UJM 11(1) 2022
UNNES Journal of Mathematics
http://journal.unnes.ac.id/sju/index.php/ujm

Perancangan dan Implementasi Aplikasi Kriptografi Algoritma *Hill Cipher* dalam Dekripsi Enkripsi Data Keuangan Nasabah Bank Sampoerna Menggunakan Kode ASCII

Yusna Warni Hasibuan✉, Isnarto, Rahayu Budhiati Veronica

Jurusan Matematika, FMIPA, Universitas Negeri Semarang, Indonesia
Gedung D7 Lt. 1, Kampus Sekaran Gunungpati, Semarang 50229

Info Artikel

Sejarah Artikel:
Diterima Januari 2019
Disetujui Maret 2019
Dipublikasikan Mei 2022

Keywords:
Kriptografi,
Enkripsi,
Dekripsi,
Keamanan Data,
Hill Cipher

Abstrak

Hill Cipher merupakan teknik kriptografi yang menggunakan matriks persegi sebagai kunci digunakan untuk proses enkripsi dan dekripsi. Masalah umum yang muncul pada algoritma ini terletak pada pemilihan kunci. Pemilihan kunci dilakukan secara sebarang dapat menyebabkan kegagalan pada proses dekripsi, karena algoritma ini syarat kunci yang digunakan yaitu matriks persegi dapat dibalik atau memiliki invers *(invertible).* Penelitian dilakukan pada Bank Sampoerna di Kota Padangsidimpuan Provinsi Sumatera Utara. Tujuan penelitian ini merancang aplikasi berbasis WEB digunakan untuk pendataan nasabah dan melakukan transaksi secara aman dengan penerapan metode autentifikasi nasabah. Sistem keamanan pengguna dibangun dengan menerapkan proses autentifikasi nasabah berupa PIN serta penggunaan metode kriptografi *Hill Cipher* pada proses transaksi yaitu saat nasabah melakukan transaksi menggunakan aplikasi WEB. Hasil pada penelitian ini adalah terciptanya suatu aplikasi berbasis WEB yang digunakan untuk melakukan transaksi oleh nasabah dan aplikasi server berbasis PHP dan menggunakan database MySQL untuk melakukan administrasi transaksi.

Abstract

Hill Cipher is a cryptographic technique that uses a square matrix as a key used for the encryption and decryption process. A common problem that arises in this algorithm lies in the selection of keys. Selection of keys carried out arbitrarily can cause failure in the decryption process, because this algorithm is the key requirement that is used, namely square matrices can be reversed or have inverse (invertible). The research was conducted at Bank Sampoerna in the City of Padangsidimpuan, North Sumatra Province. The purpose of this study is to design WEB-based applications used for customer data collection and to conduct transactions securely by implementing customer authentication methods. The user's security system is built by applying the customer authentication process in the form of a PIN and the use of the Hill Cipher cryptographic method in the transaction process, namely when the customer makes a transaction using the WEB application. The results of this study are the creation of a WEB-based application that is used to conduct transactions by customers and PHP-based server applications and use MySQL databases to perform transaction administration.

How to Cite

Hasibuan, Y. W., Isnarto, & Veronica, R. B. (2022). Perancangan dan Implementasi Aplikasi Kriptografi Algoritma *Hill Cipher* dalam Dekripsi Enkripsi Data Keuangan Nasabah Bank Sampoerna menggunakan Kode ASCII. *UNNES Journal of Mathematics,* 7(2), 54-68.

✉Alamat korespondensi:
E-mail: yusnawarni9@gmail.com

P – ISSN 2252-6943
e – ISSN 2460-5859

PENDUHULUAN

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 disalahgunakan oleh pihak-pihak tertentu yang mengancam keamanan dari sistem informasi tersebut. Keamanan, kerahasiaan dan integritas data diperlukan dalam setiap operasi yang ada di Internet. Pada waktu transmisi setiap informasi rahasia melewati jaringan, ada pemakai asing yang mengambil atau mengubah data. Untuk menghindari penyusup ini, pengamanan data diperlukan. Karena keamanan data diperlukan untuk proteksi data dari pemakai asing dan upaya-upaya yang merusak data, maka beberapa teknik keamanan data diperlukan (Pasaribu, 2016).

Enkripsi adalah satu teknik yang digunakan untuk melindungi basis data dari akses yang tidak berhak dan tindakan-tindakan yang tidak diinginkan dari pengguna-pengguna luar. Enkripsi digunakan untuk melindungi informasi rahasia dimana eknkripsi mengubah data dalam bentuk yang hanya dapat dipahami oleh penerima sah dan yang mengetahui dekripsi untuk mendapatkan data atau informasi yang asli. Berbagai teknik diimplementasikan untuk menjamin keamanan data (Widyartono 2011). Dalam penelitian ini, fokusnya pada Keamanan Basis Data (*Database Security*), dimana database (basis data) adalah sebagai tempat penyimpanan data.

Umumnya data perusahaan atau organisasi disimpan dalam basis data (*database)* dan menjadi sangat penting bagi perusahaan atau organisasi itu. Pada saat ini banyak organisasi mengizinkan pelanggan mereka dapat menggunakan servis yang diberikan (*online banking/* transaksi perbankan via internet, *online shopping/* belanja via internet, dan sebagainya) dengan mengakses tempat basis data (*database)* mereka. Hal ini mengakibatkan perlunya keamanan tingkat tinggi dalam menghadapi penyerang informasi. Seperti yang dikatakan Munir, bahwa masalah keamanan *(security)* pada komputer menjadi isu penting pada era teknologi sekarang ini. Banyak kejahatan *cyper* yang pernah terdengar dari media masa. Pelaku kejahatan memanfaatkan celah keamanan yang ada untuk dimasuki dan melakukan manipulasi (Munir, 2006:iii).

Basis data digunakan secara luas untuk berbagai bidang seperti perbankan, pendidikan, kepegawaian, dan lain-lain. Penulis akan menggunakan *record* basis data dibidang perbankan. Dibidang perbankan memiliki beberapa data yang sangat penting yang belum memiliki keamanan terhadap ancaman data. Dalam sebuah badan keuangan data nasabah adalah hal yang terpenting untuk dijaga. Data nasabah akan disimpan dalam sebuah database perusahaan. Untuk menjaga data nasabah maka diperlukan sebuah keamanan data yang biasa disebut kriptografi. Kriptografi bekerja dengan beberapa algoritma, diantara algoritma yang dapat digunakan adalah *Hill Chiper.* Algoritma ini menggunakan kunci yang susah untuk ditebak sehingga penyadap tidak mudah untuk merusak kunci yang telah digunakan (Rosnawan, 2011).

Pada penelitian ini, suatu teknik baru menggunakan Algoritma Enkripsi *Hill Chiper* diusulkan untuk menjamin keamanan bagian data pada basis data (*database*) yang diimplementasikan untuk memperkuat dan melindungi basis data tersebut. *Hill Cipher* merupakan salah satu algoritma kunci simetris yang memanfaatkan matriks n x n sebagai kunci. Algoritma *Hill Cipher* menggunakan matriks persegi sebagai kunci untuk melakukan enkripsi dan dekripsi. Dasar teori matriks yang digunakan dalam *Hill Cipher* antara lain adalah operasi perkalian dan invers pada matriks. Ide awal dari invers matriks tergeneralisasi *(generalized inverses of matrix)* adalah menggeneralisasi pengertian invers matriks. Metode ini memiliki beberapa keuntungan seperti ketahanan terhadap analisis frekuensi dan *implicity* karena metode ini menggunakan perkalian matriks dan invers untuk enkripsi dan dekripsi (Magambar *et al*., 2013).

Penelitian dilakukan pada Bank Sampoerna yang berada di Kota Padangsidimpuan. Rahasia bank adalah segala sesuatu yang berhubungan dengan keterangan mengenai nasabah penyimpan dan simpanannya. Maka dari itu dibutuhkan sebuah system informasi dengan keamanan yang memadai untuk menghindari terjadinya kebocoran data nasabah atau bahkan pencurian data nasabah. Berdasar latar belakang di atas maka di lakukan penelitian tentang perancangan dan implementasi aplikasi kriptografi pada basis data keuangan nasabah menggunakan metode *Hill Cipher* dengan mengambil studi kasus di Bank Sampoerna. Teknik kriptografi ini diciptakan dengan maksud untuk menciptakan *cipher* yang tidak dapat dipecahkan menggunakan teknik analisis frekuensi. 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.

METODE PENELITIAN

Metode penelitian yang digunakan adalah pengembangan program dan aplikasi dengan algortima *Hill Cipher.* Pengujian akan dilakukan pada proses penyimpanan data keuangan nasabah bank Sampoerna yang nantinya akan langsung terenkripsi dalam *database record* dan terdekripsi pada saat data akan dicetak. Pengumpulan data dengan data kuantitatif yaitu data nasabah keuangan bank dengan metode yang diusulkan menggunakan algoritma *Hill Cipher* dan metode pengembangan sistem menggunakan kode ASCII. Adapun langkah-langkah yang dilakukan dalam penelitian ini adalah (1) mengetahui langkah-langkah dekripsi enkripsi algoritma *Hill Cipher* (2) mengaplikasikan rancangan dengan sistem informasi berbasis WEB dengan algoritma *Hill Cipher* (3) menginplementasikan algoritma *Hill Cipher* dengan kode ASCII dalam enkripsi data keuangan nasabah Bank Sampoerna.

Kriptografi

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, otentikasi, dan autentifikasi data. Kriptografi bukan satu-satunya cara untuk menyediakan keamanan informasi, melainkan satu set teknik yang dapat digunakan untuk mengamankan informasi. Secara umum, kriptografi terdiri dari dua buah bagian utama yaitu bagian enkripsi dan bagian dekripsi. Enkripsi adalah proses transformasi informasi menjadi bentuk lain sehingga isi pesan yang sebenarnya tidak dapat dipahami, hal ini dimaksudkan agar informasi tetap terlindung dari pihak yang tidak berhak menerima. Sedangkan dekripsi adalah proses kebalikan enkripsi, yaitu transformasi data terenkripsi ke data bentuk semula. Proses transformasi dari plainteks menjadi cipherteks akan dikontrol oleh kunci. Peran kunci sangatlah penting, kunci bersama-sama dengan algoritma matematisnya akan memproses plainteks menjadi cipherteks dan sebaliknya (Ariyus, 2008).

Algoritma *Hill Cipher*

Teknik kriptografi ini diciptakan dengan maksud untuk dapat menciptakan *cipher* (kode) yang tidak dapat dipecahkan menggunakan teknik analisis frekuensi. *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. Oleh karena itu *Hill Cipher* termasuk dalam salah satu kriptosistem polialfabetik. *Cipher* Ini ini ditemukan pada tahun 1929 oleh Lester S. Hill. (Widyanarko, 2009).

Berdasarkan jenis kunci yang dipakai, kriptografi *Hill Cipher* termasuk ke dalam Algoritma Simetrik *(Symmetric Algorithms)*, karena algoritma ini menggunakan suatu kunci yang sama untuk proses enkripsi dan dekripsi pesan. Dalam melakukan proses enkripsi dan dekripsi, algoritma ini menggunakan sebuah matriks persegi sebagai kunci yang digunakan dan menerapkan aritmatika modulo (Hasugian, 2013).

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 sesuai tabel ASCII. Secara matematis, proses enkripsi pada *Hill Cipher* adalah: $\boldsymbol{C = K.P}$ (Hidayat & Alawiyah, 2013).

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

Algoritma Enkripsi *Hill Cipher*

Langkah-langkah enkripsi *Hill Cipher* sebagai berikut:

1. Tentukan *Plaintext* (teks asli) yang akan disandikan.
2. Menentukan matriks kunci dan merupakan matriks yang *invertible* yaitu memiliki *multiplicative inverse* K^{-1} sehingga $K.K^{-1} = I$
3. Mengubah *Plaintext* menjadi bentuk numerik sesuai dengan konversi yang telah ditetapkan.
4. Menghitung banyaknya karakter pada *plaintext*. Selanjutnya banyaknya karakter dari *plaintext* dibagi dengan ordo dari matriks kunci yang telah ditentukan.
5. Susun *plaintext* yang berupa numerik menjadi suatu mariks (2 x 1 jika ordo kunci 2 x 2).
6. Lakukan proses enkripsi dengan rumus $C = K.P$, sehingga diperoleh matriks baru dari hasil perkalian tersebut. Selanjutnya, modulokan hasil perkalian kedua matriks dengan 26.
7. Konversikan menjadi huruf/teks sesuai tabel konversi. Sehingga, diperoleh *ciphertext* atau karakter sandi yang merupakan hasil dari proses enkripsi**.**

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. Persamaan proses deskripsi yaitu: $\boldsymbol{P = K^{-1}.C}$ (Hidayat & Alawiyah, 2013).

P = *plaintext*.
K^{-1} = invers matriks kunci
C = *ciphertext.*

Algoritma Dekripsi *Hill Cipher*:

Langkah-langkah dekripsi *Hill Cipher* sebagai berikut:

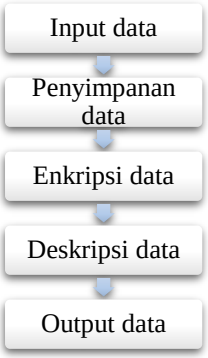
1. Mengubah *ciphertext* menjadi bentuk numerik sesuai dengan konversi yang telah ditetapkan.
2. Menentukan invers matriks kunci dari matriks kunci yang digunakan pada proses enkripsi. Dan tentukan nilai determinan matriks kunci $K = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, maka $\det K = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$.
3. Tinjaulah matriks 2×2, $K = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ jika $ad - bc \neq 0$, maka $K^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Dan jika determinan selain 1 atau -1 maka menentukan nilai invers modulo.
4. Tentukan nilai invers modulo (definisi 2.6 balikan modulo)
$$aa^{-1} \equiv 1 \, mod \, n$$
Keterangan:
a^{-1}: nilai determinan matriks kunci (K)
a : bilangan bulat positif atau negatif
mod $(modulus \, atau \, modulo)$: sisa bagi
5. Tentukan kunci dekripsi Hill Cipher. (nilai invers modulo x invers matriks kunci).
6. Rumus dekripsi *Hill Cipher* $P = K^{-1}.C$
7. Menyusun *ciphertext* yang berupa numerik menjadi suatu matriks. Kalikan invers matriks dengan matriks *ciphertext* dalam modulo 26.
8. Selanjutnya konversikan sesuai tabel konversi, diperoleh teks asli kembali (*plaintext).*
9. Pesan dapat dibaca kembali.

Pengembangan Program dan Aplikasi

Dalam penelitian ini prosedur penyelesaian yang akan dilakukan terhadap keamanan data yang dilakukan pada konversi penyandian data adalah sebagai berikut:

1. *Input* data, menginputkan pesan *plaintext* yang berupa data-data keuangan nasabah.
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.*

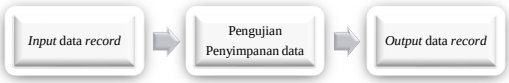
Skema proses implementasi algoritma *Hill Cipher* dalam penyandia data dengan menggunakan kode ASCII dapat dilihat pada Gambar 1.



Gambar 1. Skema Proses Implementasi Algoritma *Hill Cipher* dalam Penyandian Data dengan Menggunakan Kode ASCII.
Sumber: Palupi (2014).

Untuk proses pengembangan sistem ini menggunakan beberapa tahapan seperti.

1. Tahap Perencanaan yaitu mengimplementasikan algoritma *Hill Cipher* menggunakan Kode ASCII pada data record
2. Tahap Analysis
Analisis kebutuhan *hardware* : sistem operasi yaitu *windows* 10, bahasa pemrograman PHP *(Hypertext Preprocessor)* digunakan untuk pengimplementasian terhadap algoritma *Hill Cipher,* pembuatan basis datanya menggunakan MySQL yang digunakan untuk menyimpan *database record* yang akan digunakan dan *MS Word* digunakan untuk membuat laporan hasil penelitian.
Analisis Kebutuhan *Hardware* : Adapun *hardware* yang digunakan dalam penelitian ini adalah *Personal Computer* atau Laptop dengan spesifikasi prosesor core i3, sistem operasi windows 10 dengan RAM 2 GB dan Printer digunakan untuk mencetak hasil penelitian ke dalam bentuk *hardcopy.*
3. Tahap Perancangan Aplikasi. Tahapan Perancangan aplikasi enkripsi dan dekripsi dapat dilihat pada Gambar 2.



Gambar 2. Enkripsi – deskripsi Gambar Perancangan Desain

4. Implementasi Aplikasi
5. Uji Coba Kasus (Rahmawati 2014).

HASIL DAN PEMBAHASAN

Perhitungan Enkripsi Dekripsi Data Nasabah Bank menggunakan Algoritma *Hill Ciper*

Perhitungan *Hill Cipher* pada data keuangan nasabah, *user* melakukan input data keuangan nasabah yang nantinya jika dilakukan penyimpanan, maka nilai secara otomatis terenkripsi. Data keuangan nasabah yang akan dienkripsi dapat dilihat pada Tabel 1.

Tabel 1. Data Keuangan Nasabah Bank Sampoerna

No	Nomor Rekening	Nama Nasabah	PIN	Tanggal Pembukaan
1	6480000017	ZULHEN AHMAD SIREGAR	1231	05/02/2015

1. Enkripsi Data Keuangan Nasabah Bank Sampoerna

Enkripsi nomor rekening data nasabah bank sampoerna

Nomor Rekening 06480000017 kemudian dikonversikan menjadi bilangan desimal menggunakan Kode ASCII hasilnya yaitu 48 54 52 56 48 48 48 48 48 49 55. Karena matriks kunci berukuran 2×2, maka plainteks dibagi menjadi blok yang masing-masing bloknya berukuran 2 karakter. (berdasarkan langkah 4) Karena *plaintext* dari nomor rekeningnya memiliki sisa > 0 maka ditambah dengan karakter boneka yaitu (.). Sehingga *plaintext* menjadi 48 54 52 56 48 48 48 48 48 49 55 46 perhitungan enkripsi adalah sebagai berikut:

$$C_1 = K.P_1 = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 48 \\ 54 \end{pmatrix} mod\ 256 = \begin{pmatrix} 54 \\ 156 \end{pmatrix}$$

Karakter yang terkorespondensi dengan 54 dan 156 adalah 6 dan œ.

$$C_2 = K.P_2 = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 52 \\ 56 \end{pmatrix} mod\ 256 = \begin{pmatrix} 56 \\ 164 \end{pmatrix}$$

Karakter yang terkorespondensi dengan 56 dan 164 adalah 8 dan ¤

$$C_3 = K.P_3 = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 48 \\ 48 \end{pmatrix} mod\ 256 = \begin{pmatrix} 48 \\ 144 \end{pmatrix}$$

Karakter yang terkorespondensi dengan 48 dan 144 adalah 0 dan .

$$C_4 = K.P_4 = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 48 \\ 48 \end{pmatrix} mod\ 256 = \begin{pmatrix} 48 \\ 144 \end{pmatrix}$$

Karakter yang terkorespondensi dengan 48 dan 144 adalah 0 dan .

$$C_5 = K.P_5 = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 48 \\ 49 \end{pmatrix} mod\ 256 = \begin{pmatrix} 49 \\ 146 \end{pmatrix}$$

Karakter yang terkorespondensi dengan 49 dan 146 adalah 1 dan ’.

$$C_6 = K.P_6 = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 55 \\ 46 \end{pmatrix} mod\ 256 = \begin{pmatrix} 46 \\ 147 \end{pmatrix}$$

Karakter yang terkorespondensi dengan 46 dan 147 adalah . dan “

Maka karakter pada plainteks berubah menjadi karakter 6œ8¤001’.“ pada cipherteks. Hasil enkripsi nomor rekening nasabah Bank Sampoerna terlihat dapat dilihat pada Tabel 2.

Tabel 2. Enkripsi Nomor Rekening Nasabah Bank Sampoerna

No	Nomor Rekening	Nama Nasabah	PIN	Tanggal Pembukaan
1	6œ8¤001’. “	ZULHEN AHMAD SIREGAR	1231	05/02/2015

Enkripsi nama nasabah bank sampoerna

Nama nasabah ZULHEN AHMAD SIREGAR kemudian dikonversikan menjadi bilangan desimal menggunakan Kode ASCII hasilnya yaitu 90 85 76 72 69 78 65 72 77 65 68 83 73 82 69 71 65 82 . Karena matriks kunci berukuran 2×2 , maka plainteks dibagi menjadi blok yang masing-masing bloknya berukuran 2 karakter. Sehingga perhitungan enkripsi adalah sebagai berikut:

$$C_1 = K.P_1 = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 90 \\ 85 \end{pmatrix} mod\ 256 = \begin{pmatrix} 85 \\ 4 \end{pmatrix}$$

Karakter yang terkorespondensi dengan 85 dan 4 adalah U dan EOT.

$$C_2 = K.P_2 = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 76 \\ 72 \end{pmatrix} mod\ 256 = \begin{pmatrix} 72 \\ 220 \end{pmatrix}$$

Karakter yang terkorespondensi dengan 72 dan 220 adalah H dan Ü.

$$C_3 = K.P_3 = \begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}69\\ 78\end{pmatrix} mod\ 256 = \begin{pmatrix}78\\ 225\end{pmatrix}$$

Karakter yang terkorespondensi dengan 78 dan 225 adalah N dan á.

$$C_4 = K.P_4 = \begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}65\\ 72\end{pmatrix} mod\ 256 = \begin{pmatrix}72\\ 209\end{pmatrix}$$

Karakter yang terkorespondensi dengan 72 dan 209 adalah H dan Ñ.

$$C_5 = K.P_5 = \begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}77\\ 65\end{pmatrix} mod\ 256 = \begin{pmatrix}65\\ 207\end{pmatrix}$$

Karakter yang terkorespondensi dengan 65 dan 207 adalah A dan Ï.

$$C_6 = K.P_6 = \begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}68\\ 83\end{pmatrix} mod\ 256 = \begin{pmatrix}83\\ 234\end{pmatrix}$$

Karakter yang terkorespondensi dengan 83 dan 234 adalah S dan ê.

$$C_7 = K.P_7 = \begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}73\\ 82\end{pmatrix} mod\ 256 = \begin{pmatrix}82\\ 237\end{pmatrix}$$

Karakter yang terkorespondensi dengan 82 dan 237 adalah R dan í.

$$C_8 = K.P_8 = \begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}69\\ 71\end{pmatrix} mod\ 256 = \begin{pmatrix}71\\ 211\end{pmatrix}$$

Karakter yang terkorespondensi dengan 71 dan 211 adalah G dan Ó.

$$C_9 = K.P_9 = \begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}65\\ 82\end{pmatrix} mod\ 256 = \begin{pmatrix}82\\ 229\end{pmatrix}$$

Karakter yang terkorespondensi dengan 82 dan 229 adalah R dan å.

Maka karakter pada plainteks berubah menjadi karakter $UEOTH\ddot{U}N\acute{a}H\tilde{N}A\ddot{I}S\hat{e}R\acute{I}G\acute{O}R\mathring{a}$ pada cipherteks. Hasil enkripsi nama nasabah Bank Sampoerna dapat dilihat pada Tabel 3.

Tabel 3. Enkripsi Nama Nasabah Bank Sampoerna

No	Nomor Rekening	Nama Nasabah	PIN	Tanggal Pembukaan
1	6œ8¤001'. "	UEOTHÜNáH ÑAÏSêRíGÓRå	1231	05/02/2015

Enkripsi pin data nasabah bank sampoerna

PIN 1231 kemudian dikonversikan menjadi bilangan desimal menggunakan Kode ASCII hasilnya yaitu 49 50 51 49 . Karena matriks kunci berukuran 2, maka plainteks dibagi menjadi blok yang masing-masing bloknya berukuran 2 karakter. Sehingga perhitungan enkripsi adalah sebagai berikut:

$$C_1 = K.P_1 = \begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}49\\ 50\end{pmatrix} mod\ 256 = \begin{pmatrix}50\\ 149\end{pmatrix}$$

$$C_2 = K.P_2 = \begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}51\\ 49\end{pmatrix} mod\ 256 = \begin{pmatrix}49\\ 149\end{pmatrix}$$

Karakter yang terkorespondensi dengan 50 dan 149 adalah 2 dan •. Dan Karakter yang terkorespondensi dengan 49 dan 149 adalah 1 dan •. Maka karakter pada plainteks berubah menjadi karakter 2•1• pada cipherteks. Hasil enkripsi PIN nasabah Bank Sampoerna dapat dilihat pada Tabel 4.

Tabel 4. Enkripsi Pin Nasabah Bank Sampoerna

No	Nomor Rekening	Nama Nasabah	PIN	Tanggal Pembukaan
1	6œ8¤001'. "	UEOTHÜNáH ÑAÏSêRíGÓRå	2•1•	05/02/2015

Enkripsi tanggal pembukaan tabungan data nasabah bank sampoerna

Tanggal pembukaan tabungan nasabah 05/02/2015 kemudian dikonversikan menjadi bilangan desimal menggunakan kode ASCII hasilnya yaitu 48 53 47 48 50 47 50 48 49 53 . Karena matriks kunci berukuran 2×2, maka plainteks dibagi menjadi blok yang masing-masing bloknya berukuran 2 karakter. Sehingga perhitungan enkripsi adalah sebagai berikut:

$$C_1 = K.P_1 = \begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}48\\ 53\end{pmatrix} mod\ 256 = \begin{pmatrix}53\\ 154\end{pmatrix}$$

Karakter yang terkorespondensi dengan 53 dan 154 adalah 5 dan š

$$C_2 = K.P_2 = \begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}47\\ 48\end{pmatrix} mod\ 256 = \begin{pmatrix}48\\ 143\end{pmatrix}$$

Karakter yang terkorespondensi dengan 48 dan 143 adalah 0 dan

$$C_3 = K.P_3 = \begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}50\\ 47\end{pmatrix} mod\ 256 = \begin{pmatrix}47\\ 144\end{pmatrix}$$

Karakter yang terkorespondensi dengan 47 dan 144 adalah / dan

$$C_4 = K.P_4 = \begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}50\\ 48\end{pmatrix} mod\ 256 = \begin{pmatrix}48\\ 146\end{pmatrix}$$

Karakter yang terkorespondensi dengan 48 dan 146 adalah 0 dan ’

$$C_5 = K.P_5 = \begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}49\\ 53\end{pmatrix} mod\ 256 = \begin{pmatrix}53\\ 155\end{pmatrix}$$

Karakter yang terkorespondensi dengan 53 dan 155 adalah 5 dan ›.

Maka karakter pada plainteks berubah menjadi karakter 5š0/0’5› pada cipherteks. Hasil enkripsi tanggal pembukaan tabungan nasabah Bank Sampoerna dapat dilihat pada Tabel 5.

Tabel 5. Enkripsi Tanggal Pembukaan Tabungan Nasabah Bank Sampoerna

No	Nomor Rekening	Nama Nasabah	PIN	Tanggal Pembukaan
1	6œ8¤001’. “	UEOTHÜNáH ÑAÏSêRíGÓRå	2•1•	5š0/0’5›

2. Dekripsi Data Keuangan Nasabah Bank Sampoerna

Dari *ciphertext* yang dihasilkan terlihat bahwa algoritma *Hill Cipher* menghasilkan cipherteks yang tidak memiliki pola yang mirip dengan plainteksnya. Data nasabah Bank yang terenkripsi dapat dilihat pada Tabel 6.

Tabel 6. Enkripsi Data Nasabah Bank Sampoerna

No	Nomor Rekening	Nama Nasabah	PIN	Tanggal Pembukaan
1	6œ8¤001’. “	UEOTHÜNáH ÑAÏSêRíGÓRå	2•1•	5š0/0’5›

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:

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

Menjadi persamaan proses dekripsi:

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

Dengan menggunakan kunci $K = \begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}$,

maka:

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

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

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

Maka proses dikripsi yang dilakukan adalah pada hasil enkripsi atau cipherteks pada data keuangan nasabah proses dekripsi adalah sebagai berikut:

Dekripsi nomor rekening data nasabah bank Sampoerna

Setiap huruf pada cipherteks yang berupa karakter kode ASCII dikonversikan ke dalam bentuk desimal.

$$C_1 = \begin{pmatrix}6\\ œ\end{pmatrix} = \begin{pmatrix}54\\ 156\end{pmatrix}$$
$$C_2 = \begin{pmatrix}8\\ ¤\end{pmatrix} = \begin{pmatrix}56\\ 164\end{pmatrix}$$
$$C_3 = \begin{pmatrix}0\\ \end{pmatrix} = \begin{pmatrix}48\\ 144\end{pmatrix}$$
$$C_4 = \begin{pmatrix}0\\ \end{pmatrix} = \begin{pmatrix}48\\ 144\end{pmatrix}$$
$$C_5 = \begin{pmatrix}1\\ ’\end{pmatrix} = \begin{pmatrix}49\\ 146\end{pmatrix}$$
$$C_6 = \begin{pmatrix}.\\ “\end{pmatrix} = \begin{pmatrix}46\\ 147\end{pmatrix}$$

Selanjutnya ciperteks didekripsi dengan menggunakan kunci $K^{-1} = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}$.

Proses dekripsi dilakukan blok per blok seperti pada proses enkripsi.

$$C_1 = \begin{pmatrix}6\\ œ\end{pmatrix} = \begin{pmatrix}54\\ 156\end{pmatrix}$$

Dekripsi:

$$P_1 = K^{-1}.C$$
$$P_1 = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}54\\ 156\end{pmatrix} mod\ 256 = \begin{pmatrix}48\\ 54\end{pmatrix}$$

Karakter yang terkorespondensi dengan 48 dan 54 adalah 0 dan 6.

$$C_2 = \begin{pmatrix}8\\ ¤\end{pmatrix} = \begin{pmatrix}56\\ 164\end{pmatrix}$$

Dekripsi:

$$P_2 = K^{-1}.C$$
$$P_2 = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}56\\ 164\end{pmatrix} mod\ 256 = \begin{pmatrix}52\\ 56\end{pmatrix}$$

Karakter yang terkorespondensi dengan 52 dan 56 adalah 4 dan 8.

$$C_3 = \begin{pmatrix}0\\ \end{pmatrix} = \begin{pmatrix}48\\ 144\end{pmatrix}$$

Dekripsi:

$$P_3 = K^{-1}.C$$
$$P_3 = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}48\\ 144\end{pmatrix} mod\ 256 = \begin{pmatrix}48\\ 48\end{pmatrix}$$

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

$$C_4 = \begin{pmatrix}0\end{pmatrix} = \begin{pmatrix}48\\144\end{pmatrix}$$

Dekripsi:

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

$$P_4 = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}48\\144\end{pmatrix} \ mod\ 256$$

$$= \begin{pmatrix}48\\48\end{pmatrix}$$

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

$$C_5 = \begin{pmatrix}1\\,\end{pmatrix} = \begin{pmatrix}49\\146\end{pmatrix}$$

Dekripsi:

$$P_5 = K^{-1}.C$$

$$P_5 = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}49\\146\end{pmatrix} \ mod\ 256$$

$$= \begin{pmatrix}48\\49\end{pmatrix}$$

Karakter yang terkorespondensi dengan 48 dan 49 adalah 0 dan 1.

$$C_6 = \begin{pmatrix}\dot{}\\“\end{pmatrix} = \begin{pmatrix}46\\147\end{pmatrix}$$

Dekripsi:

$$P_6 = K^{-1}.C$$

$$P_6 = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}46\\147\end{pmatrix} \ mod\ 256$$

$$= \begin{pmatrix}55\\46\end{pmatrix}$$

Karakter yang terkorespondensi dengan 55 dan 48 adalah 7 dan . Hasil dekripsi nomor rekening nasabah Bank Sampoerna dapat dilihat pada Tabel 7.

Tabel 7. Dekripsi Nomor Rekening Nasabah Bank Sampoerna

No	Nomor Rekening	Nama Nasabah	PIN	Tanggal Pembukaan
1	6480000017	UEOTHÜNáH ÑAÏSêRíGÓRå	2•1•	5š0/0'5›

Dekripsi nama nasabah Bank Sampoerna

Setiap huruf pada cipherteks yang berupa karakter kode ASCII dikonversikan ke dalam bentuk desimal.

$$C_1 = \begin{pmatrix}\text{U}\\\text{EOT}\end{pmatrix} = \begin{pmatrix}85\\4\end{pmatrix}$$

$$C_2 = \begin{pmatrix}\text{H}\\Ü\end{pmatrix} = \begin{pmatrix}72\\220\end{pmatrix}$$

$$C_3 = \begin{pmatrix}\text{N}\\á\end{pmatrix} = \begin{pmatrix}78\\225\end{pmatrix}$$

$$C_4 = \begin{pmatrix}\text{H}\\Ñ\end{pmatrix} = \begin{pmatrix}72\\209\end{pmatrix}$$

$$C_5 = \begin{pmatrix}\text{A}\\Ï\end{pmatrix} = \begin{pmatrix}65\\207\end{pmatrix}$$

$$C_6 = \begin{pmatrix}\text{S}\\ê\end{pmatrix} = \begin{pmatrix}83\\234\end{pmatrix}$$

$$C_7 = \begin{pmatrix}\text{R}\\í\end{pmatrix} = \begin{pmatrix}82\\237\end{pmatrix}$$

$$C_8 = \begin{pmatrix}\text{G}\\Ó\end{pmatrix} = \begin{pmatrix}71\\211\end{pmatrix}$$

$$C_9 = \begin{pmatrix}\text{R}\\å\end{pmatrix} = \begin{pmatrix}82\\229\end{pmatrix}$$

Selanjutnya ciperteks didekripsi dengan menggunakan kunci $K^{-1} = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}$.

Proses dekripsi dilakukan blok per blok seperti pada proses enkripsi.

$$C_1 = \begin{pmatrix}\text{U}\\\text{EOT}\end{pmatrix} = \begin{pmatrix}85\\4\end{pmatrix}$$

Dekripsi:

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

$$P_1 = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}85\\4\end{pmatrix} \ mod\ 256 = \begin{pmatrix}90\\85\end{pmatrix}$$

Karakter yang terkorespondensi dengan 90 dan 85 adalah Z dan U.

$$C_2 = \begin{pmatrix}\text{H}\\Ü\end{pmatrix} = \begin{pmatrix}72\\220\end{pmatrix}$$

Dekripsi:

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

$$P_2 = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}72\\220\end{pmatrix} \ mod\ 256$$

$$= \begin{pmatrix}76\\72\end{pmatrix}$$

Karakter yang terkorespondensi dengan 76 dan 72 adalah L dan H.

$$C_3 = \begin{pmatrix}\text{N}\\á\end{pmatrix} = \begin{pmatrix}78\\225\end{pmatrix}$$

Dekripsi:

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

$$P_3 = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}78\\225\end{pmatrix} \ mod\ 256$$

$$= \begin{pmatrix}69\\78\end{pmatrix}$$

Karakter yang terkorespondensi dengan 69 dan 78 adalah E dan N.

$$C_4 = \begin{pmatrix}\text{H}\\Ñ\end{pmatrix} = \begin{pmatrix}72\\209\end{pmatrix}$$

Dekripsi:

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

$$P_4 = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}72\\209\end{pmatrix} \ mod\ 256$$

$$= \begin{pmatrix}65\\72\end{pmatrix}$$

Karakter yang terkorespondensi dengan 65 dan 72 adalah A dan H.

$$C_5 = \begin{pmatrix}\text{A}\\Ï\end{pmatrix} = \begin{pmatrix}65\\207\end{pmatrix}$$

Dekripsi:

$$P_5 = K^{-1}.C$$

$$P_5 = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}65\\207\end{pmatrix} \ mod\ 256$$

$$= \begin{pmatrix}77\\65\end{pmatrix}$$

Karakter yang terkorespondensi dengan 77 dan 65 adalah M dan A.

$$C_6 = \begin{pmatrix}\text{S}\\ê\end{pmatrix} = \begin{pmatrix}83\\234\end{pmatrix}$$

Dekripsi:

$$P_6 = K^{-1}.C$$

$$P_6 = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}83\\234\end{pmatrix} \ mod\ 256$$

$$= \begin{pmatrix}68\\83\end{pmatrix}$$

Karakter yang terkorespondensi dengan 68 dan 83 adalah D dan S.

$$C_7 = \begin{pmatrix} \text{R} \\ \text{í.} \end{pmatrix} = \begin{pmatrix} 82 \\ 237 \end{pmatrix}$$

Dekripsi:

$$P_7 = K^{-1}.C$$

$$P_7 = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 82 \\ 237 \end{pmatrix} mod\ 256$$

$$= \begin{pmatrix} 73 \\ 82 \end{pmatrix}$$

Karakter yang terkorespondensi dengan 73 dan 82 adalah I dan R.

$$C_8 = \begin{pmatrix} \text{G} \\ \text{Ó} \end{pmatrix} = \begin{pmatrix} 71 \\ 211 \end{pmatrix}$$

Dekripsi:

$$P_8 = K^{-1}.C$$

$$P_8 = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 71 \\ 211 \end{pmatrix} mod\ 256$$

$$= \begin{pmatrix} 69 \\ 71 \end{pmatrix}$$

Karakter yang terkorespondensi dengan 69 dan 71 adalah E dan G.

$$C_9 = \begin{pmatrix} \text{R} \\ \text{å} \end{pmatrix} = \begin{pmatrix} 82 \\ 229 \end{pmatrix}$$

Dekripsi:

$$P_9 = K^{-1}.C$$

$$P_9 = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 82 \\ 229 \end{pmatrix} mod\ 256$$

$$= \begin{pmatrix} 65 \\ 82 \end{pmatrix}$$

Karakter yang terkorespondensi dengan 65 dan 82 adalah A dan R. Dekripsi nama nasabah Bank Sampoerna dapat dilihat pada Tabel 8.

Tabel 8. Dekripsi Nama Nasabah Bank Sampoerna

No	Nomor Rekening	Nama Nasabah	PIN	Tanggal Pembukaan
1	648000001 7	ZULHEN AHMAD SIREGAR	2•1•	5š0/0'5›

Dekripsi PIN data nasabah Bank Sampoerna

Setiap huruf pada cipherteks yang berupa karakter kode ASCII dikonversikan ke dalam bentuk desimal.

$$C_1 = \begin{pmatrix} 2 \\ \bullet \end{pmatrix} = \begin{pmatrix} 50 \\ 149 \end{pmatrix}$$

$$C_2 = \begin{pmatrix} 1 \\ \bullet \end{pmatrix} = \begin{pmatrix} 49 \\ 149 \end{pmatrix}$$

Setelah dikonversikan kalikan dengan matriks kunci $K^{-1} = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix}$.

Proses dekripsi dilakukan blok per blok seperti pada proses enkripsi.

$$C_1 = \begin{pmatrix} 2 \\ \bullet \end{pmatrix} = \begin{pmatrix} 50 \\ 149 \end{pmatrix}$$

Dekripsi:

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

$$P_1 = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 50 \\ 149 \end{pmatrix} mod\ 256$$

$$= \begin{pmatrix} 49 \\ 50 \end{pmatrix}$$

Karakter yang terkorespondensi dengan 49 dan 50 adalah 1 dan 2.

$$C_2 = \begin{pmatrix} 1 \\ \bullet \end{pmatrix} = \begin{pmatrix} 49 \\ 149 \end{pmatrix}$$

Dekripsi

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

$$P_2 = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 49 \\ 149 \end{pmatrix} mod\ 256$$

$$= \begin{pmatrix} 51 \\ 49 \end{pmatrix}$$

Karakter yang terkorespondensi dengan 51 dan 49 adalah 3 dan 1. Dekripsi PIN nasabah Bank Sampoerna terlihat pada Tabel 9.

Tabel 9. Dekripsi PIN nasabah Bank Sampoerna

No	Nomor Rekening	Nama Nasabah	PIN	Tanggal Pembukaan
1	648000001 7	ZULHEN AHMAD SIREGAR	1231	5š0/0'5›

Dekripsi tanggal pembukaan data nasabah Bank Sampoerna

Setiap huruf pada cipherteks yang berupa karakter kode ASCII dikonversikan ke dalam bentuk desimal.

$$C_1 = \begin{pmatrix} 5 \\ \check{s} \end{pmatrix} = \begin{pmatrix} 53 \\ 154 \end{pmatrix}$$

$$C_2 = \begin{pmatrix} 0 \\ \end{pmatrix} = \begin{pmatrix} 48 \\ 143 \end{pmatrix}$$

$$C_3 = \begin{pmatrix} / \\ \end{pmatrix} = \begin{pmatrix} 47 \\ 144 \end{pmatrix}$$

$$C_4 = \begin{pmatrix} 0 \\ , \end{pmatrix} = \begin{pmatrix} 48 \\ 146 \end{pmatrix}$$

$$C_5 = \begin{pmatrix} 5 \\ , \end{pmatrix} = \begin{pmatrix} 53 \\ 155 \end{pmatrix}$$

Setelah dikonversikan kalikan dengan matriks kunci $K^{-1} = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix}$.

Proses dekripsi dilakukan blok per blok seperti pada proses enkripsi.

$$C_1 = \begin{pmatrix} 5 \\ \check{s} \end{pmatrix} = \begin{pmatrix} 53 \\ 154 \end{pmatrix}$$

Dekripsi:

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

$$P_1 = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 53 \\ 154 \end{pmatrix} mod\ 256$$

$$= \begin{pmatrix} 48 \\ 53 \end{pmatrix}$$

Karakter yang terkorespondensi dengan 48 dan 53 adalah 0 dan 5.

$$C_2 = \begin{pmatrix} 0 \\ \end{pmatrix} = \begin{pmatrix} 48 \\ 143 \end{pmatrix}$$

Dekripsi:

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

$$P_2 = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 48 \\ 143 \end{pmatrix} mod\ 256 = \begin{pmatrix} 47 \\ 48 \end{pmatrix}$$

Karakter yang terkorespondensi dengan 47 dan 48 adalah / dan 0.

$$C_3 = \begin{pmatrix} / \\ \end{pmatrix} = \begin{pmatrix} 47 \\ 144 \end{pmatrix}$$

Dekripsi:

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

$$P_3 = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 47 \\ 144 \end{pmatrix} mod\ 256 = \begin{pmatrix} 50 \\ 47 \end{pmatrix}$$

Karakter yang terkorespondensi dengan 50 dan 47 adalah 2 dan /.

$$C_4 = \begin{pmatrix}0\\ ,\end{pmatrix} = \begin{pmatrix}48\\146\end{pmatrix}$$

Dekripsi:

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

$$P_4 = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}48\\146\end{pmatrix} mod\ 256$$

$$= \begin{pmatrix}50\\48\end{pmatrix}$$

Karakter yang terkorespondensi dengan 50 dan 48 adalah 2 dan 0.

$$C_5 = \begin{pmatrix}5\\ ,\end{pmatrix} = \begin{pmatrix}53\\155\end{pmatrix}$$

Dekripsi:

$$P_5 = K^{-1}.C$$

$$P_5 = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}53\\155\end{pmatrix} mod\ 256 = \begin{pmatrix}49\\53\end{pmatrix}$$

Karakter yang terkorespondensi dengan 49 dan 53 adalah 1 dan5. Dekripsi tanggal pembukaan nasabah Bank Sampoerna dapat dilihat pada Tabel 10.

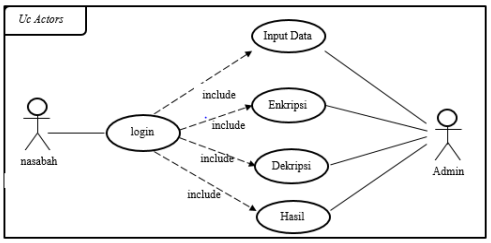
Tabel 10. Dekripsi tanggal pembukaan nasabah Bank Sampoerna

No	Nomor Rekening	Nama Nasabah	PIN	Tanggal Pembukaan
1	6480000017	ZULHEN AHMAD SIREGAR	1231	5/02/2015

2. Sistem Rancangan Aplikasi Berbasis Web dengan Algoritma *Hill Cipher*

Gambaran Umum Sistem yang Diusulkan

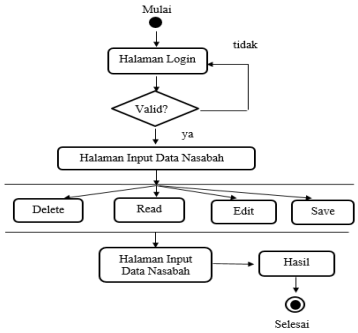
Pembuatan sistem Implementasi Algoritma *Hill Cipher* dalam Penyandian Data dengan menggunakan Kode ASCII mampu mengelola nomor rekening nasabah, nama nasabah, jenis angunan nasabah, nomor kontrak nasabah, tanggal pembukaan pembukuan nasabah, flapon nasabah, keterangan dan jenis produk nasabah. Gambaran *use case* sistem penginputan data dapat dilihat pada Gambar 3.



Gambar 3. *Use Case* sistem penginputan data

Activity Diagram

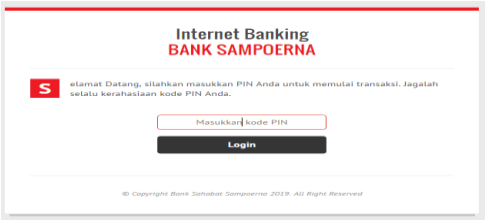
Activity Diagram Proses Input Data Nasabah oleh Admin. *Activity* Diagram untuk proses Input Data Nasabah menggambarkan alur proses penginputan mulai dari *login* untuk masuk ke dalam sistem kemudian admin mulai menginput data nasabah ke dalam form data nasabah kemudian menghasilkan nasabah. Gambaran *activity* diagram proses input data nasabah oleh Admin dapat dilihat pada Gambar 4.



Gambar 4. *Activity* Diagram Proses Input Data Nasabah oleh Admin

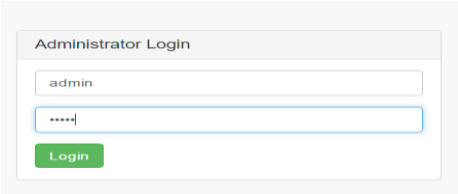
Implementasi Sistem

1. Halaman Login. Tampilan *login* sebagai *user* (nasabah) Bank Sampoerna dapat dilihat pada Gambar 5.



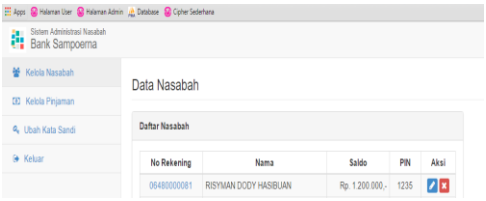
Gambar 5. Tampilan *Login* sebagai *User* (Nasabah Bank Sampoerna)

Tampilan *login* sebagai administrator Bank Sampoerna dapat dilihat pada Gambar 6.



Gambar 6. Tampilan *Login* sebagai Administrator

2. Menu Utama Sistem Administrasi Nasabah Bank Sampoerna dengan *Hill Cipher* untuk Admin. Tampilan menu utama sistem administrasi nasabah Bank Sampoerna dengan *hill cipher* untuk admin dapat dilihat pada Gambar 7.



Gambar 7. Tampilan Menu Utama Sistem Administrasi Nasabah Bank Sampoerna dengan *Hill Cipher* untuk Admin

Pada halaman *dasboard* atau halaman utama terdapat beberapa menu untuk pendataan yang digunakan untuk memasukkan data Nasabah Bank Sampoerna. Terdapat beberapa menu yaitu:

a. Kelola Nasabah merupakan menu yang digunakan untuk menginput dan mengedit data nasabah Bank Sampoerna.
b. Kelola Tabungan merupakan menu yang digunakan untuk pendataan jumlah tabungan yang telah dilakukan oleh Nasabah Bank Sampoerna.
c. Kelola Pinjaman merupakan menu yang digunakan untuk pendataan jumlah pinjaman dan mengedit data pinjaman nasabah Bank Sampoerna.
d. Ubah Kata Sandi merupakan menu yang digunakan untuk mengubah kata sandi untuk menjaga keamanan data nasabah.
e. Keluar.

3. Menu Utama Sistem Transaksi Nasabah Bank Sampoerna dengan *Hill Cipher* untuk *User*. Tampilan menu utama sistem transaksi nasabah Bank Sampoerna dengan *hill cipher* untuk *user* dapat dilihat pada Gambar 8.

Gambar 8. Tampilan Menu Utama Sistem Transaksi Nasabah Bank Sampoerna dengan *Hill Cipher* untuk *user*

Menu utama yang digunakan pada sistem transaksi *Hill Cipher* untuk *user*. Terdapat beberapa menu yaitu:

1. Informasi saldo merupakan menu yang digunakan oleh *user* untuk mengetahui isi saldo rekening nasabah Bank Sampoerna.
2. Penarikan tunai merupakan menu yang digunakan oleh user untuk mengetahui sejumlah uang yang telah diambil dari tabungan nasabah tersebut.
3. Ubah kode PIN merupakan menu yang digunakan untuk mengubah PIN untuk menjaga keamanan data nasabah.
4. Dan *cancel* menu yang digunakan untuk keluar dari sistem menu transaksi nasabah.

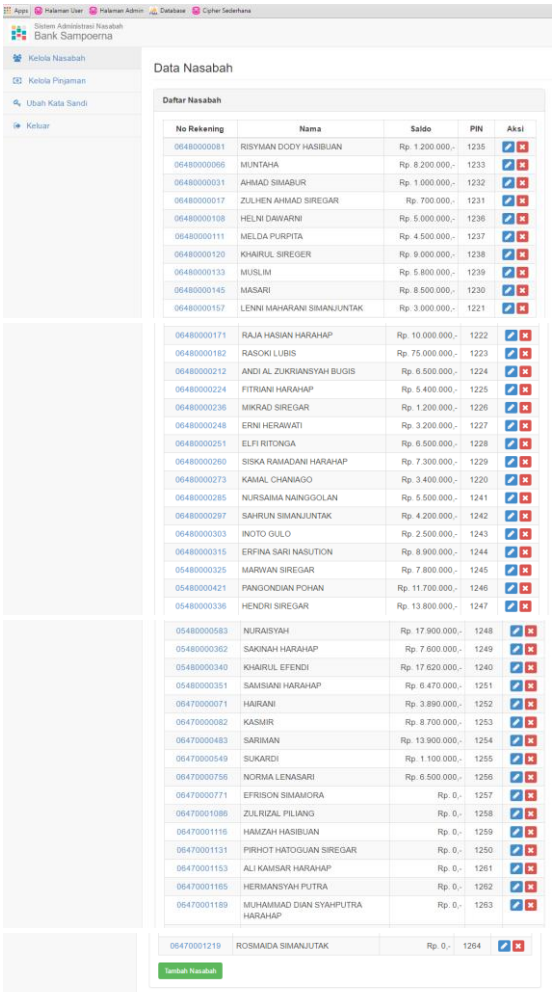
3. Implementasi WEB menggunakan Algoritma *Hill Cipher* kode ASCII dalam Enkripsi Data Keuangan Nasabah Bank Sampoerna

Pengujian pada Sistem yang Dibuat

Dalam pengujian ini, peneliti meginputkan kunci yang akan digunakan dalam proses enkripsi. Kunci yang digunakan sebelumnya sudah ditentukan terlebih dahulu dan merupakan kunci matriks yang mempunyai determinan 1 dan -1. Sistem akan secara otomatis melakukan penyimpanan sehingga pada perhitungan enkripsi dan dekripsi dapat langsung memanggil kunci tersebut. Tampilan proses penginputan kunci dekripsi dan enkripsi yang berhasil dilakukan oleh sistem dapat dilihat pada Gambar 9 sampai dengan Gambar 16.

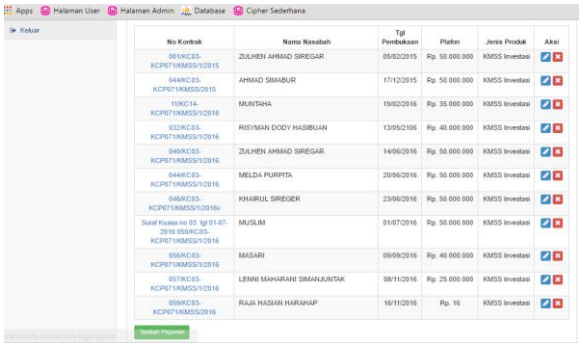
1. Dekripsi

Tampilan dekripsi kelola data nasabah dapat dilihat pada Gambar 9.



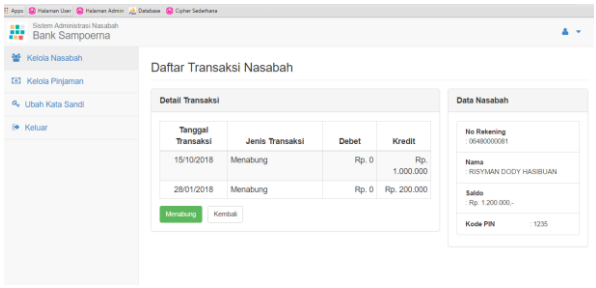
Gambar 9. Tampilan Dekripsi Kelola Data Nasabah.

Tampilan dekripsi pinjaman data nasabah dapat dilihat pada Gambar 10.



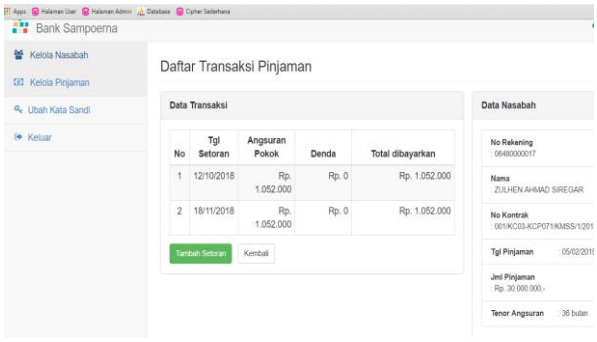
Gambar 10. Tampilan Dekripsi Pinjaman Nasabah.

Tampilan dekripsi tabungan data nasabah dapat dilihat pada Gambar 11.



Gambar 11. Tampilan Dekripsi Tabungan Nasabah.

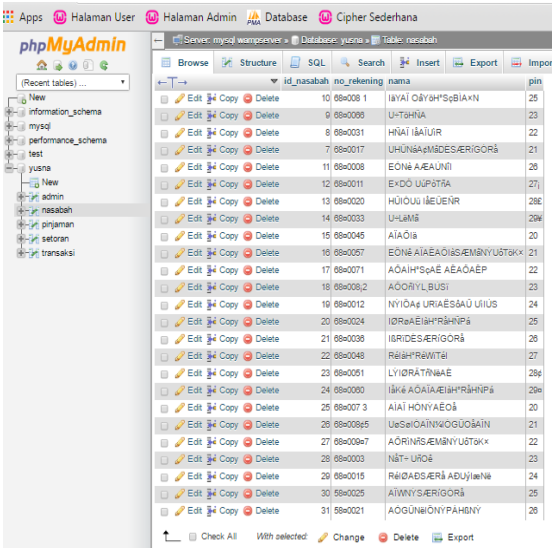
Tampilan dekripsi setoran data nasabah dapat dilihat pada Gambar 12.



Gambar 12. Tampilan Dekripsi Setoran Nasabah.

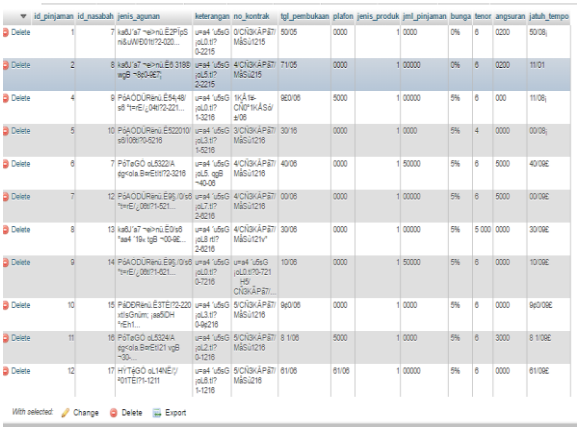
2. Enkripsi

Tampilan enkripsi kelola nasabah dapat dilihat pada Gambar 13.



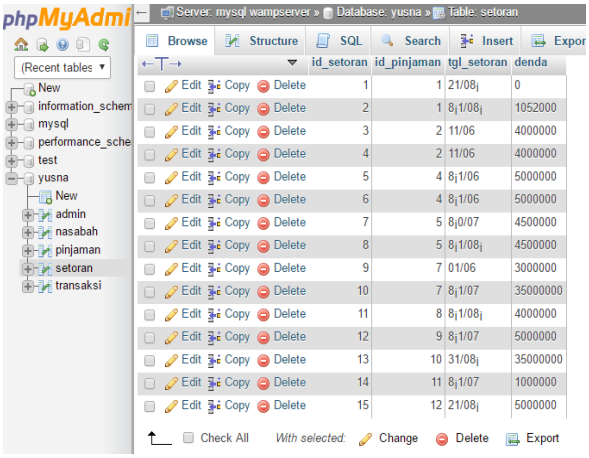
Gambar 13. Tampilan Enkripsi Kelola Nasabah

Tampilan enkripsi kelola pinjaman nasabah dapat dilihat pada Gambar 14



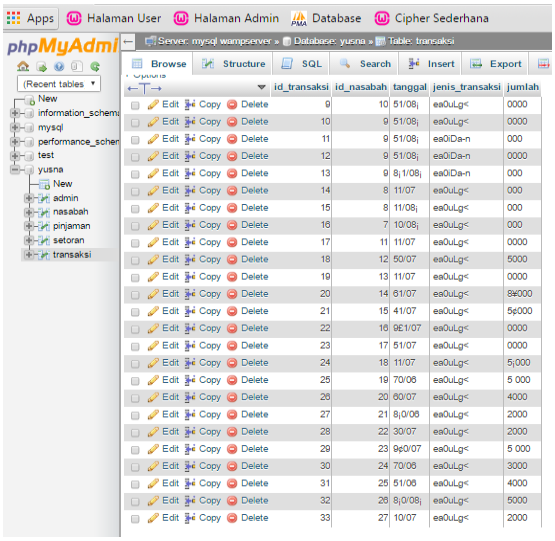
Gambar 14. Tampilan Enkripsi Kelola Pinjaman Nasabah

Tampilan enkripsi transaksi setoran nasabah dapat dilihat pada Gambar 15.



Gambar 15. Tampilan Enkripsi Transaksi Setoran Nasabah

Tampilan enkripsi detail transaksi nasabah dapat dilihat pada Gambar 16



Gambar 16. Tampilan Enkripsi Detail Transaksi Nasabah

Analisis Hasil Pengujian pada Sistem

Proses pengujian program aplikasi kriptografi ini dilakukan pada setiap halaman untuk meyakinkan apakah program aplikasi yang telah dikembangkan dapat berjalan dengan baik dan sesuai dengan tujuan awal sehingga layak digunakan. Tabel keefektifan aplikasi pada sistem terlihat pada Tabel 11.

Setelah semua halaman diuji coba dan dijalankan dapat berjalan dengan baik, maka dapat disimpulkan bahwa program aplikasi ini sangat *user friendly* dan efektif dan terjamin keamanannya karena setiap *user* yang akan menggunakan program aplikasi ini harus memasukkan PIN, dan apabila ada kesalahan pada saat pemasukkan PIN yang tidak tepat maka program memberikan kesempatan untuk memperbaiki kembali PIN sampai benar.

Dalam pengujian program aplikasi ini belum dapat diimplementasikan karena masih dalam bentuk *prototype* artinya proses pembuatan model s*oftware*-nya masih sederhana atau masih gambaran dasar tentang program serta masih dengan pengujian awal dan *Prototype* hanya mengimplementasikan beberapa bagian fungsi dari perangkat lunak yang sesungguhnya. Dengan cara ini pemakai akan mendapat gambaran tentang program yang akan di hasilkan, sehingga dapat menjabarkan lebih rinci kebutuhannya.

Tabel 11. Keefektifan Aplikasi pada Sistem

Deskripsi	Masukan	Kriteria Evaluasi Hasil	Hasil	Kesimpulan
Login dan logout (admin)	Username dan password	Admin masuk ke halaman admin	Login dan logout berhasil	**Diterima**
Login dan logout (user)	PIN	User masuk ke halaman user	Login dan logout berhasil	**Diterima**
Menampilkan halaman nasabah 1. Kelola nasabah	No rekening, nama, saldo, PIN, aksi	Menampilkan tabel nomor rekening, nama, saldo, PIN, Aksi	Kelola nasabah dapat ditampilkan	**Diterima**
Menampilkan halaman fitur menabung pada halaman transaksi nasabah	Tanggal menabung dan Jumlah tabungan	Menampilkan tambah saldo tabungan dan tersimpan	Tambah saldo tabungan tertampil dan data tersimpan	**Diterima**
Menampikan, menambah, megubah, menghapus data nasabah	No Rekening, Nama, Saldo, PIN dll	Kelola data nasabah dapat diubah, ditambah, dan dihapus	Kelola data nasabah berhasil	**Diterima**
2.Kelola pinjaman	No kontrak, nama nasabah, tanggal pembukaan, plafon, jenis produk, aksi	Menampilkan tabel nomor kontrak, nama nasabah, tanggal pembukaan, plafon, jenis produk, aksi	Kelola pinjaman dapat ditampilkan	**Diterima**
Menampilkan daftar transaksi pinjaman	Data transaksi dan data nasabah	Menampilkan daftar transaksi pinjaman nasabah sesuai dengan no rekening nasabah	Detail transaksi dan data pinjaman dapat ditampilkan	**Diterima**
Menampilkan halaman fitur tambah setoran pada halaman transaksi pinjaman	Tanggal setoran, dan denda	Menampilkan tambah setoran dan tersimpan	Tambah setoran tertampil dan data tersimpan	**Diterima**
Menampikan, menambah, megubah, menghapus data pinjaman	No kontrak, nama nasabah, tanggal pembukaan, plafon, jenis produk dll	Kelola data pinjaman dapat diubah, ditambah, dan dihapus	Kelola data pinjaman berhasil	**Diterima**
3.Ubah kata sandi	Password lama, password baru, ulangi password baru	Dapat membuat, mengubah password akun nasabah dan tersimpan	Kelola ubah kata sandi berhasil	**Diterima**
4.Halaman dashboard	PIN	Dapat menampilkan halaman dashboard dengan menu informasi saldo, penarikan tunai, ubah kode PIN dan cancel	Halaman dashboard tertampil	**Diterima**

Evaluasi Hasil Pengujian

Setelah dilakukan uji coba terhadap program aplikasi ini, didapatkan beberapa kelebihan dan kekurangan dari program aplikasi dengan algoritma *Hill Cipher* ini, yaitu sebagai berikut:

Kelebihan Program Aplikasi

1. Implementasi *Hill Cipher* pada kode ASCII dengan WEB ini akan menghasilkan suatu

deretan karakter yang sulit untuk ditebak (didekripsi) karena pada kode ASCII ini semua simbol, spasi, operator dan sebagainya dapat dikodekan menjadi suatu bilangan.

2. *Hill Cipher* merupakan algoritma kriptografi klasik yang sangat kuat dari segi keamanan dan kuat dalam menghadapi *ciphertext-only attack* dan *Hill Cipher* merupakan algoritma kriptografi kunci simetris yang sangat sulit dipecahkan, karena teknik kriptanalis seperti analisis frekuensi tidak dapat diterapkan dengan mudah untuk memecahkan algoritma ini 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.
3. Program aplikasi ini dapat dengan mudah dioperasikan oleh pengguna, karena memiliki *user interface* (tampilan antar muka) yang cukup baik dan *user friendly*. Aplikasi ini dapat mengenkripsi file rahasia dengan aman. File yang telah terenkripsi tidak dapat dibuka, sehingga meminimalkan kebocoran isi *file*.
4. Pengaksesan data yang cepat karena dapat diakses menggunakan internet, serta meningkatkan keamanan penyimpanan data untuk menghindari pengaksesan data oleh pemakai yang tidak berhak.
5. Dari hasil penelitian, perancangan yang telah dilakukan adalah sistem informasi berbasis WEB ini dirancang sebagai solusi untuk mengelola laporan data nasabah secara cepat dan tepat dibandingkan secara manual sehingga kinerja dalam mencapai pekerjaan dapat diwujudkan secara lebih maksimal.

Kekurangan Program Aplikasi

1. Aplikasi *Hill Chiper* pada penelitian ini hanya menggunakan matriks persegi dan matriks enkripsi dekripsi yang berukuran 2×2. Dan matriks kunci yang digunakan masih berukuran kecil dengan determinan 1 atau -1 sehingga memungkinkan kriptanalis lebih mudah memecahkan *Hill Cipher.*
2. Algoritma *Hill Cipher* ini dapat dipecahkan dengan mudah apabila seorang kriptanalis memiliki potongan berkas *ciphertext* dan *plaintext*-nya *(known-plaintext)* yang berkorespondensi serta mengetahui panjang kunci yang digunakan. Kelemahan dalam pengiriman kunci disebut *key distribution problem* untuk tiap pengiriman pesan dengan pengguna yang berbeda dibutuhkan kunci yang berbeda juga, sehingga akan terjadi kesulitan dalam manajemen kunci tersebut.
3. Rancangan aplikasi pada penelitian ini belum lengkap dikarenakan masih sebatas rancangan dan belum menjadi sebuah aplikasi WEB yang relevan dan rancangan sistem informasi ini dibuat bersifat *intern,* artinya pengguna program ini hanya kalangan tertentu yang memiliki hak akses terhadap sistem ini yaitu administrator dan *user*.
4. Pada rancangan aplikasi dengan WEB browser ini tidak semua karakter bisa dimunculkan pada layar browsernya karena karakter *encoding browser*-nya tidak mengenali karakter tersebut dan karena WEB *browser* hanya diperuntukkan dengan menggunakan bahasa HTML sehingga karakter yang tidak sesuai standar HTML tidak dikenali (tidak mengetahui cara menampilkan karakter asing) meski sebenarnya ada.
5. Data yang dapat diolah pada aplikasi ini hanya berbentuk huruf, angka dan karakter tertentu saja, diharapkan algoritma ini dapat dikembangkan dan diterapkan pada data selain karakter.

PENUTUP

Berdasarkan hasil dari perhitungan dan pengujian algoritma *Hill Cipher* dalam dekripsi enkripsi data keuangan nasabah bank dengan menggunakan kode ASCII yang telah dilakukan, dapat disimpulkan sebagai berikut: Proses enkripsi dan dekripsi yang dilakukan pada database Bank Sampoerna berhasil dilakukan. Database asli *(plaintext)* dapat dienkripsi menjadi database yang disandikan *(chipertext)* dan dapat didekripsi menjadi database asli kembali. Sistem keamanan pada pengguna dibangun dengan menerapkan proses autentifikasi nasabah berupa *username* dan *password* serta penggunaan metode kriptografi *Hill Cipher* pada proses transaksi yaitu pada saat nasabah melakukan transaksi menggunakan WEB. Metode algoritma *Hilll Cipher* dengan menggunakan Kode ASCII telah diimplementasikan dalam penginputan data keuangan nasabah bank dengan menggunakan *range* data sesuai dengan aturan Bank. 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.

DAFTAR PUSTAKA

Ariyus, D. (2008). *Pengantar Ilmu Kriptografi : Teori Analisis & Implementasi*.

Hasugian, A.H. (2013). Implementasi Algoritma Hill Cipher dalam Penyandian Data. *Jurnal Informatika*, IV(2): 115-122.

Hidayat, A. & Awiyah, T. (2013). Enkripsi dan Dekripsi Teks menggunakan Algoritma Hill Cipher dengan Kunci Matriks Persegi Panjang. *Jurnal Matematika*, 9(1), 39-51.

Magambar, Kondwani, et al., (2012). *Variable-length Hill Cipher with MDS Key Matrix,.*

Munir, R. (2006). *Kriptografi*. Bandung : ITB Informatika.

Pasaribu, J.S., (2016). *Penerapan Algoritma Hill Cipher dalam Pengamanan Data dengan Teknik Enkripsi dan Dekripsi*. Teknik Informatika, Politeknik Piksi Ganesha.

Rahmawati, S. (2014). Pengolahan Data untuk Keamanan Database Akademik dengan Metode Kriptografi Menggunakan Bahasa Pemrograman Php dan Database My Sql. *Majalah Ilmiah UPI YPTK*, Oktober, 21(21), 28-34.

Rosnawan, D. (2011). *Aplikasi Algoritma Rsa untuk Keamanan Data pada Sistem Informasi Berbasis Web*. Skripsi. Semarang: FMIPA Universitas Negeri Semarang.

Palupi, D.R. (2015). *Implementasi Algoritma Hill Cipher dalam Penyandian Data Nilai Akhir Semester pada Program Studi Ti-S1 Tahun Ajaran 2014/2015 dengan Menggunakan Kode ASCII*. Skripsi. Semarang: Fakultas Ilmu Komputer Universitas Dian Nuswantoro Semarang.

Widyanarko, A. (2009), Studi dan Analisis mengenai Hill Cipher, Teknik Kriptanalisis dan Upaya Penanggulangannya, *Program Studi Teknik Informatika*, Institut Teknologi Bandung.

Widyartono, A. (2011). Algoritma Elgamal untuk Enkripsi Data menggunakan GNPUG. *Jurnal informatika.* 1(1), 29-35.