Analisis Kekaburan Cipherteks Hasil Perulangan Enkripsi *Vigenere* dan Transposisi *Columnar Cipher*

Gregorius Magnus Mega Sanjaya[1], Bambang Soelistijanto[2], Vittalis Ayu[3]
[1,2,3] Program Studi Informatika Universitas Sanata Dharma, Yogyakarta, Indonesia

e-mail : **megasanjaya22@gmail.com, vittalis.ayu@usd.ac.id**

Abstrak— **Keamanan data merupakan hal yang penting. Salah satu hal yang dapat dilakukan untuk menjaga kerahasiaan data menggunakan cipher untuk menyandikan data. Penelitian ini menggabungkan Vigenere dan Transposisi Columnar serta penambahan iterasi pada proses enkripsi. Parameter yang digunakan untuk mengukur kinerja cipher gabungan ini adalah avalanche effect dan rnnning time. Analisis periodicity juga ditambahkan untuk menganalisis pengaruh dari Vigenere dan Transposisi Columnar terhadap persentase kekaburan yang dihasilkan oleh iterasi yang dilakukan terhadap cipher gabungan ini. Hasil penelitian menunjukkan bahwa penggunaan gabungan Vigenere-Transposisi maupun iterasi, keduanya menghasilkan persentase kekaburan yang lebih tinggi dibandingkan hasil enkripsi dengan Vigenere cipher saja. Namun running time untuk iterasi cipher gabungan ini sangat tinggi. Hal ini mengindikasikan beban komputasi yang besar. Pola perulangan yang terjadi pada hasil persentase kekaburan dari Iterasi-Vigenere-Transposisi dipengaruhi oleh perubahan kolom pada Transposisi Columnar cipher. Semakin banyak jumlah kolom pada Transposisi Columnar maka periode perulangannya akan semakin pendek.**

Kata Kunci— vigenere, transposisi columnar, iterasi, avalanche effect, periodicity.

I. PENDAHULUAN

Informasi kini menjadi salah satu aspek penting dalam kehidupan. Pengiriman suatu informasi penting atau dirahasiakan harus dijamin keamanannya, pentingnya keamanan agar tidak terjadi sabotase pada informasi tersebut oleh orang yang tidak berwenang. Salah satu cara untuk meningkatkan kerahasiaan data adalah penggunaan algoritma untuk mengubah pesan (plain teks) menjadi suatu rangkaian sandi (cipherteks). Algoritma ini dapat kita sebut sebagai cipher. Cipher terdiri dari sepasang proses: proses melakukan translasi dari plain teks ke cipherteks (proses ini dapat kita sebut sebagai enkripsi) pada sisi pengirim dan proses untuk melakikan translasi dari cipherteks ke plainteks (proses ini dapat kita sebut sebagai dekripsi) pada sisi penerima. Proses enkripsi dan dekripsi ini dilakukan dengan menggunakan sebuah kunci. Algoritma enkripsi yang baik harus memiliki kunci yang benar-benar acak dan panjang kunci harus sama dengan panjang plainteks sehingga plainteks yang sama tidak selalu menghasilkan cipherteks yang sama [1].

Vigenere Chiper merupakan cipher yang melakukan proses enkripsi dan dekripsi menggunakan teknik substitusi huruf abjad. Kelebihan dari Vigenere Cipher adalah mencegah frekuensi huruf-huruf di dalam chiperteks yang memiliki pola tertentu yang sama. Namun, Vigenere Cipher memilki kekurangan yaitu terdapat frasa yang berulang-ulang pada ciphertext yang dihasilkan sehingga dapat diketahui panjang kuncinya dengan menganalisis perulangan dan kombinasi huruf [2]. Penelitian yang untuk meningkatkan performa dari vigenere telah dilakukan pada penelitian Triandi [3] dan Rahmawati [4], Untuk mengatasi kekurangan dari Vigenere Cipher, pada penelitian ini dikombinasikan Vigenere Cipher dengan teknik transposisi dari Transposisi Columnar Cipher. Pada bagian berikutnya akan dijelaskan mengenai cara enkripsi dari Vigenere dan Transposisi Columnar Cipher.

Received August 19th, 2019; Reviewed September 3rd, 2019; Accepted September 8th, 2019

II. LANDASAN TEORI

Bagian ini menjelaskan contoh dari proses enkripsi yang dilakukan dengan Vigenere dan Transposisi Columnar Cipher.

A. Vigènere Cipher

Vigènere Cipher adalah metode enkripsi abjad majemuk. Proses enkripsi dan dekripsi pada Vigènere Cipher menggunakan pemetaan bujursangkar tersusun atas kolom dan barisnya berdasarkan abjad. Huruf pertama pada plainteks dienkripsi dengan huruf pertama pada kata kunci, huruf kedua plainteks akan dienkripsi dengan huruf kedua pada kata kunci, dan seterusnya. Kata kunci diulang secara periodik apabila panjang kunci kurang dari panjang plainteks.

Berikut adalah tabel bujursangkar Vigènere Chiper.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Gambar 1. Bujursangkar Vigènere [2]

Kolom paling kiri pada Gambar 1 merepresentasikan abjad untuk huruf pada kunci sedangkan baris paling atas merepresentasikan huruf – huruf pada plainteks. Cara untuk mendapatkan huruf untuk cipherteksnya adalah dengan mencari titik perpotongan dari kolom (huruf plainteks) dan baris (huruf kunci). Contoh:

Plainteks : THIS PLAINTEXT
Kunci : SONY
Cipherteks : LVVQ HZNGFHRVL

Terlihat dari contoh diatas bahwa huruf yang sama tidak selalu dienkripsi menjadi huruf cipherteks yang sama pula. Hal ini merupakan karakteristik dari cipher abjad-majemuk yaitu setiap huruf cipherteks dapat memiliki kemungkinan pemetaan ke banyak huruf plainteks.

B. Cipher transposisi columnar

Transposisi columnar merupakan cipher yang menggunakan teknik transposisi untuk melakukan proses enkripsi dan dekripsi [5]. Pada transposisi columnar, plainteks akan dimasukkan ke dalam kolom dan baris secara berurutan. Selanjutnya cipherteks didapatkan dengan membaca kolom sesuai dengan urutannya seperti diperlihatkan pada Gambar 2.

Contoh cipher transposisi columnar dengan kunci = 6

Plainteks : BUKU PESANAN TELAH DIKIRIM

Cipherteks : BSEK PNDM UAHI UALI KNAR ETI

1	2	3	4	5	6
B	P	U	U	K	E
S	N	A	A	N	T
E	D	H	L	A	I
K	M	I	I	R	

Gambar 2. Contoh enkripsi transposisi columnar dengan kunci 6

III. METODOLOGI PENELITIAN

Penelitian ini mengukur kinerja dari enkripsi vigenere cipher yang dikombinasikan dengan transposisi columnar cipher. Selain itu, dilakukan pula iterasi terhadap enkripsi vigenere-transposisi cipher untuk meningkatkan kekaburan dari cipherteks. Avalance effect dan running time digunakan untuk menentukan baik tidaknya hasil cipherteks dari kombinasi tersebut. Analisis periodicity dengan MATLAB juga digunakan dalam penelitian ini untuk meneliti apakah periodicity dari vigenere, transposisi, atau keduanya yang dapat mempengaruhi hasil dari enkripsi dari cipher kombinasi tersebut [6].

A. Avalanche Effect

Avalanche effect mengindikasikan persentase dari perubahan bit pada plaintext atau kunci yang dapat menghasilkan perubahan beberapa bit dari cipherteks [7].

$$Avalanche\ effect\ = \frac{banyak\ bit\ berubah}{total\ jumlah\ bit}\ x\ 100$$

B. Cipher Vigenere-Transposisi

Cipher Vigenere-Transposisi merupakan cipher kombinasi antara cipher Vigenere dan cipher Transposisi columnar. Cara kerja cipher ini adalah plainteks akan dienkripsi terlebih dahulu dengan menggunakan Vigenere. Selanjutnya cipherteks hasil dari Vigenere akan dienkripsi menggunakan Transposisi Columnar

C. Iterasi-Vigenere-Transposisi

Iterasi-Vigenere-Transposisi adalah metode enkripsi dengan cara mengulang teknik Vigènere cipher dan teknik transposisi columnar sebanyak beberapa iterasi dengan menggunakan kunci yang sama. Proses yang terjadi terbagi menjadi dua bagian: enkripsi vigènere cipher dan teknik transposisi yang kemudian akan di ulang sampai beberapa iterasi.

D. Running time enkripsi

Running time enkripsi adalah total waktu yang dibutuhkan untuk mengenkripsi seluruh plainteks menjadi cipherteks. Cara menghitung running time yaitu menghitung selisih dari waktu awal dan waktu akhir enkripsi. Lamanya running time ini mengindikasikan tingginya beban komputasi

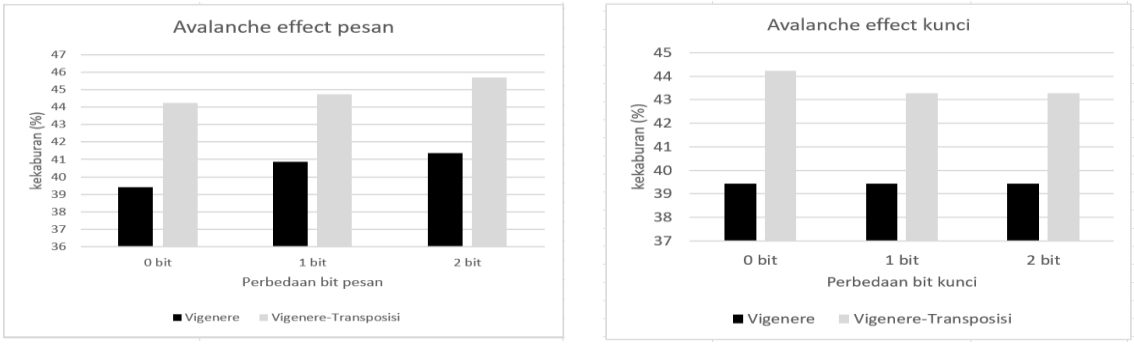
IV. PENGUJIAN DAN PEMBAHASAN

Bagian ini menjelaskan hasil dari pengujian avalanche effect, running time pada Vigenere-Transposisi dan Iterasi-Vigenere-Transposisi. Analisis periodicity juga dilakukan untuk menganalisis apakah vigenere atau transposisi yang mempengaruhi avalanche effect dari Vigenere-Transposisi.

A. Hasil avalanche effect jika kunci tetap, pesan berubah dan kunci berubah, pesan tetap.

Gambar 3 menunjukkan hasil avalanche effect jika pesan berubah (diubah bit-nya) dan kunci tetap. Variasi pesan dilakukan dengan mengubah pesan sebanyak 1 bit dan 2 bit. Hasil yang ditunjukkan dari Gambar 3 bahwa semakin banyak perbedaan bit pesan, maka persentase kekaburannya akan semakin tinggi. Hal ini baik karena semakin kabur pesannya maka pesannnya akan lebih sulit untuk dipecahkan. Penerapan kombinasi Vigenere-Transposisi juga terbukti secara signifikan menambah persentase kekaburan pesan.

Hasil pengukuran avalanche effect jika kunci diubah sebanyak 1 bit dan 2 bit diperlihatkan pada Gambar 4. Perbedaan bit kunci yang diterapkan pada Vigenere tidak berpengaruh terhadap kekaburan hasil enkripsi. Sedikit penurunan kekaburan dapat terlihat pada penerapan Vigenere-Transposisi. Hal ini disebabkan jika kuncinya diubah, maka akan berpengaruh pada pemetaan Vigenere dan urutan abjad pada transposisi columnar.



(a) (b)

Gambar 3. Hasil avalanche effect dengan perbedaan bit pesan (a) dan kunci (b) sebanyak 1 bit dan 2 bit.

B. Hasil pengukuran avalance effect Vigenere dengan Iterasi-Vigenere-Transposisi

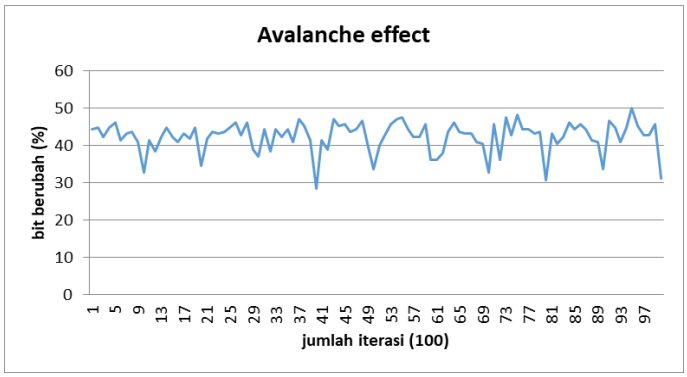
Tabel 1 menunjukkan hasil pengukuran avalanche effect Vigenere cipher dibandingkan dengan Itereasi-Vigenere-Transposisi. Iterasi pada Vigenere-Transposisi cipher dilakukan sebanyak 5 iterasi. Hasilnya menunjukkan bahwa persentase kekaburan yang dihasilkan dari penerapan Iterasi-Vigenere-Transposisi dapat mengungguli persentase yang dihasilkan oleh Vigenere cipher. Iterasi ke-5 menghasilkan nilai persentase kekaburan paling tinggi dibandingkan dengan iterasi 1-4, hal ini menunjukkan semakin banyak iterasi yang dilakukan maka tingkat kekaburannya akan semakin tinggi

TABEL 1.
HASIL AVALANCHE EFFECT VIGENERE DENGAN ITERASI-VIGENERE-TRANSPOSISI

Algoritma	Kunci transposisi columnar	Iterasi	Jumlah bit yang berubah	Avalanche effect
Vigènere Cipher	-	-	82	39,42%
Iterasi-Vigenere-Transposisi	5	1	92	44,23%
		2	93	44,71%
		3	88	42,71%
		4	93	44,71%
		5	96	46,15%

C. Hasil pengukuran avalanche effect Iterasi-Vigenere-Transposisi untuk 100 iterasi

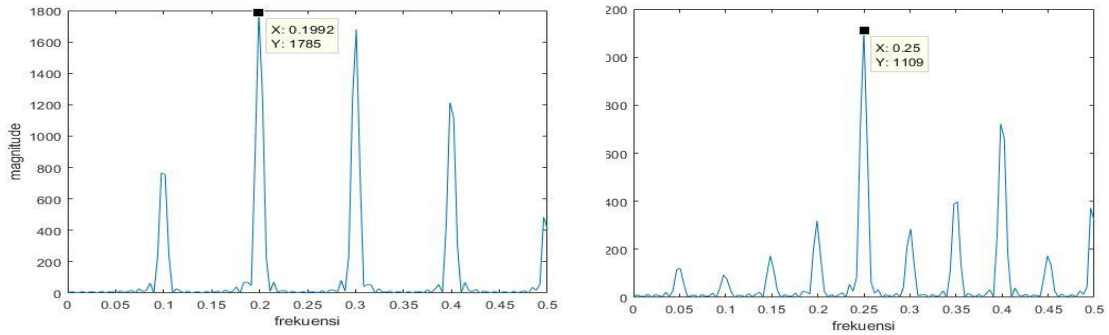
Gambar 5 menujukkan hasil pengukuran avalanche effect pada Iterasi-Vigener-Transposisi untuk 100 iterasi. Data pada Gambar 5 memperlihatkan bahwa avalanche effect terlihat memiliki pola naik turun setiap beberapa iterasi (periodicity). Oleh sebab itu, maka dilakukan analisis periodicity menggunakan MATLAB untuk melihat menganalisis apakah pola ini lebih dipengaruhi oleh Vigenere Cipher atau Transposisi Cipher



Gambar 5. Pola pergerakan avalanche effect dengan jumlah 100 iterasi

D. Pengaruh algoritma Transposisi Columnar terhadap hasil cipherteks di setiap iterasi pada perulangan enkripsi

Pengujian ini dilakukan untuk mencari periode perulangan hasil cipherteks dari Iterasi-Vigenere-Transposisi menggunakan 100 iterasi. Variabel yang diubah adalah jumlah kolom transposisi columnar yaitu 5 dan 13 kolom. Gambar 6 (a) dan (b) menunjukkan periode perulangan kekaburan yang dihasilkan dari 5 dan 13 kolom. Pada Gambar 6(a) terlihat bahwa pada setiap 10 iterasi, avalanche effect akan turun kemudian mulai meningkat lagi. Sementara itu pada Gambar 6 (b) ditunjukkan bahwa periode perulangan terjadi setiap 5 iterasi. Hal ini menunjukkan bahwa perubahan jumlah kolom akan mempengaruhi panjang iterasi secara p

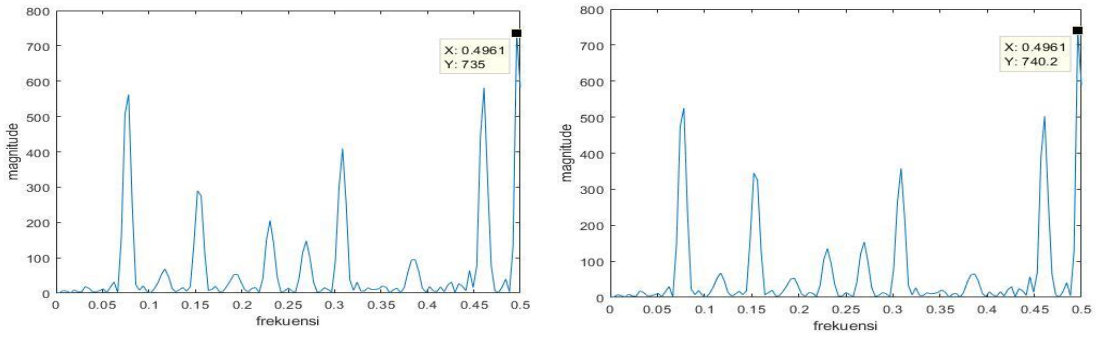


(a) (b)

Gambar 6. Hasil analisis periodicity 100 Iterasi-Vigenere-Transposisi jumlah kolom 5 (a) dan 13 (b)

E. Pengaruh algoritma substitusi Vigènere Cipher terhadap hasil cipherteks di setiap iterasi pada perulangan enkripsi

Pengujian ini dilakukan untuk melihat pengaruh perbedaan variasi kunci 0 bit (sama dengan kunci asli) dan variasi 2 bit yang dilakukan pada subsitusi Vigenere cipher. Hal ini dilakukan untuk melihat pengaruh variasi ini terhadap periodicity Iterasi-Vigenere-Transposisi. Gambar 7(a) dan 7(b) menunjukkan bahwa tidak ada perubahan yang signifikan terhadap periodicity yang dihasilkan oleh Iterasi-Vigenere-Transposisi.

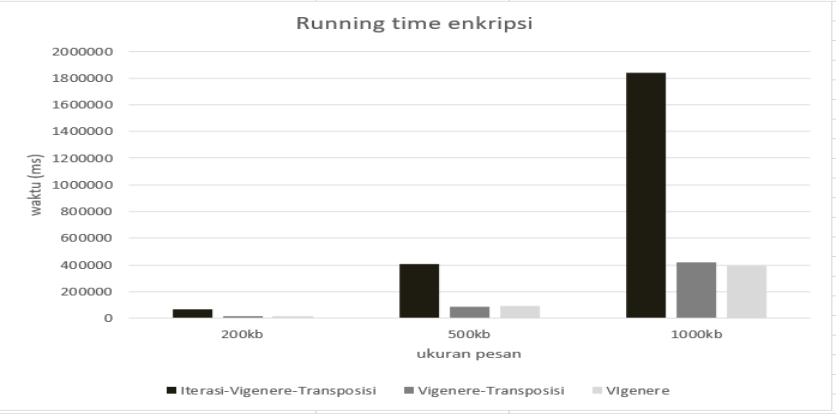


(a) (b)

Gambar 7. Hasil analisis periodicity 100 Iterasi-Vigenere-Transposisi beda kunci 0 bit dan 2 bit

F. Hasil pengukuran running time

Gambar 8 menunjukkan hasil running time enkripsi dari Vigenere, Vigenere-Transposisi dan Iterasi-Vigenere-Transposisi. Total running time memperlihatkan total waktu yang dibutuhkan dalam proses enkripsi file berupa txt yang berukuran mulai dari 10kb, 100kb, 200kb, 500kb dan 1000kb. Dari Gambar 8, ditunjukkan bahwa running time pada enkripsi pada ketiga cipher tersebut semakin tinggi apabila ukuran plainteks juga bertambah besar. Peningkatan running time secara signifikan terjadi pada proses enkripsi Iterasi-Vigenere-Transposisi. Peningkatan running time ini juga mengindikasikan bahwa beban komputasi pada proses enkripsi Iterasi-Vigenere-Transposisi juga tinggi.



Gambar 8. Hasil pengukuran running time enkripsi

V. KESIMPULAN

Setelah melakukan pengujian dan analisis pada data hasil penelitian dapat disimpulkan bahwa penggunaan Vigenere-Transposisi cipher menghasilkan persentase nilai kekaburan yang lebih tinggi dibandingkan dengan enkripsi dengan Vigenere saja. Penggunaan Iterasi-Vigenere-Transposisi cipher juga menghasilkan persentase nilai yang lebih tinggi dibandingkan enkripsi dengan Vigenere saja. Walaupun Iterasi-Vigenere-Transposisi menghasilkan nilai persentase kekaburan yang tinggi namun beban komputasinya juga besar. Hal ini diperlihatkan dengan hasil running time enkripsi yang tinggi. Perubahan jumlah kolom pada transposisi columnar berpengaruh pada periodicity dari kekaburan yang dihasilkan oleh Iterasi-Vigenere-Transposisi cipher

DAFTAR PUSTAKA

[1] Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot. 1996. *Handbook of Applied Cryptography*. CRC Press, Inc., Boca Raton, FL, USA.
[2] Niels Ferguson and Bruce Schneier. 2003. *Practical Cryptography*. John Wiley & Sons, Inc., New York, NY, USA.
[3] B. Triandi, E. Ekadiansyah, R. Puspasari, L. T. Iwan and F. Rahmad, "Improve Security Algorithm Cryptography Vigenere Cipher Using Chaos Functions," *2018 6th International Conference on Cyber and IT Service Management (CITSM)*, Parapat, Indonesia, 2018, pp. 1-5.
[4] D. Rachmawati, M. A. Budiman and M. Magdalena Batubara, "Enhancing File Security by using Vigenere Cipher and Even Rodeh Code Algorithm," *2018 International Conference on Computer, Control, Informatics and its Applications (IC3INA)*, Tangerang, Indonesia, 2018, pp. 54-59.
[5] Ariyus, Dony. *Pengantar Ilmu Kriptografi : Teori Analisis & Implementasi*. Andi. Yogyakarta. 2008.
[6] Find Periodicity Using Frequency Analysis - MATLAB & Simulink, *MATLAB Documentation*, Diakses: 3 Mei 2019. [Online]: https://www.mathworks.com/help/signal/ug/find-periodicity-using-frequency-analysis.html.
[7] Kumar, A., & Tiwari, N. (2012). Effective Implementation and Avalanche Effect of AES. International Journal of Security, Privacy and Trust Management (IJSPTM), 1(3), 31 35.

Gregorius Magnus Mega Sanjaya adalah lulusan dari Program Studi Teknik Informatika Universitas Sanata Dharma Yogyakarta tahun 2019.