JIFOTECH (JOURNAL OF INFORMATION TECHNOLOGY)
Vol. 1, No. 1, Maret 2021

Penerapan Kombinasi Algoritma *Caesar Cipher* pada *Block* Acak dan *Cipher* Transposisi Dalam Mengamankan Pesan

Mahmuda Saputra[1], Alva Hendi Muhammad[2]
Magister Teknik Informatika, Universitas AMIKOM Yogyakarta
mahmudasaputra@gmail.com, alva@amikom.ac.id

***Abstract*— The developments in technology for using security of information are still a threat to every party in processing and transaction confidentiality of messages sent received by users. In this study, the authors carried out a process of learning in terms of classical security with a Caesarean algorithm model with technical support for random blocks of messages and the use of ciphertexts in password transposition. This is to see how the flow can be controlled in describing a message to be conveyed to the required destination. This process is invincible with a few simple experiments, in order to achieve the desired results. Some of the research results carried out in this study include (1) the existence of a process in using the Caesarean cipher cryptographic algorithm, (2) For learning in an information or message that will be sent every time it is received, (3) Each stage of the Caesarean Cipher algorithm is very useful for exploring a messages with a more secure yahoo combination. (4) Can carry out a combination process with random block techniques and transposition ciphers.**

Keywords *: Cryptography, Caesar Cipher, Random selection, Transposition Cipher*

***Intisari*— Perkembangan dalam teknologi terhadap keamanan suatu informasi yang masih menjadi ancaman untuk setiap pihak dalam melakukan proses komunikasi dan transaksi kerahasiaan pesan yang dikirim maupun diterima oleh pengguna. Pada penelitian ini, penulis melakukan proses terhadap pembelajaran dalam hal keamanan yang bersifat klasik dengan model algoritma caesar cipher dengan dukungan teknik pada block acak pada pesan dan penggunaan ciphertext pada cipher transposisi. Hal tersebut untuk mengetahui, bagaimana alur yang dapat dikendalikan dalam mendeskripsikan sebuah pesan yang ingin disampaikan kepada tujuan yang dibutuhkan. Proses ini disesuaikan dengan beberapa eksperimen sederhana, agar dapat tercapaianya hasil yang diinginkan. Beberapa hasil kontribusi yang peneliti lakukan dalam penelitian ini meliputi dengan adanya setiap proses dalam menggunakan sebuah algoritma kriptografi caesar chiper, dapat digunakan sebagai pembelajaran dalam mengamankan sebuah informasi atau pesan yang akan dikirim maupun diterima, untuk setiap tahapan pada algoritma caesar chiper sangat bermanfaat untuk mengksplorasikan sebuah pesan dengan kombinasi algoritma yang lebih secure, serta dapat melakukan proses kombinasi dengan teknik block acak maupun cipher transposisi.**

Kata Kunci*— Kriptografi klasik, Caesar Cipher, Block Acak, Cipher Transposisi*

I. PENDAHULUAN

Pengamanan sebuah informasi atau kerahasiaan suatu data merupakan salah satu aspek penting dari berbagai informasi yang diterima maupun dikirim oleh pengguna. Beragamnya perkembangan peranan teknologi saat ini, setiap pengguna sangat mudah dalam memperoleh data atau informasi. Apabila data atau informasi tersebut tidak dilindungi, maka secara mudah orang lain akan mengetahui data atau informasi yang dimiliki. Kriptografi merupakan salah satu ilmu seni dengan filosofinya the art of war. Dimana pada saat itu digunakan untuk mengirim pesan rahasia pada zaman Romawi pada era raja Julius Caesar. Kriptografi adalah suatu metode untuk melindungi suatu data atau informasi dengan menggunakan sandi, dimanasandi tersebut hanya bisa dimengerti oleh orang yang berhak menerima data atau informasi tersebut. Sedangkan tujuan kriptografi adalah melindungi data dari ancaman yang disengaja atau tidak disengaja. Dewasa ini ancaman bertambah karena semakin meluasnya akses melalui internet atau teknologi bergerak secara *realtime*. Pada penelitian ini, penulis melakukan beberapa penerapan metode dari kombinasi kriptografi *caesar cipher*.

Caesar cipher merupakan salah satu algoritma tertua dan merupakan salah satu jenis cipher substitusi yang membentuk cipher dengan cara melakukan pergeseran terhadap semua karakter pada plainteks dengan nilai pergeseran yang sama. Kelemahan caesar cipher adalah kita biasa memproleh pesan asli dengan memanfaatkan metode brute force dan presentasi frekuensi huruf yang paling sering muncul dalam suatu kalimat [1].

Algoritma caesar cipher yaitu algoritma dengan mengganti posisi huruf awal dengan alphabet atau disebut dengan algoritma ROT3. Algoritma transposisi yaitu dengan cara mengubah letak dari teks pesan yang akan disandikan dengan menggunakan bentuk tertentu. Algoritma vigenere yaitu setiap teks-kode selalu menggantikan nilai teks-asli tertetu. Algoritma blok cipher yaitu mengenkripsi satu blok plaintext dengan jumlah bit tertentu dan menghasilkan blok cipher dengan jumlah bit yang sama [2].

Algoritma kriptografi Caesar Cipher sangat mudah untuk digunakan. Inti dari algoritma kriptografi ini adalah melakukan pergeseran terhadap semua karakter pada plainteks dengan nilai pergeseran yang sama. Adapun langkahlangkah yang dilakukan untuk membentuk cipherteks dengan Caesar Cipher adalah menentukan besarnya pergeseran karakter yang digunakan dalam membentuk cipherteks ke plainteks, Menukarkan karakter pada plainteks menjadi cipherteks dengan berdasarkan pada pergeseran yang telah ditentukan sebelumnya. Tujuan penelitian ini untuk mendapatkan sebuah gambaran yang kualitasnya terhadap penerapan enkripsi dari metode *Caesar Cipher* dalam penyampaian informasi dalam komunikasi yang dapat mengamankan pesan dikirim atau diterima oleh pihak pengguna, dan selanjutnya dapat diteliti

kembali untuk mengkombinasikan dengan berbagai algoritma yang lain dalam mengamankan sebuah informasi.

II. TINJAUAN PUSTAKA

Keamanan komputer adalah tentang studi tentang serangan terhadap dunia maya dengan tujuan untuk mempertahankan diri dari serangan. Kriptografi dianggap sebagai kelas sains dengan menggunakan seni atau teknik khusus yang mentransformasikan pernanan informasi dengan cara yang terlindungi dengan sedemikian rupa dalam hal untuk mengatasi sebuah serangan. Ada persyaratan yang sangat besar dari algoritma kriptografi yang kuat untuk mempertahankan dari berbagai serangan. Pada sebuah metode dengan Prinsip Kerchoff yang menyatakan bahwa algoritma enkripsi dan dekripsi selalu ada tersedia untuk siapa saja. Keamanan sandi terhadap segala jenis serangan harus bergantung hanya pada kerahasiaan kunci [3]. Kriptografi merupakan seni dan ilmu untuk melindungi informasi dari individu yang tidak diinginkan dengan mengubahnya menjadi bentuk yang tidak dapat dikenali oleh penyerangnya saat disimpan dan dikirimkan. Misalnya dalam sistem Internet Banking, sistem reservasi elektronik, keamanan data merupakan masalah yang sangat penting. Dalam situasi apa pun penyusup tidak boleh masuk ke database server atau data rahasia. Dalam semua jenis sektor layanan, kerahasiaan data merupakan masalah yang sangat penting. Tujuan utama dari sistem apa pun adalah bahwa data tidak dapat dimodifikasi oleh pengguna eksternal atau penyusup [4]. Data ataupun informasi menjadi aspek penting bagi kehidupan manusia. Selain itu data juga bisa digunakan sebagai alat untuk melakukan tindak kriminal. Untuk itulah diperlukan sebuah alat untuk mengamankannya. Teknik pengamanan data sangat beragam, diantaranya ada yang bersifat manual dan ada juga yang menggunakan sistem yang sudah terkomputerisasi. Teknik yang sudah terkomputerisasi biasanya menggunakan sebuah aplikasi untuk mengamankan data[5]

Aplikasi-aplikasi ini lah yang sering menjadi incaran para pirates untuk diambil data dan informasi rahasianya. Dengan menggunakan 4 teknik sekaligus dalam mengamankan data dan informasi rahasia diyakini dapat membuat tingkat keamanannya lebih tinggi. Diantaranya menggunakan Algoritma Caesar, yaitu dengan mengganti posisi huruf awal dari alfabet atau disebut juga dengan algoritma ROT3. Algoritma Transposisi, yaitu dengan menggunakan permutasi karakter. Algoritma Vigenere, yaitu setiap teks-kode selalu menggantikan nilai teks-asli tertentu. Algoritma Blok Cipher, yaitu mengenkripsi satu blok plaintext dengan jumlah bit tertentu dan menghasilkan blok ciphertext dengan jumlah bit yang sama. Untuk memudahkan penggunanya, aplikasi ini dibuat berbasis mobile, jadi pengguna hanya membutuhkan smartphone untuk mengenkripsi data dan informasi rahasianya ke dalam media digital. Hasilnya, aplikasi ini bisa berjalan dan melakukan proses enkripsi dan dekripsi pada platform *smartphone*.

Kriptografi adalah ilmu untuk menyamarkan atau mengubah wujud pesan asli menjadi pesan yang tidak dapat diketahui atau dipahami oleh siapa yang tidak berhak. Caesar cipher adalah metode yang klasik dan sangat mendasar dalam ilmu pengkodean pesan. Cara ini memiliki kekurangan yaitu spasi tidak bisa dienkripsi karena rumusnya menggunakan mod 26, dan juga jika setelah proses penghitungan sisa hasil untuk 0 nya juga, maka hasil ini tidak perlu dienkripsi. Namun teknik dasar sangat penting untuk mempelajari teknik-teknik kriptografi modern, maka perlu dilakukan pengujian untuk proses verifikasi plaintext menjadi ciphertext (enkripsi) dan juga ciphertext menjadi plaintext (dekripsi) dengan menggunakan software penguji yaitu Matlab R2010a dengan tujuan agar dapat lebih mudah menentukan logika proses kriptografi [6].

Kemanan data peserta dan hasil pemilihan pada proses pemilihan ketua organisasi pada STMIK KHARISMA Makassar, merupakan hal yang sangat penting dan bersifat rahasia. Untuk menjaga keamanan data maka dapat digunakan algoritma kriptografi, salah satu satunya adalah algoritma caesar cipher. Algoritma tersebut diterapkan pada sistem e-voting pemilihan ketua unit kegiatan mahasiswa (UKM) pada STMIK KHARISMA Makassar dengan metode pergeseran 3 pada proses enkripsi dan dekripsinya. Proses enkripsi dilakukan sebelum penyimpanan data pada database dilakukan, proses dekripsi dilakukan pada saat sistem melakukan proses pembacaan data hasil pemilihan. Dengan menerapkan algoritma tersebut, diperlihatkan bahwa data yang tersimpan kedalam database dalam bentuk enkripsi tidak dapat dibaca dengan mudah oleh administrator sistem. Sehingga dapat meminimalisir penyalah gunaan data hasil pemilihan maupun seluruh informasi yang ada dalam sistem. Penerapan algoritma caesar chipper pada sistem e-voting pemilihan ketua UKM pada STMIK KHARISMA Makassar, cukup aman dalam menjaga kerahasiaan data. Diharapkan penelitian ini dapat dikembangkan dengan menggabungkan dua algoritma untuk memberikan hasil yang lebih baik atau menggabungkan dua buah pola pergeseran yang berbeda, sehingga sulit untuk menemukan pola dekripsi oleh orang-orang yang ingin menyalah gunakan data tersebut [7].

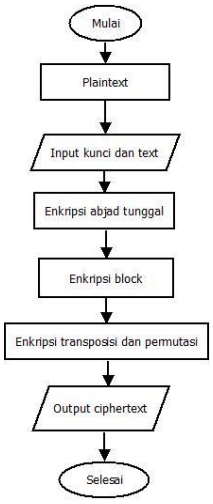
Pada Penelitian yang lain, yaitu dengan mengusulkan skema yang lebih baik dalam mengenkripsi pesan teks biasa untuk keamanannya. Semua teknik enkripsi yang konvensional sangat lemah terhadap serangan brute force dan kriptanalisis yang masih secara tradisional dapat digunakan untuk dengan mudah dalam menentukan teks biasa dari teks terenkripsi. Dalam pekerjaan teknik enkripsi ini, konsep baru dari algoritma cipher ceaser konvensional dengan algoritma hill cipher digunakan untuk membuat teknik enkripsi lebih aman dan lebih kuat dari konsep sebelumnya. Teks biasa dienkripsi sedemikian rupa sehingga menjadi sulit untuk mendekripsinya. Sistem yang diusulkan dibagi menjadi dua tahap. Pada tahap pertama, pesan teks biasa diubah menjadi teks terenkripsi pertama menggunakan pendekatan substitusi baru yang menggunakan teknik cipher polihabetik. Enkripsi dilakukan menggunakan kunci panjang variabel yang bergantung pada panjang string. Pada tahap kedua, teknik hill cipher diterapkan pada teks terenkripsi pertama untuk menghasilkan teks terenkripsi atau teks sandi baru. Di sisi penerima, jika penerima memiliki kunci dekripsi yang sesuai,

JIFOTECH (JOURNAL OF INFORMATION TECHNOLOGY)
Vol. 1, No. 1, Maret 2021

dia dapat menghasilkan pesan teks yang mirip dengan pesan asli [8].

III. METODOLOGI PENELITIAN

Adapun metode penelitian bersifat eksperimen dengan melakukan beberapa tahap dengan penarapan algoritma yang akan diproses melalui pendekatan caesar cipher, beserta adanya block acak terhadap pesan yang disematkan. Berikut bagan proses pada enkripsi, block acak, cipher transposisi pada Gambar 3.1



Gambar 3.1 Baga alur enkripsi pada cipher

Sebagai langkah penelitian awal, penulis menerapkan metode penelitian yang akan digunakan, yaitu berupa metode eksperimen dalam melakukan pengujian pada algoritma kriptografi caesar chiper. Untuk skenario awal adanya plaitext yang telah diberikan untuk memodifikasi chipertext, skenario kedua melakukan penyisipan huruf dari setiap kunci K1,K2,dan K3, skenario ketiga melakukan peranan 6 kunci secara bersamaan dan skenarion keempat menentukan pengelompokkan informasi yang telah disusun. Adapun ringkasan rancangan yang dikerjakan pada tahap ini sebagai berikut, yang termuat pada Tabel 3.1

Tabel 3.1 Kunci yang digunakan dalam penelitian

	A	B	C	D	E	F	G	H	I	J	K	L
K1	M	A	H	U	D	S	P	T	R	B	C	E
	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**
K2	R	I	S	N	T	H	A	U	L	D	B	C
	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**
K3	M	A	H	R	Y	N	I	B	E	U	T	C

Plaintext :

Dalam Situasi Penyebaran Virus Corona Sebaiknya Jaga Jarak Dengan Teman Saudara Apalagi Kekasih Anda

IV. HASIL DAN PEMBAHASAN

Adapun hasil yang diterapakan pada tahanap penggunaan algoritma caesar cipher sebagai berikut :

Tabel 4.1 Proses penerapan algoritma caesar cipher pada block acak

K1	**K2**	**K3**	**K1**	**K2**
D	A	L	A	M
U	R	C	M	E
Block 1				
K1	**K2**	**K3**	**K1**	**K2**
S	I	T	U	A
N	L	P	Q	R
Block 2				
K1	**K2**	**K3**	**K1**	**K2**
S	I	P	E	N
N	L	J	D	F
Block 3				
K1	**K2**	**K3**	**K1**	**K2**
Y	E	B	A	R
Y	T	A	M	M
Block 4				
K1	**K2**	**K3**	**K1**	**K2**
A	N	V	I	R
M	F	S	R	M
Block 5				
K1	**K2**	**K3**	**K1**	**K2**
U	S	C	O	R
Q	O	H	I	M
Block 6				
K1	**K2**	**K3**	**K1**	**K2**
O	N	A	S	E
I	F	M	N	T
Block 7				
K1	**K2**	**K3**	**K1**	**K2**
B	A	I	K	N
A	R	E	C	F
Block 8				
K1	**K2**	**K3**	**K1**	**K2**
Y	A	J	A	G
Y	R	U	M	A
Block 9				
K1	**K2**	**K3**	**K1**	**K2**
A	J	A	R	A
M	D	M	L	R
Block 10				
K1	**K2**	**K3**	**K1**	**K2**
K	D	E	N	G
C	N	Y	G	A
Block 11				
K1	**K2**	**K3**	**K1**	**K2**

A	N	T	E	M
M	F	P	D	E
		Block 12		
K1	**K2**	**K3**	**K1**	**K2**
A	N	S	A	U
M	F	O	M	Q
		Block 13		
K1	**K2**	**K3**	**K1**	**K2**
D	A	R	A	A
U	R	L	M	M
		Block 14		
K1	**K2**	**K3**	**K1**	**K2**
P	A	L	A	G
J	R	C	M	A
		Block 15		
K1	**K2**	**K3**	**K1**	**K2**
I	K	E	K	A
R	B	Y	C	R
		Block 16		
K1	**K2**	**K3**	**K1**	**K2**
S	I	H	A	N
N	L	B	M	F
		Block 17		
K1	**K2**	**K3**	**K1**	**K2**
D	A	X	X	X
U	R	X	X	X
		Block 18		

Tabel 4.2 Perubahan enkripsi terhadap plaintext dari proses acak

K1	K2	K3	K1	K2	K3
D	A	L	A	M	S
B	U	N	Y	Y	P
K1	K2	K3	K1	K2	K3
I	T	U	A	S	I
D	B	B	Y	P	N
K1	K2	K3	K1	K2	K3
P	E	N	Y	E	B
R	J	O	X	J	E
K1	K2	K3	K1	K2	K3
A	R	A	N	V	I
Y	U	H	M	N	N
K1	K2	K3	K1	K2	K3
R	U	S	C	O	R
H	C	L	Q	R	T
K1	K2	K3	K1	K2	K3
O	N	A	S	E	B
C	G	H	N	J	E
K1	K2	K3	K1	K2	K3
A	I	K	N	Y	A
Y	H	G	M	X	H

K1	K2	K3	K1	K2	K3
J	A	G	A	J	A
E	E	M	Y	L	H
K1	K2	K3	K1	K2	K3
R	A	K	D	E	N
H	E	G	K	J	O
K1	K3	K1	K2	K3	K1
G	N	T	E	M	A
U	O	I	J	Q	Y
K2	K3	K1	K2	K3	K1
N	S	A	U	D	A
G	L	Y	C	C	Y
K2	K3	K1	K2	K3	K1
R	A	A	P	A	L
U	H	Y	Q	H	P
K2	K3	K1	K2	K3	K1
A	G	I	K	E	K
E	M	D	M	Y	O
K2	K3	K1	K2	K3	K1
A	S	I	H	A	N
E	L	D	K	H	M
K2	K3				
D	A				
S	H				

Tahap selanjutnya melanjutkan dengan penerapan permutasi, pada Tabel 4.3 yaitu :

Tabel 4.3 Penerapan permutasi dengan block acak

1	2	3	4	5	6
B	**U**	**N**	**Y**	**Y**	**P**
Block 1					
↓					
5	4	6	2	1	3
Y	**Y**	**P**	**U**	**B**	**N**
1					
1	2	3	4	5	6
D	**B**	**B**	**Y**	**P**	**N**
Block 2					
↓					
5	4	6	2	1	3
P	**Y**	**N**	**B**	**D**	**B**
2					
1	2	3	4	5	6
R	**J**	**O**	**X**	**J**	**E**
Block 3					
↓					

JIFOTECH (JOURNAL OF INFORMATION TECHNOLOGY)
Vol. 1, No. 1, Maret 2021

5	4	6	2	1	3
J	**X**	**E**	**J**	**R**	**O**
3					
1	2	3	4	5	6
Y	**U**	**H**	**M**	**N**	**N**
Block 4					
↓					
5	4	6	2	1	3
N	**M**	**N**	**U**	**Y**	**H**
4					
1	2	3	4	5	6
H	**C**	**L**	**Q**	**R**	**T**
Block 5					
↓					
5	4	6	2	1	3
R	**Q**	**T**	**C**	**H**	**L**
5					
1	2	3	4	5	6
C	**G**	**H**	**N**	**J**	**E**
Block 6					
↓					
5	4	6	2	1	3
J	**N**	**E**	**G**	**C**	**H**
6					
1	2	3	4	5	6
Y	**H**	**G**	**M**	**X**	**H**
Block 7					
↓					
5	4	6	2	1	3
X	**M**	**H**	**H**	**Y**	**G**
7					
1	2	3	4	5	6
E	**E**	**M**	**Y**	**L**	**H**
Block 8					
↓					
5	4	6	2	1	3
L	**Y**	**H**	**E**	**E**	**M**
8					
1	2	3	4	5	6
H	**E**	**G**	**K**	**J**	**O**
Block 9					
↓					
5	4	6	2	1	3
J	**K**	**O**	**E**	**H**	**G**

9					
1	2	3	4	5	6
U	**E**	**O**	**I**	**J**	**Q**
Block 10					
↓					
5	4	6	2	1	3
J	**I**	**Q**	**E**	**U**	**O**
10					
1	2	3	4	5	6
Y	**G**	**L**	**Y**	**C**	**C**
Block 11					
↓					
5	4	6	2	1	3
C	**Y**	**C**	**G**	**Y**	**L**
11					
1	2	3	4	5	6
Y	**U**	**H**	**Y**	**Q**	**H**
Block 12					
↓					
5	4	6	2	1	3
Q	**Y**	**H**	**U**	**Y**	**H**
12					
1	2	3	4	5	6
P	**E**	**M**	**D**	**M**	**Y**
Block 13					
↓					
5	4	6	2	1	3
M	**D**	**Y**	**E**	**P**	**M**
13					
1	2	3	4	5	6
O	**E**	**L**	**D**	**K**	**H**
Block 14					
↓					
5	4	6	2	1	3
K	**D**	**H**	**E**	**O**	**L**
14					
1	2	3	4	5	6
M	**S**	**H**	**A**	**B**	**C**
Block 15					
↓					
5	4	6	2	1	3
B	**A**	**C**	**S**	**M**	**H**
15					

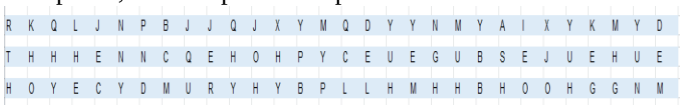
Adapun hasil dari ciphertext dirubah menjadi cipher

transposisi pada Tabel 4.4 sebagai berikut :

Tabel 4.4 Cipher Transposisi

R	Q	T	C	H	L	1
K	D	H	E	O	L	2
Q	Y	H	U	Y	H	3
L	Y	H	E	E	M	4
J	N	E	G	C	H	5
N	M	N	U	Y	H	6
P	Y	N	B	D	B	7
B	A	C	S	M	H	8
J	I	Q	E	U	O	9
J	X	E	J	R	O	10
Q	Y	H	U	Y	H	11
J	K	O	E	H	G	12
X	M	H	H	Y	G	13
Y	Y	P	U	B	N	14
M	D	Y	E	P	M	15

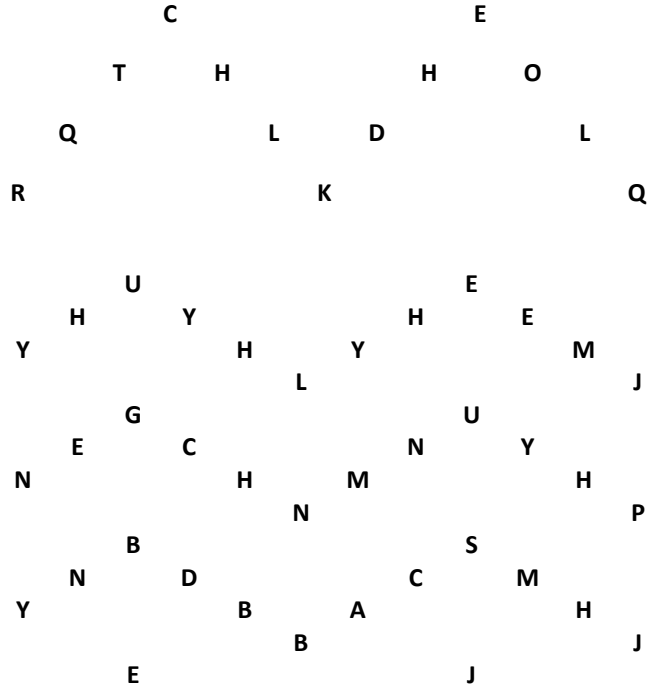
Setelah dilakukannya penerubahan pada block acak dan transposisi, maka dapat dilihat pada Gambar 4.1 :

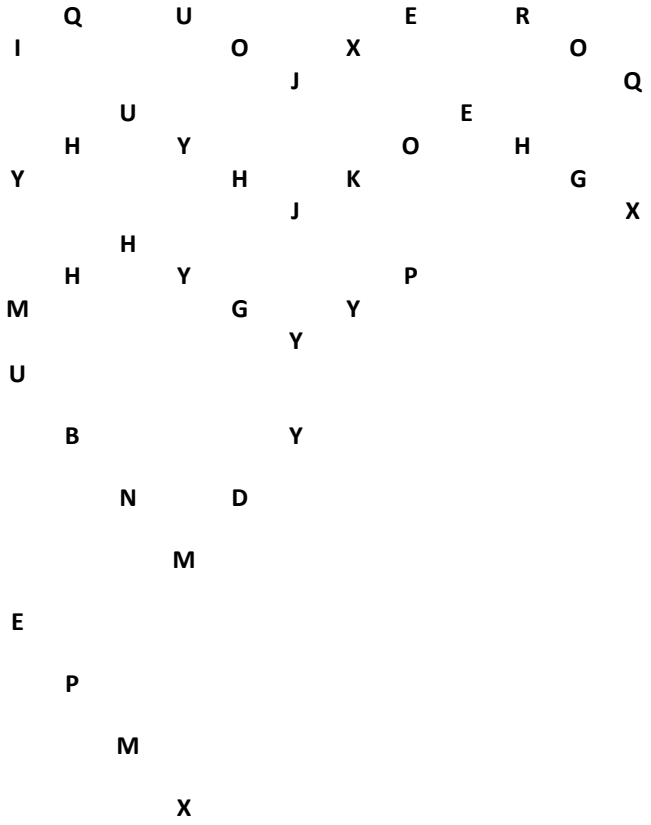


Gambar 4.1 Cipher Transposisi setalah perubahan

Untuk hasil akhir dari serangkaian teknik tersebut, maka disusun menjadi 4 baris ke atas dan 4 baris kebawah, pada Tabel 4.5 sebagai berikut :

Tabel 4.5 Penyusuna baris untuk 4 baris keatas dan kebawah





V. KESIMPULAN

Kesimpulan dari penelitian ini, masih sebatas proses penerapan enkripsi terhadap plaintext yang digunakan, dengan adanya keterbatasan dalam pengujian yang lebih efektif. Dalam pengujiannya hasil yang ditentukan berupa proses dari permutasi terhadap block pesan yang akan dikirim atau diterima oleh pengguna. Untuk penggunaan algoritma Caesar Cipher masih sangat berguna terhadap proses eksperimen yang lebih praktis terhadap informasi yang memadai, serta perlunya kombinasi yang dapat mengamankan pesan dengan tingkat akurasi yang lebih *secur*.

Adapun saran yang dapat dilakukan dengan penerapan algoritma yang lebih secure terhadap pengiriman informasi atau pesan yang dapat dikomunikasikan secara efesien.

UCAPAN TERIMA KASIH

Dalam penelitian yang dilakukan masih banyak yang belum tercapai dengan baik, sehingga dapat memberikan dukungan dalam bentuk revisi dari para reviewer oleh Tim Jurnal TI ISB.Terima kasih disampaikan kepada Tim Jurnal TI ISB yang telah meluangkan waktu untuk membuat template ini. Dengan lebih baik.

JIFOTECH (JOURNAL OF INFORMATION TECHNOLOGY)
Vol. 1, No. 1, Maret 2021

REFERENSI

[1] I. Gunawan, "Kombinasi Algoritma Caesar Cipher dan Algoritma RSA untuk pengamanan File Dokumen dan Pesan Teks," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 2, no. 2, pp. 124–129, 2018, doi: 10.30743/infotekjar.v2i2.266.

[2] A. Basuki, U. Paranita, and R. Hidayat, "Perancangan Aplikasi Kriptografi Berlapis menggunakan Algoritma Caesar, Transposisi, Vigenere, dan Blok Chiper Berbasis Mobile," *Semin. Nas. Teknol. Inf. Dan Multimed. 2016*, vol. 1, no. 2, pp. 31–35, 2016.

[3] M. Mohan, M. K. Kavitha Devi, and V. Jeevan Prakash, "Security analysis and modification of classical encryption scheme," *Indian J. Sci. Technol.*, vol. 8, no. 14, pp. 542–548, 2015, doi: 10.17485/ijst/2015/v8i14/59192.

[4] K. Goyal and S. Kinger, "Modified Caesar Cipher for Better Security Enhancement," *Int. J. Comput. Appl.*, vol. 73, no. 3, pp. 26–31, 2013, doi: 10.5120/12722-9558.

[5] A. Caesar, "Perancangan Aplikasi Kriptografi Berlapis Menggunakan," *Semin. Nas. Teknol. Inf. Dan Multimed. 2016*, vol. 6, no. 6, pp. 6–7, 2016.

[6] T. Limbong and P. D. P. Silitonga, "Testing the Classic Caesar Cipher Cryptography using of Matlab," *Int. J. Eng. Res. Technol.*, vol. 6, no. 2, pp. 175–178, 2017, doi: 10.17605/OSF.IO/PEMA5.

[7] H. Angriani and Y. Saharaeni, "Implementasi Algoritma Caesar Cipher pada Keamanan Data Sistem e-voting Pemilihan Ketua Organisasi Kemahasiswaan," *Inspir. J. Teknol. Inf. dan Komun.*, vol. 9, no. 2, p. 123, 2019, doi: 10.35585/inspir.v9i2.2499.

[8] Y. Rajput, D. Naik, and C. Mane, "An Improved Cryptographic Technique to Encrypt Text using Double Encryption," *Int. J. Comput. Appl.*, vol. 86, no. 6, pp. 24–28, 2014, doi: 10.5120/14990-2582.