Implementasi Algoritma *Hill Cipher* Menggunakan Kunci Matriks 2x2 Dalam Mengamankan Data Teks

Roman Gusmana[1], Haryansyah[2], Adimulya Dyas Wibisono[3]
[1]Sistem Informasi, STMIK PPKIA Tarakanita Rahmawati
[2, 3]Teknik Informatika, STMIK PPKIA Tarakanita Rahmawati
E-mail: [1]roman@ppkia.ac.id, [2]ary@ppkia.ac.id, [3]wibbydyas@gmail.com
Coresponden Author: *roman@ppkia.ac.id*

Diterima Redaksi: 04 September 2023 Revisi Akhir: 12 Oktober 2023 Diterbitkan Online: 24 Oktober 2023

Abstrak – *Sebagai negara yang besar, Indonesia harus memastikan keamanan data dalam semua bidang pekerjaan. Lonjakan kasus peretasan baru-baru ini telah merusak kepercayaan dan rasa aman masyarakat terhadap penyedia layanan yang mengumpulkan data pribadi atau rahasia. Kecemasan juga muncul terkait penyalahgunaan data. Upaya perlindungan data yang kuat menjadi penting dalam mengembalikan kepercayaan masyarakat dan menjaga kerahasiaan informasi. Salah satu langkah penting adalah memperkuat keamanan data melalui penerapan kriptografi, yaitu teknik yang menyamarkan data. Penelitian ini mengeksplorasi penggunaan algoritma kriptografi Hill Cipher dengan matriks 2x2 untuk menyandikan data teks. Melalui penelitian ini, diharapkan dapat lebih memahami operasi Hill Cipher dan pentingnya pemilihan kunci yang tepat untuk menjaga kerahasiaan pesan. Selain itu, penelitian semacam ini berkontribusi pada pemahaman lebih mendalam tentang perkembangan kriptografi sebagai disiplin ilmu yang terus berkembang.*

Kata Kunci *— Hill Cipher, Kriptografi, Keamanan Data, Enkripsi, Dekripsi*

Abstract – *As a large nation, Indonesia must ensure data security in all fields of work. Recent surges in hacking cases have eroded the trust and sense of security of the public in service providers that collect personal or confidential data. Concerns also arise regarding data misuse. Strong data protection efforts are crucial to restore public trust and maintain information confidentiality. One vital step is to reinforce data security through the implementation of cryptography, a technique that obfuscates data. This research explores the use of the Hill Cipher cryptography algorithm with a 2x2 matrix to encrypt textual data. Through this research, it is expected to gain a better understanding of Hill Cipher's operations and the importance of selecting the right key to maintain message confidentiality. Furthermore, studies of this nature contribute to a deeper understanding of the evolving field of cryptography.*

Keywords *— Hill Cipher, Cryptographic, Data Secure, Encryption, Decryption*

1. PENDAHULUAN

Sebagai salah satu negara dengan jumlah penduduk tertinggi di dunia, Indonesia kerap menjadi target dari tindakan pencurian data oleh pihak-pihak yang tidak bertanggung jawab. Bahkan baru-baru ini, merujuk pada salah satu laman Kompas, disebutkan bahwa dunia perbankan kembali lagi menjadi target peretasan oleh salah satu kelompok hacker. Selain itu juga dikabarkan bahwa data tersebut akan disebarluaskan di pasar gelap internet (*dark web*) apabila pihak bank tidak dapat menebus data tersebut dengan cara membayarkan sejumlah uang kepada pihak peretas.

Banyaknya tindak penyalahgunaan data berdampak pada hilangnya kepercayaan dan rasa aman dalam berbagai aspek kehidupan. Kepercayaan masyarakat terhadap institusi, perusahaan, dan layanan yang mengumpulkan dan mengelola data pribadi semakin terkikis ketika data tersebut disalahgunakan. Kepercayaan adalah pondasi utama dalam hubungan sosial dan ekonomi, dan ketika hilang, itu bisa merusak segala sesuatu, mulai dari hubungan antarindividu hingga hubungan bisnis.

Oleh karena itu, menjaga integritas data dan memberikan perlindungan yang kuat terhadap penyalahgunaan data adalah penting untuk membangun kembali kepercayaan dan rasa aman masyarakat terhadap penyedia layanan [1].

Nilai dari suatu data bisa jadi sangat penting dan harus dilindungi dengan perlindungan yang aman. Sehingga dibutuhkan sebuah sistem yang dapat menjamin kerahasiaan data, mencegah informasi dari kasus penyadapan, serta menanggulangi informasi yang penting dan sensitif [2].

Sistem yang dapat menjamin kerahasiaan data adalah kunci dalam menjaga integritas informasi yang kita miliki. Seiring dengan perkembangan teknologi, tantangan dalam menjaga kerahasiaan data semakin kompleks. Serangan siber yang terus berkembang dan metode penyalahgunaan data yang semakin canggih menuntut solusi yang inovatif dan responsif.

Kriptografi tidak hanya sebagai proses linguistik, melainkan juga proses matematika, serta representasional yang berbeda dari komputasi [3]. Kriptografi juga memiliki peran penting dalam menjaga kerahasiaan, integritas, dan otentikasi data. Ini dapat digunakan dalam berbagai aplikasi teknologi, termasuk komunikasi nirkabel, sistem keamanan pintar, bahkan sensor Internet of Things (IoT).

Kriptografi memiliki banyak ragam metode, seperti *Caesar Cipher*, *Affine*, *Monoalphabetic*, *Polyalphabetic*, *Vigenere*, Transposisi, dan banyak lagi. Salah satunya adalah *Hill Cipher*. Dari penelitian sebelumnya, disimpulkan bahwa pengamanan file teks dapat dilakukan dengan menggunakan metode Hill Cipher menggunakan kunci matriks 2x2 dan hanya berupa angka [4].

Penelitian lainnya dilakukan oleh Abd. A. ElHabshy dalam mengembangkan varian baru dari Hill Cipher yaitu *Augmented Hill Cipher* (AHC), disimpulkan bahwa AHC *has much greater key space than original Hill Cipher, which is corresponding to 3066-bit key although the complexity of AHC is almost the same with other variant of Hill Cipher* [5].

Pada penelitian ini, penulis mensimulasikan bagaimana proses algoritma Hill Cipher ini bekerja dalam mengamankan sebuah pesan teks dengan menggunakan kunci matriks 2x2. Penelitian semacam ini dapat memberikan pemahaman yang lebih baik tentang bagaimana algoritma Hill Cipher beroperasi, serta pentingnya memilih kunci yang tepat untuk menjaga kerahasiaan pesan saat menggunakan teknik ini. Selain itu, penelitian semacam ini dapat membantu dalam pengembangan dan pemahaman lebih lanjut tentang kriptografi sebagai bidang ilmu yang terus berkembang.

2. METODE PENELITIAN

Berikut ini adalah teori-teori pendukung yang menjadi acuan penulis dalam menyusun penelitian ini..

2.1. Kriptografi

Kriptografi (*cryptography*) berasal dari "*crypto*" berarti "*secret*" atau rahasia dan "*graphy*" berarti "*writing*" atau tulisan [6]. Pesan diubah dan diolah menjadi bentuk tak berarturan untuk menjaga kerahasiaan informasi yang terdapat di dalam pesan tersebut [7], [8]. Teknik ini dikenal sebagai enkripsi, dan itu adalah aspek penting dari kriptografi, yang bertujuan untuk melindungi data dari akses yang tidak sah atau penguraian pesan. Dalam proses enkripsi, pesan teks biasa diubah menjadi bentuk yang tak berarturan melalui algoritma dan kunci enkripsi tertentu.

Secara teknis kriptografi menerapkan teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan, keabsahan, integritas, serta autentikasi [9]–[11]. Pesan atau *plaintext*, bisa juga disebut teks-jelas (*cleartext*) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Pesan harus disandikan ke bentuk lain, agar informasinya tidak dapat dimengerti maknanya oleh pihak lain. Bentuk pesan yang tersandi disebut *ciphertext* atau *histogram* (*cryptogram*). Ciphertext harus dapat ditransformasi kembali menjadi plaintext.

2.2. Hill Cipherz

Hill Cipher *is likewise referred to as that the substitution ciphers system*. Teknik penyandian yang dilakukan dalam Hill Cipher melibatkan penggantian karakter teks dengan karakter lain untuk menghasilkan teks terenkripsi. Namun, yang membedakan Hill Cipher dari sebagian besar sistem sandi substitusi adalah bahwa Hill Cipher beroperasi dengan blok-blok karakter sekaligus, bukan satu karakter tunggal [12].

Hill Cipher ditemukan pada tahun 1929 oleh Lester S. Hill. Metode ini adalah salah satu dari algoritma kriptografi yang menggunakan kunci simetris, yaitu kunci yang sama untuk digunakan dalam proses enkripsi maupun dekripsi [13], [14].

Kunci dalam Hill Cipher berupa matriks n x n, dimana dasar teorinya menggunakan perkalian antara matriks K dan invers dari matriks K^{-1} [15]. Hill Cipher termasuk dalam *polyalphabetic substitution* karena melakukan perkalian matriks menggunakan metode substitusi. Teknik pertukaran karakter secara polyalfabet berarti bahwa setiap satu karakter pada plaintext dapat dipetakan ke lebih dari 1 (satu) jenis karakter. Berbeda dengan monoalfabet yang setiap satu karakter pada plaintext hanya dapat dipetakan ke 1 (satu) jenis karakter saja, polyalfabet tentu lebih sulit dipecahkan.

Enkripsi dengan menggunakan Hill Cipher dapat dinyatakan dalam persamaan [11], [16]–[18].

$$C = K_{(K1, K2, .. Kn)} * P_{(P1, P2, .. Pn)} \bmod m \quad \text{..... (1)}$$

Proses enkripsi diawali menentukan kunci matriks *K* = (*K1*, *K2*, .., *Kn*) yang akan digunakan. Selanjutnya menentukan plaintext P lalu dibagi ke dalam blok plaintext *P* = (*P1*, *P2*, .., *Pn*). Untuk mendapatkan ciphertext *C*, hasil perkalian matriks kunci dan plaintext tersebut di-modulo m.

Hasil dari operasi ini adalah blok-blok ciphertext C = (C1, C2, .., Cn), yang merupakan hasil enkripsi dari blok-blok plaintext sebelumnya. Ciphertext inilah yang kemudian dapat dikirimkan secara aman atau disimpan tanpa risiko terpapar kepada pihak yang tidak berwenang.

Sementara untuk proses dekripsi, terlebih dahulu perlu diketahui invers dari nilai K yaitu K^{-1}. Pada penelitian ini, penulis menggunakan kunci matriks ordo 2x2, yaitu jenis mastriks persegi yang terdiri dari 2 (dua) baris dan 2 (dua) kolom. Proses diawali dengan menentukan nilai determinan matriks kunci yang dinyatakan dalam persamaan

$$K \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \det K^{-1} = ad - bc \quad \text{..... (2)}$$

Selanjutnya menentukan invers modulo dengan persamaan

$$\det K \bmod m = 1 \quad \text{..... (3)}$$

Dengan det adalah nilai determinan kunci matriks, b adalah bilangan positif atau negatif, dan modulo m. nilai b didapatkan dengan persamaan

$$n(k) + 1/\det \quad \text{..... (4)}$$

Tentukan nilai K menggunakan bilangan positif 0,1,2, .., n dan negatif -1,-2, .., -n sampai hasil perhitungan mendapatkan nilai bilangan positif atau negatif.

Selanjutnya menentukan invers kunci matriks.

$$K \begin{bmatrix} a & b \\ c & d \end{bmatrix} = K^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \quad \text{..... (5)}$$

Selanjutnya, proses dekripsi dilakukan dengan menggunakan persamaan berikut.

$$P = K^{-1} * C_{(C1, C2, .. Cn)} \bmod m \quad \text{..... (5)}$$

2.3. ASCII

American Standard Code for Information Interchange (ASCII) atau Kode Standar Amerika untuk Pertukaran Informasi adalah standar pengkodean karakter untuk alat komunikasi. Kode ASCII mewakili teks dalam komputer, peralatan telekomunikasi, dan perangkat lainnya.

Kode ASCII dikelompokkan lagi ke dalam beberapa bagian, yaitu kode yang tidak terlihat simbol karakternya, kode yang terlihat simbolnya seperti alfabet maupun angka serta tanda baca, dan kode yang tidak ada di keyboard namun dapat ditampilkan, umumnya untuk kode-kode grafik [19]–[21].

Sebagai contoh, karakter alfabet "B" dalam Kode ASCII memiliki nilai hexadecimal 42 dan nilai desimal 66, dan tampilan visual karakter "B" adalah huruf "B" yang sesuai.

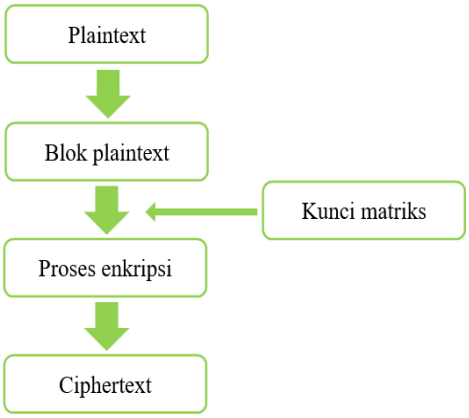
Selain karakter huruf dan angka, ada juga karakter dengan nilai hexadecimal 0D dan nilai desimal 13 dalam Kode ASCII. Namun, tampilan visualnya tidak berbentuk karakter, melainkan lebih mirip fungsi pada keyboard. Karakter ASCII yang dimaksud adalah "enter" atau "carriage return." Karakter ini digunakan untuk mengindikasikan akhir baris atau pindah ke baris baru dalam dokumen atau teks. Meskipun karakter ini tidak memiliki tampilan visual yang sesuai, peran fungsionalnya dalam pemformatan dan pemrosesan teks sangat penting, terutama dalam pengaturan teks yang memerlukan pemisahan baris atau perpindahan kursor ke baris baru..

Dec	Oct	Hex	C	Dec	Oct	Hex	C	Dec	Oct	Hex	C	Dec	Oct	Hex	C
0	0	0	^@	32	40	20		64	100	40	@	96	140	60	`
1	1	1	^A	33	41	21	!	65	101	41	A	97	141	61	a
2	2	2	^B	34	42	22	"	66	102	42	B	98	142	62	b
3	3	3	^C	35	43	23	#	67	103	43	C	99	143	63	c
4	4	4	^D	36	44	24	$	68	104	44	D	100	144	64	d
5	5	5	^E	37	45	25	%	69	105	45	E	101	145	65	e
6	6	6	^F	38	46	26	&	70	106	46	F	102	146	66	f
7	7	7	^G	39	47	27	'	71	107	47	G	103	147	67	g
8	10	8	^H	40	50	28	(	72	110	48	H	104	150	68	h
9	11	9	^I	41	51	29	)	73	111	49	I	105	151	69	i
10	12	a	^J	42	52	2a	*	74	112	4a	J	106	152	6a	j
11	13	b	^K	43	53	2b	+	75	113	4b	K	107	153	6b	k
12	14	c	^L	44	54	2c	,	76	114	4c	L	108	154	6c	l
13	15	d	^M	45	55	2d	-	77	115	4d	M	109	155	6d	m
14	16	e	^N	46	56	2e	.	78	116	4e	N	110	156	6e	n
15	17	f	^O	47	57	2f	/	79	117	4f	O	111	157	6f	o
16	20	10	^P	48	60	30	0	80	120	50	P	112	160	70	p
17	21	11	^Q	49	61	31	1	81	121	51	Q	113	161	71	q
18	22	12	^R	50	62	32	2	82	122	52	R	114	162	72	r
19	23	13	^S	51	63	33	3	83	123	53	S	115	163	73	s
20	24	14	^T	52	64	34	4	84	124	54	T	116	164	74	t
21	25	15	^U	53	65	35	5	85	125	55	U	117	165	75	u
22	26	16	^V	54	66	36	6	86	126	56	V	118	166	76	v
23	27	17	^W	55	67	37	7	87	127	57	W	119	167	77	w
24	30	18	^X	56	70	38	8	88	130	58	X	120	170	78	x
25	31	19	^Y	57	71	39	9	89	131	59	Y	121	171	79	y
26	32	1a	^Z	58	72	3a	:	90	132	5a	Z	122	172	7a	z
27	33	1b	^[	59	73	3b	;	91	133	5b	[	123	173	7b	{
28	34	1c	^\	60	74	3c	<	92	134	5c	\	124	174	7c	|
29	35	1d	^]	61	75	3d	=	93	135	5d	]	125	175	7d	}
30	36	1e	^^	62	76	3e	>	94	136	5e	^	126	176	7e	~
31	37	1f	^_	63	77	3f	?	95	137	5f	_	127	177	7f	

Gambar 1. Daftar Karakter ASCII

2.4. Proses Enkripsi

Untuk proses enkripsi plaintext menggunakan metode Hill Cipher dapat dilihat pada Gambar 2.

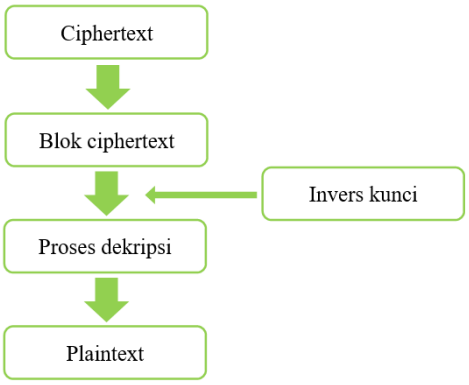


Gambar 2. Proses Enkripsi

Proses enkripsi diawali dengan menyiapkan plaintext dan kunci berupa matriks ordo 2x2. Plaintext selanjutnya dibagi dalam beberapa blog sesuai dengan ordo matriks, karena ordo matriks yang digunakan adalah ordo 2x2, maka penggalan plaintext akan diolah per 2 (dua) huruf. Contoh, diketahui plaintext “SEBAYA”, maka blok plaintext yang terbentuk adalah “SE”, “BA”, dan “YA”. Selanjutnya blok plaintext dan kunci matriks diolah dengan menggunakan Hill Cipher. Hasil pengolahan ini akan menghasilkan ciphertext dimana ini adalah hasil akhir dari proses enkripsi.

2.5. Proses Dekripsi

Proses dekripsi ciphertext menggunakan Hill Cipher dapat dilihat pada Gambar 3.



Gambar 3. Proses Dekripsi

Proses dekripsi diawali dengan menyiapkan ciphertext dan invers kunci matriks. Sama seperti proses enkripsi, ciphertext kembali dibagi dalam beberapa blok sesuai dengan ordo matriks yang digunakan. Selanjutnya diolah dengan Hill Cipher untuk menghasilkan plaintext yang merupakan hasil akhir dari proses dekripsi.

3. HASIL DAN PEMBAHASAN

Bagian pembahasan ini dibagi ke dalam beberapa sub-pembahasan, yaitu proses pembangkitan kunci, enkripsi, dekripsi dan perancangan aplikasi.

3.1. Kunci

Kunci enkripsi berupa kunci matriks dengan orde 2x2, sehingga kebutuhan panjang karakter pada implementasi program yaitu sebepanjang 4 (empat) karakter. Sebagai contoh, diketahui kunci enkripsi K = “KODE”.

Proses selanjutnya adalah mengkonversi karakter kunci ke dalam nilai desimal dengan mengacu pada tabel ASCII dan dilanjutkan dengan menyusun kunci tersebut ke dalam matriks ordo 2x2, sehingga kunci matriks enkripsi yang terbentuk adalah sebagai berikut :

$$K\begin{bmatrix} K & O \\ D & E \end{bmatrix} \rightarrow K\begin{bmatrix} 75 & 79 \\ 68 & 69 \end{bmatrix}$$

Untuk proses dekripsi, kunci matriks tersebut diolah untuk diketahui invers kunci matriks yang terbentuk. Invers kunci matriks tersebut selanjutnya digunakan sebagai pengali dengan blok ciphertext untuk didapatkan kembali plaintext.

Proses diawali dengan mencari nilai determinan (det) K terlebih dahulu dengan menggunakan persamaan 2, sehingga nilai det K yang diperoleh adalah sebagai berikut :

$$K\begin{bmatrix} K & O \\ D & E \end{bmatrix} \rightarrow det\ K = (75 * 69) - (79 * 68) = -197$$

Hasil det K tidak boleh lebih kecil dari 0 atau lebih besar dari 128, sehingga nilai det K perlu dimodulasi, sehingga nilai det K yang didapat adalah sebagai berikut :

$$det\ K = -197 \bmod 128 \rightarrow det\ K = 59$$

Selanjutnya adalah mencari invers modulo menggunakan persamaan 3. Adapun perhitungannya adalah sebagai berikut :

(59 * 0) mod 128 = 0
(59 * 1) mod 128 = 59
(59 * 2) mod 128 = 118
..

(59 * 115) mod 128 = 1

Apabila hasil dari perkalian dan modulo adalah 1, maka proses pencarian nilai invers akan terhenti pada nilai invers tersebut, sehingga nilai invers modulo dari det K = 59 adalah 115. Selanjutnya adalah menentukan matriks invers dari kunci matriks yaitu dengan merujuk pada persamaan 5.

$K^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \rightarrow K^{-1} \begin{bmatrix} 69 & -79 \\ -68 & 75 \end{bmatrix}$

Setelah mendapatkan nilai invers determinan dan invers matriks, maka kedua nilai itu dikalikan untuk menentukan kunci dekripsi.

$K^{-1} = 115 \begin{bmatrix} 69 & -79 \\ -68 & 75 \end{bmatrix} \bmod 128$

$= \begin{bmatrix} 7935 & -9085 \\ -7820 & 8625 \end{bmatrix} \bmod 128$

$= \begin{bmatrix} 127 & 3 \\ 116 & 49 \end{bmatrix}$

Jadi invers kunci matriks adalah $K^{-1} = \begin{bmatrix} 127 & 3 \\ 116 & 49 \end{bmatrix}$, kunci inilah yang digunakan dalam proses dekripsi.

3.2. Proses Enripsi

Sebagaimana yang tergambarkan pada Gambar 2, proses diawali dengan menyiapkan plaintext P dan kunci K. Plaintext P yang dijadikan contoh pada penelitian ini adalah "DATA". Dari plaintext tersebut, dilakukan pemenggalan karakter menjadi blok matriks lalu dilanjutkan dengan konversi ke dalam nilai desimal ASCII, sehingga didapatkan hasil sebagai berikut :

Plaintext = "DATA" → "DA", "TA"

DA = $\begin{bmatrix} 68 \\ 65 \end{bmatrix}$ TA = $\begin{bmatrix} 84 \\ 65 \end{bmatrix}$

Selanjutnya dilakukan perkalian plaintext matriks *P* dengan kunci matriks *K* $\begin{bmatrix} 75 & 79 \\ 68 & 69 \end{bmatrix}$. Langkah ini berdasarkan persamaan 1, sehingga nilai yang di dapat adalah sebagai berikut :

(DA) = $\begin{bmatrix} 75 & 79 \\ 68 & 69 \end{bmatrix} \begin{bmatrix} 68 \\ 65 \end{bmatrix} \bmod 128$

$= \begin{bmatrix} 5100 & + & 5135 \\ 4624 & + & 4485 \end{bmatrix} \bmod 128$

$= \begin{bmatrix} 123 \\ 21 \end{bmatrix} \rightarrow \begin{bmatrix} \{ \\ \hat{} U \end{bmatrix}$

(TA) = $\begin{bmatrix} 75 & 79 \\ 68 & 69 \end{bmatrix} \begin{bmatrix} 84 \\ 65 \end{bmatrix} \bmod 128$

$= \begin{bmatrix} 6300 & + & 5135 \\ 5712 & + & 4485 \end{bmatrix} \bmod 128$

$= \begin{bmatrix} 43 \\ 85 \end{bmatrix} \rightarrow \begin{bmatrix} + \\ U \end{bmatrix}$

Jadi hasil perhitungan enkripsi dari plaintext "DATA" didapatkan karakter baru sehingga menjadi "{ ^U + U".

3.3. Proses Dekripsi

Berdasarkan Gambar 3, proses diawali dengan menyiapkan ciphertext C dan invers kunci matriks K-1. Dari ciphertext "{ ^U + U" dilakukan pemenggalan menjadi blok matriks lalu dilanjutkan dengan konversi ke dalam nilai desimal ASCII, sehingga didapatkan hasil sebagai berikut :

Ciphertext = "{ ^U + U" → "{ ^U", "+ U"

{ ^U = $\begin{bmatrix} 123 \\ 21 \end{bmatrix}$ + U = $\begin{bmatrix} 43 \\ 85 \end{bmatrix}$

Selanjutnya dilakukan perkalian ciphertext matriks *C* dengan invers kunci matriks K^{-1} $\begin{bmatrix}127 & 3\\116 & 49\end{bmatrix}$. Langkah ini berdasarkan persamaan 6, sehingga nilai yang di dapat adalah sebagai berikut :

$$(\{\ \text{^U}) = \begin{bmatrix}127 & 3\\116 & 49\end{bmatrix}. \begin{bmatrix}123\\21\end{bmatrix} \bmod 128 \qquad (+\ \text{U}) = \begin{bmatrix}127 & 3\\116 & 49\end{bmatrix}. \begin{bmatrix}43\\85\end{bmatrix} \bmod 128$$

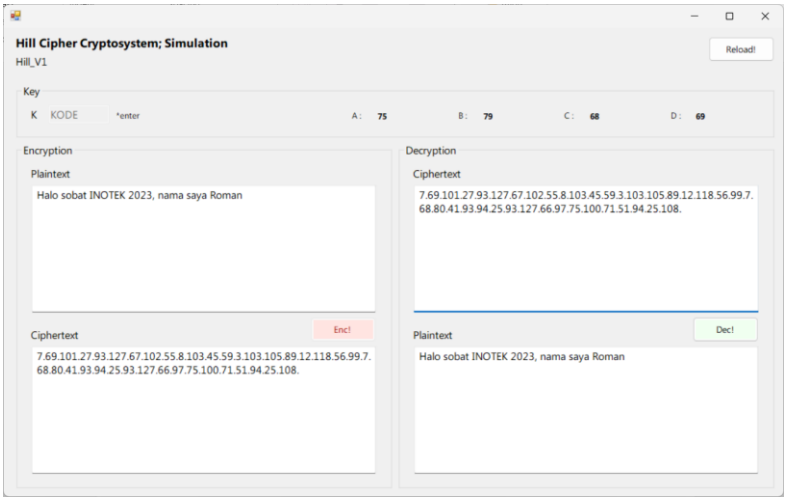
$$= \begin{bmatrix}15621 & + & 63\\14268 & + & 1029\end{bmatrix} \bmod 128 \qquad = \begin{bmatrix}5461 & + & 255\\4988 & + & 4144\end{bmatrix} \bmod 128$$

$$= \begin{bmatrix}68\\65\end{bmatrix} \rightarrow \begin{bmatrix}D\\A\end{bmatrix} \qquad = \begin{bmatrix}84\\65\end{bmatrix} \rightarrow \begin{bmatrix}T\\A\end{bmatrix}$$

Jadi hasil perhitungan enkripsi dari plaintext "{ ^U + U" didapatkan karakter baru sehingga menjadi "DATA".

3.4. Perancangan Aplikasi

Perancangan aplikasi bertujuan untuk memberikan gambaran tentang bagaimana metode Hill Cipher diterapkan dalam proses enkripsi dan dekripsi. Aplikasi ini dirancang untuk mengilustrasikan secara praktis bagaimana algoritma Hill Cipher beroperasi dan bagaimana pesan dapat dienkripsi dan didekripsi dengan menggunakan matriks kunci yang sesuai. Dengan demikian, aplikasi ini menjadi alat yang berguna untuk memahami konsep kriptografi Hill Cipher dan mengimplementasikannya dalam berbagai konteks pengamanan data. Peneliti merancang sebuah aplikasi menggunakan Microsoft Visual Studio. Berikut adalah desain antarmuka *form* simulasi proses enkripsi dan dekripsinya.



Gambar 4. Desain Antarmuka Form Simulasi

4. KESIMPULAN

Penerapan metode Hill Cipher dalam mengamankan pesan berupa teks adalah fleksibel dan dapat diterapkan dalam berbagai konteks dan jumlah pesan yang beragam. Metode ini mampu mengenkripsi pesan dalam bentuk huruf, angka, tanda baca, serta dalam format kata, kalimat, atau paragraf yang lebih panjang. Kemampuan Hill Cipher untuk mengenkripsi pesan dengan format yang beragam menjadikannya alat yang serbaguna dalam menjaga kerahasiaan informasi dalam berbagai aspek komunikasi dan keamanan data.

Penting untuk mencatat bahwa penggunaan kunci matriks ordo 2x2 dalam Hill Cipher melibatkan perhitungan determinan dan invers matriks di awal ketika kunci diproses. Hal ini memungkinkan pengguna untuk memverifikasi apakah kunci matriks dapat digunakan dalam proses enkripsi dan dekripsi. Keterlibatan perhitungan determinan dan invers matriks ini memberikan fleksibilitas tambahan dalam mengadaptasi metode Hill Cipher untuk berbagai bidang pekerjaan dan bahkan dapat dikembangkan pada berbagai platform lainnya.

Dengan demikian, Hill Cipher merupakan alat yang kuat dan serbaguna dalam menjaga keamanan data dan kerahasiaan informasi dalam dunia yang semakin terhubung dan beragam dalam komunikasi dan pertukaran informasi.

5. SARAN

Adapun saran dari penelitian ini adalah menghasilkan ciphertext dalam bentuk karakter alih-alih dalam format desimal. Ini akan meningkatkan keterbacaan hasil enkripsi dan memudahkan pengguna dalam interpretasi pesan terenkripsi. Selanjutnya menyediakan tabel karakter khusus yang memfasilitasi proses enkripsi dan dekripsi. Tabel ini dapat digunakan untuk mengatasi ketidaktersediaan karakter yang mungkin muncul saat konversi dengan ASCII, sehingga prosesnya lebih efisien. Modifikasi rumus dalam metode Hill Cipher dapat diperhitungkan untuk meningkatkan tingkat keamanan. Ini dapat melibatkan penggunaan matriks kunci yang lebih rumit atau metode enkripsi yang lebih canggih. Selain itu, disarankan untuk mengimplementasikan metode ini dalam berbagai platform, termasuk situs web dan aplikasi seluler. Hal ini akan memungkinkan pengguna untuk dengan mudah mengakses dan menggunakan metode Hill Cipher dalam berbagai konteks.

DAFTAR PUSTAKA

[1] M. Fadlan, S. Sinawati, A. Indriani, dan E. D. Bintari, "PENGAMANAN DATA TEKS MELALUI PERPADUAN ALGORITMA BEAUFORT DAN CAESAR CIPHER," *JURNAL TEKNIK INFORMATIKA*, vol. 12, no. 2, hlm. 149–158, Nov 2019, doi: 10.15408/jti.v12i2.12262.

[2] D. Maulana Sholahudin, "Implementasi Algoritma Hill Cipher untuk Proses Enkripsi dan Dekripsi Citra Berwarna dengan Modifikasi Padding".

[3] A. Amrulloh dan E. Ujianto, "Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher," *Jurnal CoreIT*, vol. 5, no. 2, 2019, [Daring]. Tersedia pada: https://program.arfianhidayat.com/kriptografi/vig

[4] N. Siregar, I. Faisal, dan D. Handoko, "Menerapkan Algoritma Hill Cipher dan Matriks 2x2 Dalam Mengamankan File Teks Menggunakan Kode ASCII Apply Hill Cipher Algorithm and 2x2 Matrix in Securing Text Files Using ASCII Code," 2022. [Daring]. Tersedia pada: https://jurnal.unity-academy.sch.id/index.php/jirsi/index70

[5] A. A. Elhabshy, "Augmented Hill Cipher," *International Journal of Network Security*, vol. 21, no. 5, hlm. 812, 2019, doi: 10.6633/IJNS.201909.

[6] I. O. Nainggolan, W. M. Kementeri, P. R. I. Balai, D. Industri, dan M. Edan, "IMPLEMENTASI SANDI AFFINE UNTUK PENGAMANAN FILE MICROSOFT OFFICE Indra Oloan Nainggolan," 2019.

[7] U. Potensi Utama Jl KLYos, "RANCANG BANGUN APLIKASI KRIPTOGRAFI PADA TEKS MENGGUNAKAN METODE REVERSE CHIPER DAN RSA BERBASIS ANDROID Yusfrizal 1)," *Jurnal Teknik Informatika Kaputama (JTIK)*, vol. 3, no. 2, 2019.

[8] E. Setyawati, C. E. Widjayanti, R. R. Siraiz, dan H. Wijoyo, "Pengujian keamanan komputer kriptografi pada surat elektronik berbasis website dengan enkripsi metode MD5," *Jurnal Manajamen Informatika Jayakarta*, vol. 1, no. 1, hlm. 56, Feb 2021, doi: 10.52362/jmijayakarta.v1i1.367.

[9] Y. Dwi Putri, S. Lutfi, J. Jati Metro, dan K. Ternate Selatan, "PENERAPAN KRIPTOGRAFI CAESAR CIPHER PADA FITUR CHATTING SISTEM INFORMASI FREELANCE," *Jurnal Informatika dan Komputer) p-ISSN*, vol. 2, no. 2, hlm. 2355–7699, 2019, doi: 10.33387/jiko.

[10] D. Pangestu dan A. Syahputra, "PERANCANGAN APLIKASI KEAMANAN CLOUD DATABASE MENGGUNAKAN OPERASI XOR DENGAN ALGORITMA AFFINE BERBASIS ANDROID DESIGN OF CLOUD DATABASE SAFETY APPLICATIONS USING XOR OPERATION WITH AFFINE ALGORITHM BASED ON ANDROID," 2020.

[11] I. Muda Siregar, "PENERAPAN ALGORITMA AFFINE CIPHER DAN ALGORITMA COLOUMNAR TRANSPOSITION DALAM KEAMANAN TEKS," 2019. [Daring]. Tersedia pada: http://www.stmik-budidama.ac.id,

[12] L. S. Mezher dan A. M. Abbass, "Mixed Hill Cipher methods with triple pass protocol methods," *International Journal of Electrical and Computer Engineering*, vol. 11, no. 5, hlm. 4449–4457, Okt 2021, doi: 10.11591/ijece.v11i5.pp4449-4457.

[13] A. Susanto, I. Utomo, W. Mulyono, M. Rizky, F. Febrian, dan G. A. Rosyida, "A Combination of Hill Cipher and LSB for Image Security," *Scientific Journal of Informatics*, vol. 7, no. 1, hlm. 2407–7658, 2020, [Daring]. Tersedia pada: http://journal.unnes.ac.id/nju/index.php/sjie

[14] S. S. Al-Kaabi dan S. B. Belhaouari, "METHODS TOWARD ENHANCING RSA ALGORITHM : A SURVEY," *International Journal of Network Security & Its Applications*, vol. 11, no. 03, hlm. 53–70, Mei 2019, doi: 10.5121/ijnsa.2019.11305.

[15] R. K. Hasoun, S. Faris Khlebus, dan H. Kadhim Tayyeh, "A New Approach of Classical Hill Cipher in Public Key Cryptography," 2021. [Daring]. Tersedia pada: http://www.ijnaa.semnan.ac.ir

[16] K. Mani dan A. Barakath Begam, "Generation Of Keymatrix For Hill Cipher Encryption Using Quadratic Form," *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH*, vol. 8, no. 10, 2019, [Daring]. Tersedia pada: www.ijstr.org

[17] F. Qazi *dkk.*, "Modification in Hill Cipher for Cryptographic Application. 3C Tecnología. Glosas de innovación aplicadas a la pyme," *Edición Especial*, hlm. 240–257, 2019, doi: 10.17993/3ctecno.2019.

[18] A. Susilo, Y. Irawan, dan N. Heryana, "Combination of Hill Cipher Algorithm and Caesar Cipher Algorithm for Exam Data Security," *Buana Information Tchnology and Computer Sciences (BIT and CS*, vol. 1, no. 2, 2020.

[19] L. Fidi Astuti, K. Agung Santoso, dan A. Kamsyakawuni, "PENGAMANAN POLYALPHABETIC DENGAN AFFINE CIPHER BERDASARKAN BARISAN FIBONACCI (Polyalphabetic Security with Affine Cipher Based on Fibonacci Sequence)," *Majalah Ilmiah Matematika dan Statistika*, vol. 19, hlm. 95–103, 2019, [Daring]. Tersedia pada: https://jurnal.unej.ac.id/index.php/MIMS/index

[20] T. Khairani, K. A. Santoso, dan A. Kamsyakawuni, "PRISMA, Prosiding Seminar Nasional Matematika Pengkodean Monoalphabetic Menggunakan Affine Cipher dengan Kunci Diffie-Hellman," vol. 4, hlm. 553–559, 2021, [Daring]. Tersedia pada: https://journal.unnes.ac.id/sju/index.php/prisma/

[21] A. Tantoni, M. Taufan, dan A. Zaen, "IMPLEMENTASI DOUBLE CAESAR CIPHER MENGGUNAKAN ASCII," *Jurnal Informatika & Rekayasa Elektronika)*, vol. 1, no. 2, 2018, [Daring]. Tersedia pada: http://e-journal.stmiklombok.ac.id/index.php/jire