MATHEMATICAL SCIENCES AND APPLICATIONS JOURNAL

Volume 4, Number 2 | ISSN: 2986-4180

https://online-journal.unja.ac.id/msa

Article

Pengamanan Nama *Customer* Shopee melalui Kombinasi Algoritma *Hill Cipher* Modifikasi dan *Rail Fence Cipher*

Laily Wadil Muqadas, Sisilia Sylviani*, Edi Kurniadi

Departemen Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Padjadjaran, Sumedang 45363, Indonesia

*Corresponding author e-mail: sisilia.sylviani@unpad.ac.id

Article Info
Received October 2023
Accepted October 2023
Published April 2024

Keyword:
Shopee
Modified Hill Cipher
Rail Fence Cipher

Abstract

Science and technology development has made human activities turn into cyberspace activities, one of which is buying and selling. Shopee is one of the e-commerce platforms available. As an online-based platform, Shopee certainly stores lots of user data. Since August 1st, 2022, Shopee has made a policy regarding user data security by censoring the buyer's name and phone number in the ordering process. This research discusses one way to secure buyer data through cryptography with the concept of super encryption. This concept itself combines more than one encryption method with the goal to create ciphertext that is difficult to solve. The chosen combination for this research is the modified Hill Cipher algorithm before proceeding with the Rail Fence Cipher encryption. Result obtained in this research is possible to be applied in Shopee buyer data security system, seen from the difficulty level of the ciphertext decryption.

1. Pendahuluan

Seiring dengan berkembangnya IPTEK, keberjalanan aktivitas manusia dengan cara konvensional yaitu bertemu secara langsung beralih menjadi kegiatan dunia maya. Aktivitas tersebut mulai dari komunikasi, kegiatan pembelajaran (pendidikan), hingga proses jual beli barang kebutuhan. Menurut [1], jual beli merupakan suatu kegiatan menjual dan membeli di mana satu pihak menyerahkan barang dan pihak lain membayar sejumlah harga barang yang dijual.

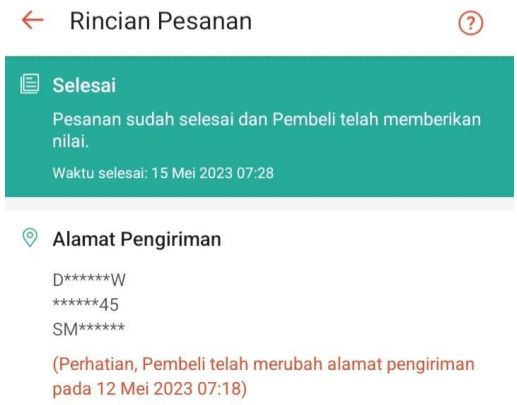
Salah satu *platform* jual beli berbasis *online* yang sering kali digunakan adalah Shopee. Shopee didirikan pada tahun 2009 oleh seseorang bernama Forrest Li [2]. Saat ini Shopee sudah dapat diakses di berbagai negara Asia, Eropa, dan Amerika (seperti yang dapat dilihat pada Gambar 1), diantaranya Singapura, Indonesia, Taiwan, Polandia, dan Brasil. Sebagai *platform* jual beli berbasis *online*, Shopee menyimpan data pribadi pengguna dengan jumlah yang tidak sedikit, baik itu data penjual (*seller*) maupun data pembeli (*customer*). Sayangnya, data pribadi tersebut sering kali disalahgunakan oleh pihak yang tidak berkepentingan, misalnya kebocoran data pengguna Shopee Taiwan [3].

Gambar 1. Peta persebaran wilayah negara yang dapat mengakses Shopee

Dilansir dari CNN Indonesia, informasi data pribadi pembeli yang berupa nama dan nomor telepon disembunyikan atau disensor dalam seluruh tahap proses pemenuhan pesanan sejak tanggal 01 Agustus 2022 [4]. Latar belakang dari adanya kebijakan ini ialah untuk menjaga privasi dan memastikan keamanan data pengguna [5]. Sensor dilakukan dengan mengganti seluruh karakter nama dan nomor telepon menggunakan tanda bintang (*) kecuali pada karakter pertama dan terakhirnya seperti yang dapat dilihat pada Gambar 2. Hal

https://doi.org/10.22437/msa.v4i2.28865

ini memicu berbagai pro dan kontra dari pihak penjual maupun pembeli. Beberapa penjual merasa dirugikan karena tidak dapat melihat informasi nama dan nomor telepon pembeli guna mengirimkan barang pesanan mereka. Kebalikannya, beberapa pembeli merasa diuntungkan karena data mereka aman terjaga dari pihak-pihak yang tidak berkepentingan. Sebelum adanya kebijakan ini, tak jarang pembeli harus menggunting kemasan barang belanjaannya menjadi bagian-bagian kecil agar informasi pribadi mereka tidak tersebar ketika kemasan barang tersebut dibuang. Dari permasalahan ini, peneliti termotivasi untuk membuat opsi lain dalam mengamankan data pribadi *customer* berupa nama menjadi suatu teks rahasia melalui kriptografi dibandingkan hanya dengan mengubahnya menjadi tanda bintang.



Gambar 2. Sensor data pembeli dalam proses pesanan

Kriptografi merupakan sebuah ilmu mengenai teknik enkripsi di mana naskah asli (*plaintext*) diacak menggunakan suatu kunci enkripsi menjadi naskah acak yang sulit dibaca (*ciphertext*) oleh seseorang yang tidak memiliki kunci dekripsi [6]. Penelitian mengenai kriptografi sudah banyak dilakukan, diantaranya penerapan *Hill Cipher* menggunakan kode ASCII dalam mengamankan *file* teks [7] dan implementasi *Hill Cipher* dalam penyandian data [8]. Selain itu, ada pula algoritma *Rail Fence Cipher* yang diterapkan pada data rekam medis [9] dan pengamanan basis data [10]. Aplikasi kriptografi dengan melakukan kombinasi dua algoritma juga sudah banyak dilakukan, misalnya algoritma *Hill Cipher* dan *Caesar Cipher* [11], *Playfair Cipher* dan zig-zag [12], serta *Vigenere Cipher* dan zig-zag [13].

Secara garis besar, kriptografi klasik terdiri atas dua teknik utama [14]. Pertama, teknik yang mengganti karakter *plaintext* menjadi karakter lain, yaitu teknik substitusi. Kedua, teknik yang mengubah urutan setiap karakter *plaintext*, yaitu teknik transposisi. Adapun salah satu contoh kriptografi dengan teknik substitusi bernama algoritma *Hill Cipher*. Algoritma ini dikemukakan oleh seorang matematikawan bernama Lester Hill pada tahun 1929 [15]. Meskipun tergolong ke dalam kriptografi klasik, algoritma *Hill Cipher* cukup sulit untuk dipecahkan karena pada karakter *plaintext* yang sama dapat digantikan oleh karakter *ciphertext* yang berbeda.

Algortima *Hill Cipher* yang akan digunakan dalam penelitian ini adalah *Hill Cipher* yang sudah dimodifikasi. Modifikasi dilakukan dengan mengganti tabel ekuivalensi alfabet A–Z menjadi kode ANSI ASCII 33–126 seperti yang dilakukan dalam penelitian sebelumnya [16]. Hal ini dikarenakan nama *customer* Shopee dapat berupa huruf, simbol, ataupun angka.

ASCII sendiri merupakan karakter yang digunakan dalam standar pengkodean. ASCII terdiri dari 255 kode yang terbagi menjadi dua fungsi. ASCII bernilai ANSI 0–127 berfungsi sebagai pengubah teks, sementara ASCII bernilai ANSI 128–255 berfungsi sebagai pengubah grafik [17]. Tak jarang Kode ASCII diterapkan dalam permasalahan sehari-sehari, contohnya penerapan pada sistem keamanan *e-voting* [18].

Selanjutnya terdapat pula algoritma *Rail Fence Cipher* yang merupakan salah satu contoh kriptografi dengan teknik transposisi. Algoritma ini dilakukan dengan cara memasukkan tiap karakter *plaintext* ke dalam sebuah tabel dengan pola zig-zag [19]. Ukuran tabel disesuaikan dengan jumlah karakter *plaintext* dan kunci yang digunakan. Penentuan kunci optimal dilakukan dengan cara menghitung nilai fungsi *floor* dari akar kuadrat jumlah karakter *plaintext* [20].

Kriptografi dalam penelitian ini menggunakan kombinasi algoritma *Hill Cipher* modifikasi dan *Rail Fence Cipher*. Gabungan kedua algoritma ini dilakukan agar tercipta konsep super enkripsi yang dapat mempersulit kriptanalis untuk memecahkan hasil enkripsi [21]. Harapannya, hasil yang diberikan dapat membantu Shopee mengamankan data pribadi *customer* dalam seluruh tahap proses pemenuhan pesanan.

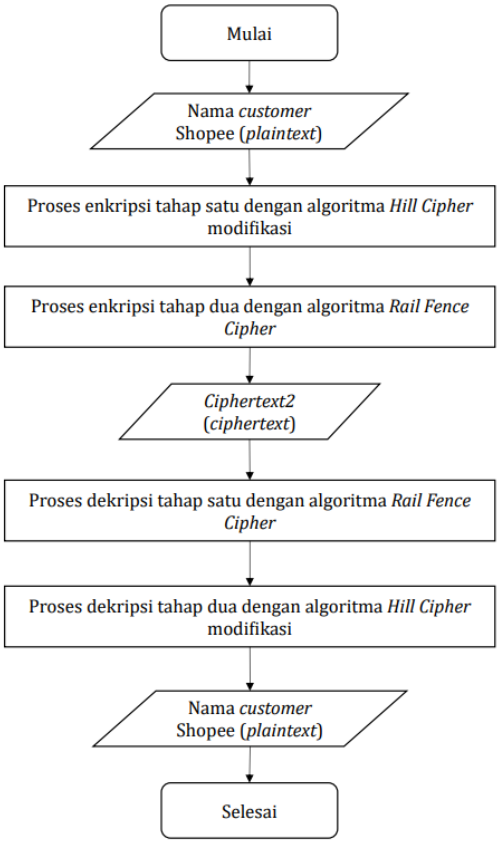
2. Metode Penelitian

Penelitian ini menggunakan pendekatan studi literatur dan eksperimental dengan tujuan utama untuk meningkatkan keamanan data pelanggan (*customer*) Shopee dengan menggabungkan dua algoritma enkripsi, yaitu *Hill Cipher* modifikasi dan *Rail Fence Cipher*. Desain eksperimen ini akan memungkinkan kami untuk mengevaluasi keefektifan kombinasi algoritma tersebut dalam melindungi informasi nama *customer* Shopee.

Data yang digunakan dalam penelitian ini adalah nama *customer* Shopee yang telah diambil secara anonim. Data ini mencakup beragam jenis nama untuk menggambarkan keragaman karakter dalam data. Sampel data dibatasi untuk menghindari pelanggaran privasi *customer*.

Pada tahap implementasi, kami menggunakan kombinasi algoritma *Hill Cipher* modifikasi dan *Rail Fence Cipher* untuk mengenkripsi nama *customer*. *Hill Cipher* modifikasi digunakan untuk mengacak karakter nama *customer*, sedangkan *Rail Fence Cipher* digunakan untuk mengacak susunan karakter yang dihasilkan oleh *Hill Cipher* modifikasi. Proses ini akan menciptakan lapisan ganda enkripsi dan meningkatkan tingkat keamanan.

Terdapat langkah-langkah yang digunakan, yaitu melakukan proses enkripsi dua tahap terhadap nama *customer* Shopee dan melakukan proses dekripsi dua tahap pula untuk mengubah *ciphertext* Shopee seperti semula. Berikut diagram alir dan rincian langkah-langkahnya.



Gambar 3. Diagram alir penelitian

2.1. Enkripsi

Enkripsi dilakukan melalui dua tahap. Tahap satu ialah enkripsi *Hill Cipher* modifikasi. Proses dilakukan dengan memilih matriks kunci $K_{n\times n}$ yang merupakan matriks modulo 94 dan memenuhi sifat $\gcd(\det(K_{n\times n}), 94) = 1$. Selanjutnya, memilih nama *customer* Shopee untuk dijadikan sebagai *plaintext* dan mengelompokkan setiap karakternya menjadi n pasang terurut. Jika jumlah karakter *plaintext* bukan merupakan kelipatan n maka perlu ditambahkan sejumlah karakter *dummy* hingga n habis membagi jumlah karakter *plaintext*. Kemudian, konversi setiap karakter sesuai tabel ASCII ekuivalensi. Karakter ekuivalensi yang digunakan dalam penelitian ini hanya mengambil sebagian kode ASCII, yaitu ANSI ASCII 33–126, yang disajikan oleh Tabel 1.

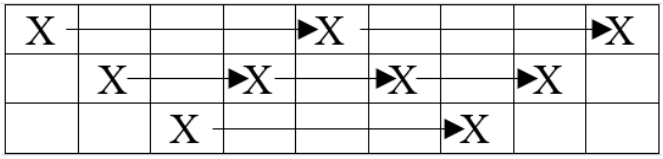
Kolom pertama pada Tabel 1 merupakan nilai desimal yang didefinisikan oleh [16]. Nilai desimal inilah yang digunakan untuk mengonversi *plaintext* maupun *ciphertext* dalam algoritma *Hill Cipher*. Setelah mengonversi semua karakter, ubah tiap n pasang *plaintext* secara berurutan menjadi vektor kolom $P = \begin{bmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{bmatrix}$ dan melakukan perkalian matriks $C = KP$. Terakhir, konversi hasil perkalian matriks tersebut sesuai karakter ekuivalensinya. Lebih jauh, hasil enkripsi tahap satu dalam penelitian ini disebut sebagai *ciphertext1*.

Berikutnya, tahap dua ialah enkripsi *Rail Fence Cipher*. Proses diawali dengan menghitung jumlah karakter *ciphertext1*. Kemudian memilih kunci dengan cara menentukan jumlah baris optimal. Selanjutnya, membuat tabel dengan jumlah baris sesuai kunci dan jumlah kolom sesuai jumlah karakter *ciphertext1*. Setelah itu, mengisi tabel dengan karakter *ciphertext1* berdasarkan pola zig-zag sesuai Gambar 4.

Hasil *ciphertext* diperoleh dengan membaca tabel secara horizontal mulai dari baris pertama sampai baris terakhir seperti yang diilustrasikan oleh Gambar 5. Dalam penelitian ini, hasil enkripsi tahap dua disebut sebagai *ciphertext2*.

X				X				X
	X		X		X		X	
		X				X		

Gambar 4. Pola zig-zag *rail fence cipher*



Gambar 5. Enkripsi *Rail Fence Cipher*

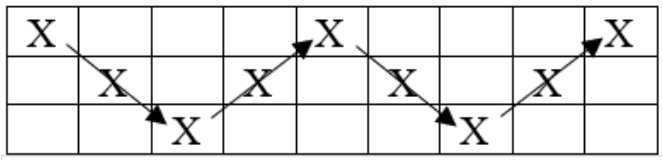
Tabel 1. Tabel ASCII ekuivalensi

Desimal	Karakter	Nilai ANSI ASCII
0	!	33
1	“	34
2	#	35
3	$	36
4	%	37
5	&	38
6	‘	39
7	(	40
8	)	41
9	*	42
10	+	43
11	,	44
12	-	45
13	.	46
14	/	47
15	0	48
16	1	49
17	2	50
18	3	51
19	4	52
20	5	53
21	6	54
22	7	55
23	8	56
24	9	57
25	:	58
26	;	59
27	<	60
28	=	61
29	>	62
30	?	63
31	@	64
32	A	65
33	B	66
34	C	67
35	D	68
36	E	69
37	F	70
38	G	71
39	H	72
40	I	73
41	J	74
42	K	75
43	L	76
44	M	77
45	N	78
46	O	79
47	P	80
48	Q	81
49	R	82
50	S	83
51	T	84
52	U	85
53	V	86
54	W	87

55	X	88
56	Y	89
57	Z	90
58	[	91
59	\	92
60	]	93
61	^	94
62	_	95
63	`	96
64	a	97
65	b	98
66	c	99
67	d	100
68	e	101
69	f	102
70	g	103
71	h	104
72	i	105
73	j	106
74	k	107
75	l	108
76	m	109
77	n	110
78	o	111
79	p	112
80	q	113
81	r	114
82	s	115
83	t	116
84	u	117
85	v	118
86	w	119
87	x	120
88	y	121
89	z	122
90	{	123
91	|	124
92	}	125
93	~	126

2.2. Dekripsi

Dekripsi dilakukan melalui dua tahap pula seperti enkripsi. Tahap satu ialah dekripsi *Rail Fence Cipher*. Dalam langkah ini digunakan cara yang sama dengan langkah enkripsi tahap dua untuk menentukan kunci serta jumlah baris dan kolom tabel. Dekripsi dilakukan dengan mengisi tabel oleh *ciphertext2* mulai dari baris pertama hingga baris terakhir sampai terbentuk pola zig-zag seperti pada Gambar 4. Selanjutnya, hasil dekripsi diperoleh dengan membaca tabel secara zig-zag seperti yang diilustrasikan oleh Gambar 6. Lebih jauh, hasil dekripsi tahap satu dalam penelitian ini disebut sebagai *ciphertext1*.



Gambar 6. Dekripsi *rail fence cipher*

Berikutnya, tahap dua ialah dekripsi *Hill Cipher* modifikasi. Proses diawali dengan mencari invers matriks kunci $K_{n\times n}$ terhadap modulo 94. Hasil dari invers matriks $K_{n\times n}$ dinotasikan oleh K^{-1}. Perhatikan bahwa invers matriks kunci $K_{n\times n}$ ada jika $\gcd(\det(K_{n\times n}), 94) = 1$.

Selanjutnya, mengelompokkan setiap karakter *ciphertext2* menjadi n pasang terurut dilanjutkan dengan mengonversinya sesuai tabel ASCII ekuivalensi. Setelah itu, ubah tiap pasang *ciphertext2* secara berurutan menjadi vektor kolom $C = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix}$ dan melakukan perkalian matriks $P = K^{-1}C$. Terakhir, konversi hasil perkalian matriks tersebut sesuai karakter ekuivalensinya. Nantinya *chipertext2* ini akan terdekripsi menjadi *plaintext* seperti semula, yaitu nama *customer* Shopee.

3. Hasil dan Diskusi

Pada bagian ini akan diuraikan proses enkripsi dan dekripsi dengan menggunakan kombinasi algoritma *Hill Cipher* modifikasi dan *Rail Fence Cipher*. Misalkan diberikan "Username1472" sebagai nama *customer* Shopee di mana nama tersebut mengandung abjad kapital, abjad kecil, dan angka yang menggambarkan keragaman karakter dalam data.

3.1. Enkripsi

Dalam proses ini, *plaintext* "Username1472" akan dienkripsi melalui dua tahap. Pertama, akan dilakukan enkripsi tahap satu, yaitu enkripsi *Hill Cipher* modifikasi. Pilih $K_{2\times2} = \begin{bmatrix} 2 & 1 \\ 5 & 4 \end{bmatrix}$ sebagai matriks kunci modulo 94. Perhatikan bahwa $\det(K) = 3$ dan $\gcd(3,94) = 1$. Oleh karena itu, matriks ini dapat dijadikan sebagai matriks kunci. Kelompokkan tiap karakter *plaintext* menjadi 2 pasang terurut dan konversikan sesuai tabel ASCII ekuivalensi.

- "U" dan "s" : 52 dan 82
- "e" dan "r" : 68 dan 81
- "n" dan "a" : 77 dan 64
- "m" dan "e" : 76 dan 68
- "1" dan "4" : 16 dan 19
- "7" dan "2" : 22 dan 17

Dari pengelompokkan di atas, akan diperoleh matriks kolom $\begin{bmatrix} 52 \\ 82 \end{bmatrix}, \begin{bmatrix} 68 \\ 81 \end{bmatrix}, \begin{bmatrix} 77 \\ 64 \end{bmatrix}, \begin{bmatrix} 76 \\ 68 \end{bmatrix}, \begin{bmatrix} 16 \\ 19 \end{bmatrix}$, dan $\begin{bmatrix} 22 \\ 17 \end{bmatrix}$.

$$C = \begin{bmatrix} 2 & 1 \\ 5 & 4 \end{bmatrix}\begin{bmatrix} 52 \\ 82 \end{bmatrix} = \begin{bmatrix} 186 \\ 588 \end{bmatrix} mod\ 94 = \begin{bmatrix} 92 \\ 24 \end{bmatrix}$$
$$C = \begin{bmatrix} 2 & 1 \\ 5 & 4 \end{bmatrix}\begin{bmatrix} 68 \\ 81 \end{bmatrix} = \begin{bmatrix} 217 \\ 664 \end{bmatrix} mod\ 94 = \begin{bmatrix} 29 \\ 6 \end{bmatrix}$$
$$C = \begin{bmatrix} 2 & 1 \\ 5 & 4 \end{bmatrix}\begin{bmatrix} 77 \\ 64 \end{bmatrix} = \begin{bmatrix} 218 \\ 641 \end{bmatrix} mod\ 94 = \begin{bmatrix} 30 \\ 77 \end{bmatrix}$$
$$C = \begin{bmatrix} 2 & 1 \\ 5 & 4 \end{bmatrix}\begin{bmatrix} 76 \\ 68 \end{bmatrix} = \begin{bmatrix} 220 \\ 652 \end{bmatrix} mod\ 94 = \begin{bmatrix} 32 \\ 88 \end{bmatrix}$$
$$C = \begin{bmatrix} 2 & 1 \\ 5 & 4 \end{bmatrix}\begin{bmatrix} 16 \\ 19 \end{bmatrix} = \begin{bmatrix} 51 \\ 156 \end{bmatrix} mod\ 94 = \begin{bmatrix} 51 \\ 62 \end{bmatrix}$$
$$C = \begin{bmatrix} 2 & 1 \\ 5 & 4 \end{bmatrix}\begin{bmatrix} 22 \\ 17 \end{bmatrix} = \begin{bmatrix} 61 \\ 178 \end{bmatrix} mod\ 94 = \begin{bmatrix} 61 \\ 84 \end{bmatrix}$$

Ketika hasil perkalian matriks di atas dikonversikan kembali akan diperoleh *ciphertext1*-nya adalah "}9>'?nAyT_^u".

Kedua, akan dilakukan enkripsi tahap dua, yaitu enkripsi *Rail Fence Cipher*. Perhatikan bahwa jumlah karakter pada *ciphertext1* terdiri dari 12 karakter (Tabel 2). Oleh karena itu, kunci yang akan digunakan untuk enkripsi tahap dua adalah $\lfloor\sqrt{12}\rfloor = 3$.

Ciphertext1 : }9>'?nAyT_^u
Kunci : 3

Ketika dibaca secara horizontal mulai dari baris pertama hingga baris ketiga akan diperoleh hasil *ciphertext2*-nya adalah "}?T9'ny_u>A^". Jadi, nama *customer* Shopee yang semula bernama "Username1472" akan berubah menjadi "}?T9'ny_u>A^".

3.2. Dekripsi

Dalam proses ini, *ciphertext2* "}?T9'ny_u>A^" akan didekripsi untuk kembali menjadi *plaintext* berupa nama *customer* Shopee melalui dua tahap. Pertama, akan dilakukan dekripsi tahap satu, yaitu dekripsi *Rail Fence Cipher* (Tabel 3).

Tabel 2. Proses enkripsi tahap dua

}				?				T			
	9		'		n		y		_		U
		>				A				^	

Tabel 3. Proses dekripsi tahap satu

}				?				T			
	9		'		n		y		_		U
		>				A				^	

Ciphertext2 : }?T9‘ny_u>A^
Kunci : 3
Ketika dibaca mengikuti pola zig-zag akan diperoleh hasil *ciphertext1*-nya adalah “}9>‘?nAyT_^u”.

Kedua, akan dilakukan dekripsi tahap dua, yaitu enkripsi *Hill Cipher* modifikasi. Akan dicari invers dari $K_{2\times2} = \begin{bmatrix} 2 & 1 \\ 5 & 4 \end{bmatrix}$ terhadap modulo 94. Perhatikan bahwa $\det(K) = 3$ dan $3^{-1}(mod\ 94) \equiv 63(mod\ 94)$. Oleh karena itu,

$$K^{-1} = 63\begin{bmatrix} 4 & -1 \\ -5 & 2 \end{bmatrix} = \begin{bmatrix} 252 & -63 \\ -315 & 126 \end{bmatrix} mod\ 94 = \begin{bmatrix} 64 & 31 \\ 61 & 32 \end{bmatrix}.$$

Selanjutnya kelompokkan tiap karakter *ciphertext1* menjadi 2 pasang terurut dan konversikan sesuai tabel ASCII ekuivalensi.

- “}” dan “9” : 92 dan 24
- “>” dan “” : 29 dan 6
- “?” dan “n” : 30 dan 77
- “A” dan “y” : 32 dan 88
- “T” dan “_” : 51 dan 62
- “^” dan “u” : 61 dan 84

Dari pengelompokkan di atas, akan diperoleh matriks kolom $\begin{bmatrix} 92 \\ 24 \end{bmatrix}, \begin{bmatrix} 29 \\ 6 \end{bmatrix}, \begin{bmatrix} 30 \\ 77 \end{bmatrix}, \begin{bmatrix} 32 \\ 88 \end{bmatrix}, \begin{bmatrix} 51 \\ 62 \end{bmatrix}$, dan $\begin{bmatrix} 61 \\ 84 \end{bmatrix}$.

$$P = \begin{bmatrix} 64 & 31 \\ 61 & 32 \end{bmatrix}\begin{bmatrix} 92 \\ 24 \end{bmatrix} = \begin{bmatrix} 6632 \\ 6380 \end{bmatrix} mod\ 94 = \begin{bmatrix} 52 \\ 82 \end{bmatrix}$$
$$P = \begin{bmatrix} 64 & 31 \\ 61 & 32 \end{bmatrix}\begin{bmatrix} 29 \\ 6 \end{bmatrix} = \begin{bmatrix} 2042 \\ 1961 \end{bmatrix} mod\ 94 = \begin{bmatrix} 68 \\ 81 \end{bmatrix}$$
$$P = \begin{bmatrix} 64 & 31 \\ 61 & 32 \end{bmatrix}\begin{bmatrix} 30 \\ 77 \end{bmatrix} = \begin{bmatrix} 4307 \\ 4294 \end{bmatrix} mod\ 94 = \begin{bmatrix} 77 \\ 64 \end{bmatrix}$$
$$P = \begin{bmatrix} 64 & 31 \\ 61 & 32 \end{bmatrix}\begin{bmatrix} 32 \\ 88 \end{bmatrix} = \begin{bmatrix} 4776 \\ 4768 \end{bmatrix} mod\ 94 = \begin{bmatrix} 76 \\ 68 \end{bmatrix}$$
$$P = \begin{bmatrix} 64 & 31 \\ 61 & 32 \end{bmatrix}\begin{bmatrix} 51 \\ 62 \end{bmatrix} = \begin{bmatrix} 5186 \\ 5095 \end{bmatrix} mod\ 94 = \begin{bmatrix} 16 \\ 19 \end{bmatrix}$$
$$P = \begin{bmatrix} 64 & 31 \\ 61 & 32 \end{bmatrix}\begin{bmatrix} 61 \\ 84 \end{bmatrix} = \begin{bmatrix} 6508 \\ 6409 \end{bmatrix} mod\ 94 = \begin{bmatrix} 22 \\ 17 \end{bmatrix}$$

Ketika hasil perkalian matriks di atas dikonversikan kembali akan diperoleh *plaintext*-nya adalah “Username1472”. Dari sini dapat dilihat bahwa diperoleh *plaintext* hasil dekripsi secara dua tahap adalah “Username1472” dan hal ini sama dengan nama *customer* Shopee yang diberikan. Oleh karena itu, proses dekripsi dilakukan dengan benar.

4. Kesimpulan

Kombinasi algoritma *Hill Cipher* modifikasi dan *Rail Fence Cipher* dapat diterapkan pada sistem keamanan data *customer* Shopee. Hasil yang diperoleh juga mampu menjaga kerahasiaan data tersebut karena konsep super enkripsi membuat *ciphertext* sulit dipecahkan oleh pihak yang tidak berkepentingan. Namun, prosedur enkripsi dan dekripsi dalam penelitian ini masih dilakukan secara manual sehingga dapat merepotkan *seller*, kurir ekspedisi, dan *customer* ketika ingin mengetahui data yang dimaksud. Oleh karena itu, tinjauan lebih lanjut mengenai program yang tepat untuk pengaplikasian algoritma *Hill Cipher* modifikasi dan *Rail Fence Cipher* perlu dilakukan agar dapat digunakan dengan lebih efisien.

Daftar Pustaka

1. Bahasa, B. P. dan P. 2016. KBBI Daring. Diakses: 15 Oktober 2023, https://kbbi.kemdikbud.go.id/.
2. Contributors, W. 2023. Shopee. Diakses: 15 Oktober 2023, https://id.wikipedia.org/wiki/Shopee.
3. Ssu-yun, S., Chiang, E., & Hsin-yin, L. 2023. Shopee, Eslite bookstore fined following data leaks. Diakses: 16 Oktober 2023, https://focustaiwan.tw/society/202305300021.
4. Tim. 2022. Shopee Sensor Nama dan Nomor HP Pembeli bagi Penjual. Diakses: 15 Oktober 2023, https://www.cnnindonesia.com/ekonomi/20220808082920-92-831524/shopee-sensor-nama-dan-nomor-hp-pembeli-bagi-penjual.
5. Tim. 2022. Alasan Shopee Sensor Nama dan Nomor HP Pembeli dari Penjual. Diakses: 15 Oktober 2023, https://www.cnnindonesia.com/ekonomi/20220808142326-92-831739/alasan-shopee-sensor-nama-dan-nomor-hp-pembeli-dari-penjual.
6. Putra, P. P., & Toresa, D. 2021. *Buku Ajar Keamanan Informasi Dan Jaringan Komputer*. Pekanbaru: LPPM Universitas Lancang Kuning. Diambil dari http://repository.unilak.ac.id/id/eprint/2758%0Ahttps://repository.unilak.ac.id/2758/1/Buku Ajar 2021 - Keamanan informasi dan jaringan.pdf
7. Siregar, N., Faisal, I., & Handoko, D. 2022. Menerapkan Algoritma Hill Cipher dan Matriks 2x2 Dalam Mengamankan File Teks Menggunakan Kode ASCII. *Jurnal Ilmu Komputer dan Sistem Informasi (JIRSI)*, *1*(2), 70–83. Diambil dari https://jurnal.unity-academy.sch.id/index.php/jirsi/index70%0Ahttp://creativecommons.org/licenses/by-sa/4.0/
8. Hasugian, A. H. 2013. Implementasi Algoritma Hill Cipher dalam Penyandian Data. *Pelita Informatika Budi Darma*, *IV*(2), 115–122.
9. Dinata, S. J. 2020. Implementasi Algoritma Penyandian Transposisi Rail Fence pada Data Rekam Medis. *Jurnal Informasi dan Teknologi Ilmiah (INTI)*, *7*(3), 305–309. Diambil dari https://www.ejurnal.stmik-

budidarma.ac.id/index.php/inti/article/view/2406
10. Fadlan, M., Bintari, E. D., & Tasya, A. 2023. Pengamanan Basis Data dengan Algoritma Transposisi Rail Fence. *Jurnal Sistem Informasi dan Sistem Komputer*, *8*(2), 66–72. https://doi.org/10.51717/simkom.v8i2.135.
11. Wardani, I. E. 2013. Pemecahan Sandi Kriptografi dengan Menggabungkan Metode Hill Cipher dan Metode Caesar Chipher. *CAUCHY: Jurnal Matematika Murni dan Aplikasi*, *2*(4), 232–236. https://doi.org/10.18860/ca.v2i4.3120.
12. Hariati, A., Hardiyanti, K., & Putri, W. E. 2018. Kombinasi Algoritma Playfair Cipher dengan Metode Zig-zag dalam Penyandian Teks. *SinkrOn*, *2*(2), 13–17. Diambil dari https://jurnal.polgan.ac.id/index.php/sinkron/index
13. Fardianto, F. A. E., Yanto, F., Iskandar, I., & Pizaini, P. 2023. Kombinasi Algoritma Kriptografi Vigenere Cipher dengan Metode Zig-zag dalam Pengamanan Pesan Teks. *Jurnal Computer Science and Information Technology (CoSciTech)*, *4*(1), 182–192. https://doi.org/10.37859/coscitech.v4i1.4787.
14. Permanasari, Y. 2017. Kriptografi Klasik Monoalphabetic. *Matematika*, *16*(1), 7–10. https://doi.org/10.29313/jmtm.v16i1.2543.
15. Stallings, W. 2011. *Cryptography and Network Security: Principles and Practice*. *Computer Science Handbook, Second Edition*. New York: Pearson Education. https://doi.org/10.1201/9781420057133.
16. Hamdani, D., & Junaidi, J. 2020. Modifikasi Karakter Kode pada Cipher Hill Menggunakan Kode ASCII. *Eigen Mathematics Journal*, *03*(01), 23–28. https://doi.org/10.29303/emj.v3i1.54.
17. Contributors, W. 2022. ASCII. Diakses: 14 Oktober 2023, https://id.wikipedia.org/wiki/ASCII.
18. Cop, P., & Purnama, R. A. 2015. Sistem Keamanan E-Voting Menggunakan Algoritma Kode ASCII. *Jurnal Teknik Komputer AMIK BSI*, *1*(1), 84–95.
19. Siahaan, A. P. U. 2016. Rail Fence Cryptography in Securing Information. *International Journal of Scientific & Engineering Research*, *7*(7), 535–538.
20. Godara, S., Kundu, S., & Kaler, R. 2018. An Improved Algorithmic Implementation of Rail Fence Cipher. *International Journal of Future Generation Communication and Networking*, *11*(2), 23–32. https://doi.org/10.14257/ijfgcn.2018.11.2.03.
21. Mubarak B, M. A., Salim, Y., & Sugiarti, S. 2022. Implementasi Metode Kriptografi Menggunakan Cipher Substitusi dan Cipher Transposisi pada Data Teks. *Buletin Sistem Informasi dan Teknologi Islam*, *3*(1), 42–51. https://doi.org/10.33096/busiti.v3i1.960.