


## Algoritma hill chiper

jepri ENDO

### Related papers

[Download a PDF Pack](#) of the best related papers 



[Penerapan Algoritma Hill Cipher Dan Least Significant Bit \(LSB\) Untuk Pengamanan Pesan Pa...](#)  
Anita Sindar

[Penerapan Metode Dynamic Cell Spreading \(DCS\) Untuk Menyembunyikan Teks Tersandi Pada Citra](#)  
Taronisokhi Zebua

[makalah kriptografi](#)  
evinda tarigan

# IMPLEMENTASI ALGORITMA HILL CIPHER DALAM PENYANDIAN DATA

Abdul Halim Hasugian

Dosen Tetap STMIK Budi Darma Medan

Jl. Sisingamangaraja No. 338 Sp. Pos Medan

<http://www.stmik-budidarma.ac.id> // Email : [abdul\\_halim.budidarma@gmail.com](mailto:abdul_halim.budidarma@gmail.com)

## ABSTRAK

*Secara umum data dikategorikan menjadi dua, yaitu data yang bersifat rahasia dan data yang tidak bersifat rahasia. Data yang tidak bersifat rahasia biasanya tidak akan terlalu diperhatikan. Yang sangat perlu diperhatikan adalah data yang bersifat rahasia, di mana setiap informasi yang ada didalamnya akan sangat berharga bagi pihak yang membutuhkan karena data tersebut dapat dengan mudah digandakan. Untuk mendapatkan informasi didalamnya, biasanya dilakukan berbagai cara yang tidak sah. Data dapat berupa sebuah file dan berbentuk string.*

*Hill Cipher termasuk kepada algoritma kriptografi klasik yang sangat sulit dipecahkan oleh kriptanalisis apabila dilakukan hanya dengan mengetahui berkas ciphertext saja. Karena Hill Cipher tidak mengganti setiap abjad yang sama pada plaintext dengan abjad lainnya yang sama pada ciphertext karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya.*

*Kata Kunci : Hill Cipher, Enkripsi, Dekripsi*

## 1. Pendahuluan

### 1.1 Latar Belakang Masalah

Keamanan dan kerahasiaan data merupakan salah satu aspek yang sangat penting dalam sistem informasi pada saat ini. Disebabkan pesatnya perkembangan ilmu pengetahuan dan teknologi yang memungkinkan munculnya teknik-teknik baru, yang disalah gunakan oleh pihak-pihak tertentu yang mengancam keamanan dari sistem informasi tersebut. Jatuhnya informasi ke tangan pihak lain dapat menimbulkan kerugian bagi pemilik informasi.

Secara umum data dikategorikan menjadi dua, yaitu data yang bersifat rahasia dan data yang tidak bersifat rahasia. Data yang tidak bersifat rahasia biasanya tidak akan terlalu diperhatikan. Yang sangat perlu diperhatikan adalah data yang bersifat rahasia, di mana setiap informasi yang ada didalamnya akan sangat berharga bagi pihak yang membutuhkan karena data tersebut dapat dengan mudah digandakan. Untuk mendapatkan informasi didalamnya, biasanya dilakukan berbagai cara yang tidak sah. Data dapat berupa sebuah file dan berbentuk string.

Karena itu muncul suatu gagasan yang mengacu pada permasalahan tersebut, yaitu untuk membuat suatu sistem keamanan yang dapat melindungi data yang dianggap penting dengan penyandian data, serta membuat kunci rahasia untuk dapat membuka data tersebut yang sulit untuk di deteksi oleh pihak yang tidak berhak.

Banyak teknik kriptografi yang telah dipergunakan untuk menjaga keamanan data saat ini, contohnya seperti LOKI, GOST, Blowfish, Vigenere, MD2, MD4, RSA dan lain sebagainya. Masing-masing teknik kriptografi tersebut

memiliki kelemahan dan kelebihan. Selain teknik kriptografi yang telah disebutkan di atas masih ada teknik kriptografi lainnya maka disini penulis mencoba membahas mengenai teknik kriptografi Hill Cipher.

Hill Cipher termasuk kepada algoritma kriptografi klasik yang sangat sulit dipecahkan oleh kriptanalisis apabila dilakukan hanya dengan mengetahui berkas ciphertext saja. Karena Hill Cipher tidak mengganti setiap abjad yang sama pada plaintext dengan abjad lainnya yang sama pada ciphertext karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya.

### 1.2 Perumusan Masalah

Berdasarkan uraian latar belakang masalah diatas, maka yang menjadi perumusan masalah adalah

1. Bagaimana menerapkan teknik penyandian data menggunakan metode hill cipher?
2. Bagaimana merancang sebuah aplikasi penyandian data dengan metode hill cipher?
3. Bagaimana implementasi hill cipher bisa digunakan oleh orang lain?

### 1.3 Batasan Masalah

Dari uraian perumusan masalah di atas, agar tidak menyimpang dari tujuan yang diharapkan maka dibuat beberapa pembatasan masalah antara lain :

1. Data yang diproses berupa karakter (string).
2. Melakukan enkripsi dan dekripsi hill cipher terhadap record
3. Panjang karakter yang dienkripsi maksimal lebih dari seratus karakter

4. Penulis membatasi basis matriks kunci yang digunakan adalah perkalian  $2 \times 2$  dan elemen berupa bilangan bulat.

#### 1.4 Tujuan Penelitian

Adapun yang menjadi tujuan penelitian ini adalah :

1. Mengetahui sistem kriptografi baik secara teoritis maupun mengaplikasikan metode algoritma tersebut pada data dengan menggunakan algoritma hill cipher.
2. untuk mengkaji sekaligus menganalisa bagaimana metode hill cipher digunakan dalam penyandian data..
3. Mengimplementasikan hill cipher untuk keamanan data.

#### 1.5 Manfaat Penelitian

Adapun yang menjadi manfaat dalam penelitian ini adalah :

1. Sebagai bahan perbandingan bagi penulis lain mengenai metode kriptografi yang telah ada pada saat ini.
2. Dapat digunakan untuk pengamanan data.
3. Dapat memperkaya literature mengenai kriptografi khususnya algoritma hill cipher, sehingga nantinya dapat bermamfaat untuk menjaga keamanan data dan dapat diimplementasikan.

## 2. Landasan Teori

### 2.1 Kriptografi

Kriptografi (*cryptography*) berasal dari Bahasa Yunani: "*cryptos*" artinya "*secret*" (rahasia), sedangkan "*graphein*" artinya "*writing*" (tulisan), Jadi, kriptografi berarti "*secret writing*" (tulisan rahasia).

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. (Rinaldi Munir, 2006)

Definisi yang digunakan di dalam buku menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Definisi ini mungkin cocok pada masa lalu di mana kriptografi digunakan untuk keamanan komunikasi penting seperti komunikasi di kalangan militer, diplomat, dan mata-mata . Namun saat ini kriptografi lebih dari sekadar *privacy*, tetapi juga untuk tujuan *data integrity*, *authentication*, dan *non-repudation*.

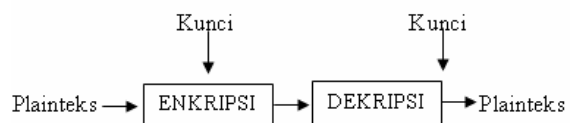
#### 2.1.1 Enkripsi

Enkripsi merupakan bagian dari kriptografi, dan merupakan hal yang sangat penting supaya keamanan data yang dikirimkan bisa terjaga kerahasiaannya. Enkripsi bisa diartikan dengan

chiper atau kode, di mana pesan asli (plaintext) diubah menjadi kode-kode tersendiri sesuai metode yang disepakati oleh kedua belah pihak, baik pihak pengirim pesan maupun penerima pesan. ( Andy Pramono, 2009)

#### 2.1.2 Dekripsi

Dekripsi merupakan proses sebaliknya dari enkripsi yaitu mengembalikan sandi-sandi atau informasi yang telah dilacak kebentuk file aslinya dengan menggunakan kunci atau kode. (Munawar, 2012)



Gambar 1 Proses Enkripsi Dan Dekripsi  
(sumber : Andy Pramono, 2009)

### 2.2 Karakteristik Sistem Kriptografi

Sistem kriptografi dapat dikarakteristikan berdasarkan (Rifki Sadikin, 2012):

1. Tipe Operasi dipakai dalam enkripsi dan dekripsi  
Dua tipe yang dipakai dalam enkripsi dan dekripsi substitusi, elemen pesan (karakter, byte atau bit) ditukar / disubstitusikan dengan elemen lain dari ruang pesan.
2. Tipe kunci yang dipakai  
Umumnya sistem kriptografi klasik dan beberapa system kriptografi modern menggunakan kunci yang sama pada sisi penyandian dan penyulih sandi. Sistem kriptografi seperti ini disebut dengan kriptografi dengan kunci simetri.
3. Tipe pengolahan pesan  
Ketika melakukan penyandian pesan yang akan dienkripsi ataupun didekripsi diolah persatuan blok elemen disebut dengan block cipher.

### 2.3 Algoritma Kriptografi

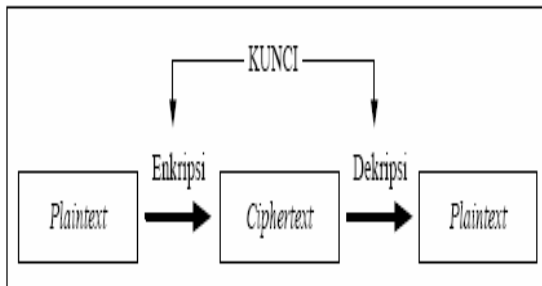
Algoritma kriptografi disebut juga cipher yaitu aturan untuk enciphering dan deciphering, atau fungsi yang digunakan untuk enkripsi dan dekripsi. Beberapa cipher memerlukan algoritma yang berbeda untuk enciphering dan deciphering.

Keamanan algoritma kriptografi sering diukur dari banyaknya kerja yang dibutuhkan untuk memecahkan cipertext menjadi plaintext tanpa mengetahui kunci yang digunakan. Apabila semakin banyak proses yang diperlukan berarti juga semakin lama waktu yang dibutuhkan, maka semakin kuat algoritma tersebut dan semakin aman digunakan untuk menyandikan pesan. (Eko Satria, 2009)

Dalam kriptografi terdapat dua macam algoritma kriptografi, yaitu: algoritma simetris dan algoritma asimetris. (yulita, 2010)

### 2.3.1 Algoritma Simetris

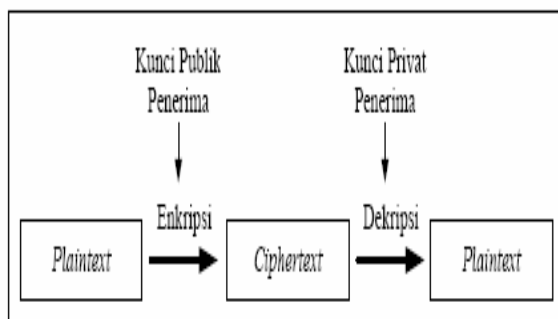
Algoritma Kriptografi Simetris atau disebut juga Algoritma Kriptografi konvensional. Algoritma ini menggunakan kunci yang sama untuk proses enkripsi dan proses dekripsi.



Gambar 2. Prosedur Kerja Algoritma Asimetris

### 2.3.2 Algoritma Asimetris

Algoritma Kriptografi Asimetris adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Algoritma ini disebut juga Algoritma Kunci Umum (*Public Key Algorithm*) karena kunci untuk enkripsi dibuat umum (*publik key*) atau dapat diketahui oleh setiap orang, tapi kunci untuk dekripsi hanya diketahui oleh orang yang berwenang mengetahui data yang disandikan atau sering disebut Kunci Pribadi (*Private Key*).



Gambar 3. Prosedur Kerja Algoritma Asimetris Privat Penerima (sumber : yulita, 2010)

### 2.4 Algoritma Hill Cipher

Algoritma kriptografi atau cipher, dan juga sering disebut dengan istilah sandi adalah suatu fungsi matematis yang digunakan untuk melakukan enkripsi dan dekripsi. Ada dua macam algoritma kriptografi, yaitu algoritma simetris (*symmetric algorithms*) dan algoritma asimetris (*asymmetric algorithms*).

Hill cipher yang merupakan *polyalphabetic cipher* dapat dikategorikan sebagai *block cipher*, karena teks yang akan diproses akan dibagi menjadi blok-blok dengan ukuran tertentu. Setiap karakter dalam satu blok akan saling mempengaruhi karakter lainnya dalam proses enkripsi dan dekripsinya, sehingga karakter yang sama tidak

dipetakan menjadi karakter yang sama pula (Arya Widyanarko, 2009).

Teknik kriptografi ini menggunakan sebuah matriks persegi sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi. *Hill Cipher* diciptakan oleh Lester S. Hill pada tahun 1929. *Hill Cipher* tidak mengganti setiap abjad yang sama pada *plaintext* dengan abjad lainnya yang sama pada *ciphertext* karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya. *Hill Cipher* termasuk kepada algoritma kriptografi klasik yang sangat sulit dipecahkan oleh kriptanalis apabila dilakukan hanya dengan mengetahui berkas *ciphertext* saja. Namun, teknik ini dapat dipecahkan dengan cukup mudah apabila kriptanalis memiliki berkas *ciphertext* dan potongan berkas *plaintext*. Teknik kriptanalis ini disebut *known-plaintext attack*. (Arya Widyanarko, 2009)

### 2.5 Dasar Teknik Hill Cipher

Dasar dari teknik *Hill Cipher* adalah aritmatika modulo terhadap matriks. Dalam penerapannya, *Hill Cipher* menggunakan teknik perkalian matriks dan teknik invers terhadap matriks. Kunci pada *Hill Cipher* adalah matriks  $n \times n$  dengan  $n$  merupakan ukuran blok. Jika kunci disebut dengan  $K$ , maka  $K$  adalah sebagai berikut (Arya Widyanarko, 2009) :

$$K = \begin{bmatrix} k_{11} & k_{12} & \dots & k_{1n} \\ k_{21} & k_{22} & \dots & k_{2n} \\ \dots & \dots & \dots & \dots \\ k_{m1} & k_{m2} & \dots & k_{mn} \end{bmatrix}$$

Matriks  $K$  yang menjadi kunci harus merupakan matriks yang *invertible*, yaitu memiliki *multiplicative inverse*  $K^{-1}$  sehingga :

$$K \cdot K^{-1} = I$$

Kunci harus memiliki invers karena matriks  $K^{-1}$  tersebut adalah kunci yang digunakan untuk melakukan dekripsi.

### 2.6 Teknik Enkripsi pada Hill Cipher

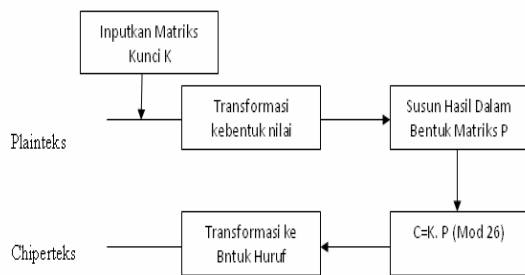
Proses enkripsi pada *Hill Cipher* dilakukan per blok *plaintext*. Ukuran blok tersebut sama dengan ukuran matriks kunci. Sebelum membagi teks menjadi deretan blok-blok, *plaintext* terlebih dahulu dikonversi menjadi angka, masing-masing sehingga A=0, B=1, hingga Z=25. Secara matematis, proses enkripsi pada *Hill Cipher* adalah:

$$C = K \cdot P$$

$$C = \text{Ciphertext}$$

$$K = \text{Kunci}$$

$$P = \text{Plaintext}$$



**Gambar 4. Ilustrasi Proses Enkripsi Hill Cipher**

### 2.7 Teknik Dekripsi pada Hill Cipher

Proses dekripsi pada *Hill Cipher* pada dasarnya sama dengan proses enkripsinya. Namun matriks kunci harus dibalik (invers) terlebih dahulu. Secara matematis, proses dekripsi pada *Hill Cipher* dapat diturunkan dari persamaan :

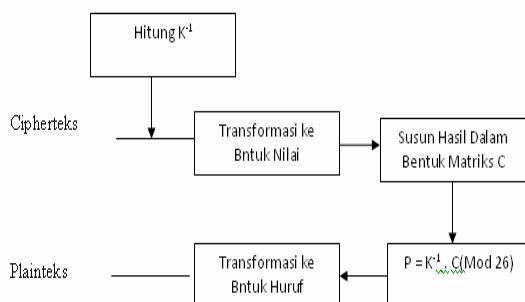
$$\begin{aligned}
 C &= K \cdot P \\
 K^{-1} \cdot C &= K^{-1} \cdot K \cdot P \\
 K^{-1} \cdot C &= I \cdot P \\
 P &= K^{-1} \cdot C
 \end{aligned}$$

Menjadi persamaan proses deskripsi :

$$P = K^{-1} \cdot C$$

Di mana untuk menentukan  $K^{-1}$  dengan menggunakan rumus:

$$\frac{1}{\det K} \bmod 26 = x \quad \text{atau} \quad (\det K * x \bmod 26 = 1)$$



**Gambar 5. Ilustrasi Proses Dekripsi Hill Cipher**

### 2.8 Keamanan Data

Secara umum data dibagi menjadi dua, yaitu: data yang bersifat rahasia dan tidak bersifat rahasia. Dalam hal ini, pesan yang diperhatikan dan perlu diamankan adalah pesan yang bersifat rahasia.

Beberapa ancaman dan serangan yang terjadi saat data tidak lagi dipertukarkan dengan menggunakan media penyimpanan yang bersifat mobile, dan saat data melalui jalur telekomunikasi. Di sini banyak yang akan terjadi dalam keamanan data sehingga menimbulkan beberapa ancaman yaitu (Agustinus Widyartono, 2011):

#### 1. Interruption

Mengancam ketersediaan data dan informasi yang ada didalam sistem komputer dan komunikasi secara fisik, sehingga saat data dan informasi dibutuhkan mengalami kesulitan dalam mengaksesnya.

#### 2. Interception

Mengancam kerahasiaan sebuah data, merupakan penyadapan informasi oleh pihak-pihak yang tidak berhak atas sebuah informasi.

#### 3. Modification

Mengancam validitas isi sebuah data, selain berhasil melakukan penyadapan juga dilakukan perubahan atas data sehingga informasi yang dihasilkan menjadi bias.

#### 4. Fabrication

Mengancam integritas sumber pengiriman data, pihak yang tidak berhak berhasil melakukan peniruan sehingga dianggap sebagai pihak yang benar-benar dikehendaki.

Menurut stalling, ada beberapa hal yang terpenting dalam issue keamanan data, yaitu: (yulita setiayanti pertiwi, 2010)

#### 1. Confidentiality

Menjamin bahwa data-data tersebut hanya bisa diakses oleh pihak tertentu saja.

#### 2. Authentication

Pada saat mengirim atau menerima informasi, kedua belah pihak perlu mengetahui bahwa pengirim dari pesan tersebut adalah orang yang sebenarnya seperti yang diklaim.

#### 3. Integrity

Tuntutan ini berhubungan dengan jaminan setiap pesan yang dikirim pasti sampai pada penerimaannya tanpa ada bagian dari pesan tersebut yang diganti, diduplikasi, dirusak, diubah urutannya, dan ditambahkan.

#### 4. Non-repudiation

Mencegah pengirim maupun penerima mengingkari bahwa mereka telah mengirimkan atau menerima suatu pesan atau informasi. Jika sebuah pesan dikirim, penerima dapat membuktikan bahwa pesan tersebut memang dikirim oleh pengirim yang tertera. sebaliknya, jika sebuah pesan diterima, pengirim dapat membuktikan bahwa pesannya telah diterima oleh pihak yang ditujunya.

#### 5. Access control

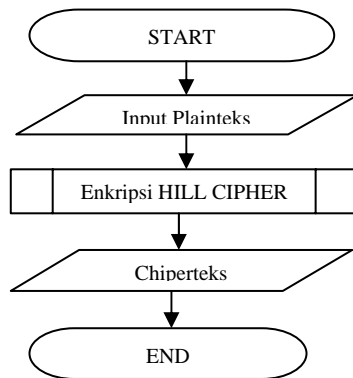
Membatasi sumber-sumber data hanya kepada orang-orang tertentu.

#### 6. Availability

Diperlukan setiap saat semua informasi pada system komputer harus tersedia bagi semua pihak yang berhak atas informasi tersebut.

### 3. Pembahasan

*Enkripsi* merupakan suatu proses untuk mengolah plainteks menjadi sebuah chipherteks yang tidak dapat diterjemahkan secara langsung. Proses kerja *enkripsi* dapat digambarkan seperti *flowchart* pada gambar berikut.



**Gambar 6. Flowchart Sistem Enkripsi**

Proses enkripsi pada *hill cipher* dilakukan per blok plainteks. Ukuran blok tersebut sama dengan ukuran matriks kunci. Sebelum membagi teks menjadi deretan blok-blok, plainteks terlebih dahulu dikonversi menjadi angka, masing-masing sehingga A=0, B=1, hingga Z=25.

**Tabel 1. Konversi Karakter Ke Bilangan Desimal**

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

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

Secara matematis, proses enkripsi pada *hill cipher* adalah:

$$C = K \cdot P \pmod{26}$$

$C$  = Cipherteks  
 $K$  = Kunci  
 $P$  = Plainteks

Contoh kasus yang dibuat yaitu berupa data record dalam database yang terdiri beberapa tabel dan beberapa field-field.

Jika sebuah database dengan nama database dbperpustakaan yang terdiri beberapa tabel yang terdiri dari atribut dan field sebagai berikut.

**Tabel 2. Database Perpustakaan Tabel Mahasiswa**

NPM	NAMA_MAHASISWA	JENJANG	JURUSAN	GRUP
0511068	ABDUL HALIM	S1	TI	MA
0211044	SUPRIADI	S1	SI	PA
0711231	YUDA JAYA	D3	MI	MA
0711213	SURYA DARMA	D3	KA	SI

Maka dalam database ini yang berupa record tersebut akan dikonversikan terlebih dahulu menjadi nilai.

**Tabel 3. Database Perpustakaan Pada Tabel Mahasiswa Dikonversikan Ke Dalam Nilai**

NPM	NAMA_MAHASISWA	JENJANG	JURUSAN	GRUP
0511068	01320117011812	S1	198	120
0211044	SUPRIADI	S1	SI	PA
0711231	JULHAM	D3	MI	MA
0711213	SURYA DARMA	KA	KA	SI

Plainteks tersebut yang terdapat pada tabel database db perpustakaan akan dienkripsi dengan teknik hill cipher dengan kunci K yang merupakan matriks 2x2.

Setiap plainteks yang telah dikonversikan akan dibagi perblok dan setelah itu tiap blok akan dienkripsi dengan kunci K melalui persamaan berikut.

Sebelum memulai untuk proses enkripsi jadi terlebih dahulu dipilih dulu record yang ingin diamankan dan tentukan kuncinya.

Tahap pertama yang dimulai untuk melakukan enkripsi yaitu pada field nama\_mahasiswa.

Plainteks ABDUL HALIM maka akan dienkrip sebagai berikut:

**Tabel 4. Plainteks Dikonversi Ke Bilangan Desimal**

1	2	3	4	5
0 1	3 20	11 7	0 11	8 12

Blok I:

$$= \begin{vmatrix} 5 & 3 \\ 3 & 2 \end{vmatrix} \begin{vmatrix} 0 & 1 \\ 3 & 20 \end{vmatrix} = \begin{vmatrix} 5*0+3*1 & 5*3+3*20 \\ 3*0+2*1 & 3*3+2*20 \end{vmatrix} = \begin{vmatrix} 3 & 39 \\ 2 & 49 \end{vmatrix}$$

Setelah itu hasil di mod 26 kan seperti berikut :

$$3 \bmod 26 = 3$$

$$2 \bmod 26 = 2$$

$$\text{Hasilnya: } 3 - 2 \text{ atau } D - C$$

Blok II:

$$= \begin{vmatrix} 5 & 3 \\ 3 & 2 \end{vmatrix} \begin{vmatrix} 3 & 20 \\ 11 & 7 \end{vmatrix} = \begin{vmatrix} 5*3+3*20 & 5*11+3*7 \\ 3*3+2*20 & 3*11+2*7 \end{vmatrix} = \begin{vmatrix} 75 & 75 \\ 49 & 49 \end{vmatrix}$$



Setelah itu hasil mod 26 kan seperti berikut :

$$75 \bmod 26 = 23$$

$$49 \bmod 26 = 23$$

Hasilnya : 23-23 atau X – X

Blok III:

$$= \begin{vmatrix} 5 & 3 \\ 3 & 2 \end{vmatrix} \begin{vmatrix} 11 \\ 7 \end{vmatrix} = \begin{vmatrix} 5*11+3*7 \\ 3*11+2*7 \end{vmatrix} = \begin{vmatrix} 55+21 \\ 33+14 \end{vmatrix} = \begin{vmatrix} 76 \\ 47 \end{vmatrix}$$

Setelah itu hasil mod 26 kan seperti berikut :

$$76 \bmod 26 = 24$$

$$47 \bmod 26 = 21$$

Hasilnya : 24 – 21 atau Y – V

Blok IV:

$$= \begin{vmatrix} 5 & 3 \\ 3 & 2 \end{vmatrix} \begin{vmatrix} 0 \\ 11 \end{vmatrix} = \begin{vmatrix} 5*0+3*11 \\ 3*0+2*11 \end{vmatrix} = \begin{vmatrix} 33 \\ 22 \end{vmatrix}$$

Setelah itu hasil dijumlahkan dengan mod 26

seperti berikut :

$$33 \bmod 26 = 7$$

$$22 \bmod 26 = 22$$

Maka hasil dari penjumlahan mod yaitu: 7-22 atau H – W

Blok V:

$$= \begin{vmatrix} 5 & 3 \\ 3 & 2 \end{vmatrix} \begin{vmatrix} 8 \\ 12 \end{vmatrix} = \begin{vmatrix} 5*8+3*12 \\ 3*8+2*12 \end{vmatrix} = \begin{vmatrix} 76 \\ 48 \end{vmatrix}$$

Setelah itu hasil dijumlahkan dengan mod 26

seperti berikut :

$$76 \bmod 26 = 24$$

$$48 \bmod 26 = 22$$

Maka hasil dari penjumlahan mod yaitu: 7-22 atau Y – W

Chiperteks ABDUL HALIM = DCXXYVHWYW

Tahap Kedua yang dimulai untuk melakukan enkripsi yaitu pada field Jurusan.

Plainteks yang akan dienkrip adalah TI .

**Tabel : 5. Plainteks Dikonversi Ke Bilangan Desimal Pada Record TI Field Jurusan**

1
19 8

Pada plainteks ini hanya terdapat Cuma 1 blok. Maka penyelesaian nya sebagai berikut:

Blok I:

$$= \begin{vmatrix} 5 & 3 \\ 3 & 2 \end{vmatrix} \begin{vmatrix} 19 \\ 8 \end{vmatrix} = \begin{vmatrix} 5*19+3*8 \\ 3*19+2*8 \end{vmatrix} = \begin{vmatrix} 119 \\ 73 \end{vmatrix}$$

Setelah itu hasil di mod 26 kan seperti berikut :

$$119 \bmod 26 = 15$$

$$73 \bmod 26 = 21$$

Hasilnya: 15– 21 atau P – V

Chiperteks TI = P – V

Tahap Ketiga yang dimulai untuk melakukan enkripsi yaitu pada field grup

Plainteks yang dienkrip adalah MA.

**Tabel 6 : Plainteks Dikonversi Ke Bilangan Desimal Pada Record MA Field GRUP**

1
12 0

Pada plainteks ini ada satu blok yang akan dproses. Maka penyelesaiannya sebagai berikut:

Blok I:

$$= \begin{vmatrix} 5 & 3 \\ 3 & 2 \end{vmatrix} \begin{vmatrix} 12 \\ 0 \end{vmatrix} = \begin{vmatrix} 5*12+3*0 \\ 3*12+2*0 \end{vmatrix} = \begin{vmatrix} 60 \\ 36 \end{vmatrix}$$

Setelah itu hasil di mod 26 kan seperti berikut :

$$60 \bmod 26 = 8$$

$$36 \bmod 26 = 10$$

Hasilnya: 8– 10 atau

Chiperteks MA = I – K

**Tabel: 7. Tabel Database Perpustakaan Salah Satu Recordnya Telah Dienkrip**

NPM	NAMA_MAHASISWA	JENJANG	JURUSAN	GRUP
0511068	DCXXYVHWYW	S1	PV	IK
0211044	SUPRIADI	S1	SI	PA
0711231	YUDA JAYA	D3	MI	MA
0711213	SURYA DARMA	D3	KA	SI

### 3.1 Analisa Dekripsi

Proses dekripsi merupakan sistem untuk mengolah data acak (cipherteks) menjadi data awal (plainteks). Dalam proses dekripsi ini terdapat proses dekripsi Hill Cipher.

Proses dekripsi pada *hill cipher* pada dasarnya sama dengan proses enkripsinya. Namun matriks kunci harus dibalik (invers) terlebih dahulu. Secara matematis, proses dekripsi pada *hill cipher* dapat diturunkan dari persamaan berikut :

$$C = K \cdot P$$

$$K^{-1} \cdot C = K^{-1} \cdot K \cdot P$$

$$K^{-1} \cdot C = I \cdot P$$

$$P = K^{-1} \cdot C$$

Menjadi persamaan proses deskripsi :

$$P = K^{-1} \cdot C$$

Proses dekripsi diawali dengan menghitung invers dari matriks *K*. Maka proses dekripsi sebagai berikut :

$$K = \begin{vmatrix} 3 & 2 \end{vmatrix} \bmod 26$$

$$\text{Det}(K) = 5 \times 2 - 3 \times 3 = 1$$

Maka untuk mencari  $K^{-1}$  :

$$K^{-1} = \frac{1}{K} \text{Adj}(K)$$

$$K^{-1} = \frac{1}{1} \begin{vmatrix} 2 & -3 \\ -3 & 5 \end{vmatrix}$$

$$= \frac{1}{1} \begin{vmatrix} 2 & -3 \\ -3 & 5 \end{vmatrix}$$

$$= \begin{vmatrix} 2 & -3 \\ -3 & 5 \end{vmatrix}$$

Setiap bilangan yang bernilai negative ditambah 26 agar nilai tetap positif, ini digunakan karena bilangan 0 – 25.

$$K^{-1} = \begin{vmatrix} 2 & 23 \\ 23 & 5 \end{vmatrix}$$

Untuk membuktikan bahwa K saling invers dengan K-1 dilakukan pembuktian dengan melakukan perkalian dan hasil akhirnya harus matriks identitas, pembuktiannya sebagai berikut :

$$K = \begin{vmatrix} 5 & 3 \\ 3 & 2 \end{vmatrix} \quad K^{-1} = \begin{vmatrix} 2 & 23 \\ 23 & 5 \end{vmatrix}$$

$$= \begin{vmatrix} 5 & 3 & 2 & 23 \\ 3 & 2 & 23 & 5 \end{vmatrix} = \begin{vmatrix} 5*2 + 3*23 & 5*23 + 3*5 \\ 3*2 + 2*23 & 3*23 + 2*5 \end{vmatrix}$$

$$= \begin{vmatrix} 10 + 69 & 115 + 15 \\ 6 + 46 & 69 + 10 \end{vmatrix}$$

$$= \begin{vmatrix} 79 & 130 \\ 52 & 79 \end{vmatrix}$$

Hasil masing-masing di mod 26 kan

$$79 \bmod 26 = 1$$

$$52 \bmod 26 = 0$$

$$130 \bmod 26 = 0$$

$$79 \bmod 26 = 1$$

Hasilnya :

$$= 1 \begin{vmatrix} 0 & \\ 0 & 1 \end{vmatrix}$$

Setelah di mod 26 maka hasilnya adalah matriks identitas, hal ini membuktikan bahwa matriks K saling invers dengan K-1. Selanjutnya lakukan proses dekripsi dengan mengalikan matriks K-1 dengan ciphertext yang telah didapat sebelumnya.

Untuk tahap selanjutnya pada proses dekripsi yang akan dilakukan pada record, di mana sebelumnya telah terjadi enkripsi pada record tersebut. Maka untuk proses dekripsinya antara lain sebagai berikut.

Tahap pertama yang dilakukan adalah record yang telah dienkripsi akan diproses yang terdapat pada field yang telah ditentukan.

Record yang terdapat pada field nama\_mahasiswa yang telah dienkripsi sebagai berikut:

Cipherteks dari ABDUL HALIM = DCXXYVHWYW

Hasil dari enkripsi tersebut akan didekripsi dengan cara membagi dengan blok pada hasil cipherteks yang sudah ada.

Cipherteks Blok – I : D – C = 3 – 2

$$554 \bmod 26 = 8$$

$$662 \bmod 26 = 12$$

Hasilnya: 8 – 12 maka I – M

Setelah semua blok selesai di dekripsi maka didapatkan hasil plainteksnya sebagai berikut : ABDULHALIM

Tahap kedua yang dilakukan adalah record yang telah dienkripsi akan diproses yang terdapat pada field yang telah ditentukan.

Record yang terdapat pada field jurusan yang telah dienkripsi sebagai berikut:

Cipherteks dari TI = P – V

Selanjutnya akan diproses dekripsinya dengan cipherteks yang sudah ada.

Maka hasil dari beberapa record yang telah didekripsikan pada database perpustakaan yang diambil dari tabel mahasiswa yaitu:

DCXXYVHWYW = ABDUL HALIM  
PV = TI  
IK = MA

Dari contoh kasus ini dapat diambil hasilnya bahwa dalam proses enkripsi dan dekripsi dengan tehnik hill cipher bisa dilakukan pada record. Di mana record yang ingin diproses dapat ditentukan oleh pemakai untuk pengamanan data pada record yang dipilih oleh user.

### 3.2 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 pengaturan kunci, pemilihan data yang akan dienkripsi dan didekripsi. 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 Simulasi

Form ini merupakan suatu tampilan simulasi terjadinya proses enkrip dan deskrip dengan algoritma hill cipher.

**Gambar 7. Simulasi Enkripsi /Dekripsi**

## 2. Form Enkripsi/Dekripsi

Form ini ditampilkan untuk proses enkripsi dan dekripsi pada data yang mau dilakukan proses. Form dapat dilihat pada gambar 8.

**Gambar 8 : Proses Enkripsi Dan Dekripsi**



**Gambar 9 : Hasil Implementasi Sistem**

## 4. Kesimpulan Dan Saran

### 4.1. Kesimpulan

Setelah selesai menyusun tesis ini, penulis menarik kesimpulan sebagai berikut:

1. Dalam Pembuatan Sistem ini dapat digunakan sebagai penyandian data yang berupa karakter yang berbentuk huruf dengan cara membagi perblok setiap karakter yang dienkripsi.
2. Sistem ini dirancang dengan menggunakan bahasa pemrograman visual basic 6.0 dengan menggunakan algoritma hill cipher.
3. Sistem ini bisa digunakan oleh orang lain dengan mudah.

### 5.2. Saran

Saran penulis untuk pengembangan lebih lanjut penelitian ini yaitu berupa kelayakan pada sistem antara lain:

1. Sistem ini digunakan pada pengamanan data yang tidak hanya menggunakan berupa karakter yang berupa angka.
2. Sistem ini masih perlu pengembangan lebih lanjut untuk pengembangan algoritma yang digunakan dan bisa digabungkan dengan algoritma kriptografi lainnya.

## DAFTAR PUSTAKA

1. Rinaldi Munir. "Kriptografi". Bandung. Informatika. 2006.
2. Rifki Sadikin. "Kriptografi untuk Keamanan Jaringan". Yogyakarta. Andi. 2012.
3. Suryani Esti dan Sri Martini Titin, "Kombinasi Kriptografi Dengan Hill Cipher Dan Steganografi Dengan LSB Untuk Keamanan Data Teks". 2008.
4. Widyanarko Arya, "Studi Dan Analisis mengenai Hill Cipher, Teknik Kriptanalisis dan upaya Penanggulangannya".
5. Munawar, "Perancangan Algoritma Sistem Keamanan Data Menggunakan Metode Kriptografi Asimetris", Vol.1, 2012.
6. Pramono Andy dan sujada Alun, "Implementasi Algoritma Hill Cipher Sebagai media Steganografi Menggunakan Metode LSB, 2009.
7. Widyartono Agustinus, "Algoritma Elgamal Untuk Enkripsi Data menggunakan GNPUG", Vol.1, 2011.