IMPLEMENTASI ALGORITMA HILL CIPHER DALAM PENYANDIAN DATA NILAI AKHIR SEMESTER PADA PROGRAM STUDI TI-S1 TAHUN AJARAN 2014/2015 DENGAN MENGGUNAKAN KODE ASCII

Diah Retno Palupi[1], Umi Rosyidah[2]
[1,2]Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Jl. Nakula I No. 5-11,Semarang,Jawa Tengah 50131 – (024) 3517261
E-mail : diahpalupi17@gmail.com[1], umi.rosyidah@dsn.dinus.ac.id[2]

Abstrak

Sistem keamanan seharusnya dapat meningkatkan keamanan data para penggunanya. Suatu kerahasian data dan informasi merupakan suatu hal yang sangat penting. Data tersebut biasanya disimpan dalam suatu sistem yang disebut dengan sistem basis data. Dalam pengamanan data dapat dilakukan dengan mengenkripsi data tersebut . Metode enkripsi algoritma Hill Cipher termasuk algoritma kriptografi klasik yang sulit dipecahkan, apabila dilakukan hanya dengan mengetahui berkas ciphertext saja. Karena Hill Cipher tidak mengganti setiap abjad yang sama pada ciphertext karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya. Untuk semakin meningkatkan keamanan penyandian data maka dalam penelitian ini metode enkripsi algoritma Hill Cipher dimodifikasi dengan menggunakan kode ASCII.

Kata Kunci: *Kriptografi, Hill Cipher, Enkripsi Data, Deskripsi Data, Basis Data, Kode ASCII*

Abstract

The security system should be able to increase the security of the data of its users. A confidentiality of data and information is a very important thing. Such data is usually stored in a system called the system data base. In the safeguarding of data can be done by encrypting data. Hill Cipher algorithm encryption methods including classical cryptographic algorithms that are difficult to solve when done just by knowing the ciphertext files only. Because of the Hill Cipher does not replace any of the alphabet the same ciphertext because using matrix multiplication on basic encryption and decryption. To further improve the security encoding of data then this encryption method in the research of algorithm of the Hill Cipher modified using ASCII code.

Keywords: *Cryptography, Hill Cipher, Data Encryption, Data Descriptions, Database, ASCII Code*

1. PENDAHULUAN

1.1 Latar Belakang

Pesatnya perkembangan ilmu pengetahuan dan teknologi yang memungkinkan munculnya teknik-teknik baru, yang disalahgunakan oleh pihak tertentu dapat mengancam keamanan data dalam sistem informasi. Jatuhnya informasi ke tangan pihak lain dapat menimbulkan kerugian bagi pemilik informasi.

Data sebaiknya tidak mudah dibaca oleh semua orang. Sistem keamanan seharusnya dapat meningkatkan keamanan data para penggunanya. Data tersebut biasanya disimpan dalam suatu sistem yang disebut dengan sistem basis data. Basis data merupakan sekumpulan data yang saling terintegrasi satu sama lain dan terorganisasi berdasarkan skema atau struktur tertentu dan tersimpan pada sebuah perangkat keras komputer[2]. Dalam perkembangan teknologi, sistem basis data telah

menjadi simbol dari salah satu bentuk aset yang paling berharga. Basis data digunakan secara luas untuk berbagai bidang seperti perbankan, pendidikan, kepegawaian, dan lain-lain. Dengan semakin luasnya pengunaan sistem basis data pada suatu sistem informasi, perlindungan terhadap informasi yang disimpan didalamnya menjadi sangat diperlukan untuk melindungi dari berbagai macam ancaman diantaranya pembaca data, manipulasi data danperusakan data oleh pihak yang tidak berwenang[3].

Mengacu dalam permasalahan tersebut, muncul suatu gagasan yaitu untuk membuat suatu sistem keamanan yang dapat melindungi data penting dengan penyandian data, sehingga sulit untuk di deteksi oleh pihak yang tidak berhak. Sistem keamanan yang akan dibuat adalah enkripsi pada basis data, sehingga pada saat penginputan data, data tersebut telah tersimpan dan terenkripsi dengan menggunakan teknik kriptografi *Hill Cipher*.

Metode enkripsi algoritma *Hill Cipher* termasuk algoritma kriptografi klasik yang sulit dipecahkan oleh kriptanalis apabila dilakukan hanya dengan mengetahui berkas *ciphertext* saja. *Hill Cipher* tidak mengganti setiap abjad yang sama pada ciphertext karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya. Untuk semakin meningkatkan keamanan penyandian data maka penulis menggabungkan metode enkripsi algoritma *Hill Cipher* dengan menggunakan kode ASCII. Kode ASCII *(American Standart Code for Information Interchange)* merupakan representasi numerik dari suatu karakter yang tidak tercetak.

1.2 Rumusan Masalah

Latar belakang masalah yang telah dikemukakan di atas dan judul yang dipilih maka dapat diperoleh suatu perumusan masalah yaitu: Bagaimana mengimplementasikan algoritma *Hill Cipher* dengan menggunakan kode ASCII dalam penyandian data nilai akhir semester pada program studi TI-S1 tahun ajaran 2014/2015?

1.3 Batasan Masalah

Agar permasalahan tidak menyimpang dari maksud dan tujuan yang diharapkan, maka dibuat beberapa pembatasan masalah antara lain :

1. Data yang diproses adalah data nilai akhir semester pada program studi TI-S1 tahun ajaran 2014/2015 yang berupa karakter yaitu string dan integer.
2. Metode yang digunakan Algoritma *Hill Cipher* mengunakan ordo matrik 2 x 2.
3. Menggunakan kode ASCII.

1.4 Tujuan Penelitian

Adapun tujuan yang hendak dicapai dalam penelitian ini, penulis berharap untuk mencapai tujuan yang diinginkan yaitu :

Mengaplikasikan metode algoritma *Hill Cipher* dengan menggunakan kode ASCII dalam penyandian data nilai akhir semester pada program studi TI-S1 tahun ajaran 2014/2015

2. METODE PENELITIAN

Metode yang digunakan dalam penelitian yaitu mengkombinasikan algoritma *Hill Cipher* dan Kode ASCII terhadap data nilai mahasiswa yang nantinya akan disandikan. Enkripsi data akan dilakukan melalui perhitungan dengan mengkonversikan terlebih dahulu setiap karakter kedalam bentuk desimal pada Kode ASCII.

2.1 Sumber Data

Data yang digunakan untuk penelitian ini adalah data kuantitatif yaitu berupa *record* data nilai siswa.

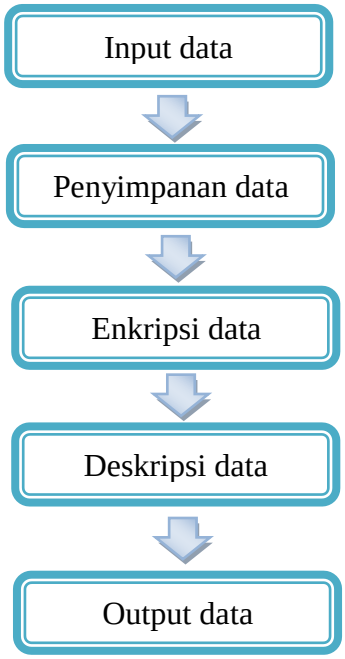
Sumber data yang digunakan adalah data primer yang diperoleh secara langsung dari objek penelitian yaitu bagian pusat data nilai mahasiswa Universitas Dian Nuswantoro Semarang yang berupa data nilai akhir semester pada program studi TI-S1 tahun ajaran 2014/2015. Sedangkan data sekunder diperoleh dari buku-buku kepustakaan, jurnal-jurnal ilmiah, paper, tesis, dan mencari informasi dari internet, yang dijadikan sebagai landasan teori serta pelengkap data primer. Data sekunder yang penulis dapatkan berupa literatur sebagai pelengkap landasan teori tugas akhir ini dari berbagai sumber kepustakaan

2.2 Metode Yang Diusulkan

Dalam penelitian, penulis mengusulkan prosedur penyelesaian yang akan dilakukan dalam pelaksanaan penelitian yaitu terhadap keamanan data yang dilakukan pada konversi penyandian data adalah sebagai berikut:

1. *Input data*, menginputkan pesan plaintext yang berupa data nilai.
2. *Penyimpanan data*, proses penyimpanan data pada database.
3. *Enkripsi data*, proses mengolah plaintext yang sudah tersimpan dalam database menjadi sebuah ciphertext yang tidak dapat diterjemahkan secara langsung.
4. *Deskripsi data*, proses mengolah ciphertext menjadi data awal (plaintext).
5. *Output data*, pencetakan hasil penyimpanan data yang diinginkan oleh user.

Proses kerja enkripsi dapat digambarkan dengan skema sebagai berikut:



Gambar 2.1 Skema Proses Implementasi Algoritma Hill Cipher Dalam Penyandian Data Dengan Menggunakan Kode ASCII.
[Sumber: Diah Retno Palupi, 2014]

2.3 Proses Enkripsi Data

Enkripsi pada data nilai dilakukan dengan memanfaatkan algoritma Hill Cipher dan Kode ASCII. Terdapat database dengan nama database dbnilai, yang terdiri dari beberapa atribut dan beberapa tabel sebagai berikut:

Tabel 2.1 Database Nilai Kalkulus I

No.	NIM	Nama	Nilai	Ket
1.	A11.2014.08552	MONICA CYNTIA PRATIWI	90	A
2.	A11.2014.08553	FARIZ RACHMAT SAIPIN NOHA	80	B
3.	A11.2014.08554	RISTI YULIANA	85	A
4.	A11.2014.08555	FISKHA ANGGRAINA MURTI	88	A
5.	A11.2014.08557	FAROKH ZUMAINI	76	B

Dalam database yang berupa record tersebut yang pertama dilakukan adalah dikonversikan kedalam nilai terlebih dahulu menggunakan kode ASCII sebagai berikut ini:

Tabel 2.2 Database Nilai Kalkulus I Dikonversikan Kedalam Nilai Desimal Pada Tabel Kode ASCII

No.	NIM	Nama	Nilai	Ket
1.	A11.2014.08552	MONICA CYNTIA PRATIWI	5748	A
2.	A11.2014.08553	FARIZ RACHMAT SAIPIN NOHA	5648	B
3.	A11.2014.08554	RISTI YULIANA	5653	A
4.	A11.2014.08555	FISKHA ANGGRAINA MURTI	5656	A
5.	A11.2014.08557	FAROKH ZUMAINI	5554	B

Setelah dikonversikan, plainteks tersebut yang terdapat pada database nilai akan dienkripsi menggunakan algoritma *Hill Cipher* dengan kunci *K* yang merupakan matriks 2 x 2. Setiap plainteks yang sudah dikonversikan akan dibagi perblok, setelah dibagi perblok tiap blok tersebut akan dienkripsi dengan kunci *K*. Sebelum memlai proses enkripsi terlebih dahuluh memilih record yang akan disandikan atau diamankan, kemudian menentukan kunci matriksnya.

Secara sistematis, proses enkripsi ada Hill Cipher adalah:

$$C = K.P$$

C = Cipherteks
K = Kunci
P = Plainteks

Dengan kunci K = $\begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}$

Kunci yang digunakan dalam penelitian ini adalah kunci yang sudah terbukti memiliki nilai invers. Apabila kunci matriks sudah ditentukan, langkah pertama untuk melalukan proses enkripsi adalah plainteks nilai pada mata kuliah Kalkulus I maka akan dienkripsi sebagai berikut:

1. Nilai dikonversikan menjadi bilangan desimal yang menggunakan Kode ASCII. Jadi terdapat plainteks *P*:
   P_1 = 90 P_4 = 88
   P_2 = 80 P_5 = 76
   P_3 = 85

   Maka plainteks tersebut dikonversikan menjadi:

Tabel 2.3 Plainteks yang sudah dikonversikan dengan kode ASCII

No.	NIM	Nama	Nilai	Ket
1.	A11.2014.08552	MONICA CYNTIA PRATIWI	5748	A
2.	A11.2014.08553	FARIZ RACHMAT SAIPIN NOHA	5648	B
3.	A11.2014.08554	RISTI YULIANA	5653	A
4.	A11.2014.08555	FISKHA ANGGRAINA MURTI	5656	A
5.	A11.2014.08557	FAROKH ZUMAINI	5554	B

2. Karena matriks kunci berukuran 2, maka plainteks dibagi menjadi blok yang masing-masing bloknya berukuran 2 karakter.

3. Blok plainteks ini kemudian dienkripsi.
   - Blok plainteks P_1 adalah sebagai berikut:
     $P_1 = \begin{bmatrix} 57 \\ 48 \end{bmatrix}$
   - Blok plainteks P_2 adalah sebagai berikut:
     $P_2 = \begin{bmatrix} 56 \\ 48 \end{bmatrix}$
   - Blok plainteks P_3 adalah sebagai berikut:
     $P_3 = \begin{bmatrix} 56 \\ 55 \end{bmatrix}$
   - Blok plainteks P_4 adalah sebagai berikut:
     $P_4 = \begin{bmatrix} 56 \\ 56 \end{bmatrix}$
   - Blok plainteks P_5 adalah sebagai berikut:
     $P_5 = \begin{bmatrix} 55 \\ 54 \end{bmatrix}$

4. Blok plainteks tersebut kemudian dienkripsi dengan kunci K melalui rumus:

   $$C = K.P$$

   - Blok plainteks P_1 dienkripsi sebagai berikut:
     $P_1 = \begin{bmatrix} 57 \\ 48 \end{bmatrix}$

     $C_1 = K.P_1$

     $= \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 57 \\ 48 \end{bmatrix} \text{mod } 256$

     $= \begin{bmatrix} 48 \\ 153 \end{bmatrix}$

Karakter yang terkorespondensi dengan 48 dan 153 adalah 0 dan ™. Maka karakter pada plainteks berubah menjadi karakter 0™ pada cipherteks.

- Blok plainteks P_2 dienkripsi sebagai berikut:

$$P_2 = \begin{bmatrix}56\\48\end{bmatrix}$$

$$C_2 = K.P_2 = \begin{bmatrix}0 & 1\\1 & 2\end{bmatrix}\begin{bmatrix}56\\48\end{bmatrix} \bmod 256 = \begin{bmatrix}48\\152\end{bmatrix}$$

Karakter yang terkorespondensi dengan 48 dan 152 adalah 0 dan ˜. Maka karakter pada plainteks berubah menjadi karakter 0˜ pada cipherteks.

- Blok plainteks P_3 dienkripsi sebagai berikut:

$$P_3 = \begin{bmatrix}56\\55\end{bmatrix}$$

$$C_3 = K.P_3 = \begin{bmatrix}0 & 1\\1 & 2\end{bmatrix}\begin{bmatrix}56\\55\end{bmatrix} \bmod 256 = \begin{bmatrix}55\\166\end{bmatrix}$$

Karakter yang terkorespondensi dengan 55 dan 166 adalah 7 dan ¦. Maka karakter pada plainteks berubah menjadi karakter 7¦ pada cipherteks.

- Blok plainteks P_4 dienkripsi sebagai berikut:

$$P_4 = \begin{bmatrix}56\\56\end{bmatrix}$$

$$C_4 = K.P_4 = \begin{bmatrix}0 & 1\\1 & 2\end{bmatrix}\begin{bmatrix}56\\56\end{bmatrix} \bmod 256 = \begin{bmatrix}56\\168\end{bmatrix}$$

Karakter yang terkorespondensi dengan 56 dan 168 adalah 8 dan ¨ . Maka karakter pada plainteks berubah menjadi karakter 8¨ pada cipherteks.

- Blok plainteks P_5 dienkripsi sebagai berikut:

$$P_5 = \begin{bmatrix}55\\54\end{bmatrix}$$

$$C_5 = K.P_5 = \begin{bmatrix}0 & 1\\1 & 2\end{bmatrix}\begin{bmatrix}55\\54\end{bmatrix} \bmod 256 = \begin{bmatrix}54\\163\end{bmatrix}$$

Karakter yang terkorespondensi dengan 54 dan 163 adalah 6 dan £. Maka karakter pada plainteks berubah menjadi karakter 6£ pada cipherteks.

5. Setelah melakukan enkripsi pada semua blok plainteks P maka dapat dihasilkan ciperteks C adalah sebagai berikut:

Tabel 2.4 Tabel Database Nilai Kalkulus I Pada Data Record Yang Telah Dienkripsi

No.	NIM	Nama	Nilai	Ket
1.	A11.2014.08552	MONICA CYNTIA PRATIWI	0™	A
2.	A11.2014.08553	FARIZ RACHMAT SAIPIN NOHA	0˜	B
3.	A11.2014.08554	RISTI YULIANA	7¦	A
4.	A11.2014.08555	FISKHA ANGGRAINA MURTI	8¨	A
5.	A11.2014.08557	FAROKH ZUMAINI	6£	B

2.4 Proses Deskripsi Data

Proses dekripsi pada hill cipher hampir sama dengan proses enkripsi, tetapi matriks kunci harus dibalik (invers) terlebih dahulu. Secara sistematis, proses dekripsi pada algoritma hill cipher sebagai berikut:

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

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

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

Menjadi persamaan proses dekripsi:

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

Dengan menggunakan kunci K = $\begin{bmatrix}0 & 1\\1 & 2\end{bmatrix}$, maka proses dikripsi yang dilakukan adalah pada hasil enkrips atau cipherteks nilai pada mata kuliah Kalkulus I proses dekripsi adalah sebagai berikut:

1. Setiap huruf pada cipherteks yang berupa karakter Kode ASCII dikonversikan kedalam bentuk desimal.
   - C_1 = 0TM maka menjadi, $C_1 = \begin{bmatrix}48\\153\end{bmatrix}$
   - C_2 = 0˜ maka menjadi, $C_2 = \begin{bmatrix}48\\152\end{bmatrix}$
   - C_3 = 7¦ maka menjadi, $C_3 = \begin{bmatrix}55\\166\end{bmatrix}$
   - C_4 = 8¨ maka menjadi, $C_4 = \begin{bmatrix}56\\168\end{bmatrix}$
   - C_5 = 6£ maka menjadi, $C_5 = \begin{bmatrix}54\\163\end{bmatrix}$

2. Setelah dikonversikan maka kunci K terlebih dahulu di invers maka menjadi:

   $K = \begin{bmatrix}a & b\\c & d\end{bmatrix} \Rightarrow K^{-1} = \frac{1}{ad-bc}\begin{bmatrix}d & -b\\-c & a\end{bmatrix}$

   $K = \begin{bmatrix}0 & 1\\1 & 2\end{bmatrix} \Rightarrow K^{-1} \frac{1}{0.2-1.1}\begin{bmatrix}2 & -1\\-1 & 0\end{bmatrix}$

   $= \frac{1}{0-1}\begin{bmatrix}2 & -1\\-1 & 0\end{bmatrix}$

   $= \frac{1}{-1}\begin{bmatrix}2 & -1\\-1 & 0\end{bmatrix}$

   $= \begin{bmatrix}-2 & 1\\1 & 0\end{bmatrix}$

   Maka $K^{-1} = \begin{bmatrix}-2 & 1\\1 & 0\end{bmatrix}$

3. Selanjutnya ciperteks didekripsi dengan mnggunakan kunci K^{-1}. Proses dekripsi dilakukan blok per blok seperti pada proses enkripsi.
   - C_1 = 0^{TM} maka menjadi, $C_1 = \begin{bmatrix}48\\153\end{bmatrix}$

   ∗ Dekripsi:

   $P_1 = K^{-1} . C$

   $P_1 = \begin{bmatrix}-2 & 1\\1 & 0\end{bmatrix}\begin{bmatrix}48\\153\end{bmatrix} \bmod 256$

   $= \begin{bmatrix}57\\48\end{bmatrix}$

   Karakter yang terkorespondensi dengan 57 dan 48 adalah 9 dan 0.

   - C_2 = 0˜ maka menjadi, $C_2 = \begin{bmatrix}48\\152\end{bmatrix}$

   ∗ Dekripsi:

   $P_2 = K^{-1} . C$

   $P_2 = \begin{bmatrix}-2 & 1\\1 & 0\end{bmatrix}\begin{bmatrix}48\\152\end{bmatrix} \bmod 256$

   $= \begin{bmatrix}56\\48\end{bmatrix}$

   Karakter yang terkorespondensi dengan 56 dan 48 adalah 8 dan 0.

   - C_3 = 7¦ maka menjadi, $C_3 = \begin{bmatrix}55\\166\end{bmatrix}$

   ∗ Dekripsi:

   $P_3 = K^{-1} . C$

   $P_3 = \begin{bmatrix}-2 & 1\\1 & 0\end{bmatrix}\begin{bmatrix}55\\166\end{bmatrix} \bmod 256$

   $= \begin{bmatrix}56\\55\end{bmatrix}$

   Karakter yang terkorespondensi dengan 56 dan 55 adalah 8 dan 7.

   - C_4 = 8¨ maka menjadi, $C_4 = \begin{bmatrix}56\\168\end{bmatrix}$

   ∗ Dekripsi:

   $P_4 = K^{-1} . C$

   $P_4 = \begin{bmatrix}-2 & 1\\1 & 0\end{bmatrix}\begin{bmatrix}56\\168\end{bmatrix} \bmod 256$

   $= \begin{bmatrix}56\\56\end{bmatrix}$

   Karakter yang terkorespondensi dengan 56 dan 56 adalah 8 dan 8.

   - C_5 = 6£ maka menjadi, $C_5 = \begin{bmatrix}54\\163\end{bmatrix}$

   ∗ Dekripsi:

   $P_1 = K^{-1} . C$

$$P_1 = \begin{bmatrix} -2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 54 \\ 163 \end{bmatrix} \bmod 256$$
$$= \begin{bmatrix} 55 \\ 54 \end{bmatrix}$$

Karakter yang terkorespondensi dengan 55 dan 54 adalah 7 dan 6.

4. Setelah semua blok selesai didekripsi, maka didapatkan basil plainteks sesuai dengan nilai yang telah diinputkan sebagai berikut:

Tabel 2.5 Hasil Dekripsi Nilai Mahasiswa

No.	NIM	Nama	Nilai	Ket
1.	A11.2014.08552	MONICA CYNTIA PRATIWI	90	A
2.	A11.2014.08553	FARIZ RACHMAT SAIPIN NOHA	80	B
3.	A11.2014.08554	RISTI YULIANA	85	A
4.	A11.2014.08555	FISKHA ANGGRAINA MURTI	88	A
5.	A11.2014.08557	FAROKH ZUMAINI	76	B

Selanjutnya dari hasil nilai deskripsi tersebut akan konversikan ke dalam nilai huruf sesuai *standart range* dari universitas.

3. HASIL DAN PEMBAHASAN

Data yang digunakan dalam penelitian ini adalah data nilai akhir semester pada program studi TI-S1 tahun ajaran 2014/2015 meliputi data mahasiswa, nilai mahasiswa, mata kuliah yang diambil. Pada data tersebut sebelumnya akan dilakukan pengelompokan terhadap data nilai mahasiswa per setiap mata kuliah.

4.1 Perhitungan *Hill Cipher*

Dalam perhitungan *Hill Cipher* pada data nilai akhir semester, user melakukan input nilai mahasiswa yang nantinya jika dilakukan penyimpanan, maka nilai tersebut secara otomatis terenkripsi. Berikut ini adalah perhitungan enkripsi data nilai akhir semester pada mahasiswa Monica Cyntia Pratiwi dengan mata kuliah Kalkulus I:

Tabel 4.1 Database Nilai Kalkulus I

No	NIM	Nama	Nilai	Ket
1.	A11.2014.08552	MONICA CYNTIA PRATIWI	90	A

Nilai 90 kemudian dikonversikan menjadi bilangan desimal menggunakan Kode ASCII hasilnya yaitu 5748. Proses enkripsi Hill Cipher adalah $C = K.P$, dengan kunci K = $\begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}$. Jadi terdapat Plainteks (P) adalah 90 yang sudah dikonversikan menjadi 5748. Karena matriks kunci berukuran 2, maka plainteks dibagi menjadi blok yang masing-masing bloknya berukuran 2 karakter. Sehingga perhitungan enkripsi adalah sebagai berikut:

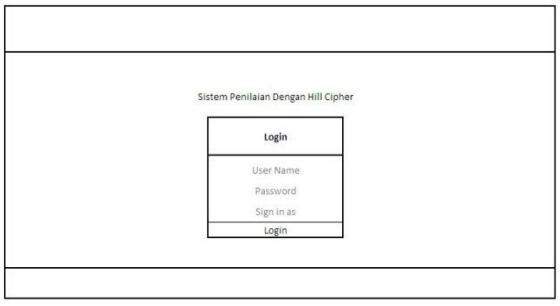
$$C_1 = K.P_1$$
$$= \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 57 \\ 48 \end{bmatrix} \bmod 256$$
$$= \begin{bmatrix} 48 \\ 153 \end{bmatrix}$$

Karakter yang terkorespondensi dengan 48 dan 153 adalah 0 dan ™. Maka karakter pada plainteks berubah menjadi karakter 0 ™ pada cipherteks.

4.2 Perancangan Interface

Perancangan interface yang akan dibuat sebagai berikut:

4.2.1 Tampilan Halaman Login

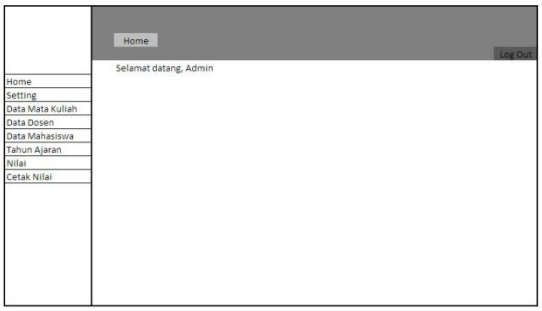


Gambar 4.1 Desain halaman login

Tampilan halaman pertama saat sistem akan diakses. Untuk dapat mengakses harus melakukan login terlebih dahulu sesuai dengan

kebutuhan sebagai user atau admin.

4.2.2 Tampilan Halaman Sistem Penilaian Pada Admin



Gambar 4.2 Desain Halaman Sistem Penilaian Pada Admin

Halaman utama saat admin melakukan login terhadap sistem penilaian. Didalamnya terdapat beberapa menu untuk melakukan implementasi penilaian *Hill Cipher*. Diantaranya terdapat menu setting yaitu untuk merubah kunci pada penyandian data nilai. Data mata kuliah yaitu menu yang digunakan untuk pendataan data mata kuliah mahasiswa. Data dosen yaitu untuk pendataan data dosen, dan data mahasiswa yaitu menu yang digunakan untuk pendataan mahasiswa dimana nanti akan menghasilkan laporan data mahasiswa sesuai dengan kelompok mata kuliah dan dosen yang mengampunya. Terdapat pula menu tahun ajaran yang digunakan untuk menambah dan merubah tahun ajaran pada perkuliahan. Menu nilai yaitu untuk input data nilai- nilai mahasiswa. Cetak nilai yaitu menu yang dimenghasilkan laporan nilai dari mahasiswa. Sedangkan Logout digunakan untuk keluar dari sistem.

4.2.3 Tampilan Halaman Sistem Penilaian Pada Dosen atau User

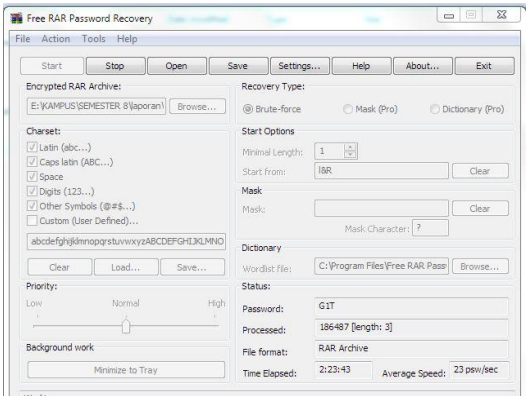
Gambar 4.3 Desain Halaman Sistem Penilaian Pada Dosen atau Admin

Halaman utama saat user melakukan login terhadap sistem penilaian. Didalamnya terdapat menu input nilai mahasiswa yaitu menu yang digunakan user untuk menginput nilai-nilai mahasiswa yang sudah dikelompokkan sesuai dengan mata kuliah dan dosen. Menu cetak nilai merupakan menu yang digunakan untuk mencetak laporan data nilai yang sudah diinputkan oleh user.

4.2 Pengujian Pada Metode

Proses selanjutnya dari penelitian ini adalah melakukan pengujian dari hasil enkripsi yang sudah dilakukan pada sistem tersebut. Proses pengujian ini digunakan untuk mengetahui seberapa kuat algoritma *Hill Cipher* ini akan digunakan dalam keamanan data. Dalam pengujiannya penulis menggunakan *Brute Force*. *Brute Force* adalah cara yang sangat sedehana untuk menemukan hasil enkripsi, yaitu dengan mencoba semua kemungkinan yang ada. Dengan kata lain semakin banyak kemungkinanya maka semakin lama proses pencarian hasil enkripsi.

Berikut ini adalah screenshot proses *recovery password:*



Gambar 4.1 Tampilan proses dan hasil recovery password

Pada Gambar 4.1 merupakan hasil dari *recovery password* yang belum terselasaikan dalam waktu 2:23:43. Pengujian *Brute Force* yaitu mencoba kemungkinan yang ada, cepat dan lamanya sustu proses berdasarkan seberapa panjang *password*.

Dari hasil pengujian yang telah penulis lakukan dapat disimpulkan bahwa metode yang diusulkan merupakan metode yang aman sebagai pengamanan data, karena metode yang digunakan adalah algoritma *Hill Cipher* dengan mengkombinasikan Kode ASCII didalamnya sehingga hasil enkripsi yang diperoleh berupa karakter yang terdiri dari kombinasi huruf besar, huruf kecil, digits desimal, simbol yang mempengaruhi pengujian dengan mengunakan *Brute Force* membutuhkan waktu yang lama lebih dari 2:23:43.

4. KESIMPULAN DAN SARAN

4.1 Kesimpulan

Berdasarkan hasil dari perhitungan dan pengujian algoritm *Hill Cipher* dalam penyandian data nilai akhir semester pada tahun ajaran 2014/2015 dengan menggunakan kode ASCII yang telah dilakukan, dapat disimpulkan bahwa metode algoritma *Hilll Cipher* dengan menggunakan Kode ASCII telah diimplementasikan dalam penginputan nilai mahasiswa dengan menggunakan range nilai sesuai dengan aturan universitas. Dari hasil perhitungan enkripsi dengan menggunakan metode *Hill Cipher* yang telah dikombinasi dengan Kode ASCII menghasilkan ketahanan dalam pengamanan suatu keamanan data yang aman digunakan, karena hasil enkripsi yang diperoleh berupa karakter yang terdiri dari kombinasi huruf besar, huruf kecil, digits desimal, simbol yang mempengaruhi pengujian dengan mengunakan *Brute Force* membutuhkan waktu yang lama.

4.2 Saran

Saran penulis untuk pengembangan penelitian lebih lanjut diantaranya adalah sebagai berikut ini:

1. Penelitian dapat dilanjutkan dengan memodifikasi algoritma *Hill Cipher* teknik kriptografi Steganografi atau dengan teknik lainnya.
2. Penelitian dapat dilanjutkan dengan memperluas asumsi matriks kunci yang digunakan dalam algoritma *Hill Cipher*.

5. DAFTAR PUSTAKA

[1] Abdul Halim Hasugian, "Implementasi Algoritma Hill Cipher Dalam penyandian Data," *Pelita Informatika Budi Darma Medan*, vol. -, no. -, p. 1, Agustus 2013.

[2] M. Rudyanto Arief, *Pemograman Basis Data menggunakan Transact-SQL dengan Microsoft SQL Server*. Yogyakarta: Andi Ofset, 2005.

[3] Ari Suhendra, "Analisis Dan Implementasi Enkripsi Basis Data Dengan Algoritma Kriptografi Blowfish," in *Sekolah Tinggi Manajemen INformatika dan Komputer AMIKOM*, Yogyakarta, 2012, p. 2.

[4] Kuswari Hernawati, "Implementasi Cipher Hill Pada Kode ASCII Dengan Memanfaatkan Digit

Desimal Bilangan Euler," *Jurusan Pedidikan Matematika FMIPA Universitas Negeri Yogyakarta*, vol. -, no. -, p. 2, Agustus 2006.

[5] Yulita Setyani Pertiwi, , 2010.

[6] Agustinus Widyantono, "Algoritma Elgamal Untuk Enkripsi Data menggunakan GNPUG," vol. 1, 2011.

[7] Rinaldi Munir, "Kriptografi," *Informatika*, 2006.

[8] Dony Ariyus, *Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi*. Yogyakarta: Andi offset, 2008.

[9] Bruce Schneier, "Decription of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)," Agustus 2011.

[10] Yusuf Kurniawan, , 2004.

[11] Arya Widyanarko, "Studi dan Analisis mengenai Hill Cipher, Teknik Kriptanalis dan Upaya Penanggulangannya," 2009.

[12] Sembodo Ichwan Haryo, "Password cracking Menggunakan Brute Force Attack," Teknik Informatika ITB, Bandung, Mei 2014.