PENGEMBANGAN MODEL RANTAI MARKOV UNTUK MENGUJI KETERDUGAAN PADA BARISAN ABJAD

Sari Agustini H.,[1] Anang Kurnia[2] dan Agus Buono[3]

Lembaga Sandi Negara
Email : hafman76@yahoo.com
Departemen Statistika, FMIPA IPB
Email : akstk29@yahoo.com
Departemen Ilmu Komputer, FMIPA IPB
Email : pudesha@yahoo.com

Abstrak. Rantai Markov dapat digunakan untuk menguji keterdugaan dari suatu barisan abjad karena beberapa algoritma pembangkit bilangan acaksemu (PBAS) adalah *markov cipher* yang memiliki sifat markov. Penelitian ini menggunakan 35 barisan abjad yang dibangkitkan dari empat kelas PBAS yaitu PBAS berbasis algoritma penyandian blok, berbasis faktorisasi bilangan bulat, berbasis LCG dan berbasis *linear feedback shift-register* (LFSR). Hasil penelitian menunjukkan bahwa barisan abjad yang dibangkitkan oleh PBAS kelas kesatu, kedua dan keempat tidak dapat dimodelkan dengan rantai markov orde pertama sampai dengan orde ketiga. PBAS kelas ketiga, kecuali PBAS LCG1, LCG2,coveyou, rand dan randu tidak layak digunakan dalam kriptografi karena memiliki kemungkinan yang tinggi untuk dapat dimodelkan dengan rantai markov orde-orde tinggi (diatas ode tiga).

***Kata kunci** : rantai markov, PBAS, peluang transisi, tingkat kecocokan.*

1. PENDAHULUAN

Salah satu dampak negatif perkembangan TIK adalah timbulnya kerawanan dalam komunikasi seperti pemalsuan, penyadapan, perusakan, pengubahan informasi. Dalam pengamanan informasi terdapat tiga aspek yang harus diperhatikan yaitu pengamanan fisik, administratif dan *logic*. Penggunaan kriptografi merupakan salah satu upaya pengamanan secara *logic*.

Berdasarkan prinsip Kerckhoffs [4], keamanan sistem kriptografi harus hanya bergantung pada kunci. Dalam sistem kriptografi, kunci umumnya dihasilkan oleh pembangkit bilangan acak nyata (PBAN) atau pembangkit bilangan acaksemu (PBAS). Output dari PBAN atau PBAS ini berupa barisan kunci berbentuk bit atau diubah menjadi bentuk barisan lain, bergantung pada kebutuhan sistem kriptografi seperti barisan digit (0-9), barisan bilangan heksadesimal (0-F), barisan karakter (0-255) dan barisan abjad (A-Z).

Tidak semua barisan kunci yang dihasilkan oleh PBAN atau PBAS dapat digunakan dalam sistem kriptografi. Barisan kunci yang dapat digunakan dalam sistem kriptografi adalah *cryptographically secure pseudo-random sequences* (barisan acaksemu yang aman secara kriptografis) dan *real random sequences* (barisan yang acak nyata). Suatu barisan dikatakan aman secara kriptografis bila barisan tersebut memenuhi dua syarat, yaitu secara statistik terlihat acak (berdistribusi seragam dan saling bebas) serta *unpredictable* (ketidakterdugaan). Suatu barisan dikatakan nyata acak bila memenuhi tiga syarat yaitu barisan tersebut secara statistik terlihat acak, ketidakterdugaan dan barisan yang sama tidak dapat dihasilkan kembali [7].

Sistem *One Time Key* (OTK) yang menggunakan kunci berupa barisan abjad merupakan salah satu contoh sistem kriptografi yang masih digunakan di Indonesia untuk mengamankan informasi yang bersifat rahasia. Berdasarkan hukum Kerckhoff [4], barisan abjad pada OTK minimal harus berupa barisan acaksemu yang aman secara kriptografis.

Uji statistik untuk menguji bentuk distribusi dari suatu barisan kunci mulai berkembang sejak masa perang dunia I yang dipelopori oleh Kendall dan Smith [3]. Uji ini bertujuan menguji barisan digit dan terdiri atas empat uji yaitu uji frekwensi, uji serial, uji poker dan uji gap. Keempat uji tersebut merupakan pengembangan dari uji kecocokan *chi-square*. Sejak tahun 1938 sampai dengan tahun 2005, uji-uji statistik untuk menguji barisan abjad hanya bertujuan mengetahui bentuk distribusi dari barisan kunci sedangkan untuk menguji kesalingbebasan dan ketidakterdugaan belum diteliti lebih jauh. Marsaglia [6] mengajukan sebuah uji *overlapping m-tuple test* yang merupakan pengembangan dari uji serial yang dikembangkan oleh Beker dan Piper [1]. Uji tersebut tidak hanya dapat digunakan untuk menguji barisan abjad tapi juga dapat digunakan untuk menguji barisan dalam bentuk lain seperti bit, digit, karakter maupun heksadesimal. Meskipun demikian, uji tersebut hanya bertujuan mengetahui bentuk distribusi dan kesalingbebasan.

Selama ini kunci yang digunakan dalam sistem OTK di Indonesia hanya diuji dengan menggunakan *overlapping m-tuple test* yang dikembangkan oleh Marsaglia [6]. Padahal seperti yang telah disebutkan sebelumnya, uji tersebut hanya bertujuan menguji bentuk distribusi dan kesalingbebasan. Akibatnya, barisan kunci yang telah lulus *overlapping m-tuple test* belum dapat digunakan sebagai kunci pada sistem OTK karena ketidakterdugaan dari barisan tersebut belum diketahui.

Mengingat belum adanya penelitian mengenai ketidakterdugaan maka dilakukan penelitian untuk membahas pengujian terhadap keterdugaan suatu barisan abjad dengan menggunakan pendekatan rantai markov. Penelitian dibatasi pada pemodelan rantai markov karena beberapa algorirtma pembentuk PBAS yaitu DES dalam Lai [5] serta AES dalam Daemen dan Rijmen [2] merupakan markov cipher yang memiliki sifat markov. Hal ini menyebabkan jika suatu barisan kunci membentuk rantai markov maka barisan kunci tersebut tidak memenuhi ketidakterdugaan. Tetapi jika barisan kunci tersebut tidak membentuk rantai markov maka belum tentu barisan kunci tersebut memenuhi ketidakterdugaan. Penelitian ini bertujuan mengembangkan model rantai markov waktu diskrit yang dapat digunakan untuk menguji keterdugaan suatu barisan abjad yang dihasilkan oleh suatu PBAS sehingga diperoleh rekomendasi mengenai PBAS yang dapat atau tidak dapat digunakan dalam sistem kriptografi.

2. METODE PENELITIAN

Data yang digunakan dalam penelitian ini merupakan data simulasi yang berasal dari PBAS yang masing-masing berukuran satu juta huruf. Data simulasi ini dibangkitkan langsung dari empat kelas PBAS seperti yang diperlihatkan pada Tabel 1.

Tabel 1 Empat kelas PBAS

Kelas	Basis	Nama PBAS
Satu	Algoritma penyandian blok	PBAS ANSI X9.17 dan ANSI X9.31
Dua	Faktorisasi bilangan bulat	*Blum Blum Shub* (BBS)
Tiga	*Linear Congruential Generator* (LCG)	coveyou, fishman18, fishman20, fishman2x, knuthran, knuthran2, lecuyer21, minstd, LCG1, LCG2, cmrg, mrg, rand,rand48, randu, ran0, ran1, ran2, ran3, gfsr4 dan zuf
Empat	*Linear Feedback Shift-Register* (LFSR)	rand128_bsd, rand128_glibc2, rand128_libc5, rand32_bsd, rand32_glibc2, rand32_glibc2, rand64_bsd, rand64_libc2, mt19937, mt19937_1999 dan mt19937_1998

Langkah-langkah untuk menganalisis sifat keterdugaan dari barisan abjad yang dihasilkan oleh PBAS dibagi kedalam dua tahap yaitu :

2.1 Membangkitkan barisan huruf dari rantai markov waktu diskrit orde satu,dua dan tiga. Langkah-langkah untuk membangkitkan barisan adalah sebagai berikut :

2.1.1 Membangkitkan barisan huruf dari keempat kelas masing-masing sebesar satu juta huruf.

2.1.2 Mengelompokkan barisan huruf kedalam tiga tipe gugus data seperti pada Tabel 2. Pengambilan ketiga tipe gugus data ini dilakukan secara *overlap* (tumpang tindih) dan tanpa *overlap* dengan jumlah huruf yang *overlap* sebanyak 10.000 huruf.

Tabel 2 Tipe gugus data

Tipe	Perbandingan	Jumlah Huruf	
		Data Pelatihan	Data Observasi
Satu	50:50	50.000	50.000
Dua	75:25	75.000	25.000
Tiga	100:10	100.000	10.000

2.1.3 Menghitung frekwensi 2-*gram* (AA-ZZ) s.d. 4-*gram* (AAAA-ZZZZ) dari data pelatihan pada ketiga tipe gugus data dengan menggunakan algoritma *sliding window counts*.

2.1.4 Menduga peluang matriks transisi orde pertama s.d orde ketiga berdasarkan frekwensi 2-*gram* s.d. 4-*gram* dari data pelatihan

orde 1 : $P(j|i) = \frac{N(i,j)}{\sum_{l=0}^{25} N(i,l)}, 0 \leq i,j < 26$

orde 2 : $P(k|i,j) = \frac{N(i,j,k)}{\sum_{l=0}^{25} N(ij,l)}, 0 \leq i,j,k < 26$

orde 3 : $P(m|i,j,k) = \frac{N(i,j,k,m)}{\sum_{l=0}^{25} N(i,j,m,l)}, 0 \leq i,j,k,m < 26$

2.1.5 Membangkitkan huruf sebesar ukuran data simulasi ketiga tipe gugus data berdasarkan peluang transisi rantai markov mulai orde pertama s.d. orde ketiga. Langkah tersebut diulang sebanyak 10 kali.

2.2 Analisis tingkat kecocokan barisan huruf antara data bangkitan dengan data simulasi. Pada tahap ini dilakukan langkah-langkah sebagai berikut :

2.2.1 Menghitung tingkat kecocokan dengan cara :

a. Mencocokan gugus data simulasi dengan gugus data hasil bangkitan rantai markov pada berbagai orde untuk mengetahui jumlah huruf yang cocok diantara kedua gugus data tersebut.

b. Menghitung tingkat kecocokan dengan membandingkan banyaknya huruf yang sama dengan jumlah seluruh huruf dalam gugus data menggunakan persamaan:

$$tingkat\ kecocokan = \frac{\sum huruf\ yang\ cocok}{\sum huruf\ yang\ diuji}$$

c. Menghitung rataan tingkat kecocokan dari 10 ulangan gugus data.

d. Melakukan analisis karakteristik tingkat kecocokan untuk memperoleh rekomendasi PBAS yang dapat atau tidak dapat digunakan dalam sistem kriptografi.

3. HASIL DAN PEMBAHASAN

Untuk memperoleh rekomendasi PBAS yang dapat digunakan dalam sistem kriptografi maka dilakukan analisis terhadap karakteristik tingkat kecocokan pada keempat kelas PBAS. Analisis dilakukan dengan mengamati matriks peluang transisi serta grafik tingkat kecocokan yang dihasilkan oleh gugus data tanpa *overlap* maupun *overlap* dalam kelas tersebut.

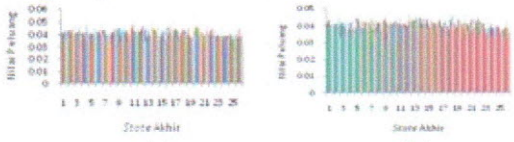
3.1 Kelas Kesatu

Nilai peluang pada matriks transisi berpengaruh terhadap tingkat kecocokan yang akan dicapai oleh suatu gugus data karena ketika *state* awal ke-*i* bertransisi ke semua *state* akhir *j* maka kemungkinan untuk memperoleh huruf yang cocok akan semakin sedikit (peluang = 1/26). Ketika *state* awal ke-*i* hanya bertransisi ke beberapa *state* saja maka kemungkinan untuk memperoleh huruf yang cocok memiliki peluang lebih besar dari 1/26. Identifikasi awal dapat dilihat pada plot nilai peluang matriks transisi setiap PBAS pada ketiga tipe gugus data. Gambar

1 dan Gambar 2 menunjukkan plot nilai peluang transisi orde satu dan orde dua PBAS X9.17 dan X9.31 pada gugus data tipe ketiga tanpa *overlap*.

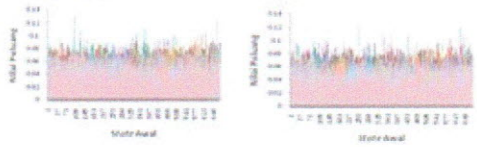
Pada Gambar 1 terlihat bahwa nilai peluang transisi orde satu PBAS X9.17 pada ketiga tipe gugus data berada diantara nilai 2.76×10^{-2} s.d. 5.20×10^{-2} sedangkan pada PBAS X9.31 berada diantara 2.12×10^{-2} s.d. 5.36×10^{-2}. Hal ini menyebabkan semua *state* pada matriks peluang transisi X9.17 dan X9.31 dapat bertransisi secara langsung dari satu *state* ke *state* lain sehingga rantai markov yang terbentuk merupakan rantai markov tidak tereduksi dan hanya terdiri atas satu kelas *state* tertutup yaitu {A,B,C,D,E,F, ...,Z}.

Pada Gambar 2 terlihat bahwa nilai peluang transisi orde dua pada ketiga tipe gugus data X9.17 dan X9.31 mengalami perubahan. Nilai peluang transisi orde dua PBAS X917 berada diantara nilai 0 s.d 1.54×10^{-1} sedangkan pada PBAS X9.31 diantara 0 s.d. 1.62×10^{-1}.



(a) (b)

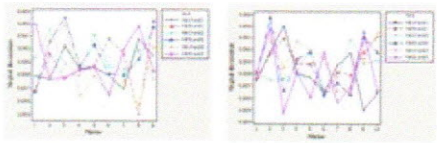
Gambar 1 Plot nilai peluang matriks transisi orde satu kelas kesatu gugus data tipe 3 tanpa *overlap* (a) PBAS X9.17; (b) PBAS X9.31.



(a) (b)

Gambar 2 Plot nilai peluang matriks transisi orde dua kelas kesatu gugus data tipe 3 tanpa *overlap* (a) PBAS X9.17; (b) PBAS X9.31.

Dari Gambar 3 terlihat bahwa bahwa perubahan nilai peluang matriks transisi orde dua tidak berpengaruh secara signifikan pada perolehan tingkat kecocokan di orde dua. Tingkat kecocokan yang dicapai baik pada data tanpa *overlap* maupun dengan *overlap* pada ketiga orde relatif sama yaitu berada diantara 3.4×10^{-2} s.d. 4.3×10^{-2}. Atau dengan kata lain, barisan huruf yang dihasilkan oleh PBAS X9.17 dan PBAS X9.31 pada ketiga tipe gugus data dengan *overlap* maupun tanpa *overlap*, belum dapat dimodelkan dengan rantai markov orde satu,dua maupun tiga.



(a) (b)

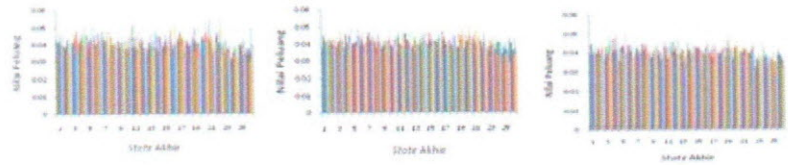
Gambar 3 Plot Tingkat Kecocokan Gugus Data Tipe 3 Kelas Kesatu Orde Satu, Dua dan Tiga (a) tanpa *Overlap* ; (b) dengan *Overlap*

3.2 Kelas Kedua

Tidak seperti kelas kesatu, kelas kedua hanya terdiri atas satu PBAS yaitu PBAS BBS. Gambar 4 dan Gambar 5 menunjukkan plot nilai peluang transisi orde satu dan orde dua PBAS BBS pada ketiga tipe gugus data tanpa *overlap*.

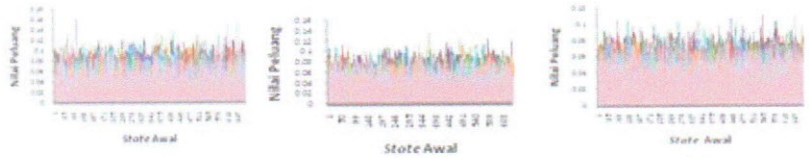
Pada Gambar 4 terlihat bahwa nilai peluang transisi orde satu PBAS BBS pada ketiga tipe gugus data berada diantara nilai 2.43×10^{-2} s.d. 5.53×10^{-2}. Hal ini menyebabkan semua *state* pada matriks peluang transisi BBS dapat bertransisi secara langsung dari satu *state* ke *state* lain sehingga rantai markov yang terbentuk merupakan rantai markov tidak tereduksi dan hanya

terdiri atas satu kelas *state* tertutup yaitu {A,B,C,D,E,F, ...,Z}. Gambar 5 menunjukkan bahwa nilai peluang transisi orde dua pada ketiga tipe gugus data BBS mengalami perubahan. Nilai peluang transisi orde dua berada diantara nilai 0 s.d. 1.62×10^{-1}.



(a) (b) (c)

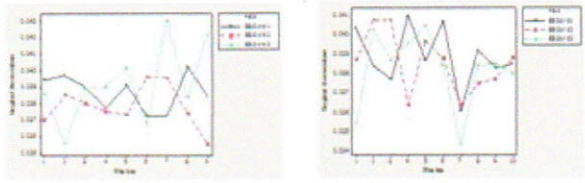
Gambar 4 Plot nilai peluang matrik transisi orde satu kelas kedua tanpa *overlap* (a) tipe 1; (b) tipe 2; (c) tipe 3.



(a) (b) (c)

Gambar 5 Plot nilai peluang matrik transisi orde dua kelas kedua tanpa *overlap* (a) tipe 1; (b) tipe 2; (c) tipe 3.

Dari Gambar 6 terlihat bahwa perubahan nilai peluang matriks transisi orde dua tidak berpengaruh secara signifikan pada perolehan tingkat kecocokan di orde dua. Tingkat kecocokan yang dicapai baik pada data tanpa *overlap* maupun dengan *overlap* pada ketiga orde relatif sama yaitu berada diantara 3.4×10^{-2} s.d. 4.3×10^{-2}. Atau dengan kata lain, barisan huruf yang dihasilkan oleh PBAS BBS pada ketiga gugus data dengan *overlap* maupun tanpa *overlap*, belum dapat dimodelkan dengan rantai markov orde satu,dua maupun tiga.



(a) (b)

Gambar 6 Plot tingkat kecocokan gugus data tipe 3 kelas kedua (a) tanpa *overlap*; (b) dengan *overlap*.

3.3 Kelas Ketiga

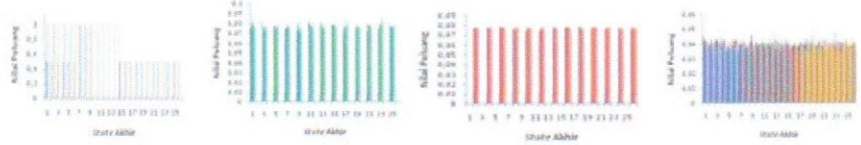
Kelas ketiga terdiri atas dua puluh PBAS berbasis LCG. Disebut berbasis LCG karena algoritma pembangkitan huruf yang digunakan pada kedua puluh PBAS ini pada dasarnya sama yaitu menggunakan persamaan:

$$x_n = ax_{n-1} + b \bmod m, \; n \geq 1,$$

Perbedaannya hanya terletak pada pemilihan nilai parameter a, b, m dan x_{n-1}. Gambar 7 dan 8 menunjukkan plot nilai peluang transisi orde satu dan dua PBAS LCG1, Coveyou, LCG2 dan gfsr4 pada tipe gugus data tipe ketiga tanpa *overlap*.

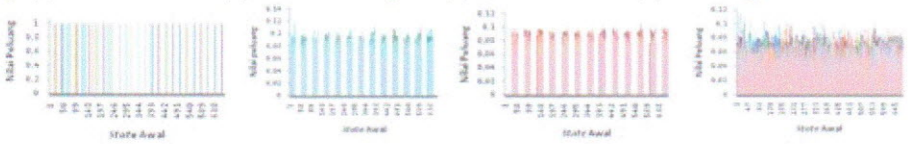
Pada Gambar 7 dan Gambar 8 terlihat bahwa nilai peluang transisi orde satu dan orde dua dari kelas ketiga pada ketiga tipe gugus data terbagi dalam tiga kelompok yaitu (a) kelompok 1 berisi nilai peluang transisi LCG1, (b) kelompok 2 berisi nilai peluang transisi coveyou, LCG2, rand, dan randu, (c) kelompok 3 berisi nilai peluang transisi keenam belas PBAS lain. Pada kelompok 1, nilai peluang transisi orde satu hanya berada pada nilai 0, 4.99×10^{-1} , 0.5 dan 1 sedangkan pada orde dua nilai peluangnya hanya bernilai 0 dan 1. Pada kelompok 2, nilai peluang matrik transisi orde satu selain bernilai 0 juga berada pada nilai 6.67×10^{-2} s.d. $8.88 \times$

10^{-2} sedangkan pada orde dua selain bernilai 0 juga berada pada nilai 2.25×10^{-2} s.d. 1.47×10^{-1}. Pada kelompok 3 nilai peluang matrik transisi orde satu pada ketiga tipe gugus data berada diantara nilai 2.62×10^{-2} s.d. 4.99×10^{-2} sedangkan pada orde dua selain bernilai 0 juga berada diantara nilai 5.75×10^{-3} s.d. 1.58×10^{-1}.



(a) (b) (c) (d)

Gambar 7 Plot nilai peluang matrik transisi orde satu kelas ketiga gugus data tipe 3 tanpa *overlap* (a) PBAS LCG1; (b) PBAS Coveyou; (c) PBAS LCG2; (d) PBAS gfsr4.

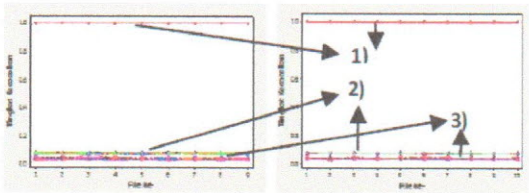


(a) (b) (c) (d)

Gambar 8 Plot nilai peluang matrik transisi orde dua kelas ketiga gugus data tipe 3 tanpa *overlap* (a) PBAS LCG1; (b) PBAS Coveyou; (c) PBAS LCG2; (d) PBAS gfsr4.

Perilaku rantai markov orde satu kelompok 1 dan 2 menunjukkan bahwa *state* pada matriks transisi coveyou, LCG1, LCG2, rand dan randu tidak dapat bertransisi secara langsung dari satu *state* ke *state* lain sedangkan *state* dari matriks transisi PBAS lainnya dapat bertransisi secara langsung. Meskipun demikian, rantai markov dari ke-21 PBAS ini tidak tereduksi dan hanya terdiri atas satu kelas *state* yang tertutup yaitu {A,B,C,D,E,F, ...,Z}.

Pada Gambar 9 terlihat bahwa tingkat kecocokan PBAS LCG1 pada ketiga tipe gugus data mulai dari orde dua mencapai 1. Hal ini berarti PBAS LCG1 dapat dimodelkan dengan rantai markov orde dua atau barisan yang dihasilkan oleh LCG1 merupakan barisan yang dapat diduga dengan rantai markov orde dua.



Ket : 1) PBAS LCG1 orde2 dan orde3, 2) PBAS LCG2, Coveyou, Rand dan Randu, 3)PBAS fishman18, fishman20, fishman2x, knuthran, knuthran2, lecuyer21, minstd, cmrg, mrg, rand48, ran0, ran1, ran2, ran3, gfsr4 dan zuf

Gambar 9 Plot tingkat kecocokan gugus data tipe 3 kelas ketiga orde 2 dan orde 3 (a) tanpa *overlap*; (b) dengan *overlap*.

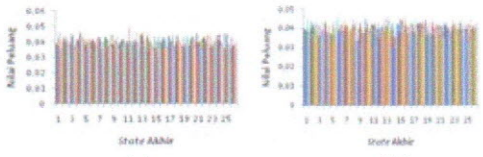
Pada PBAS coveyou, LCG2, rand dan randu, perubahan nilai peluang matrik transisi orde dua dan tiga tidak berpengaruh secara signifikan pada perolehan tingkat kecocokan di orde dua dan tiga. Tingkat kecocokan yang dicapai baik pada data tanpa *overlap* maupun dengan *overlap* pada orde dua dan tiga relatif sama dengan tingkat kecocokan pada orde satu yaitu berada diantara 7.02×10^{-2} s.d. 8.39×10^{-2}. Hal ini pun terjadi pada keenam belas PBAS lain. Perubahan nilai peluang transisi orde dua dan tiga tidak berpengaruh secara signifikan pada perolehan tingkat kecocokan di orde dua dan tiga. Tingkat kecocokan yang dicapai baik pada data tanpa *overlap* maupun dengan *overlap* pada orde dua dan ketiga relatif sama dengan tingkat kecocokan pada orde satu yaitu berada diantara 3.34×10^{-2} s.d. 4.44×10^{-2}. Atau dengan kata lain, barisan huruf yang dihasilkan oleh ke-20 PBAS pada kelas kedua di ketiga tipe gugus data

baik dengan *overlap* maupun tanpa *overlap* tidak dapat dimodelkan dengan rantai markov orde satu,dua maupun tiga.

3.4 Kelas Keempat

Kelas keempat terdiri atas sebelas PBAS. Gambar 10 dan Gambar 11 menunjukkan plot nilai peluang transisi orde satu dan orde dua PBAS mt19937_1999 dan rand128_bsd pada gugus data tipe ketiga tanpa *overlap*.

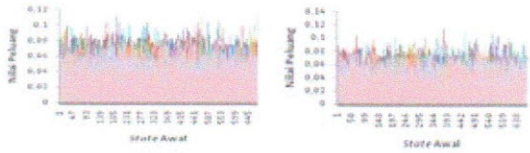
Pada Gambar 10 terlihat bahwa nilai peluang matriks transisi orde satu PBAS mt19937_1999 pada ketiga tipe gugus data berada diantara nilai 2.39×10^{-2} s.d. 5.29×10^{-2} sedangkan pada PBAS rand128_bsd berada diantara 2.42×10^{-2} s.d. 5.31×10^{-2}. Hal ini menyebabkan semua *state* pada matriks peluang transisi PBAS mt19937_1999 dan rand128_bsd dapat bertransisi secara langsung dari satu *state* ke *state* lain sehingga rantai markov yang terbentuk merupakan rantai markov tidak tereduksi dan hanya terdiri atas satu kelas *state* tertutup yaitu {A,B,C,D,E,F, ...,Z}.



(a) (b)

Gambar 10 Plot nilai peluang matriks transisi orde satu kelas keempat gugus data tipe 3 tanpa *overlap* (a) PBAS mt19937_1999; (b) PBAS random128_bsd.

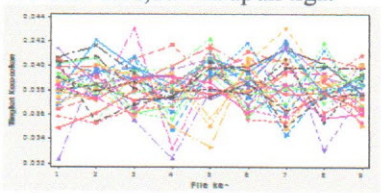
Gambar 11 menunjukkan bahwa nilai peluang matriks transisi orde dua pada ketiga tipe gugus data PBAS mt19937_1999 dan rand128_bsd mengalami perubahan. Nilai peluang matriks transisi orde dua PBAS mt19937_1999 selain bernilai 0 juga berada pada nilai 5.53×10^{-3} s.d. 1.67×10^{-1} sedangkan pada PBAS rand128_bsd selain bernilai 0 juga berada pada nilai 5.53×10^{-3} s.d. 1.88×10^{-1}.



(a) (b)

Gambar 11 Plot nilai peluang matrik transisi orde dua kelas keempat gugus data tipe 3 tanpa *overlap* (a) PBAS mt19937_1999; (b) PBAS random128_bsd.

Pada Gambar 12 terlihat bahwa perubahan nilai peluang matriks transisi orde dua dan tiga tidak berpengaruh secara signifikan pada perolehan tingkat kecocokan di orde dua dan tiga. Akibatnya tingkat kecocokan yang dicapai baik pada data tanpa *overlap* maupun dengan *overlap* pada orde dua dan orde tiga relatif sama dengan orde satu yaitu berada diantara 3.23×10^{-2} s.d. 4.09×10^{-2}. Atau dengan kata lain, barisan huruf yang dihasilkan oleh PBAS kelas keempat pada ketiga tipe gugus data dengan *overlap* maupun tanpa *overlap*, belum dapat dimodelkan dengan rantai markov orde satu,dua maupun tiga.



Gambar 12 Plot tingkat kecocokan gugus data tipe 3 pbas kelas keempat tanpa *overlap* pada ketiga orde.

Berdasarkan hasil penelitian *yang* telah dilakukan, dapat disimpulkan bahwa barisan abjad yang dihasilkan oleh PBAS kelas kesatu, kedua, dan keempat tidak dapat dimodelkan dengan rantai markov. Demikian pula dengan PBAS kelas ketiga kecuali barisan yang dihasilkan oleh PBAS LCG1, LCG2, coveyou, rand dan randu. Bila barisan tersebut juga acak secara statistik maka barisan huruf adalah barisan acaksemu yang aman secara kriptografis sehingga layak digunakan dalam kriptografi.

Meskipun barisan yang dihasilkan oleh PBAS LCG2, coveyou, rand dan randu tidak dapat dimodelkan dengan rantai markov orde satu, dua dan tiga tetapi memiliki kemungkinan yang tinggi untuk dapat dimodelkan dengan rantai markov orde-orde tinggi (diatas orde tiga). Oleh karena itu barisan yang dihasilkan oleh keempat PBAS tersebut tidak layak digunakan dalam kriptografi.

4. KESIMPULAN

Penggunaan rantai markov menunjukkan bahwa :

a. Barisan abjad yang dihasilkan oleh PBAS kelas kesatu, kedua, dan keempat tidak dapat dimodelkan dengan rantai markov. Demikian pula dengan PBAS kelas ketiga kecuali barisan yang dihasilkan oleh PBAS LCG1, LCG2, coveyou, rand dan randu.
b. Barisan yang dihasilkan oleh PBAS LCG2, coveyou, rand dan randu tidak layak digunakan dalam kriptografi karena memiliki kemungkinan yang tinggi untuk dapat dimodelkan dengan rantai markov orde-orde tinggi (diatas orde tiga).

DAFTAR PUSTAKA

[1] Beker,H. (1983). *Cipher System the Protection of Communications*, Northwood Books, London.

[2] Daemen,J. Rijmen,V. (2007). "Probability Distributions of Correlation and Differentials in Block Cipher", *Journal of Mathematical Cryptology*; **1**; 221-241.

[3] Kendall,MG, Smith,BB. (1938). "Randomness and Random Sampling Numbers", *Journal of the Royal Statistical Society*; **101 No.1**; 147-166.

[4] Kerckhoffs,A. (1883). "La Cryptographic Militaire", *Journal des Sciences Militaires*; **IX**; 5-38.

[5] Lai,X. (1995). *On the Design and Security of Block Ciphers*. Hartung-Gorre Verlag Konstanz, Zurich.

[6] Marsaglia,G. (2005). "Monkeying Goodness of Fit Test", *Journal of Statistics Software*; **13 Issue 14**.

[7] Schneier,B. (1996). *Applied Cryptography : Protocols, Algorithms and Source Code in C* Ed ke-2. John Wiley & Sons, Canada.