MODIFIKASI ALGORITMA HILL CIPHER DENGAN TABEL PERIODIK UNSUR KIMIA MENGGUNAKAN KODE NOMOR OPERATOR SELULER DI INDONESIA

Nindy Devita Sari, Dony Arius

Magister Teknik Informatika, Universitas AMIKOM Yogyakarta
Jl. Ring Road Utara, Kabupaten Sleman, Daerah Istimewa Yogyakarta
nindy.9243@students.amikom.ac.id, dony.a@amikom.ac.id

Abstract - The exchange of information through the virtual world has various benefits as an example of fast time estimation, physical distance, and unlimited space limit. But in such activities can also pose a security risk in confidential information. This remote information exchange demands security for the confidentiality of information exchanged. One way of hiding messages in a shipment is to convert data into one that is not understood by encoding and insertion using cryptographic techniques. One of the cryptographic techniques for text encoding is the Hill Cipher algorithm. The Hill Cipher algorithm utilizes arithmetic modulo towards the matrix as a key for encryption and decryption. The study aims to secure secret messages by building text message cryptographic applications using the Hill Cipher algorithm modifications to provide more security to the information exchange process. This study uses mod 26 which means there are 26 symbol input data. The periodic table of chemical elements is used for modification on the ciphertext result of the Hill Cipher algorithm and the mobile Operator number code in Indonesia is used for modification of the Hill Cipher key.
Keywords - Cryptography, Hill Chipper, Encryption, Decryption, Data Security.

Abstrak - Pertukaran informasi melalui dunia maya memiliki berbagai manfaat sebagai contoh estimasi waktu yang cepat, jarak fisik dan batas ruang tidak terbatas. Namun dalam kegiatan tersebut juga dapat menimbulkan resiko keamanan dalam informasi yang bersifat rahasia. Pertukaran informasi jarak jauh ini menuntut keamanan terhadap kerahasiaan informasi yang dipertukarkan. Salah satu cara penyembunyian pesan dalam pengiriman adalah merubah data menjadi yang tidak dimengerti dengan penyandian dan penyisipan menggunakan teknik kriptografi. Salah satu teknik kriptografi untuk penyandian teks adalah algoritma Hill Cipher. Algoritma Hill Cipher memanfaatkan aritmatika modulo terhadap matriks sebagai kunci untuk melakukan enkripsi dan dekripsi. Penelitian ini bertujuan untuk mengamankan pesan rahasia dengan membangun aplikasi kriptografi teks pesan menggunakan modifikasi algoritma Hill Cipher untuk memberikan keamanan lebih pada proses pertukaran informasi. Pada penelitian ini menggunakan mod 26 yang berarti ada 26 simbol inputan data. Tabel Periodik Unsur Kimia digunakan untuk modifikasi pada hasil ciphertext algoritma Hill Cipher dan Kode Nomor Operator Seluler di Indonesia digunakan untuk modifikasi pada kunci Hill Cipher.
Kata Kunci - Kriptografi, Hill Chiper, Enkripsi, Dekripsi, Keamanan Data.

I. PENDAHULUAN

Seiring dengan perkembangan teknologi sekarang ini, terdapat berbagai macam teknik untuk melindungi atau meyembunyikan pesan rahasia dari orang yang tidak berhak untuk mengakses pesan tersebut seperti percobaan hacking dan pencurian data.

Keamanan dalam pengiriman pesan sangat dibutuhkan bagi sesorang ketika akan mengirimkan pesan kepada orang lain yang berisi informasi penting dan sangat rahasia sehingga pesan tersebut tidak boleh diketahui oleh orang lain dan hanya boleh diketahui oleh pihak penerima pesan saja, maka biasanya pengirim akan mengirim pesan tersebut secara tersembunyi. Oleh karena itu, maka dikembangkanlah suatu cabang ilmu pengetahuan yang mempelajari tentang cara-cara penyandian dan pengamanan data yang dikenal dengan istilah kriptografi.

Kriptografi merupakan sebuah cabang ilmu pengetahuan yang mempelajari tentang bagaimana menjaga kerahasiaan pesan agar pesan tersebut tetap aman saat dikirimkan dan sampai ke penerima pesan tanpa mengalami gangguan dari pihak ketiga. Ada dua konsep utama dalam kriptografi yaitu ekripsi dan dekripsi [1].

Algoritma simetris dan algoritma asimetris merupakan kelompok dari algoritma kriptografi. Algoritma simetris menggunakan kunci yang sama baik dalam proses enkripsi maupun proses dekripsi-nya. Algoritma simetris dikelompokkan menjadi dua kategori yaitu cipher aliran dan cipher blok. Cipher aliran beroperasi dalam bentuk bit tunggal, sedangkan cipher blok beroperasi dalam bentuk blok bit [2].

Salah satu algoritma simetris untuk mengenkripsi data adalah algoritma *Hill Cipher*. Algoritma *Hill Cipher* mengenkripsi pesan dengan menggunakan matriks sebagai kunci dan memanfaatkan aritmetika modulo [3]. Setiap karakter pada *plaintext* dan *ciphertext* dirubah terlebih dahulu ke dalam bentuk angka dan memakai kunci simetris untuk merubah

plaintext ke *ciphertext*. Pada proses enkripsi, kunci harus di *invers* terlebih dahulu sebelum digunakan untuk mendekripsikan *ciphertext* [4].

Beberapa penelitian terdahulu dalam bidang kriptografi dengan menggunakan algoritma *Hill Cipher* diantaranya, "pengamanan pesan menggunakan algoritma *Hill Cipher* dalam keamanan komputer" [5]. Pada penelitian ini karakter yang akan dienkripsi terlalu sedikit sehingga mudah dibaca oleh orang yang tidak berhak menerima pesan, akan lebih baik jika karakter atau modulus yang digunakan kedalam *plaintext* dan *ciphertext* memakai karakter atau modulus yang lebih besar sehingga pesan rahasia akan sulit dibaca oleh orang lain.

Penelitian sejenis dengan judul "pengamanan pesan rahasia menggunakan metode algoritma *Hill Cipher*" [6]. Penelitian ini menghasilkan tingkat keberhasilan dekripsi untuk memperoleh *plaintext* sebesar 100% dengan menggunakan modifikasi algoritma *Hill Cipher* untuk pengamanan pesan rahasia teks serta file teks. Penelitian sejenis dengan judul "algoritma kriptografi *Hill Cipher* untuk pengamanan file gambar dan pesan teks" [7]. Penelitian ini menyatakan bahwa teknik kriptografi algoritma *Hiil Cipher* dapat meningkatkan keamanan dan kerahasiaan originalitas dari pesan teks dan gambar.

Berdasarkan latar belakang yang sudah dikemukakan diatas, penulis akan membangun sebuah aplikasi kriptografi teks pesan menggunakan modifikasi algoritma *Hill Cipher* dengan Tabel Periodik Unsur Kimia untuk melakukan modifikasi pada hasil *ciphertext* dan Kode Nomor Operator Seluler di Indonesia digunakan untuk melakukan modifikasi pada kunci *Hill Cipher*.

Penelitian ini bertujuan untuk menjaga keaslian pengirim serta menjaga keaslian dan kerahasiaan sebuah data atau informasi, berupa penyandian data atau informasi tersebut agar mempersulit para pihak yang tidak bertanggug jawab akan kejahatan komputer.

A. Kriptografi

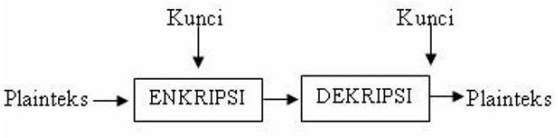
Istilah kriptografi atau *cryptography* berasal dari bahasa Yunani yaitu "*The Art of Secreet Writing*" yang berarti sebuah seni dan ilmu pengetahuan untuk menulis pesan rahasia yang bertujuan agar pesan tidak memiliki makna dan tidak dapat. Kriptografi menggunakan teknik-teknik matematika untuk keamanan data atau informasi seperti penyandian, kredibilitas data serta originalitas data [8].

B. Enkripsi dan Dekripsi

Enkripsi atau *encryption* merupakan proses untuk mengamankan sebuah pesan (*plaintext*) dengan mengubahnya menjadi kode-kode yang sudah disepakati oleh pengirim dan penerima pesan, menjadi pesan rahasia (*ciphertext*) agar data atau informasi yang dikirimkan dapat terjaga kerahasiaannya [9].

Sedangkan, dekripsi atau *decryption* merupakan kebalikan dari proses enkripsi, yaitu merubah pesan rahasia (*ciphertext*) menjadi pesan asli (*plaintext*) dengan mengembalikan kode-kode yang sudah diacak sebelumnya kebentuk *file* asli dengan menggunakan kunci yang sama [10].

Adapun proses Enkripsi dan Dekripsi dapat dilihat pada Gambar 1.



Gambar 1. Proses Enkripsi dan Dekripsi

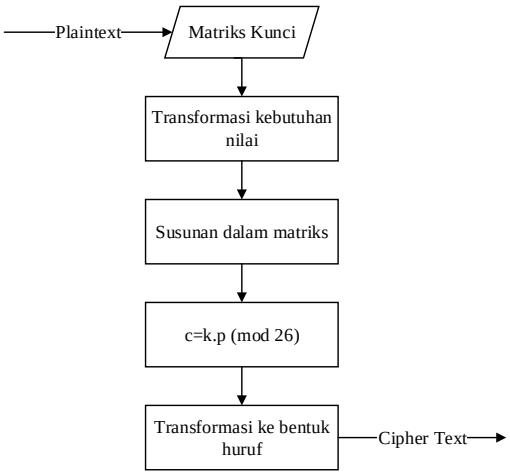
C. Algoritma Hill Cipher

Algoritma *Hill Cipher*, pertama kali dikemukakan oleh ahli matematika Lester S. Hill pada tahun 1929. *Hill Cipher* menggunakan teknik dasar aritmatika *modulo* terhadap matriks sehingga sangat sulit dipecahkan atau dibobol oleh kriptanalis. Implementasi *Hill Cipher* menggunakan teknik perkalian matriks dan teknik *invers* terhadap matriks. Matriks *n x n* merupakan kunci pada *Hill Cipher*, dengan *n* diartikan sebagai ukuran blok [11].

Proses enkripsi pada algoritma *Hill Cipher* dilakukan masing-masing per blok *plaintext*. Ukuran blok-nya disesuaikan dengan ukuran matriks kunci-nya. Pertama, *plaintext* dirubah menjadi angka, mulai dari A=0, B=1, sampai Z=25, yang kemudian akan dibagi teks menjadi deretan blok-blok. Proses enkripsi pada algoritma *Hill Cipher* adalah [12]:

C = K.P
C = *Ciphertext*
K = Kunci
P = *Plaintext*

Tahapan proses enkripsi algoritma *Hill Cipher* dapat dilihat pada Gambar 2 berikut ini.



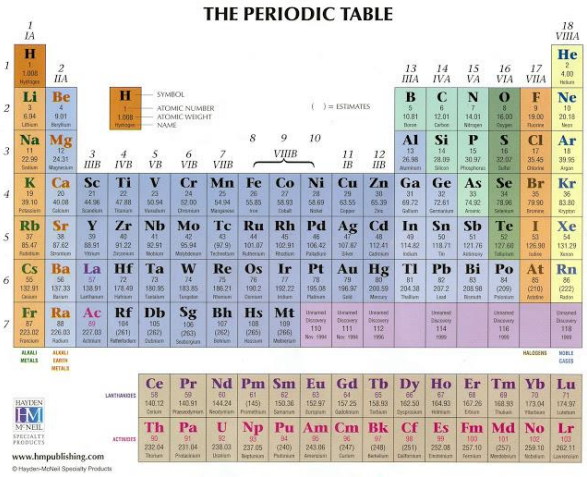
Gambar 2. Tahapan Proses Enkripsi *Hill Cipher*

Langkah awal, *plaintext* yang akan digunakan kemudian diinputkan sesuai dengan matriks kunci, yang selanjutnya akan diproses dan dirubah sesuai

dengan keperluan nilai. Kemudian *plaintext* yang sudah ditransformasi disusun kedalam matriks dan dilakukan proses perkalian c=k.p dan menggunakan *modulo* 26 yang berarti terdapat 26 karakter mulai dari 0 sampai 25, kemudian akan dirubah kebentuk huruf yang selanjutnya akan menghasilkan *ciphertext*.

D. Tabel Periodik Unsur Kimia

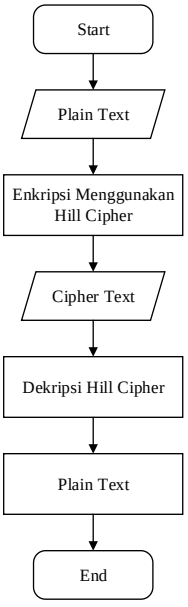
Tabel Periodik Unsur Kimia digunakan untuk melakukan modifikasi pada hasil *ciphertext* algoritma *Hill Cipher* dengan mentransformasikan hasil *ciphertext* kedalam bentuk elemen-elemen yang ada pada Tabel Periodik Unsur Kimia. Adapun Tabel Periodik Unsur Kimia yang digunakan pada penelitian dapat dilihat pada Gambar 3 berikut.



Gambar 3. Tabel Periodik Unsur Kimia

II. METODE PENELITIAN

Penelitian ini terdiri dari beberapa proses tahapan, untuk lebih memperjelas langkah-langkah dalam penelitian ini maka dapat dilihat pada gambar 3 Alur penelitian.



Gambar 3. Alur Penelitian

Tahapan awal dalam penelitian ini adalah *plaintext* yang akan digunakan diinputkan ke dalam sistem. Langkah kedua, kemudian *plaintext* yang telah diinputkan akan dilakukan proses enkripsi dengan menggunakan modifikasi algoritma *Hill Cipher* menggunakan Kode Nomor Operator Seluler di Indonesia sebagai kunci sehingga akan menghasilkan *ciphertext* yang kemudian akan ditransformasikan kedalam bentuk elemen-elemen pada Tabel Periodik Unsur Kimia.

Selanjutnya hasil *ciphertext* yang sudah ditransformasikan kedalam bentuk elemen-elemen pada Tabel Periodik Unsur Kimia tersebut akan di dekripsi menggunakan modifikasi algoritma *Hill Cipher* dengan mengkombinasikan kunci dari Kode Nomor Operator Seluler di Indonesia. Hasilnya akhirnya adalah *ciphertext* akan berubah menjadi pesan asli (*plaintext*) seperti inputan awal sebelum dilakukan tahapan proses enkripsi dan dekripsi.

III. HASIL DAN PEMBAHASAN

A. Kode Nomor Operator Seluler di Indonesia

Kode Nomor Operator Seluler di Indonesia digunakan untuk melakukan modifikasi pada kunci *Hill Cipher*. Adapun daftar Kode Nomor Operator Seluler di Indonesia yang digunakan pada penelitian dapat dilihat pada tabel 1 sebagai berikut:

Tabel 1. Daftar Kode Nomor Operator Seluler di Indonesia

Kode Nomor Operator Seluler	Modifikasi	Keterangan Kode Nomor Operator Seluler
0-8-1-9	1-8-1-9	XL Axiata
0-8-1-1	1-8-1-1	Kartu Halo
0-8-2-1	1-8-2-1	simPATI
0-8-5-3	1-8-5-3	Kartu As
0-8-9-9	1-8-9-9	Kartu TRI/3
0-8-1-5	1-8-1-5	Kartu Indosat M2 Broadband
0-8-5-7	1-8-5-7	Kartu IM3
0-8-8-1	1-8-8-1	Kartu Smartfren
0-8-8-9	1-8-8-9	Kartu Smartfren
0-8-3-1	1-8-3-1	Kartu Axis
0-8-5-5	1-8-5-5	Kartu Matrix

Tabel 1 merupakan beberapa daftar Kode Nomor Operator Seluler di Indonesia yang akan dirubah kedalam bentuk matriks 2×2 yang selanjutnya akan digunakan untuk modifikasi kunci algoritma *Hill Cipher* pada penelitian ini.

B. Enkripsi Hill Cipher

Plaintext yang digunakan pada proses enkripsi penelitian ini adalah kalimat "UNIVERSITAS AMIKOM JOGJA". Selanjutnya, pada penelitian ini algoritma *Hill Cipher* dimodifikasi dengan menambahkan beberapa kunci menggunakan Kode

Nomor Operator Seluler di Indonesia yang kemudian akan disusun ke dalam matriks. Adapun beberapa daftar kunci yang digunakan pada modifikasi algoritma *Hill Cipher* terdapat pada Tabel 2.

Tabel 2. Daftar Kunci

Bentuk Matriks					
K1 =	1	8	K6 =	1	8
	1	9		1	5
K2 =	1	8	K7 =	1	8
	1	1		5	7
K3 =	1	8	K8 =	1	8
	2	1		8	1
K4 =	1	8	K9 =	1	8
	5	3		8	9
K5 =	1	8	K10 =	1	8
	9	9		3	1
			K11 =	1	8
				5	5

Pada Tabel 2 merupakan transformasi bentuk susunan Kode Nomor Operator Seluler di Indoneisa yang akan dijadikan kunci pada modifikasi algoritma hill cipher, yang disusun dengan pola matrix 2×2. Berdasarkan banyaknya blok-blok yang terbentuk dari *plaintext* yang akan di enkripsi, ada 11 (sebelas) kunci yang akan digunakan pada proses enkripsi dan dekripsi pada modifikasi algoritma *Hill Cipher*.

Selanjutnya, kunci-kunci tersebut akan digunakan untuk proses enkripsi dan dekripsi, yang sebelumnya akan diinisialisasikan terlebih dahulu dengan mentransformasikan *plaintext* menjadi deretan angka. Tahap inisialisasi *plaintext* dapat dilihat pada Tabel 3.

Tabel 3. Mengubah *Plaintext* Menjadi Angka

Inisialisasi Pertama									
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**
0	1	2	3	4	5	6	7	8	9
K	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**
10	11	12	13	14	15	16	17	18	19
U	**V**	**W**	**X**	**Y**	**Z**				
20	21	22	23	24	25				

Pada Tabel 3 merupakan hasil inisialisasi pertama yang diperoleh setelah *plaintext* ditransformasikan ke dalam deret angka dan menghasilkan simbol berbentuk angka pada setiap huruf abjad sesuai dengan urutannya, sehingga mendapatkan nilai setiap abjad pada *plaintext* yang akan di enkripsi.

Tabel 4. Bentuk Baru *Plaintext*

Inisialisasi Kedua										
U	**N**	**I**	**V**	**E**	**R**	**S**	**I**	**T**	**A**	**S**
20	13	8	21	4	17	18	8	19	0	18
A	**M**	**I**	**K**	**O**	**M**	**J**	**O**	**G**	**J**	**A**
0	12	8	10	14	12	9	14	6	9	0

Pada Tabel 4 merupakan hasil insialisasi kedua berupa *plaintext* berikut dengan nilai dari setiap abjad yang diambil dari tabel 3. Selanjutnya, *plaintext* beserta nilai dari setiap abjad tersebut dikelompokkan menjadi blok-blok matriks, dimana setiap blok matriks terdiri dari 2 (dua) nilai abjad, kemudian setiap blok tersebut dikalikan dengan kunci yang dibentuk dari Kode Nomor Operator Seluler di Indonesia.

Langkah selanjutnya, deretan angka dibagi menjadi blok-blok matriks yang sesuai dengan kolom matriks kunci, dapat dilihat pada Tabel 5.

Tabel 5. Blok *Plaintext*

BLOK 1		**BLOK 2**		**BLOK 3**		**BLOK 4**	
U	N	I	V	E	R	S	I
20	13	8	21	4	17	18	8
BLOK 5		**BLOK 6**		**BLOK 7**		**BLOK 8**	
T	A	S	A	M	I	K	O
19	0	18	0	12	8	10	14
BLOK 9		**BLOK 10**		**BLOK 11**			
M	J	O	G	J	A		
12	9	14	6	9	0		

Maka *plaintext* yang dihasilkan adalah "U N I V E R S I T A S A M I K O M J O G J A" yang ditransformasikan kedalam angka yaitu "20, 13, 8, 21, 4, 17, 18, 8, 19, 0, 18, 0, 12, 8, 10, 14, 12, 9, 14, 6, 9, 0" kemudian akan dienkripsi menggunakan modifikasi algoritma *Hill Cipher*. Berikut hasil *ciphertext* :

1. Blok 1 (U N)

$$\begin{bmatrix}1 & 8\\1 & 9\end{bmatrix}\begin{bmatrix}20\\13\end{bmatrix}=\begin{bmatrix}124\\137\end{bmatrix} Mod\ 26=\begin{bmatrix}20\\7\end{bmatrix}=\begin{bmatrix}U\\H\end{bmatrix}=\begin{bmatrix}Ca\\N\end{bmatrix}$$

2. Blok 2 (I V)

$$\begin{bmatrix}1 & 8\\1 & 1\end{bmatrix}\begin{bmatrix}8\\21\end{bmatrix}=\begin{bmatrix}176\\29\end{bmatrix} Mod\ 26=\begin{bmatrix}20\\3\end{bmatrix}=\begin{bmatrix}U\\D\end{bmatrix}=\begin{bmatrix}Ca\\Li\end{bmatrix}$$

3. Blok 3 (E R)

$$\begin{bmatrix}1 & 8\\2 & 1\end{bmatrix}\begin{bmatrix}4\\17\end{bmatrix}=\begin{bmatrix}140\\25\end{bmatrix} Mod\ 26=\begin{bmatrix}10\\25\end{bmatrix}=\begin{bmatrix}K\\Z\end{bmatrix}=\begin{bmatrix}Ne\\Mn\end{bmatrix}$$

4. Blok 4 (S I)

$$\begin{bmatrix}1 & 8\\5 & 3\end{bmatrix}\begin{bmatrix}18\\8\end{bmatrix}=\begin{bmatrix}82\\114\end{bmatrix} Mod\ 26=\begin{bmatrix}4\\10\end{bmatrix}=\begin{bmatrix}E\\K\end{bmatrix}=\begin{bmatrix}Be\\Ne\end{bmatrix}$$

5. Blok 5 (T A)

$$\begin{bmatrix}1 & 8\\9 & 9\end{bmatrix}\begin{bmatrix}19\\0\end{bmatrix}=\begin{bmatrix}19\\171\end{bmatrix} Mod\ 26=\begin{bmatrix}19\\15\end{bmatrix}=\begin{bmatrix}T\\P\end{bmatrix}=\begin{bmatrix}K\\P\end{bmatrix}$$

6. Blok 6 (S A)

$$\begin{bmatrix}1 & 8\\1 & 5\end{bmatrix}\begin{bmatrix}18\\0\end{bmatrix}=\begin{bmatrix}18\\18\end{bmatrix} Mod\ 26=\begin{bmatrix}18\\18\end{bmatrix}=\begin{bmatrix}S\\S\end{bmatrix}=\begin{bmatrix}Ar\\Ar\end{bmatrix}$$

7. Blok 7 (M I)

$$\begin{bmatrix}1 & 8\\5 & 7\end{bmatrix}\begin{bmatrix}12\\8\end{bmatrix}=\begin{bmatrix}76\\116\end{bmatrix} Mod\ 26=\begin{bmatrix}24\\12\end{bmatrix}=\begin{bmatrix}Y\\M\end{bmatrix}=\begin{bmatrix}Cr\\Mg\end{bmatrix}$$

8. Blok 8 (K O)

$$\begin{bmatrix}1 & 8\\8 & 1\end{bmatrix}\begin{bmatrix}10\\14\end{bmatrix}=\begin{bmatrix}122\\94\end{bmatrix} Mod\ 26=\begin{bmatrix}18\\16\end{bmatrix}=\begin{bmatrix}S\\Q\end{bmatrix}=\begin{bmatrix}Ar\\S\end{bmatrix}$$

9. Blok 9 (M J)

$$\begin{bmatrix}1 & 8\\ 8 & 9\end{bmatrix}\begin{bmatrix}12\\ 9\end{bmatrix} = \begin{bmatrix}84\\ 177\end{bmatrix} Mod\ 26 = \begin{bmatrix}6\\ 21\end{bmatrix} = \begin{bmatrix}G\\ V\end{bmatrix} = \begin{bmatrix}C\\ Sc\end{bmatrix}$$

10. Blok 10 (O G)

$$\begin{bmatrix}1 & 8\\ 3 & 1\end{bmatrix}\begin{bmatrix}14\\ 6\end{bmatrix} = \begin{bmatrix}62\\ 48\end{bmatrix} Mod\ 26 = \begin{bmatrix}10\\ 22\end{bmatrix} = \begin{bmatrix}K\\ W\end{bmatrix} = \begin{bmatrix}Ne\\ Ti\end{bmatrix}$$

11. Blok 11 (J A)

$$\begin{bmatrix}1 & 8\\ 5 & 5\end{bmatrix}\begin{bmatrix}9\\ 0\end{bmatrix} = \begin{bmatrix}9\\ 45\end{bmatrix} Mod\ 26 = \begin{bmatrix}9\\ 19\end{bmatrix} = \begin{bmatrix}J\\ T\end{bmatrix} = \begin{bmatrix}F\\ K\end{bmatrix}$$

Selanjutnya akan diperoleh hasil *ciphertext* pada tabel 5. Hasi enkripsi.

Tabel 5. Hasil Enkripsi

Kalimat Baru Hasil Enkripsi								
20	7	20	3	10	25	4	10	19
Ca	**N**	**Ca**	**Li**	**Ne**	**Mn**	**Be**	**Ne**	**K**
5	18	18	24	12	18	16	6	21
P	**Ar**	**Ar**	**Cr**	**Mg**	**Ar**	**S**	**C**	**Sc**
10	22	9	19					
Ne	**Ti**	**F**	**K**					

Pada tabel 5 merupakan hasil *ciphertext* diperoleh nilai dan kalimat baru setelah dilakukan proses enkripsi dengan kunci Kode Nomor Operator Seluler di Indonesia menggunakan modifikasi algoritma *Hill Cipher*, yang kemudian ditransformasikan kedalam bentuk elemen-elemen pada Tabel Periodik Unsur Kimia.

Blok yang telah dienkripsi berubah menjadi UN menjadi CaN, IV menjadi CaLi, ER menjadi NeMn, SI menjadi BeNe, TA menjadi KP, SA menjadi ArAr, MI menjadi CrMg, KO menjadi ArS, MJ menjadi CSc, OG menjadi NeTi, JA menjadi FK.

C. Dekripsi Algoritma Hill Cipher

Pada tahapan proses dekripsi algoritma *Hill Cipher* pada dasarnya sama dengan proses enkripsinya. Tetapi, kunci yang digunakan harus dibalik atau di *invers* terlebih dahulu. Tahapan proses dekripsi pada algoritma *Hill Cipher* dapat dirumuskan:

$C = K.P$

$K^{-1}.K = K^{-1}.K.P$

$K^{-1}.C = I.P$

Sehingga Persamaan Proses Dekripsinya adalah :

$P = K^{-1}.C$

Berikut ini adalah proses dekripsi pada blok "UN" :

Blok 1 (U N)

$$\begin{bmatrix}1 & 8\\ 1 & 9\end{bmatrix}\begin{bmatrix}20\\ 13\end{bmatrix} = \begin{bmatrix}124\\ 137\end{bmatrix} Mod\ 26 = \begin{bmatrix}20\\ 7\end{bmatrix} = \begin{bmatrix}U\\ H\end{bmatrix} = \begin{bmatrix}Ca\\ N\end{bmatrix}$$

1. Det K = (1×9) – (1×8) = 1
2. Nilai invers Modulo 1^{-1} mod 26

$$K = 1 \rightarrow \frac{26(1)+1}{1} = 27$$

3. Invers Kunci

$$K^{-1} = \begin{bmatrix}9 & -8\\ -1 & 1\end{bmatrix}$$

4. Matriks kunci *Hill Cipher*

$$27\begin{bmatrix}9 & -8\\ -1 & 1\end{bmatrix} = \begin{bmatrix}243 & -216\\ -27 & 27\end{bmatrix} Mod\ 26 = \begin{bmatrix}9 & 18\\ 25 & 1\end{bmatrix}$$

5. Dekripsi

$$\begin{bmatrix}9 & 18\\ 25 & 1\end{bmatrix}\begin{bmatrix}20\\ 7\end{bmatrix} = \begin{bmatrix}306\\ 507\end{bmatrix} Mod\ 26 = \begin{bmatrix}20\\ 13\end{bmatrix} = \begin{bmatrix}U\\ N\end{bmatrix}$$

Setelah proses dekripsi menggunakan algoritma *Hill Cipher* pada semua blok maka akan didapatkan *plaintext* yaitu "UNIVERSITAS AMIKOM JOGJA".

D. Desain Sistem Antar Muka

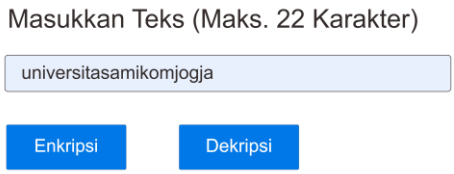
Sistem antarmuka pemakai merupakan sistem tampilan yang memudahkan pengguna (*user*) dalam menggunakan aplikasi. Sistem yang dirancang harus memiliki *user interface* yang baik agar *user* dapat lebih mudah dalam berinteraksi dengan sistem tersebut.

Desain sistem ini menggambarkan atau menjelaskan bagaimana cara pemilihan data yang akan di enkripsi dan di dekripsi. Dengan *desain form* yang baik maka *user* dapat dengan cepat mengenali dan memahami cara kerja dari *form* tersebut, dan hal ini tentu saja menguntungkan bagi *user* tersebut dalam menyelesaikan pekerjaannya.

Berdasarkan rancangan diatas, aplikasi ini dirancang dengan beberapa *form* yaitu:

1. *Form Enkripsi*

Form ini merupakan implementasi dari proses enkripsi *text* menggunakan algoritma *Hill Cipher*, *plaintext* yang di enkripsi adalah kalimat "UNIVERSITAS AMIKOM JOGJA", dilakukan dengan modifikasi kunci menggunakan Kode Nomor Operator Seluler di Indonesia, dapat di lihat pada gambar 4 berikut ini.



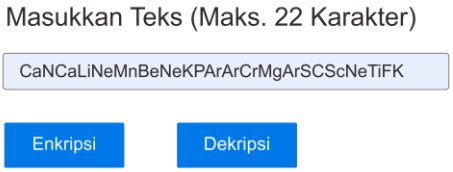
Gambar 4. Input Enkripsi

Setelah di enkripsi menggunakan algoritma *Hill Cipher* maka hasil *ciphertext* akan berubah menjadi *file* rusak berbentuk *symbol* elemen pada tabel periodik unsur kimia, sehinnga terlindungi dari oleh pihak-pihak yang tidak bertanggung jawab. Hasil enkripsi berupa *file* rusak ini akan menyulitkan pihak yang tidak berhak dalam membaca informasi yang ada karena simbol yang dihasilkan bersifat acak dan tidak terbaca. Hasil enkripsi dapat dilihat pada gambar 5.

Gambar 5. Hasil Enkripsi

2. *Form Dekripsi*

Hasil enkripsi kemudian didekripsikan kembali untuk mengembalikan informasi yang telah di acak kebentuk *file* aslinya dengan menggunakan kunci Kode Nomor Operator Seluler di Indonesia, dapat dilihat pada gambar 6 berikut.



Gambar 6. Input Dekripsi

Hasil dekripsi algoritma *Hill Cipher* dapat dilihat pada gambar 7.

Gambar 7. Hasil Dekripsi

IV. KESIMPULAN

Berdasarkan dari analisa, perancangan dan implementasi pada aplikasi penyembunyian atau penyandian pesan dengan menggunakan modifikasi algoritma *Hill Cipher* dengan Tabel Periodik Unsur Kimia menggunakan Kode Nomor Operator Seluler di Indonesia dapat diambil kesimpulan bahwa, pengujian pesan teks berhasil dilakukan sesuai tepat dengan alur atau langkah-langkah sehingga menghasilkan *ciphertext* yang berupa pengacakan huruf abjad yang sudah ditransformasikan kedalam bentuk elemen-elemen pada Tabel Periodik Unsur Kimia.

DAFTAR PUSTAKA

[1] D. Ariyus, Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi, Yogyakarta: Andi Offset, 2008.

[2] D. A. Meko, "Perbandingan Algoritma DES, AES, IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data," *Jurnal Teknologi Terpadu, Vol. 4, No. 1*, pp. 8-15, 2018.

[3] A. P. U. Siahaan, "Algoritma Genetika Untuk Pembentukan Kunci Matriks 3 X 3 Pada Kriptografi Hill Cipher," *In Seminar Nasional Sains Dan Teknologi*, pp. 1-6, 2016.

[4] J. C. &. M. Davis, Extending the Hill Cipher, 2010.

[5] M. Z. S. D. H. Akbar Serdano, "Pengamanan Pesan Menggunakan Algoritma Hill Cipher Dalam Keamanan Komputer," *Jurnal Mahajana Informasi, Vo.4, No.2*, pp. 5-9, 2019.

[6] R. T. Tarigan, "Pengamanan Pesan Rahasia Menggunakan Metode Algoritma Hill Cipehr," *Publikasi Ilmiah Teknologi Informasi Neumann*, pp. 77-81, 2018.

[7] S. H. S. T. I. O. K. Indra Gunawan, "Fungsi Algoritma Kriptografi Hill Cipher Untuk Pengamanan File Gambar Dan Pesan Teks," *TECHSI: Vol. 10, No. 1*, pp. 119-128, 2018.

[8] R. Munir, Kriptografi, Bandung: Informatika, 2007.

[9] P. A. d. s. Alun, Implementasi Algoritma Hill Cipher Sebagai media Steganografi Mneggunakan Metode LSB, 2009.

[10] Munawar, "Perancangan Algoritma Sistem Keamanan Data Menggunakan Metode Kriptografi Asimetris," *Jurnal Ilmiah Komputer dan Informatika*, 2012.

[11] A. H. Hasugian, "Implementasi Algoritma Hill Cipher Dalam," *Pelita Informatika Budi Darma, Volume : IV, Nomor: 2*, pp. 115-122, 2013.

[12] E. P. D. A. Kaharuddin, "Kombinasi Arnold Cat Map dan Modifikasi Hill Cipher Menggunakan Kode Bunyi Beep BIOS PHOENIX," *Jurnal Ilmiah SISFOTENIKA, Vol. 9, No. 2*, pp. 159-168, 2019.