ciphertext, Graf yang digunakan dalam ciphertext ini adalah graf Tribun untuk d = 0 dan n = 4. Kalimat rahasia yang akan dikirim adalah "2001 password anda". Untuk membuat pesan rahasia tersebut, langkah awal yang dilakukan adalah melabeli graf Tribun dengan d=0. Label titik dan label sisi pada graf Tribun d = 0 dan n = 4 digunakan angka dari 1 hingga 47. Sebelum meletakkan huruf pada diagram pohon, pengeliminasian cabang perlu dilakukan agar tidak ada kode yang berulang.

Tahap awal untuk mengeliminasi cabang yaitu dengan menjumlahkan titik graf tribun dengan jumlah keseluruhan huruf alfabet. Jumlah titik yang digunakan adalah 15 dan jumlah alfabet adalah 26, maka penjumlahan keduanya diperoleh 41. Label sisi atau cabang yang harus di eliminasi yaitu label sisi yang lebih besar dari jumlah titik graf Tribun dengan jumlah alfabet. Dengan demikian, label sisi yang harus di eliminasi adalah label 49, 50, 51, 52, 53, 54. Setelah pengeliminasian dilakukan, langkah selanjutnya adalah membuat digram pohon yang berakar di label 13 dengan dilengkapi label sisinya.

Langkah selanjutnya yaitu memasang semua alfabet yaitu dari a sampai z pada setiap cabang diagram pohon. Penempatan alfabet ini harus berurutan dari kiri ke kanan dan dimulai dari layer pertama. Setelah penempatan alfabet dilakukan, selanjutnya adalah menghitung nilai modulo dari setiap cabang atau label sisi sesuai dengan letak alfabet. Pesan rahasia dipecahkan dengan menerapkan teknik kriptosistem modulo 26 terhadap masing-masing huruf alfabet sehingga menjadi a = mod(44,26) = 18, b = mod(47,26) = 21, c = mod(48, 26) = 22, d = mod(41,26) = 15, e = mod(40, 26) = 14, f = mod(43, 26) = 17, g = mod(45, 26) =19, h = mod(46, 26) = 20, i = mod(39, 26) = 13, j = mod(38, 26) = 12, k = mod(36, 26) = 10, l = mod(42, 26) = 16, m = mod(34, 26) =8, n = mod(32, 26) = 6, o = mod(33, 26) = 7, p = mod(37, 26) = 11, q = mod(35, 26) = 9, r = mod(27,26) = 1, s = mod(29, 26) = 3, t = mod(30, 26) = 4, u = mod(28, 26) = 2, v = mod(31, 26) = 5, w = mod(23, 26) = 23, x = mod(24, 26) = 24, y = mod(25, 26) = 25, dan z = mod(26, 26) = 26. Teknik modulo dilihat pada tabel 1.

Tabel 1. Teknik Modulo 26 untuk Ciphertext pada Super (a,d)-sisi Antimagic Total pada graf Tribun untuk d=0

abjad	Label sisi	Modulo 26	ciphertext
A	44	18	R
B	47	21	U
C	48	22	V
D	41	15	O
E	40	14	N
F	43	17	Q
G	45	19	S
H	46	20	T
I	39	13	M
J	38	12	L
K	36	10	J
L	42	16	P
M	34	8	H
N	32	6	F
O	33	7	G
P	37	11	K
Q	35	9	I
R	27	1	A
S	29	3	C
T	30	4	D
U	28	2	B
V	31	5	E
W	23	23	W
X	24	24	X
Y	25	25	Y
Z	26	26	Z

Maka ciphertext dari semua alfabet yaitu a = r, b = u, c = v, d = o, e = n, f = q, g = s, h = t, i = m, j = l, k = j, l = p, m = h, n = f, o = g, p = k, q = i, r = a, s = c, t = p, u =b, v = e, w = w, x =x, y = y, z = z. Oleh karena itu, dengan menggunakan proses substitusi pesan ke dalam ciphertext tanpa spasi dan tanda baca, maka ciphertext dari pesan "duanolenamsatuduasatuadalahpasswordanda" adalah “obrimuucrpbyqwxqnqfqibqyyuczn” .

KESIMPULAN

A. Graf yang memiliki sisi ganjil yaitu graf Tribun untuk tunggal memiliki pelabelan total super (a, d)-sisi antimagic untuk d = 0,1,2.

B. Untuk aplikasi pengembangan kriptosistem polyalphabetic cipher terhadap pelabelan total super (a,d)-sisi pada graf Tribun menggunakan proses substitusi pesan ke dalam ciphertext tanpa spasi dan tanda baca, maka ciphertext dari pesan "2001 adalah password anda". adalah “obrimuucrpbyqwxqnqfqibqyyuczn”

DAFTAR PUSTAKA

Dafik. 2007. Structural Properties and Labeling of Graph.Australia: Tidak dipublikasikan (Tesis).

K.A. Sugeng, M.Miller and M.Ba·ca, Super edge-antimagic total labelings, Utilitas Math.,71 (2006) 131-141.

K.A. Sugeng, M.Miller,Slamin and M.Baca, (a, d)-edge-antimgic total labelings of caterpillars, Lecture Notes in Computer Science, 3330 (2005) 169-180

M. Baca, Antoni Muntaner-Batle, Andrea Semanecova Fenovcikova, On super (a,2)- edge-antimagic total labeling of disconnected Graphs, Ars Combinatoria,113(2014) 129-137

M. Baca, Dafik, M.Miller and J.Ryan, On super (a,d)-edge-antimagic total labeling,J.Combin. Math.Combin. Comput., 65 (2008),61-70.

M. Baca,Yuqing Lin, Andrea Semanecova Fenovcikova, 2009, Note On Super An- timagicness of Disconnected Graphs,AKCE International J.of Graphs and Combinatorics, 6(1), 47-55

Menezes,A., Ooschot,P.V., dan Vanstone. 1996. Handbook of Applied Cryptography. CRC Press:Boca Raton.

Mirka Miller, Oudone Phanalasy, Joe Ryan, and Leanne Raylands, Note on Antimagic Labeling of Trees, Bulletin of the ICA, 72 (2014) 94-100.

R.Simanjuntak, F.Bertault and M.Miller, Two new (a,d)-antimagic graph labeling, Proc. of Eleventh Australasian Workshop on Combinatorial Algorithms,(2000), 179-189