Terakreditasi SINTA Peringkat 2
Surat Keputusan Dirjen Pendidikan Tinggi, Riset dan Teknologi No. 158/E/KPT/2021
masa berlaku mulai Vol. 5 No. 2 tahun 2021 s.d Vol. 10 No.1 tahun 2026

Terbit online pada laman web jurnal: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 5 No. 6 (2021) 1113 – 1119 ISSN Media Elektronik: 2580-0760

Pengamanan Data melalui Model Super Enkripsi Autokey Cipher dan Transposisi Kolom

Muhammad Fadlan[1], Haryansyah[2], Rosmini[3]
[1,3]Sistem Informasi, STMIK PPKIA Tarakanita Rahmawati
[2]Teknik Informatika, STMIK PPKIA Tarakanita Rahmawati
[1]fadlan@ppkia.ac.id, [2]haryansyah@ppkia.ac.id, [3]rosmini@ppkia.ac.id

Abstract

One of the essential instruments in the cyber era is data. Therefore, maintaining data security is an important thing to do. One way that can be done to maintain data security is through cryptography. In cryptography, two basic techniques are commonly used, namely substitution techniques and transposition techniques. One of the weaknesses of the basic cryptographic techniques is the lower level of data security. This study proposed a super encryption model in securing data by combining cryptographic algorithms with substitution techniques, i.e., autokey cipher and transposition, i.e., columnar transposition cipher. This study used the Avalanche Effect method as a measurement tool for the proposed super encryption model. The test results have shown that the proposed super encryption model can provide a better level of security. The avalanche effect test on the five data test shows that the average AE value of the proposed super encryption model is 30.76%. This value is higher than the single autokey cipher algorithm of 1.66% and column transposition with a value of 18.03%. Other results from the five data test have shown that the proposed model has a high level of accuracy of 100% in terms of the decryption process results, which is the same as the initial data before going through the encryption process.

Keywords: autokey, cryptography, data, transposition, super encryption

Abstrak

Salah satu instrumen penting di era digital saat ini adalah data. Menjaga keamanan data merupakan hal yang penting untuk dilakukan. Salah satu cara yang dapat dilakukan untuk menjaga keamanan data adalah melalui kriptografi. Dalam kriptografi terdapat dua teknik dasar yang umum digunakan, yaitu teknik substitusi dan teknik transposisi. Salah satu kekurangan dari teknik dasar kriptografi adalah tingkat keamanan data yang rendah. Penelitian ini mengusulkan sebuah model super enkripsi dalam mengamankan data melalui perpaduan algoritma kriptografi teknik substitusi autokey cipher dan transposisi kolom. Penelitian ini menggunakan Avalanche Effect (AE) sebagai alat ukur model super enkripsi yang diusulkan. Hasil pengujian menunjukkan bahwa model super enkripsi yang diusulkan mampu memberikan tingkat keamanan yang lebih baik. Pengujian avalanche effect terhadap lima data uji coba menunjukkan rata-rata nilai AE dari model super enkripsi yang diusulkan sebesar 30.76%. Nilai ini lebih tinggi dibandingkan algoritma tunggal autokey cipher sebesar 1.66% maupun transposisi kolom dengan nilai sebesar 18.03%. Hasil lainnya dari lima data uji coba tersebut menunjukkan model yang diusulkan memiliki tingkat akurasi yang tinggi sebesar 100% dari sisi hasil proses dekripsi yang sama seperti data awal sebelum melalui proses enkripsi.

Kata kunci: autokey, data, kriptografi, transposisi, super enkripsi

1. Pendahuluan

Isu keamanan data menjadi salah satu isu pokok di era digital. Berbagai kasus pembobolan maupun pencurian data terjadi akibat kurangnya protokol keamanan data yang dimiliki. Data merupakan salah satu elemen terpenting bagi setiap organisasi saat ini. Hal ini membuat setiap organisasi, perusahaan, maupun instansi memiliki kewajiban untuk memiliki protokol keamanan data yang baik [1], [2].

Keamanan maupun keutuhan data dapat dijaga dengan baik melalui teknik kriptografi [3]. Penggunaan kriptografi telah digunakan sejak lama dan terus mengalami perkembangan hingga saat ini. Melalui kriptografi, data akan disamarkan ke dalam sebuah bentuk yang sulit dikenali oleh pihak yang tidak berkepentingan terhadap data tersebut [4], [5]. Terdapat dua teknik dasar dalam kriptografi, yaitu teknik substitusi dan transposisi.

Diterima Redaksi: 21-10-2021 | Selesai Revisi: 02-12-2021 | Diterbitkan Online: 30-12-2021

Setiap algoritma kriptografi memiliki tingkat keamanan yang berbeda-beda, tergantung pada sulitnya algoritma tersebut untuk dipecahkan. Kelemahan utama algoritma kriptografi yang menerapkan teknik substitusi maupun transposisi adalah dari sisi tingkat keamanan yang cenderung lebih rendah [6]. Salah satu cara yang dapat digunakan untuk mengatasi kelemahan algoritma kriptografi dasar tersebut adalah melalui perpaduan antara teknik substitusi dan transposisi. Cara tersebut dikenal dengan istilah model super enkripsi [7], [8].

Beberapa penelitian terkait keamanan data dengan teknik substitusi maupun transposisi telah dilakukan sebelumnya, salah satunya adalah penelitian yang dilakukan oleh Fina Triana., dkk [4]. Penelitian tersebut melakukan pengembangan aplikasi berbasis android dengan mengusulkan modifikasi pada algoritma caesar cipher dalam mengamankan data. Salah satu kekurangan dari peneltian ini adalah terdapat beberapa karakter hasil proses enkripsi yang tidak dapat dibaca maupun ditampilkan dengan baik.

Penelitian terkait algoritma transposisi dilakukan oleh As'ad Djamalilleil, dkk., mengusulkan algoritma transposisi cipher dalam mengamankan gambar digital. Cara kerja algoritma ini adalah dengan melakukan transposisi terhadap pixel yang terdapat pada gambar digital tersebut. Hasil penelitian ini menunjukkan bahwa algoritma transposisi kolom yang diusulkan mampu digunakan dalam melakukan enkripsi dan dekripsi gambar digital menjadi kebentuk semula [9].

Penelitian yang telah dilakukan oleh M. Azman Maricar, dkk., untuk menguji efektifitas dari beberapa algoritma kriptografi yang menggunakan teknik substitusi dan teknik transposisi. Penelitian ini hanya menggunakan parameter waktu dan ukuran file sebagai alat untuk mengukur atau membandingkan antara satu algoritma dengan algoritma lainnya [10].

Penelitian yang dilakukan oleh Risma Septiana, dkk., dengan mengimplementasikan algoritma transposisi kolom yang telah dimodifikasi dalam sebuah bot telegram. Hasil penelitian menunjukkan bahwa dari beberapa pengujian terdapat hasil dekripsi yang tidak sama dengan pesan awal sebelum dienkripsi [11]. Penelitian yang dilakukan oleh Adnan Buyung Nasution melalui kombinasi algoritma caesar cipher dan transposisi cipher dalam mengamankan data berupa teks. Hasil penelitian ini menunjukkan bahwa kombinasi algoritma tersebut mampu membuat pesan menjadi sulit dikenali setelah melalui proses enkripsi. Namun, penelitian ini menggunakan jumlah karakter yang terbatas yaitu sebanyak 26 karakter saja (A-Z) [12].

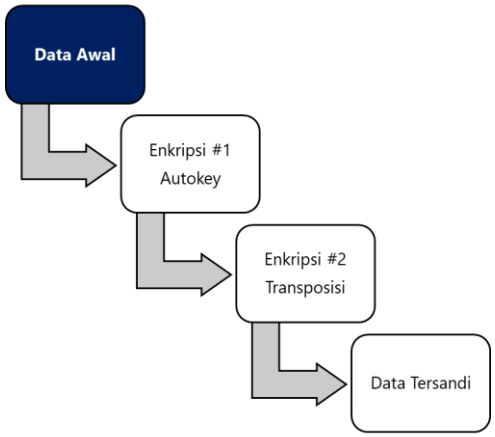
Oleh karena itu, penelitian ini mengusulkan sebuah model super enkripsi dalam mengamankan data melalui perpaduan algoritma kriptografi teknik substitusi dan transposisi. Terdapat dua algoritma yang digunakan dalam penelitian ini, yaitu autokey cipher dan transposisi kolom. Autokey cipher merupakan salah satu algoritma yang menerapkan teknik substitusi dan memiliki tingkat keamanan yang cukup baik dibanding dengan algoritma teknik substitusi lainnya, seperti caesar maupun viginere cipher [13]. Sedangkan, transposisi kolom merupakan algoritma kriptografi kunci simetris yang memiliki prinsip kerja dengan menggantikan posisi karakter yang akan disandikan tanpa mengganti atau merubah karakter tersebut [14]. Dalam penelitian ini, pendekatan Avalanche Effect digunakan sebagai alat ukur model super enkripsi yang diusulkan. Diharapkan model yang diusulkan melalui perpaduan antara autokey cipher dan transposisi kolom mampu memberikan tingkat keamanan data yang lebih baik dibandingkan algoritma kriptografi subtitusi maupun transposisi tunggal.

2. Metode Penelitian

Model yang diusulkan dalam penelitian ini dibagi menjadi dua bagian utama, yaitu model enkripsi dan dekripsi melalui perpaduan algoritma kriptografi substitusi dan transposisi.

2.1. Model Usulan Proses Enkripsi

Model enkripsi yang diusulkan dapat dilihat pada Gambar 1.



Gambar 1. Tahapan Usulan Proses Enkripsi

Pada Gambar 1 proses mengubah data awal menjadi data tersandi dilakukan melalui dua lapis proses enkripsi, yaitu enkripsi autokey cipher dan transposisi kolom. Terdapat beberapa komponen utama yang diperlukan dalam model enkripsi ini, yakni data awal dan kunci yang akan digunakan pada setiap lapisan proses enkripsi.

Tahapan enkripsi pertama adalah autokey cipher. Pada proses autokey cipher ini data awal akan dienkripsi menggunakan algoritma autokey cipher. Persamaan 1 menunjukkan proses enkripsi lapisan ini [13].

$$C(i) = (p(i) + k(i)) \bmod m \quad (1)$$

Dengan ketentuan, c(i) merupakan hasil proses enkripsi, p(i) merupakan indeks dari karakter yang dienkripsi, k(i)

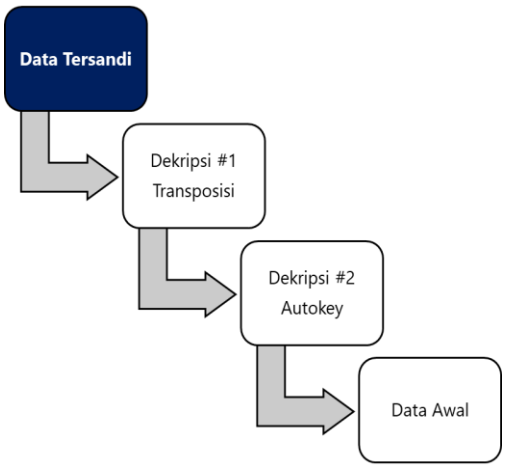
DOI: https://doi.org/10.29207/resti.v5i6.3566

merupakan indeks dari kunci dan "m" merupakan jumlah keseluruhan karakter yang digunakan. Dalam algoritma autokey, jika kunci memiliki panjang yang kurang dari data awal maka kunci tersebut akan digabungkan dengan data awal itu sendiri.

Tahapan berikutnya adalah transposisi kolom. Ini merupakan tahapan terakhir dalam proses enkripsi yang diusulkan. Dalam lapisan ini, hasil enkripsi dari lapisan pertama akan dienkripsi kembali dengan transposisi kolom. Dalam transposisi kolom, total kolom memiliki yang peran penting, dikarenakan dalam algoritma tersebut setiap karakter akan dibagi dengan total kolom. Total kolom ini ditentukan dari banyaknya karakter pada kunci yang digunakan. Transposisi kolom memiliki prinsip kerja dengan menggantikan posisi karakter yang akan disandikan tanpa mengganti atau merubah karakter tersebut. Algoritma ini menggunakan kunci simetris, artinya penggunaan kunci digunakan untuk proses enkripsi maupun dekripsi.

2.2. Model Usulan Proses Dekripsi

Model dekripsi merupakan kebalikan dari model proses enkripsi. Model ini bertujuan untuk mengembalikan data tersandi menjadi bentuk semula. Model dekripsi yang diusulkan dapat dilihat pada Gambar 2.



Gambar 2. Tahapan Usulan Proses Dekripsi

Proses dekripsi yang diusulkan akan melalui dua tahapan proses dekripsi, antara lain dekripsi transposisi kolom dan dekripsi autokey cipher.

Berdasarkan Gambar 2, model dekripsi yang diusulkan menempatkan transposisi kolom menjadi tahapan pertama. Pada tahapan ini, cipherteks akan di dekripsi menggunalan algoritma transposisi kolom. Proses yang dilalui dalam lapisan ini sama seperti proses yang terdapat pada tahapan enkripsi transposisi kolom.

Tahapan kedua adalah dekripsi menggunakan algoritma autokey cipher. Pada tahapan dekripsi ini, hasil dekripsi tahapan pertama akan didekripsi kembali menggunakan autokey cipher. Proses dekripsi dilakukan dengan mengacu pada Persamaan 2 yang merupakan kebalikan dari proses yang terdapat pada Persamaan 1.

$$p(i) = (C(i) - k(i)) \bmod m \quad (2)$$

Dengan ketentuan simbol-simbol yang digunakan pada Persamaan 2 sama dengan simbol yang terdapat dalam Persamaan 1.

2.3. Pengujian Model Kriptografi

Dalam melakukan pengujian terhadap model kriptografi yang diusulkan, maka dibutuhkan sebuah alat ukur yang dapat memberikan informasi terkait kualitas dari sebuah model kriptografi. Penelitian ini menggunakan Avalanche Effect sebagai alat ukur untuk mengevaluasi model super enkripsi yang diusulkan. Pengukuran dalam avalanche effect dilakukan dengan melihat setiap perubahan bit yang terjadi dalam data tersandi yang diakibatkan oleh perubahan yang dilakukan terhadap data awal maupun kunci, dalam avalanche effect semakin banyak perubahan bit maka semakin baik model tersebut [15]–[17]. Proses yang terdapat dalam avalanche effect dapat dilihat pada Persamaan (3).

$$AE = Dx/total \ x \ 100\% \quad (3)$$

Dengan ketentuan, Dx merupakan jumlah bit yang berbeda, AE merupakan nilai Avalanche Effect dan total merupakan total keseluruhan bit dalam data tersandi.

3. Hasil dan Pembahasan

Proses pengujian model kriptografi yang diusulkan dilakukan terhadap sebuah data awal *"Jurnal RESTI Desember 2021"*, kunci untuk transposisi kolom adalah "SINTA" dan kunci yang digunakan dalam autokey cipher adalah *"plagiarisme"*.

3.1. Proses Enkripsi

Sesuai dengan tahapan model enkripsi yang diusulkan pada Gambar 1, tahapan pertama yang dilakukan terhadap data awal adalah enkripsi menggunakan autokey cipher dengan kunci "plagiarisme". Dalam algoritma ini setiap karakter data awal akan memiliki pasangan kuncinya masing-masing, dengan ketentuan jika panjang kunci lebih pendek dibandingkan data awal maka beberapa karakter data awal dimulai dari karakter pertama akan diambil sebagai kunci. Dalam hal ini kunci yang awalnya "plagiarisme" diperpanjang hingga memiliki jumlah karakter yang sama dengan data awal menjadi *"plagiarismeJurnal RESTI"*. Setelah jumlah karakter kunci sama dengan karakter data awal, maka dilakukan proses perhitungan menggunakan Persamaan 1.

Dalam penelitian ini jumlah karakter yang digunakan adalah sebanyak 93 karakter. Sebagai contoh karakter data awal "J" sebelum dilakukan proses enkripsi akan dilakukan konversi terlebih dahulu ke dalam bentuk indeks karakter. Dalam hal ini karakter "J" tersebut memiliki indeks karakter 9. Karakter "J" tersebut akan

DOI: https://doi.org/10.29207/resti.v5i6.3566

dienkripsi menggunakan pasangan kuncinya, yaitu karakter "p" yang memiliki indeks karakter 41. Berikut contoh enkripsi karakter "J" tersebut dengan menggunakan Persamaan 1,

$C(i) = (p(i) + k(i)) \bmod m = (9 + 41) \bmod 93 = 50 \bmod 93 = 50 = y$

Berdasarkan proses perhitungan tersebut dapat terlihat bahwa karakter data awal "J" setelah melalui proses enkripsi mendapatkan hasil nilai indeks 50. Nilai ini kemudian dikonversi kembali sehingga menjadi karakter "y". Berikutnya adalah karakter data awal "u" yang memiliki indeks 46 dan karakter kunci "l" dengan indeks 37. Perhitungan dilakukan menggunakan Persamaan 1, sehingga didapatkan hasil

$C(i) = (p(i) + k(i)) \bmod m = (46 + 37) \bmod 93 = 83 \bmod 93 = 83 = \backslash$

Berdasarkan proses perhitungan terlihat bahwa karakter data awal "u" setelah melalui proses enkripsi berubah menjadi karakter "\". Proses seperti ini dilakukan secara berulang terhadap semua karakter data awal. Secara ringkas hasil proses enkripsi tahap pertama tersebut dapat dilihat di Tabel 1.

Tabel 1. Hasil Enkripsi Tahap 1

Data awal	Kunci	Cipherteks
J	p	y
u	l	\
r	a	&
n	g	(
a	i	8
l	a	!
spasi	r	Y
R	i	z
E	s	w
S	m	4
T	e	x
I	J	R
spasi	u	b
D	r	u
e	n	&
s	a	*
e	l	%
m	*spasi*	T
b	R	s
e	E	i
r	S	9
spasi	T	A
2	I	~
0	*spasi*	h
2	D	5
1	e	\

Berdasarkan Tabel 1 dapat dilihat bahwa dari data awal *Jurnal RESTI Desember 2021* setelah melalui proses enkripsi tahap pertama menjadi cipherteks *y\&(8!Yzw4 xRbu&*%Tsi9A~h5*. Selanjutnya, dilakukan enkripsi tahap kedua menggunakan transposisi kolom. Ilustrasi tahapan proses enkripsi tahap kedua ini dapat dilihat pada Tabel 2.

Tabel 2. Proses Enkripsi Tahap 2

S	**I**	**N**	**T**	**A**
4	2	3	5	1
y	\	&	(	8
i	Y	z	w	4
x	R	b	u	&
*	%	T	s	i
9	A	~	h	5
\				

Dalam Tabel 2 langkah pertama proses enkripsi transposisi kolom adalah menuliskan kunci yang digunakan ke dalam baris pertama Tabel 2 tersebut. Berikutnya, baris kedua dari Tabel 2 merupakan nomor urut dari karakter kunci yang dimulai dari karakter yang pertama kali muncul dalam susunan abjad. Sehingga, dari karakter kunci "SINTA" memiliki susunan abjad secara berurutan "42351". Selanjutnya, seluruh karakter hasil enkripsi tahap pertama dimasukkan ke dalam masing-masing sel pada Tabel 2 tersebut.

Langkah terakhir untuk mendapatkan hasil enkripsi tahap kedua adalah mengambil karakter dalam setiap kolom dimulai dari kolom yang memiliki indeks terkecil atau angka pada baris kedua terkecil, sehingga didapatkan hasil akhir enkripsi tahap kedua adalah *84&i5 \YR%A &zbT~ y!x*9\(wush.* Hasil tersebut menunjukkan bahwa karakter enkripsi tahap pertama mengalami perbedaan dengan karakter enkripsi tahap kedua. Karakter enkripsi tahap kedua inilah yang menjadi data tersandi akhir dalam pendekatan proses enkripsi yang diusulkan.

3.2. Proses Dekripsi

Dalam penelitian ini proses dekripsi yang dilalui merupakan kebalikan dari proses enkripsi. Berdasarkan Gambar 2 terlihat bahwa proses dekripsi dimulai dari dekripsi transposisi kolom, kemudian dilanjutkan dengan dekripsi autokey cipher. Sebagai contoh, karakter tersandi yang dimiliki adalah *84&i5 \YR%A &zbT~ y!x*9\(wush.*

Tahap pertama adalah melakukan proses dekripsi dengan transposisi kolom, hal pertama yang harus dilakukan adalah dengan membagi jumlah karakter data tersandi sebanyak 26 karakter dengan jumlah karakter kunci 5 karakter. Proses ini dilakukan untuk mengetahui jumlah baris dari setiap kolom dalam melakukan proses dekripsi.

Berdasarkan hasil pembagian tersebut didapatkan nilai akhir adalah 5 dengan sisa hasil bagi 1 karakter. Dapat disimpulkan bahwa dari 5 kolom yang ada sesuai dengan karakter kunci "SINTA" maka tiap kolom tersebut akan berisi 5 baris karakter data tersandi, kecuali untuk kolom pertama yang akan memiliki 6 baris karakter cipherteks (1 baris karakter didapat dari sisa hasil bagi 1 karakter sebelumnya). Proses dekripsi tersebut dapat dilihat pada Tabel 3.

DOI: https://doi.org/10.29207/resti.v5i6.3566

Tabel 3. Proses Dekripsi Tahap 1 Pengisian Kolom Pertama

S	I	N	T	A
4	2	3	5	1
				8
				4
				&
				i
				5

Pada Tabel 3 terlihat proses pengisian 5 karakter data tersandi pertama dalam kolom yang memiliki indeks terkecil, yaitu kolom A. Proses pengisian ke dalam tiap sel dari tabel tersebut terus dilakukan sesuai dengan urutan indeks yang ada, sehingga didapatkan hasil akhir seperti dalam Tabel 4.

Tabel 4. Proses Dekripsi Tahap 1 Akhir

S	I	N	T	A
4	2	3	5	1
y	\	&	(	8
i	Y	z	w	4
x	R	b	u	&
*	%	T	s	i
9	A	~	h	5
\				

Dalam Tabel 4 terlihat bahwa seluruh karakter data tersandi telah masuk ke dalam selnya masing-masing. Langkah berikutnya adalah mengambil tiap karakter dalam tiap sel tersebut secara berurutan dimulai dari karakter yang terdapat dalam sel pertama kolom pertama, dalam hal ini adalah karakter "y". Proses ini terus dilakukan hingga didapatkan hasil akhir proses dekripsi berupa susunan karakter *y\&(8!Yzw4 xRbu &*%Tsi9A~h5*. Hasil ini merupakan hasil akhir dari proses dekripsi tahap pertama dengan transposisi kolom.

Selanjutnya, dilakukan proses dekripsi terhadap hasil dekripsi tahap pertama dengan autokey cipher. Proses dekripsi pada tahapan ini dilakukan berdasarkan Persamaan 2. Berikut contoh proses dekripsi karakter hasil dekripsi tahap pertama yaitu karakter "y" dengan menggunakan Persamaan 2,

$$p(i) = (C(i) - k(i)) \bmod m = (50 - 41) \bmod 93 = 9 \bmod 93 = 9 = J$$

Berdasarkan proses perhitungan tersebut dapat terlihat bahwa karakter "y" setelah melalui proses dekripsi mendapatkan hasil nilai indeks 9. Nilai ini kemudian dikonversi kembali menjadi karakter "J". Proses dekripsi seperti ini terus dilakukan berulang terhadap seluruh karakter hasil dekripsi tahap pertama, sehingga didapatkan nilai akhir proses dekripsi berupa karakter data awal *"Jurnal RESTI Desember 2021"*.

Beberapa uji coba lain terhadap implementasi dari model yang diusulkan dapat dilihat dalam Tabel 5.

Tabel 5. Hasil Uji Coba

Data awal	Hasil Enkripsi	Hasil Dekripsi	Ket
Jurnal RESTI Desember 2021	*84&i5 \YR%A &zbT~ y!x*9\(wush*	Jurnal RESTI Desember 2021	√
Bersama kita cegah Covid-19	8)_mI %&b@/A&PL78 q@+6_\={(3K	Bersama kita cegah Covid-19	√
Awas ada Bom di pagar istana	Pn[H_ :)m%VU08d3)%p0* 3s8=Z36Z	Awas ada Bom di pagar istana	√
Isu keamanan data menjadi salah satu isu pokok di era digital	u+#4@8(?"VK3 !*##9]Z3WWY+ 6;T3H0*[_&38 am4(;UO]bR$@(\|H 3%%$!*{*Pa	Isu keamanan data menjadi salah satu isu pokok di era digital	√
Tetap patuhi protokol kesehatan, jangan lupa bermasker dan mencuci tangan	%[\-]\!1ZK4P* !Y3*(37j+=&@([(+ ~L:(#H@;Y=# 48+O-f~:&- 1\K4[,::~4aQ#H=(U	Tetap patuhi protokol kesehatan, jangan lupa bermasker dan mencuci tangan	√

Pada Tabel 5 uji coba yang dilakukan menunjukkan model yang diusulkan memiliki tingkat akurasi yang tinggi dari sisi proses dekripsi yang mampu mengembalikan data tersandi menjadi bentuk data semula. Hal ini dibuktikan dengan 5 dari 5 data uji coba berhasil didekripsi ke dalam bentuk data awal sebelum dienkripsi.

3.3. Pengujian Model

Pengujian model kriptografi yang diusulkan menggunakan Avalanche Effect (AE) seperti yang terdapat dalam Persamaan 3. Pengujian dilakukan dengan memanfaatkan perubahan pada kunci yang digunakan untuk proses enkripsi. Terdapat beberapa alternatif yang bisa digunakan terhadap perubahan kunci tersebut, salah satunya adalah dengan mengubah karakter yang berada ditengah dari keseluruhan karakter kunci. Sebagai contoh, jika kunci yang dimiliki adalah karakter "SINTA", maka dapat dilakukan perubahan menjadi karakter "SIZTA". Beberapa contoh hasil pengujian tersebut dapat dilihat pada Tabel 6.

Tabel 6. Hasil Pengujian

Kasus	Jumlah Bit	Selisih Bit
Kasus 1	208	57
Kasus 2	216	67
Kasus 3	224	56
Kasus 4	488	124
Kasus 5	536	241

Pada Tabel 6 terdapat lima buah kasus data awal dengan jumlah bit yang beragam. Jumlah bit ini didapat berdasarkan karakter data tersandi yang digunakan dalam tiap-tiap kasus tersebut. Dalam penelitian ini tidak ada batasan jumlah karakter yang digunakan pada saat proses enkripsi maupun dekripsi. Berdasarkan Tabel 6, dari beberapa kasus yang ada ketika dilakukan

DOI: https://doi.org/10.29207/resti.v5i6.3566

perubahan terhadap satu karakter kunci yang digunakan maka dapat menimbulkan perubahan atau selisih pada bit dari data tersandi tersebut.

Dalam pendekatan avalanche effect, semakin besar nilai yang dihasilkan dari proses perhitungan maka semakin baik kualitas model tersebut [15]. Sebagai contoh, Kasus 4 dalam Tabel 6 dengan jumlah bit data tersandi sebesar 488 bit. Setelah dilakukan perubahan satu karakter dari kunci maka menimbulkan selisih bit sebesar 124 bit. Berikutnya, dilakukan proses perhitungan nilai AE menggunakan Persamaan 3, sehingga didapatkan hasil nilai AE untuk kasus tersebut sekitar 25.41%.

Selanjutnya, dilakukan proses perbandingan antara nilai AE dari model yang diusulkan dengan nilai AE dari algoritma kriptografi tunggal autokey cipher maupun transposisi kolom. Hasil perbandingan tersebut dapat dilihat dalam Tabel 7.

Tabel 7. Perbandingan Nilai Avalanche Effect

Kasus	Nilai Avalanche Effect		
	Autokey	Transposisi	Usulan
Kasus 1	2.40%	20.19%	27.40%
Kasus 2	2.31%	21.88%	31.02%
Kasus 3	1.79%	13.39%	25.00%
Kasus 4	1.23%	16.39%	25.41%
Kasus 5	0.56%	18.28%	44.96%
Rata-rata	1.66%	18.03%	30.76%

Pada Tabel 7 terdapat lima buah kasus uji coba yang dienkripsi menggunakan kriptografi tunggal autokey cipher, kriptografi tunggal transposisi kolom, dan model super enkripsi yang diusulkan. Lima data uji coba tersebut diproses menggunakan kunci yang sama, baik pada kriptografi tunggal maupun model super enkripsi yang diusulkan.

Berdasarkan Tabel 7 terlihat bahwa dari lima data uji coba, model super enkripsi yang diusulkan melalui perpaduan autokey cipher dan transposisi kolom memiliki nilai rata-rata AE sebesar 30.76%. Nilai ini lebih tinggi dibandingkan dengan algoritma kriptografi tunggal lainnya yang terdapat dalam Tabel 7. Sebagai contoh pada Kasus 2, kriptografi tunggal autokey cipher hanya memiliki nilai sebesar 2.31% dan transposisi kolom dengan nilai sebesar 21.88%. Pada kasus yang sama model super enkripsi yang diusulkan memiliki nilai lebih tinggi sebesar 31.02%, sehingga dapat disimpulkan bahwa mengacu pada hasil perhitungan dan perbandingan nilai AE, model yang diusulkan mampu menghasilkan tingkat keamanan data yang lebih baik dari algoritma kriptografi tunggal autokey cipher maupun transposisi kolom.

4. Kesimpulan

Penelitian ini menunjukkan bahwa model super enkripsi yang diusulkan melalui perpaduan algoritma autokey cipher dan transposisi kolom mampu memberikan tingkat keamanan yang lebih baik. Berdasarkan pengujian avalanche effect yang telah dilakukan menunjukkan model super enkripsi yang diusulkan memiliki rata-rata nilai AE sebesar 30.76%. Nilai ini lebih tinggi dibandingkan dengan algoritma kriptografi tunggal autokey cipher sebesar 1.66% dan transposisi kolom sebesar 18.03%. Model yang diusulkan juga menunjukkan tingkat akurasi yang sangat baik dari sisi hasil proses dekripsi data tersandi yang sama seperti data awal. Dari lima data uji coba yang telah dilakukan memiliki tingkat akurasi sebesar 100%. Hal ini menunjukkan bahwa keseluruhan data uji coba tersebut setelah melalui proses dekripsi yang diusulkan dalam penelitian ini mampu kembali ke dalam bentuk data awal sebelum dienkripsi.

Ucapan Terimakasih

Artikel ini merupakan salah satu luaran dari pelaksanaan penelitian yang didanai oleh Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi Republik Indonesia melalui hibah kompetitif nasional penelitian dosen pemula Tahun 2021 berdasarkan Surat Keputusan Nomor 1867/E4/AK.04/2021 dan Kontrak Nomor 30/LL11/KM/2021.

Daftar Rujukan

[1] N. Matondang, I. N. Isnainiyah, and A. Muliawatic, "Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ)," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 2, no. 1, pp. 282–287, 2018, doi: 10.29207/resti.v2i1.96.

[2] P. R. Kumar, P. H. Raj, and P. Jelciana, "Exploring Data Security Issues and Solutions in Cloud Computing," *Procedia Comput. Sci.*, vol. 125, no. 2009, pp. 691–697, 2018, doi: 10.1016/j.procs.2017.12.089.

[3] R. Ravida and H. A. Santoso, "Advanced Encryption Standard (AES) 128 Bit for Hydroponic Plant Internet of Things (IoT) Data Security," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 6, pp. 1157–1164, 2020, doi: 10.29207/resti.v4i6.2478.

[4] F. Triana, J. Endri, and I. Salamah, "Implementasi Teknik Kriptografi CAESAR CIPHER Untuk Keamanan Data Informasi Berbasis Android," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 4, pp. 627–634, 2020, doi: 10.29207/resti.v4i4.1984.

[5] M. K. Harahap, "Analisis Perbandingan Algoritma Kriptografi Klasik Vigenere Cipher Dan One Time Pad," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 1, no. 1, pp. 61–64, 2016, doi: 10.30743/infotekjar.v1i1.43.

[6] P. Poonia and P. Kantha, "Comparative Study of Various Substitution and Transposition Encryption Techniques," *Int. J. Comput. Appl.*, vol. 145, no. 10, pp. 24–27, 2016, doi: 10.5120/ijca2016910783.

[7] D. Abdullah *et al.*, "Super-Encryption Cryptography with IDEA and WAKE Algorithm," *J. Phys. Conf. Ser.*, vol. 1019, no. 1, 2018, doi: 10.1088/1742-6596/1019/1/012039.

[8] M. A. Budiman, Amalia, and N. I. Chayanie, "An Implementation of RC4+ Algorithm and Zig-zag Algorithm in a Super Encryption Scheme for Text Security," *J. Phys. Conf. Ser.*, vol. 978, no. 1, 2018, doi: 10.1088/1742-6596/978/1/012086.

[9] A. Djamalilleil, M. Muslim, Y. Salim, E. I. Alwi, H. Azis, and Herman, "Modified Transposition Cipher Algorithm for Images Encryption," in *Proceedings - 2nd East Indonesia Conference on Computer and Information Technology: Internet of Things for Industry, EIConCIT 2018*, 2018, pp. 1–4, doi: 10.1109/EIConCIT.2018.8878326.

DOI: https://doi.org/10.29207/resti.v5i6.3566

[10] M. A. Maricar and N. P. Sastra, "Efektivitas Pesan Teks Dengan Cipher Substitusi, Vigenere Cipher, dan Cipher Transposisi," *Maj. Ilm. Teknol. Elektro*, vol. 17, no. 1, p. 59, 2018, doi: 10.24843/mite.2018.v17i01.p08.

[11] R. Septiana, A. F. Hastawan, R. C. Aryani, and V. Marsha, "Implementasi Algoritma Modifikasi Transposisi Columnar Pada Bot Telegram," *Edu Komputika J.*, vol. 7, no. 2, pp. 84–93, 2020, doi: 10.15294/edukomputika.v7i2.42479.

[12] A. B. Nasution, "Implementasi Pengamanan Data Dengan Menggunakan Algoritma Caesar Cipher Dan Transposisi Cipher," *J. Teknol. Inf.*, vol. 3, no. 1, p. 1, 2019, doi: 10.36294/jurti.v3i1.680.

[13] O. Grošek, E. Antal, and T. Fabšič, "Remarks on breaking the Vigenère autokey cipher," *Cryptologia*, vol. 43, no. 6, pp. 486–496, 2019, doi: 10.1080/01611194.2019.1596997.

[14] G. Lasry, N. Kopal, and A. Wacker, "Cryptanalysis of columnar transposition cipher with long keys," *Cryptologia*, vol. 40, no. 4, pp. 374–398, 2016, doi: 10.1080/01611194.2015.1087074.

[15] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish," *Procedia Comput. Sci.*, vol. 78, no. December 2015, pp. 617–624, 2016, doi: 10.1016/j.procs.2016.02.108.

[16] H. N. Noor Muchsin, D. E. Sari, D. R. Ignatius Moses Setiadi, and E. H. Rachmawanto, "Text Encryption using Extended Bit Circular Shift Cipher," in *Proceedings of 2019 4th International Conference on Informatics and Computing, ICIC 2019*, 2019, pp. 0–4, doi: 10.1109/ICIC47613.2019.8985708.

[17] K. D. Muthavhine and M. Sumbwanyambe, "An analysis and a comparative study of cryptographic algorithms used on the Internet of Things (IoT) based on avalanche effect," *2018 Int. Conf. Inf. Commun. Technol. ICOIACT 2018*, vol. 2018-Janua, pp. 114–119, 2018, doi: 10.1109/ICOIACT.2018.8350759.

DOI: https://doi.org/10.29207/resti.v5i6.3566