Kombinasi Arnold Cat Map dan Modifikasi *Hill Cipher* Menggunakan Kode Bunyi Beep BIOS PHOENIX

Combination of Arnold Cat Map and Modification of Hill Cipher Uses Beep Sound Code BIOS PHOENIX

Kaharuddin *[1], Elvis Pawan[2], Dony Arius[3]
[1,2,3]Universitas Amikom Yogyakarta Jl. Ring Road Utara, Yogyakarta, Tlp (0274) 884201
[1,2,3]Magister Teknik Informatika, Universitas Amikom Yogyakarta
e-mail: ***[1]**kahar.osvaldo@gmail.com, [2]elvispawan09@gmail.com, [3]dony.a@amikom.ac.id

Abstrak

Menjaga dan mengamankan suatu data rahasia adalah sesuatu yang wajib dilakukan baik itu data pribadi, organisasi, perusahaan ataupun bidang pemerintahan akan tetapi tidak sedikit yang belum mengetahui cara untuk mengamankan data dan informasi, secara khusus pada sebuah pesan, sehingga penelitian ini dilakukan untuk memberikan cara melakukan pengamanan atau enkripsi terhadap pesan atau informasi. Dalam penelitian ini digunakan kolaborasi antara algoritma Hill Cipher dan algoritma Arnold Cat Map, hal ini dilakukan dengan tujuan dapat memberikan sebuah hasil yang maksimal terhadap hasil enkripsi data atau pesan. Dalam penerapannya algoritma Hill Cipher akan dimodifikasi dengan menggunakan kode bunyi beeb bios phoenix. Algoritma Hill Cipher dan Arnold Cat Map cocok untuk di kombinasikan karena akan menghasilkan enkripsi yang cukup kuat dibandingkan dengan algoritma yang hanya melakuakan enkripsi satu kali, misalnya pada algoritma MD4, MD5 RSA dan beberapa algortima lain, hal ini diakibatkan karena hasil enkripsi berbasis teks dari algoritma Hill Cipher akan dilakukan enkripsi sekali menggunakan algoritma Arnold Cat Map yang berbasis gambar sehingga terdapat dua kali proses enkripsi yang dilakukan. Penelitian ini menghasilkan modifikasi sebuah algoritma Hill Cipher dan Arnold Cat Map dalam proses enkripsi dan dekripsi untuk meningkatkan keamanan suatu data dan informasi.
Kata kunci*—Hill Cipher, Arnold Cat Map, Kriptografi, Steganografi*

Abstract

Maintaining and securing a secret data is something that must be done either personal, organizational, corporate or governmental data, but not a few who do not know how to secure data and information, specifically on a message, so that this research is conducted to provide a way of doing security or encryption of messages or information. In this research used collaboration between the Hill Cipher algorithm and Arnold Cat Map algorithm, this was done with the aim of being able to provide a maximum result of the results of data encryption or messages. In its application, the Hill Cipher algorithm will be modified using a bios phoenix sound code. Hill Cipher and Arnold Cat Map algorithms are suitable to be combined because they will produce strong enough encryption compared to algorithms that only do one-time encryption, for example in the MD4, MD5 RSA algorithm, and some other algorithms, this is due to the result of text-based encryption of algorithms Hill Cipher will be encrypted once using the image-based Arnold Cat Map algorithm so that the encryption process is done twice. This research resulted in the modification of a Hill Cipher algorithm and Arnold Cat Map in the process of encryption and decryption to improve the security of data and information
Keywords— *Hill Cipher, Arnold Cat Map, Cryptography, Steganography*

1. PENDAHULUAN

Dalam mengirim sebuah pesan pribadi mesti tidak ingin diketahui oleh orang-orang yang tidak berkepentingan dengan pesan yang dikirim, akan tetapi persoalan yang terjadi adalah bagaimana dapat percaya begitu saja terhadap orang ataupun jasa penitipan pesan bahwa pesan tersebut benar-benar aman untuk sampai pada orang yang ditujukan. Untuk mengatasi hal tesbut maka dilakukanlah enkripsi demi menjaga kerahasiaan dari pesan itu sendiri.

Pada penelitian ini diberikan bagaimana cara mengamankan sebuah pesan yang hendak dikirim, dengan menggunakan bantuan algoritma *Hill Cipher* dan *Arnold Cat Map.* Penggabungan kedua algoritma ini tidak lain mempunyai tujuan agar keamanan pesan dapat benar-benar terjaga, hal ini disebabkan karena pengaman pesan dilakukan dengan cara enkripsi sebanyak dua kali, enkripsi yang pertama adalah merubah pesan asli menjadi *cipher text* hingga menjadi *plain image* selanjutnya dienkripsi lagi menjadi *cipher image.*

Beberapa algoritma yang pernah diciptakan oleh pakar kriptografi diantaranya algoritma DES, algoritma 3DES, algoritma IDEA, algoritma Blowfish, Algoritma RSA, Algoritma MD4, algoritma MD5, Algoritma SHA-1, algoritma McEliecce dan lain-lain. Algoritma tersebut semua sudah diuji kemampuanya oleh para pakar akan tetapi tidak semua metode diatas dapat bertahan dari serangan para penyadap informasi [1].

Enkripsi *Hill Cipher* merupakan suatu cara dalam mengenkripsi sebuah pesan yang menggunakan matriks sebagai kunci [2]. Algoritma *Hill Cipher* juga merupakan salah satu algoritma kriptografi yang memanfaatkan aritmetika modulo dan matriks, setiap karakter pada *plaintext* dan *ciphertext* dikonversikan kedalam angka [3].

Seperti diketahui bahwa dalam bidang pemerintahan tentu sangat banyak hal-hal yang bersifat rahasia yang secara terus menerus dikirkamkan baik itu melalui bantuan internet ataupun melalui jasa penitipan pesan. Masalah lain banyak orang yang ingin melakukan enkripsi terhadap sebuah data yang akan dikirim akan tetapi tidak mengetahui cara dalam melakukan enkripsi tersebut, penelitian ini mencoba memberikan sebuah solusi kepada orang-orang yang memiliki kepentingan dalam bidang itu.

Beberapa penelitian dalam bidang kriptografi dengan menggunakan *hill cipher* diantaranya, Enkripsi dan depkripsi teks menggunakan algoritma *hill cipher* dengan kunci matriks persegi Panjang [3]. kelemahan pada penelitian ini adalah teks yang di enkripsi hanya menyamarkan sebuah pesan dalam matrik persegi panjang kemungkinan untuk diketahui sangat cepat karena tidak ada kombinasi dengan algoritma lain dalam proses enkripsi misalnya dengan menggabungkan audio, gambar dan lain-lain. Penelitian sejenis dengan judul algoritma genetika untuk pembentukan kunci matriks 3x3 pada kriptografi *Hill Cipher* [2]. Kelemahan dari penelitian ini semua *plaintext* diterjemahkan ke dalam angka sehingga kemungkinan untuk muncul angka secara berulang sangat besar.

Penelitianlain dengan melakukan enkripsi pada gambar dengan menggunakan algoritma *Hill Cipher* [4]. Penelitian ini membahas tentang bagaimana cara melakukan enkripsi dengan menggunakan gambar dan membandingkan dengan *hill cipher* yang asli. Penelitan yang berjudul *dinamyc key matrix of Hill cipher using genetic algorithm* [5]. Penelitian lain yang membahas implementasi algoritma Hill Cipher pada penyediaan data [6]. Pada penelitian ini menyarankan adanya pengembangan terhadap modifikasi algoritma dalam kriptografi.

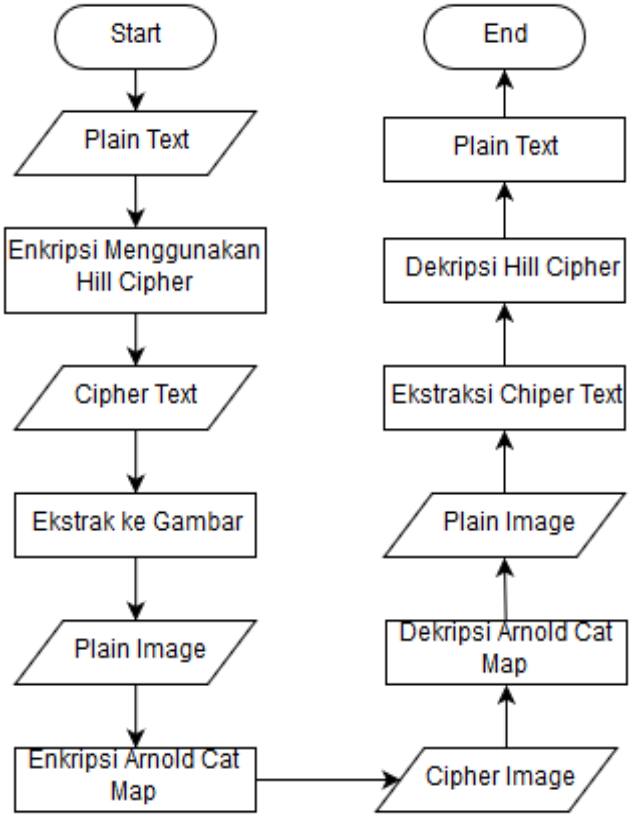
Penelitian lain yang membahas ekripsi citra digital dengan bantuan algoritma *Arnold Cat Map* dan algoritma *non linear chaotic*[7]. Pada penelitian ini menyimpulkan bahwa analisis histogram memperlihatkan perbedaan antara *plain image* dan *cipher image,* dimana intesitas *pixel* pada *cipher image* menyebar di seluruh ruang nilai *pixel*, sehingga serangan menggunakan analisis statistik tidak dimungkinkan. Penelitian lain yang membahas cara enkripsi dengan bantuan algoritma *mono alphabetic* dan *one time pad* [8]. Kelemahan pada penelitian ini memiliki mekasnisme enkripsi yang sangat sederhana sehingga kemungkinan untuk mengetahui proses dekripsi sangat mungkin.

Penelitian yang menggunakan bantuan algoritma *Arnold Cat Map* [9]. Pada penelitian tersebut melakukan modifikasi Algoritma *Arnold Cat Map* sehingga memiliki pola yang berbeda dari sebelumnya, dan yang terakhir adalah penelitian yang menggunakan bantuan *algoritma Arnold Cat Map* [10]. Pada penelitian tersebut membuat skema permutasi enkripsi gambar dengan permutasi *bit-level* pada algoritma *Anold Cat Map*, dan untuk melakukan difusi tingkat piksel menggunakan affince cipher.

2. METODE PENELITIAN

2.1 Alur Penelitian

Untuk lebih memperjelas langkah-langkah dalam penelitian ini maka dapat dilihat pada gambar 2.1. Alur penelitian.



Gambar 1. Alur Penelitian

Pada penelitian ini memiliki pedoman langkah-langkah agar dapat diperoleh gambaran alur data, langka pertama dengan menginput *plain teks* pada sistem, langkah kedua *plain text* tersebut akan dienkripsi menggunakan algoritma *Hill Cipher* yang telah dimodifikasi dengan menggunakan kode bunyi *beeb bios phoenix* sehingga menghasilkan *cipher text*, setelah *chipper teks* didapatkan langkah ketiga mendapatkan *cipher text* kemudian langkah keempat akan diekstrak kedalam sebuah gambar langkah kelima mendapatkan *plain image*, langkah keenam dilakukan enkripsi dengan menggunakan algoritma *Arnold Cat Map*, langkah ketujuh didapatkan *cipher image*, selanjutnya langkah kedelapan dilakukan proses dekripsi menggunakan algoritma *Arnold Cat Map* sehingga pada langkah kesembilan didapatkan kembali *plain image*, pada langkah kesepuluh chiper text yang ada di plain image kemudian diekstraksi kedalam bentuk teks, kemudian pada langkah kesebelas dilakukan proses dekripsi dengan menggunakan algoritma *Hill Cipher*, pada langkah kedua belas didapatkan *plain text* semula.

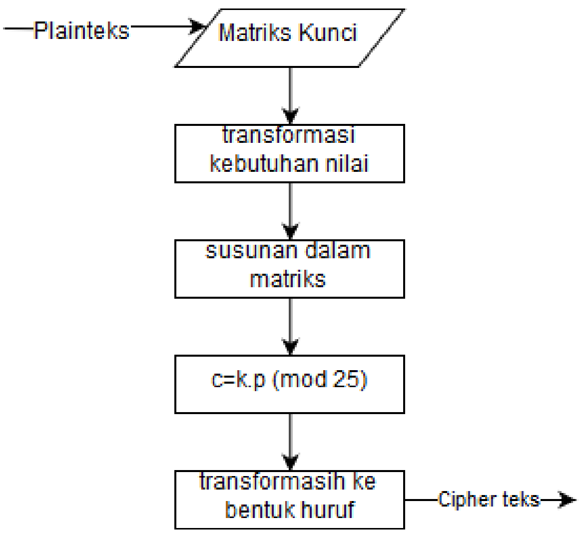
2.2 *Hill Cipher*

Hill Cipher merupakan algoritma kriptografi klasik yang sangat sulit dipecahkan oleh kriptanalis, dasar dari teknik *Hill Cipher* adalah aritmatika modulo terhadap matriks. Pada penerapannya, *Hill Cipher* menggunakan teknik perkalian matriks dan teknik *invers* terhadap matriks. Kunci pada *Hill Cipher* adalah matriks n x n dengan n merupakan ukuran blok [6].

Dalam melakukan enkripsi pada algoritma *Hill Cipher* dilakukan blok per blok *plainteks*. Ukuran blok tersebut sama dengan ukuran matriks kunci. Sebelum membagi teks menjadi deretan blok-blok, *plainteks* mula-mula dikonversi menjadi angka, misalnya A=0, B=1, sampai Z=25. Secara matematis, proses enkripsi pada *Hill Cipher* adalah:

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

Agar dapat diperoleh gambaran proses melakukan enkripsi maka dijelaskan melalui langkah-langkah seperti pada Gambar 2.2 Gambaran Proses enkrips *Hill Cipher*



Gambar 2. Gambaran Proses enkripsi *Hill Cipher*

Tahap pertama plainteks yang telah tersedia selanjutnya diinputkan sesuai matriks kunci, kemudian diproses sesuai dengan transformasi kebutuhan nilai, langkah ketiga dengan menyusun kedalam matriks selanjutnya dilakukan proses perkalian c=k.p dan mod 25 karena kareakter disusun mulai dari 0 sampai 25 selanjutnya di transformasikan ke bentuk huruf untuk mendapatkan *cipherteks*

2.3 *Arnold Cat Map*

Metode *Arnold's Cat Map (ACM)* pertama kali perkenalkan oleh seorang ahli matematik Rusia yang bernama Vladimir I. Arnold, pada tahun 1960 yang mempublikasikan algoritmanya tersebut dengan memakai citra kucing [7]. Algoritma *Arnold's Cat Map* dapat didefenisikan sesuai Persamaan 1.

$$\begin{bmatrix} X_{i+1} \\ Y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix} \begin{bmatrix} X_i \\ Y_i \end{bmatrix} mod\ (N) = \ldots \quad (1)$$

Yang mana (x dan y) posisi pixel di dalam citra berukuran N x N dan (xi+1, yi+1) sehingga posisi pixel yang baru setelah transformasi, b dan c adalah bulat positif sembarang. Determinan matriks harus sama dengan 1 dengan demikian hasil transformasinya tetap berada

pada area citra yang sama (area-preserving). Algoritma *Arnold Cat Map* termasuk one-to-one mapping, yang berarti setiap titik dalam matriks dapat ditransformasikan ke titik lainnya.

2.4 Kode Bunyi *Beep* PHOENIX

Untuk melakukan modifikasi pada kunci *Hill Cipher* digunakan kode bunyi *beep* BIOS PHOENIX. Adapun kode bunyi *beep* yang digunakan dapat dilihat pada tabel 1. Daftar Kode Bunyi *Beep* BIOS PHOENIX.

Tabel 1. Daftar Kode Bunyi *Beep* BIOS PHOENIX

Kode *Beep*	Deskripsi
1-1-2-1	*Get CPU Type*
1-1-2-3	*Initialize System hardware*
1-1-3-1	*Initialize chipset registers with initial value*
1-1-3-2	*Set in POST flag*
1-1-4-1	*Initialize cache to initial values*
1-1-4-3	*Initialize Input / Output*
1-2-1-1	*Initialize power management*
1-2-1-3	*Jump to User Patch 0*
1-2-2-1	*Initialize timer initialization*
1-2-4-1	*Reset programmable Interrupt Controller*

Tabel 1 adalah daftar kode bunyi *beep* yg digunakan, setiap kode bunyi *beep* memiliki makna yang berbeda-beda untuk memberikan indikasi kerusakan pada PC. Sebagai contoh kode 1-1-2-1 akan di ubah menjadi bentuk matriks 2×2 yang berguna segai kunci pada algoritma *Hill Cipher.*

3. HASIL DAN PEMBAHASAN

3.1 Enkripsi *Hill Cipher*

Pada Penelitian ini *plaintext* yang di enkripsi adalah kalimat “RENCANA OKTOBER WISUDA”, pada penelitian ini *Hill Cipher* dikembangkan dengan cara memodifikasi kunci menggunakan matriks yang berdasarkan kepada kode bunyi *Beep BIOS Pheonix*. Beberapa daftar kunci yang digunakan pada modifikasi algoritma *Hill Cipher* terdapat pada tabel 2 Daftar Kunci.

Tabel 2. Daftar Kunci

Bentuk Matriks			
k1 =	$\begin{matrix}\mathbf{1} & \mathbf{1} \\ \mathbf{2} & \mathbf{1}\end{matrix}$	k6 =	$\begin{matrix}1 & 1 \\ 2 & 1\end{matrix}$
k2 =	$\begin{matrix}\mathbf{1} & \mathbf{1} \\ \mathbf{2} & \mathbf{3}\end{matrix}$	k7 =	$\begin{matrix}1 & 1 \\ 2 & 3\end{matrix}$
k3 =	$\begin{matrix}\mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{1}\end{matrix}$	k8 =	$\begin{matrix}1 & 1 \\ 1 & 1\end{matrix}$
k4 =	$\begin{matrix}\mathbf{1} & \mathbf{1} \\ \mathbf{3} & \mathbf{2}\end{matrix}$	k9 =	$\begin{matrix}1 & 1 \\ 3 & 2\end{matrix}$
k5 =	$\begin{matrix}\mathbf{1} & \mathbf{1} \\ \mathbf{4} & \mathbf{1}\end{matrix}$	k10 =	$\begin{matrix}1 & 1 \\ 4 & 1\end{matrix}$

Pada Tabel 2 Merupakan perubahan bentuk susunan kode bunyi *beeb BIOS phoenix* menjadi pola matriks 2×2 yang berfungsi sebagai kunci pada algoritma *Hill Cipher*. Berdasarkan banyaknya blok yang terbentuk dari kalimat yang di enkripsi maka terpilih sebanyak sepuluh kunci untuk proses enkripsi dan dekripsi pada algoritma *Hill Cipher*.

Setelah mendapatkan kunci yang digunakan untuk proses enkripsi dan dekripsi selanjutnya dilakukan inisialisasi yaitu mengubah *plaintext* menjadi deretan angka yang ditampilkan pada Tabel 3 Mengubah *plaintext* menjadi angka.

Tabel 3. Mengubah *Plaintext* Menjadi Angka

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

Pada Tabel 3 dilakukan inisialisasi pertama sehingga diperoleh simbol berbentuk angka pada masing-masing huruf abjad sesusai dengan urutannya. Proses inisialisasi ini bertujuan untuk mendapatkan nilai setiap abjad pada kalimat yang di enkripsi.

Tabel 4. Bentuk Baru *Plaintext*

Inisialisasi Kedua																			
R	**E**	**N**	**C**	**A**	**N**	**A**	**O**	**K**	**T**	**O**	**B**	**E**	**R**	**W**	**I**	**S**	**U**	**D**	**A**
17	4	13	2	0	13	0	14	10	19	14	1	4	17	22	8	18	20	3	0

Pada Tabel 4 merupakan *plain text* beserta dengan nilai dari setiap abjad yang diambil dari tabel 3. Setiap nilai dari abjad plain text dikelompokkan menjadi blok-blok matriks setiap blok terdiri dari dua nilai abjad, setiap blok dikalikan dengan kunci yang dibentuk dari kode bunyi *Beep BIOS Phoenix*.

Pembagian deretan angka menjadi blok matrix yang sesuai dengan urutan RE=17dan 4, NC= 13 dan 2, AN= 0 dan 13, AO=0 dan 14, KT= 10 dan 19, OB =14 dan 1, ER= 4 dan 17, WI=22 dan 8, SU= 18 dan 20, DA= 3 dan 0.

a. C(RE)

$$\begin{bmatrix}1 & 1\\ 2 & 1\end{bmatrix}\begin{bmatrix}17\\ 4\end{bmatrix} = \begin{bmatrix}17+4\\ 34+4\end{bmatrix} = \begin{bmatrix}21\\ 38\end{bmatrix} \ mod\ 26 = \begin{bmatrix}21\\ 12\end{bmatrix} = \begin{bmatrix}V\\ M\end{bmatrix}$$

b. C(NC)

$$\begin{bmatrix}1 & 1\\ 2 & 3\end{bmatrix}\begin{bmatrix}13\\ 2\end{bmatrix} = \begin{bmatrix}13+2\\ 26+6\end{bmatrix} = \begin{bmatrix}15\\ 32\end{bmatrix} \ mod\ 26 = \begin{bmatrix}15\\ 6\end{bmatrix} = \begin{bmatrix}P\\ G\end{bmatrix}$$

c. C(AN)

$$\begin{bmatrix}1 & 1\\3 & 1\end{bmatrix}\begin{bmatrix}0\\13\end{bmatrix} = \begin{bmatrix}0+13\\0+13\end{bmatrix} = \begin{bmatrix}13\\13\end{bmatrix} mod\ 26 = \begin{bmatrix}13\\13\end{bmatrix} = \begin{bmatrix}N\\N\end{bmatrix}$$

d. C(AO)

$$\begin{bmatrix}1 & 1\\3 & 2\end{bmatrix}\begin{bmatrix}0\\14\end{bmatrix} = \begin{bmatrix}0+14\\0+28\end{bmatrix} = \begin{bmatrix}14\\28\end{bmatrix} mod\ 26 = \begin{bmatrix}14\\2\end{bmatrix} = \begin{bmatrix}O\\C\end{bmatrix}$$

e. C(KT)

$$\begin{bmatrix}1 & 1\\4 & 1\end{bmatrix}\begin{bmatrix}10\\19\end{bmatrix} = \begin{bmatrix}10+19\\40+19\end{bmatrix} = \begin{bmatrix}29\\59\end{bmatrix} mod\ 26 = \begin{bmatrix}3\\7\end{bmatrix} = \begin{bmatrix}D\\H\end{bmatrix}$$

f. C(OB)

$$\begin{bmatrix}1 & 1\\4 & 3\end{bmatrix}\begin{bmatrix}14\\1\end{bmatrix} = \begin{bmatrix}14+1\\56+3\end{bmatrix} = \begin{bmatrix}15\\59\end{bmatrix} mod\ 26 = \begin{bmatrix}15\\7\end{bmatrix} = \begin{bmatrix}P\\H\end{bmatrix}$$

g. C(ER)

$$\begin{bmatrix}1 & 2\\1 & 1\end{bmatrix}\begin{bmatrix}4\\17\end{bmatrix} = \begin{bmatrix}4+34\\4+17\end{bmatrix} = \begin{bmatrix}38\\21\end{bmatrix} mod\ 26 = \begin{bmatrix}12\\21\end{bmatrix} = \begin{bmatrix}M\\V\end{bmatrix}$$

h. C(WI)

$$\begin{bmatrix}1 & 2\\1 & 3\end{bmatrix}\begin{bmatrix}22\\8\end{bmatrix} = \begin{bmatrix}22+16\\22+24\end{bmatrix} = \begin{bmatrix}38\\46\end{bmatrix} mod\ 26 = \begin{bmatrix}12\\20\end{bmatrix} = \begin{bmatrix}M\\U\end{bmatrix}$$

i. C(SU)

$$\begin{bmatrix}1 & 2\\2 & 1\end{bmatrix}\begin{bmatrix}18\\20\end{bmatrix} = \begin{bmatrix}18+40\\36+20\end{bmatrix} = \begin{bmatrix}58\\56\end{bmatrix} mod\ 26 = \begin{bmatrix}6\\4\end{bmatrix} = \begin{bmatrix}G\\E\end{bmatrix}$$

j. C(DA)

$$\begin{bmatrix}1 & 2\\4 & 1\end{bmatrix}\begin{bmatrix}3\\0\end{bmatrix} = \begin{bmatrix}3+0\\12+0\end{bmatrix} = \begin{bmatrix}3\\12\end{bmatrix} mod\ 26 = \begin{bmatrix}3\\12\end{bmatrix} = \begin{bmatrix}D\\M\end{bmatrix}$$

Sehingga diperoleh *Cipher text* pada tabel 5. Hasi enkripsi

Tabel 5. Hasil Enkripsi

Kalimat Baru Hasil Enkripsi																			
21	12	15	4	13	13	14	2	3	7	15	7	12	21	14	20	2	4	3	12
V	**M**	**P**	**G**	**N**	**N**	**O**	**C**	**D**	**H**	**P**	**H**	**M**	**V**	**M**	**U**	**G**	**E**	**D**	**M**

Pada tabel 5 diperoleh nilai dan kalimat baru atau disebut dengan *cipher text*, setelah dilakukan proses enkripsi menggunakan algoritma *Hill Cipher*. Blok yang telah dienkripsi berubah menjadi RE menjadi VM, NC menjadi PG, AN menjadi NN, AO menjadi OC, KT menjadi DH, OB menjadi PH, ER menjadi MV, WI menjadi MU, SU menjadi GE, DA menjadi DM.

3.2 *Arnold Cat Map*

Algoritma *Arnold Cat Map* digunakan untuk melakukan proses enkripsi kedua. *Cipher Text* yang telah diperoleh pada proses enkripsi menggunakan *Hill Cipher*. Betujuan untuk memberikan keamanan ganda terhadap informasi atau data yang akan dikirim. Secara garis besar algoritma *Arnold Cat Map* bekerja dengan cara melakukan pengacakan *pixel-pixel* citra sesuai dengan nilai *p* dan *q* serta jumlah iterasi yang ditentukan. Proses pertama enkripsi menggunakan algoritma *Arnold Cat Map* melakukan yaitu ekstraki teks ke gambar.

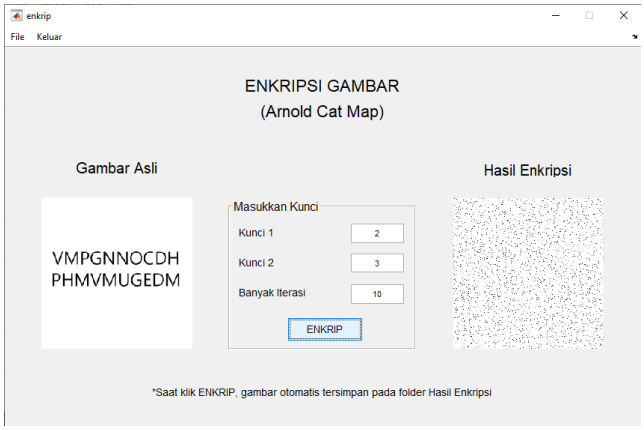
Cipher Text yang telah diperoleh dari hasil enkripsi menggunakan *Hill Cipher* kemudian di ekstraksi kedalam citra warna, grayscale ataupun *biner* dengan format file.JPEG, untuk melihat hasil ekstraksi teks pada gambar dapat dilihat pada gambar 3.1 *Plain Image.*

Gambar 3. *Plain Image*

Pada Gambar 3.1 merupakan *plain image* yang terbentuk setelah dilakukan ekstraksi dari *cipher text* yang dihasilkan oleh algoritma *Hill Cipher*. Bentuk *plain image* pada gambar 3.1 dapat berupa file JPEG atau PNG.

1. Enkripsi

Proses yang terjadi di dalam setiap *iterasi ACM* adalah pergeseran (*shear*) dalam arah *y*, kemudian dalam arah *x*, dan semua hasilnya (yang mungkin berada di luar area gambar) dimodulokan dengan *N* agar tetap berada di dalam area gambar (*area preserving*). Parameter *ACM*, yaitu *p* dan *q*, dan jumlah iterasi *m*, berperan sebagai kunci rahasia. Untuk melihat hasil enkripsi menggunakan Algoritma *Arnold Cat Map* dapat dilihat pada gambar 2. *Cipher Image*

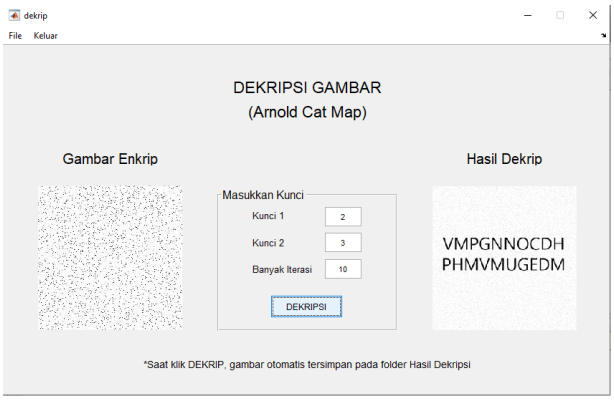


Gambar 4. *Cipher Image*

Pada gambar 3.2 merupakan implementasi dari proses enkripsi citra menggunakan Algoritma Arnold Cat Map, proses enkripsi menggunakan kunci yang pertama yaitu 2 dan kunci yang kedua yaitu 3 dan dilakukan iterasi sebanyak 10 kali sehingga mendapatkan *Chiper Image* yang berada disebelah kanan.

3.3 Dekripsi Algoritma *Arnold Cat Map*

Proses dekripsi yang pertama dilakukan adalah dekripsi *image* yang dienkripsi menggunakan algoritma *Arnold Cat Map*. Proses dekripsi mengembalikan *pixel* yang telah diacak berdasarkan nilai *p*, *q* jumlah iterasi yang digunakan pada proses enkirpsi seperti pada gambar 3.3 Proses Dekripsi ACM



Gambar 5. Proses *Dekripsi* ACM

Pada gambar 3.3 merupakan proses dekripsi *chiper image* menjadi *plain image*, proses dekripsi harus menggunakan kunci yang sama dengan proses enkripsi yaitu kunci pertama adalah 2 dan kunci yang kedua adalah 3 dan dilakukan iterasi sebanyak 10 kali untuk mendapatkan *plain image*.

3.4 Dekripsi algoritma *Hill Cipher*

Dekripsi image berhasil kemudian chipper text yang ada di gambar hasil dekripsi menggunakan *Arnold Cat Map* diekstrak untuk dilakukan dekripsi menggunakan Algoritma *Hill Cipher* untuk mendapatkan *Plain text* atau pesan yang asli. Proses dekripsi pada *Hill Cipher* pada dasarnya sama dengan proses enkripsinya. Akan tetapi kunci harus dibalik (invers) terlebih dahulu. Secara matematis, proses dekripsi pada *Hill Cipher* dapat diturunkan dari persamaan berikut :

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

Sehingga Persamaan Proses Dekripsinya adalah :

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

Berikut ini adalah proses dekripsi pada blok “RE” :

$$\begin{bmatrix}1 & 1\\2 & 1\end{bmatrix}\begin{bmatrix}17\\4\end{bmatrix} = \begin{bmatrix}17 & + & 4\\34 & + & 4\end{bmatrix} = \begin{bmatrix}21\\38\end{bmatrix} mod\ 26 = \begin{bmatrix}21\\12\end{bmatrix} = \begin{bmatrix}V\\M\end{bmatrix}$$

Det K = (1×1) – (2×1) = -1

1^{-1} Mod 26 = $x = 1 \text{ Mod } 26$

$x = 1 + 26\ x$

$x = \frac{1+26}{-1} = -27$

$K^{-1} = -27\begin{bmatrix}1 & -1\\-2 & 1\end{bmatrix} = \begin{bmatrix}-27 & 27\\54 & -27\end{bmatrix} Mod\ 26$

$= \begin{bmatrix}25 & 1\\2 & 25\end{bmatrix}\begin{bmatrix}21\\12\end{bmatrix} = \begin{bmatrix}525 & + & 12\\42 & + & 300\end{bmatrix} = \begin{bmatrix}537\\342\end{bmatrix}$

$\begin{bmatrix}537\\342\end{bmatrix} \text{ mod } 26 = \begin{bmatrix}17\\4\end{bmatrix} = \begin{bmatrix}R\\E\end{bmatrix}$

Setelah proses dekripsi menggunakan algoritma *Hill Cipher* pada semua blok maka akan didapatkan *plain text* yaitu “RENCANA OKTOBER WISUDA”.

4. KESIMPULAN

Setelah melakukan proses analisis terdapat beberapa kesimpulan yang dapat ditarik dari penelitian ini :

a. Dalam melakukan modifikasi *enkripsi* dan *dekripsi* secara manual dengan menggunakan algoritma *Hill Cipher* dan *Arnold Cat Map* memiliki alur yang cukup Panjang, mulai dari mengubah bentuk susunan kode bunyi *beeb BIOS Phoenix* menjadi bentuk perkalian matriks 2×2 kemudian melakukan operasi *modulus* 26 untuk mendapatkan *cipher text*, selajutnya cipher teks diekstrak menjadi file.JPG atau file.PNG yang digunakan sebagai *plain image* untuk melakukan enkripsi menggunakan algoritma Arnold Cat Map.
b. Aplikasi yang telah dirancang dapat membantu *user* untuk melakukan enkripsi dengan mengacu pada cara kerja algoritma *Hill Cipher dan Arnold Cat Map (ACM).*

5. SARAN

Beberapa hal yang perlu diperhatikan dalam melakukan penelitian dalam bidang *cryptography* :

a. Sampai pada saat dilakukan penelitian ini belum ditemukan sebuah metode yang benar-benar dapat menguji ketahanan sebuah algoritma, sehingga hal tersebut dapat diteliti lebih lanjut bagi calon peneliti dibidang *cryptography*.
b. Untuk mendapatkan hasil enkripsi yang lebih aman calon peneliti selanjutnya dapat melakukan enkripsi pesan atau data dengan menggunakan beberapa metode *cryptography.*

DAFTAR PUSTAKA

[1] Eddy And M. R. Pahlevi, "Pembelajaran Enkripsi Metode Word Auto Key Encryption," *Sisfotenika*, Vol. 4, No. 1, Pp. 23–32, 2014.
[2] A. Putera, U. Siahaan, And A. H. Cipher, "Algoritma Genetika Untuk Pembentukan Kunci Matriks 3 X 3 Pada Kriptografi Hill Cipher," In *Seminar Nasional Sains Dan Teknologi*, 2016, No. November, Pp. 1–6.
[3] A. Hidayat And T. Alawiyah, "Enkripsi dan Dekripsi Teks Menggunakan Algoritma Hill Cipher Dengan Kunci Matriks Persegi Panjang," *J. Mat. Integr.*, Vol. 9, No. 1, Pp. 39–51, 2013.
[4] B. Acharya, S. K. Panigrahy, S. K. Patra, And G. Panda, "Image Encryption Using Advanced Hill Cipher Algorithm," *Int. J. Recent Trends Eng.*, Vol. 1, No. 1, Pp. 663–667, 2009.
[5] A. Putera And U. Siahaan, "Dynamic Key Matrix Of Hill Cipher Using Genetic Algorithm," In *Prosiding Seminar Nasional Pendidikan Teknik Informatika*, 2016, No. Senapati, Pp. 162–166.
[6] A. H. Hasugian, "Implementasi Algoritma Hill Cipher Dalam Penyandian Data," *Pelita Inform. Budi Darma*, Vol. 4, No. 2, Pp. 115–122, 2013.
[7] R. Purba, A. Halim, And I. Syahputra, "Enkripsi Citra Digital Menggunakan Arnold ' S Cat Map dan Nonlinear Chaotic Algorithm," *Jsm Stmik Mikroskil*, Vol. 15, No. 2, Pp. 61–71, 2014.
[8] Sugianto And T. Yuniarto, "Kriptografi Gabungan Menggunakan Algoritma Mono Alphabetic dan One Time," *Sisfotenika*, Vol. 4, No. 1, Pp. 53–63, 2014.
[9] C. Wang And Q. Ding, "A New Two-Dimensional Map With Hidden Attractors," *Entropy*, Vol. 20, Pp. 1–10, 2018.
[10] H. Zhu, C. Zhao, X. Zhang, And L. Yang, "An Image Encryption Scheme Using Generalized Arnold Map and Affine Cipher," *Opt. - Int. J. Light Electron Opt.*, Vol. 125, No. 22, Pp. 6672–6677, 2014.