E ISSN 2615-0697 dan P ISSN 2622-8149
11 – 19

Aplikasi *Kriptosistem Polyalphabetic Cipher*

Muhlisatul Mahmudah [1], Tri Novita Irawati [2]
maxlisa742@gmail.com
Universitas Islam Jember

Abstrak

Kriptosistem polyalphabetic cipher merupakan studi tentang teknik-teknik matematika yang berhubungan dengan aspek-aspek pengamanan informasi seperti kerahasiaan, keutuhan data, otentikasi dan otentikasi asal data. Dengan adanya internet, komunikasi jarak jauh dapat dilakukan dengan cepat dan murah. Namun internet tidak terlalu aman karena merupakan media komunikasi umum yang dapat digunakan oleh siapapun sehingga sangat rawan terhadap penyadapan informasi. *Kriptografi* telah banyak digunakan dalam kehidupan contohnya pin atm perbankan, no rekening diperbankan, pengiriman pesan rahasia militer. Dengan menerapkan *kriptosistem polyalphabetic cipher* maka pin, no rekening dan pesan rahasia yang dikirim akan lebih terjaga kerahasiannya dan tidak akan mudah diketahui informasi yang disampaikan.
Kata kunci: *kriptosistem polyalphabetic cipher,* perbankan, pin

Abstrack

Polyalphabetic cipher cryptosystem is the study of mathematical techniques that related to aspects of information security such as confidentiality, data integrity, authentication and authentication of data origin. With the internet, long distance communication can be done quickly and cheaply. However, the internet is not very secure because it is a public communication medium that can be used by anyone so it is very vulnerable to information tapping. Cryptography has been widely used in life for example banking atm ATMs, account numbers sacrificed, sending secret military messages. By applying polyalphabetic cipher cryptosystems, pins, account numbers and secret messages sent will be more secure and the information will not be easily known.
Keywords: *polyalphabetic cipher cryptosystem, banking, pin.*

PENDAHULUAN

[1]Dosen Program Studi Pendidikan Matematika FKIP Universitas Islam Jember
[2]Dosen Program Studi Pendidikan Matematika FKIP Universitas Islam Jember

Teori graf dapat diaplikasikan dalam berbagai bidang, seperti bidang pertanian, perhutanan, keamanan dan lain-lain. Dalam kaitannya dengan keamanan salah satu topik yang menarik pada teori graf yang dapat digunaka adalah *kriptositem polyalphabetic cipher*. Penelitian ini nantinya juga akan menarik topic tentang *kriptositem polyalphabetic cipher*.

Kemajuan dan perkembangan teknologi informasi dewasa ini telah berpengaruh hampir pada semua aspek kehidupan manusia, tak terkecuali dalam hal berkomunikasi. Dengan adanya internet, komunikasi jarak jauh dapat dilakukan dengan cepat dan murah. Namun di sisi lain, ternyata internet tidak terlalu aman karena merupakan media komunikasi umum yang dapat digunakan oleh siapapun sehingga sangat rawan terhadap penyadapan informasi oleh pihak-pihak yang tidak berhak mengetahui informasi tersebut. Oleh karena penggunaan internet yang sangat luas seperti pada bisnis, perdagangan, bank, industri dan pemerintahan yang umumnya mengandung informasi yang bersifat rahasia keamanan informasi menjadi faktor utama yang harus dipenuhi. Berbagai hal telah dilakukan untuk mendapatkan jaminan keamanan informasi rahasia. Oleh karena itu, dibutuhkan penyandian isi informasi menjadi suatu kode-kode yang tidak dimengerti sehingga apabila disadap atau dilacak maka akan kesulitan untuk mengetahui isi informasi yang sebenarnya. Salah satu alat yang digunakan untuk mengamankan data informasi adalah *Kriptografi (Kriptosistem polyalphabetic cipher). Kriptografi* berasal dari kata Yunani kripto artinya tersembunyi dan grafia artinya tulisan.

Dalam teori graf *kriptosistem polyalphabetic cipher* (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 (*data origin authenrication*). Sistem kriptografi (*cryptosystem*) adalah kumpulan yang terdiri dari algoritma kriptografi, semua *plaintext, ciphertext*, dan kunci yang mungkin. *Plaintext* atau pesan adalah data yang dapat dibaca dan dimengerti maknanya, sedangkan ciphertext adalah bentuk pesan yang tersandi ke bentuk lain yang tidak dapat dipahami.

Kriptografi telah banyak digunakan dalam kehidupan contohnya pin atm perbankan, no rekening diperbankan, pengiriman pesan rahasia militer. Dengan menerapkan kriptosistem polyalphabetic cipher maka pin, no rekening dan pesan rahasia yang dikirim akan lebih terjaga kerahasiannya dan tidak akan mudah diketahui informasi yang disampaikan. Salah satu aplikasi graf seperti SEATL dapat digunakan dalam pengembangan *kriptosistem polyalpabhetic cipher*. Misalnya kalimat rahasia yang akan dikirim adalah "nama dena kode nemo" permasalahan ini adalah termasuk bagian aplikasi SEATL dalam *cryptography*. *Cryptography* adalah sebuah teknik merubah dari *plaintext* (kalimat pesan) ke dalam *ciphertext* (kalimat rahasia yang akan dikembangkan). *Ciphertext* merupakan bentuk pesan yang tersandi ke bentuk lain yang tidak dapat dipahami.

Dalam penelitian ini, penulis meneliti aplikasi dalam pengembangan *kriptosistem polyalphabetic cipher* terhadap kehidupan sehari-hari dengan menggunakan graf bersisi genap yaitu graf H terhadap alphabet.

METODE

Metode yang digunakan dalam penelitian ini adalah pendeteksian pola *(pattern recognition),* yaitu dengan cara mencari label graf yang digunakan yaitu graf H sebanyak huruf alfabet yang ada. Selanjutnya dari graf H tersebut dibuat menjadi graf pohon dengan dilengkapi label sisinya. Selain itu metode yang digunakan dalam penelitian ini adalah deduktif aksiomatik yaitu metode penelitian yang menggunakan prinsip-prinsip pembuktian deduktif yang berlaku dalam logika matematika dengan menggunakan aksioma atau teorema yang telah ada untuk memecahkan masalah. Penelitian ini akan menghasilkan teorema-teorema baru yang telah dibuktikan secara deduktif sehingga kebenarannya berlaku secara umum.

HASIL DAN PEMBAHASAN

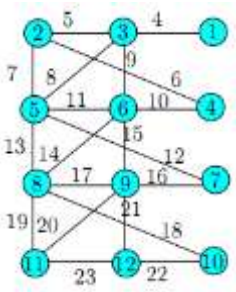
(1) Memilih sembarang graf

Untuk pembuatan chipertext alfabet memilih beberapa sembarang graf yang telah dilabeli, pilihlah graf dimana jumlah sisinya harus sesuai dengan banyaknya jumlah alphabet yang ada yaitu 26. Sedangkan untuk pembuatan chipertext angka,

pilih grf yang memiliki jumlah sisi sesuai dengan banyaknya jumlah angka yang ada yaitu 10. Peneliti memilih graf H dengan sisi genap untuk dilabeli sisinya, hal ini dikarenakan graf yang bersisi genap belum banyak ditemukan pelabelannya hal itu dapat menambah kesulitan untuk meretas kata sandi yang akan dibuat. Graf H mempunyai pelabelan total super (a,d)-sisi antimagic untuk mendapatkan EAV $d = 1$ dan SEATL $d = 0,2$. Teorema 5.1 adalah teorema yang berkaitan dengan pelabelan titik (a,1)-sisi antimagic pada graf H.

Teorema 5.1 Ada pelabelan titik (4,1)-sisi antimagic pada graf H yang bersisi genap jika n ≥ 1.

Dengan demikian wf_1 adalah suatu pelabelan titik (4,1).



Gambar 5.1 Pelabelan Titik dan Sisi (4,1) pada Graf H

Gambar 5.1 merupakan contoh pelabelan titik dan sisi (4,1)-sisi antimagic beserta bobot sisi EAVL untuk graf H dengan d = 1. Selanjutnya setelah ditemukan rumus EAV untuk d = 1 maka akan ditentukan rumus SEATL untuk d= 0,2. Berdasarkan Teorema 5.1 maka diperoleh pelabelan titik (4,1)-sisi antimagic selanjutnya pelabelan total super sisi antimagic dengan nilai awal *a* dan nilai beda d = 0 dan d = 2. Menurut Proporsisi 1 didapat:

Teorema 5.2: Ada pelabelan total super (9n + 9, 0)-sisi antimagic dan (3n +8,2) sisi antimagic pada graf H untuk n≥1.

Bukti. Untuk d = 0 kita telah membuktikan bahwa graf H memiliki pelabelan titik (4,1)-sisi antimagic pada teorema 4.1.4. Dengan menggunakan proporsisi 1 maka didapat pelabelan sisi $p + 1, p + 2, \ldots, p + q$, sehingga terdapat pelabelan wf_2 untuk pelabelan total super $(a,0)$-sisi antimagic, dimana $p = 3n + 3$ dan $q = 6n + 2$,maka $a = 4 + p + q = 4 + 3n + 3 + 6n + 2 = 9n + 9$

Jika wf_2didefinisikan sebagai bobot sisi pelabelan total graf H berdasarkan

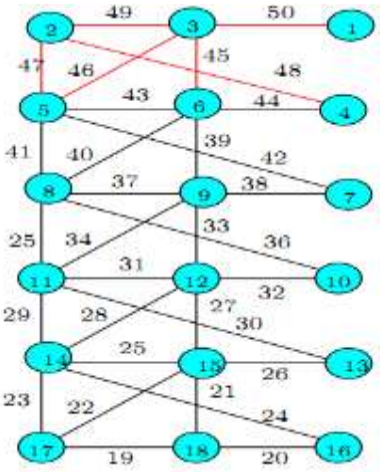
penjumlahan bobot sisi dengan label sisinya maka wf_2 sehingga didapat himpunan bobot sisi untuk wf_2 dapat ditulis $wf_2 = \{9n + 9, 9n + 9, \dots, 9n + 9\}$. Dapat disimpulkan bahwa graf H dengan n≥1, mempunyai pelabelan total super(a, d)-sisi antimagic dengan $a = 9n + 9$ dan d = 0, dengan kata lain graf H mempunyai pelabelan total super $(9n + 9, 0)$ −sisi antimagic. Untuk d = 2 kita juga telah membuktikan bahwa graf H memiliki pelabelan titik (4,1)-sisi antimagic pada teorema 5.1

Dengan menggunakan proporsisi 1 maka didapat pelabelan sisi $p + 1, p + 2, \dots, p + q$, sehingga terdapat pelabelan wf_3 untuk pelabelan total super (a, 2)-sisi antimagic, dimana $p = 3n + 3$, sehingga $a = 4 + p + 1 = 4 + 3n + 3 + 1 = 3n + 8$. Jika wf_3 didefinisikan sebagai bobot sisi pelabelan total graf H berdasarkan penjumlahan bobot sisi dengan label sisinya maka wf_3 maka dapat dikatakan bahwa wf_3 membentuk barisan aritmatika dengan suku awal $a = 3n + 8$ yang ada pada fungsi $wf_3(x_i y_i)$ dan beda 2 (dua), sehingga kita dapat menentukan bobot sisi terbesar berada pada fungsi $wf_3(y_i z_i)$ dengan mensubstitusikan nilai awal $a = 3n + 8$ dan nilai $d = 2$ ke persamaan $Un = a + (n - 1)b = 3n + 8 + (6n + 2 - 1)2$ dan didapatkan $u_n = 15n + 10$. Sehingga didapat $\{3n + 8, 3n + 10, \dots, 15n + 10\}$ Dapat disimpulkan bahwa graf H mempunyai pelabelan total super(a,d)-sisi antimagic dengan $a = 3n + 8$ dan $d = 2$.

Dari teorema 5.1 dan 5.2 terbukti bahwa graf yang memiliki sisi genap dimana diambil contohgraf H memiliki pelabelan titik (4, 1)-sisi antimagic, dan pelabelan total super (a, d)-sisi antimagic untuk d = 0, d = 2.

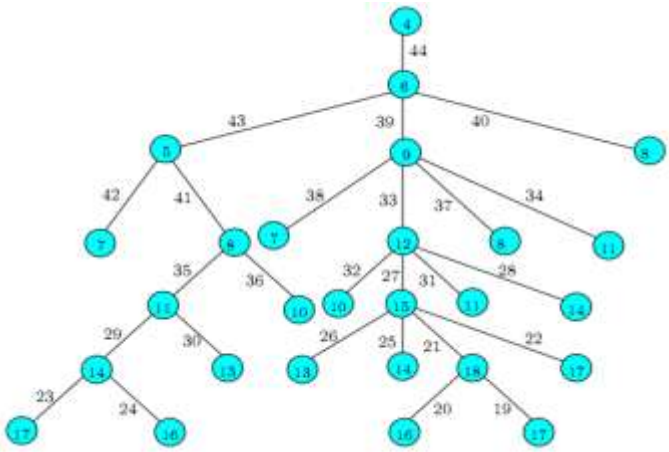
(2) Menjadikan graf yang dipilih kebentuk graf pohon dilengkapi label sisinya

Untuk *chipertext alphabet* graf yang digunakan dalam adalah contoh graf yang bersisi genap yang kita misalkan dengan graf H dengan n=5. Sandi yang akan dirubah dari *plaintext* menuju *chipertext* adalah password dan ussername dosen pendidikan matematika Universitas Islam Jember. Untuk membuat *chipertext*, langkah awalnya yaitu melabeli graf graf H dengan d=0 untuk n=5.



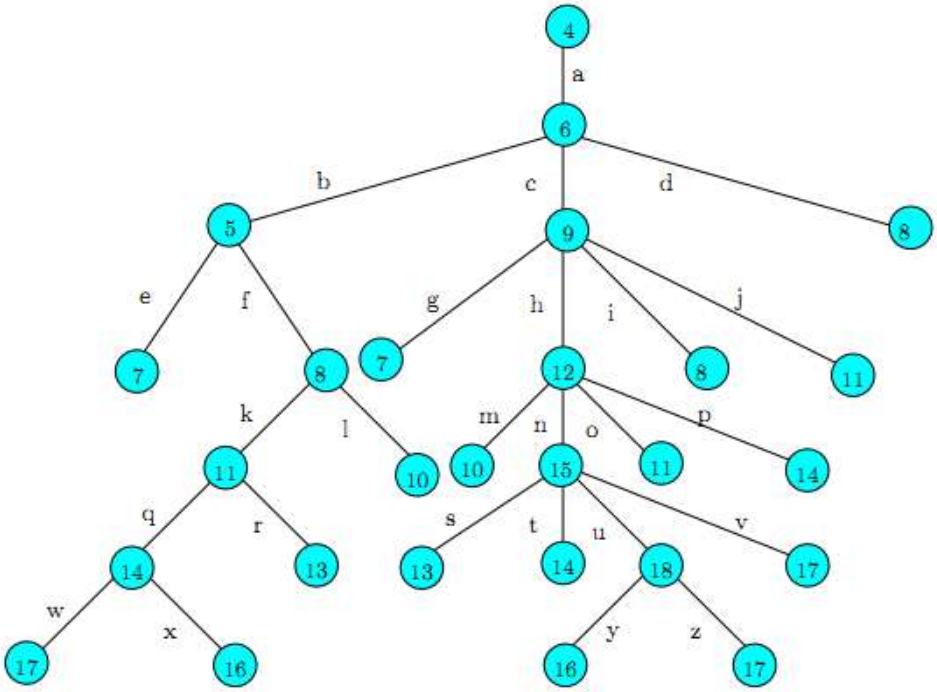
Gambar 5.2. d=0 n=5 Contoh Graf Sisi Genap (Graf H)

Label titik dan label sisi pada Gambar 5.2 menggunakan angka 1 sampai 50. 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 H dengan jumlah keseluruhan huruf alfabet. Jumlah titik yang digunakan pada Gambar 5.2 adalah 18 dan jumlah alfabet adalah 26, maka penjumlahan keduanya diperoleh 44. Label sisi atau cabang yang harus di eliminasi yaitu label sisi yang lebih besar dari jumlah titik graf H dengan jumlah alfabet. Dengan demikian, label sisi yang harus dieliminasi adalah label 45,46,47, 48,49,50. Setelah pengeliminasian dilakukan, langkah selanjutnya adalah membuat digram pohon yang berakar di label titik 4 dengan dilengkapi label sisinya seperti yang terlihat pada Gambar 5.3 (Label sisi yang sudah di eliminasi tidak perlu di gambarkan pada diagram pohon).



Gambar 5.3 Diagram pohon graf H pada n=5

(3) 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. Penempatan alfabet tersebut seperti yang tertera pada Gambar 5.6 .



Gambar 5.6 Penempatan Alfabet Pada Diagram Pohon

(4) 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. Pesan rahasia dipecahkan dengan menerapkan teknik kriptosistem modulo 26 terhadap masing-masing huruf alfabet sehingga menjadi a= mod(44,26) = 18, b = mod(43, 26) = 17, c = mod(39, 26) = 13, d = mod(40,26) = 14, e = mod(42, 26) = 16, f = mod(41, 26) = 15, g = mod(38, 26) = 12,mh = mod(33, 26) = 7, i = mod(37 26) = 11, j = mod(34, 26) = 8, k = mod(35, 26) = 9, l = mod(36, 26) = 10, m = mod(32, 26) = 6, n = mod(27, 26) = 1, o =nmod(31, 26) = 5, p = mod(28, 26) = 2, q = mod(29, 26) = 3, r = mod(30, 26) = 4, s = mod(26, 26) = 0, t = mod(25, 26) = 25, u = mod(21, 26) = 21, v = mod(22, 26) = 22, w = mod(23, 26) = 23, x = mod(24, 26) = 24, y = mod(20, 26) = 20, dan z = mod(19, 26) = 19. Teknik modulonya dapat dilihat pada Tabel 5.1

Tabel 5.1 Teknik Modulo 26 untuk *Ciphertext* pada Super (a, d)-Sisi Antimagic Total pada Graf Bersisi Genap untuk d = 0

Abjad	Label Sisi	Modulo 26	Chipertext
a	44	18	s
b	43	17	r
c	39	13	n
d	40	14	o
e	42	16	q
f	41	15	p
g	38	12	m
h	33	7	h
i	37	11	l
j	34	8	i
k	35	9	j
l	36	10	k
m	32	6	g
n	27	1	b
o	31	6	f
p	28	2	c
q	29	3	d
r	30	4	e
s	26	0	a
t	25	25	z
u	21	21	v
v	22	22	w
w	23	23	x
x	24	24	y
y	20	20	u
z	19	19	t

Selanjutnya diperoleh a = s, b = r, c = n, d = o, e = q, f = p, g = m, h = h, i = l, j = i, k = j, l = k,m = g, n = b, o = f, p = c, q = d, r = e, s = a, t = z, u = v, v = w, w = x, x = y, y = u, z = t. Pada tahap ini bentuk pesan yang tersandi dapat diubah ke bentuk lain atau dengan kata lain password dan ussername dosen yang pada awalnya adalah nidn dapat dirubah kebentuk sandi lain dengan kriptografi.

KESIMPULAN DAN SARAN

Graf yang digunakan untuk aplikasi kriptosystem polyalphabetic cipher adalah graf H dengan sisi genap. Ada pelabelan titik (4,1)-sisi antimagic pada graf H yang bersisi genap pada $n \geq 1$. Graf H mempunyai pelabelan total super (a,d)-sisi antimagic untuk mendapatkan EAV d = 1 dan SEATL d = 0. 2

DAFTAR PUSTAKA

Ariyus, Dony. 2008. *Pengantar Ilmu Kriptografi.* Yogyakarta: Andi Yogyakarta.

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

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

Muktyas, I.B. dan Sugeng, K. A. 2014. *Pemanfaatan Pelabelan Graceful pada Symmetric Tree untuk Kriptografi Polyalphabetic*.Jakarta : Gramedia Pustaka Utama.

Munir, R. 2004. *Algoritma Greedy*. Departemen Teknik Informatika Institut Teknologi Bandung.

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

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

Schneier, B. 1996.*Applied Cryptography: protocols, algorithms, and source code in C*, John Wiley and Sons, Inc.

Slamin. 2009. *Desain Jaringan Pendekatan Teori Graf*. Jember: Universitas Jember.

Subiono. 2015. *Aljabar Sebagai Suatu Fondasi Matematika Versi 1.0.0. Modul Mata Kuliah Aljabar*.

Mahmudah, M. 2016. ” *Analisis Keterkaitan Seatl Graf Konektif Dan Diskonektif Serta Aplikasi Dalam Pengembangan Kriptosistem Polyalphabetic Cipher*”. Tidak Diterbitkan. Tesis. Jember: Universitas Jembe