PERANCANGAN APLIKASI KRIPTOGRAFI ENKRIPSI DAN DESKRIPSI ALGORITMA MATRIKS HILL CIPHER PADA PERANGKAT ANDROID

Zulhamdani Napitupulu
Ilmu Komputer, Universitas Nahdlatul Ulama Sumatera Utara
Email: zulhamdani@gmail.com

Abstrak

Perkembangan Teknologi komunikasi yang berkembang terus setiap tahunnya salah satunya adalah Android, diikuti tindak kejahatan yang dilakukan oleh hacker untuk melakukan pencurian informasi atau data yang berguna bagi kepentingan dirinya sendiri atau kepentingan dari suatu kelompok. Oleh sebab itu diperlukan ilmu pengamanan pesan salah satunya adalah ilmu kriptografi. Ilmu kriptografi yaitu ilmu atau seni untuk merahasiakan pesan. Maka dalam penulisan penelitian ini, penulis akan menggunakan algoritma Hill Cipher untuk diimplementasikan ke dalam sebuah aplikasi kriptografi yang berfungsi untuk melakukan enkripsi dan deskripsi terhadap pesan yang akan dikirim. Diharapkan ini dapat membantu dalam hal pengamanan pesan yang akan dikirim dan juga perkembangan ilmu kriptografi selanjutnya.

Kata kunci : Kriptografi, Enkripsi, Dekripsi, Hill Cipher

PENDAHULUAN

Berkembangnya teknologi komunikasi seiring zaman mempermudah dalam hal melakukan komunikasi. Perkembangan teknologi komunikasi bertujuan untuk memenuhi komunikasi yang lebih terhubung secara realtime, cepat, dan efisien. Zaman dulu sebuah pesan atau informasi dikirim dalam waktu beberapa hari, berkembang menjadi dalam waktu peredetik. Dan pesan atau informasi yang disampaikan lebih update dan realtime pada zaman sekarang daripada zaman dulu, ini disebabkan oleh kecepatan pengiriman pesan. Komunikasi adalah dua entitas atau lebih yang berhubungan untuk mengirim dan menerima pesan atau informasi. [1].

Banyaknya kejahatan pencurian informasi yang timbul, maka zaman dahulu sudah mulai mengembangkan sebuah ilmu penyamaran pesan salah satunya adalah kriptografi. Kriptografi berasal dari bahasa Yunani yaitu berasal dari kata crypto dan graphia. *Crypto* adalah rahasia, sedangkan graphia adalah tulisan, dasar ilmu kriptografi berasal dari ilmu matematika memanfaatkan perhitungan matematika dengan mengunakan algoritma matematika yang ada. Dan algoritma yang dipilih oleh penulis dalam penulisan skripsi kriptografi ini adalah algoritma matriks *Hill Cipher*. Matriks adalah kumpulan fungsi atau bilangan yang membentuk kotak persegi panjang maupun bujur sangkar yang disusun berdasarkan baris dan kolom diapit dua kurung siku.[2]

Penulis merancang algoritma Hill Cipher dengan menggunakan aplikasi adroid. Pemilihan aplikasi dikarenakan pemakai android yang sangat banyak daripada aplikasi lain sehingga menjadi target para pengguna untuk melakukan pencurian informasi. Aplikasi android bersifat open source yang memudahkan untuk mengembangkan program dan pengembang android sendiri

mengembangkan sebuah software untuk membuat aplikasi di android salah satunya ADT (Android Developer Tool). ADT merupakan kerja sama antara pengembang android dengan eclipse. Dalam penulisan coding di ADT harus dikuasai bahasa pemrograman Java dan XML. Pemakaian dua bahasa ini dengan tujuan untuk memanage kode program, yaitu bahasa Java digunakan untuk menulis algoritma pemrograman proses dan XML digunakan untuk mendesign interface program input dan output, sedangankan SQLite adalah bahasa pemrograman database yang bertujuan untuk menyimpan kunci.[3]

TINJAUAN PUSTAKA

2.1 Kriptografi

Kriptografi menurut beberapa pakar terkenal yaitu [4] :

1. Bruce Schiener dalam buku berjudul "Applied Cryptography" Kriptografi adalah sebuah ilmu atau seni untuk menjaga kerahasian pesan.
2. Alferd J. Menezes, Paul C van Oorschot, dan Scott A. Vanstone dalam buku berjudul "Handbook of Apllied Cryptography"
   Kriptografi adalah ilmu yang memperlajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasian, integritas data, serta otentikasi.

2.2 Terminologi

Ada beberapa istilah yang akan sering ditemukan di dalam ilmu kriptografi. Oleh sebab itu penulis akan menjelaskan beberapa istilah penting [5] yang perlu diketahui dalam ilmu kriptografi yaitu:

1. Pesan, Plainteks, dan Cipherteks
   Pesan adalah sebuah informasi ataupun data yang dapat dibaca dan dimengerti maknanya. nama lain pesan dalam ilmu kriptografi yaitu plainteks atau cleartext. Cipherteks adalah sebuah pesan yang telah diacak atau telah disandikan ke dalam bentuk lain yang tidak dapat dimengerti. Cipherteks harus dapat disandikan kembali menjadi pesan asli atau plainteks agar dapat dimengerti.
2. Enkripsi dan Dekripsi
   Enkripsi yaitu proses yang menyandikan plainteks (pesan, informasi, data) ke dalam bentuk lain yang tidak dimengerti yang disebut dengan cipherteks. Dekripsi adalah proses mengembalikan bentuk cipherteks kembali menjadi palinteks agar pesan bisa dimengerti.
3. Pengirim, Penerima, dan Penyadap
   Pengirim yaitu merupakan sumber infomasi (dapat berupa pesan atau data) yang akan dikirimkan ke si penerima, jadi pengirim dan penerima saling berkomunikasi. Penyadap adalah orang yang berusaha untuk mendapatkan pesan yang ditransmisikan.
4. Cipher dan kunci
   Cipher disebut juga sebagai algoritma kriptografi. Alogartima kriptografi yaitu kumpulan perintah atau fungsi matematika yang berfungsi untuk melakukan proses enkripsi dan dekripsi. Kunci merupakan sebuah parameter yang ditetapkan oleh pemakai agar algoritma enkripsi dan dekripsi melakukan pengacakan dan pengembalian pesan sesuai dengan ketentuan kunci yang diberikan atau ditetapkan.

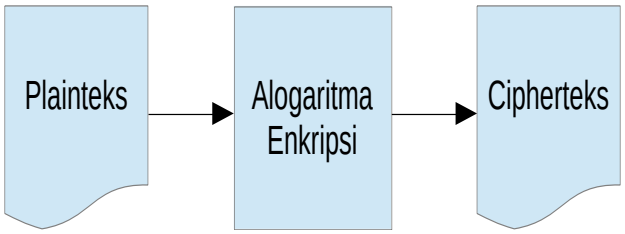
5. Kriptanalisis
   Kriptanalisis adalah ilmu atau seni yang berusaha untuk memecahkan cipherteks menjadi plainteks tanpa mengetahui algoritma atau kunci yang digunakan. Tujuan kriptanalisis adalah untuk menguji algoritma kriptografi seberapa kuatnya dalam mengrahasiakan plainteks.

2.3 Kriptografi Klasik dan Modern

1. Kriptografi Klasik
   Kriptografi klasik adalah kriptografi yang mengunakan perhitungan secara manual atau sederhana (pensil dan kertas) dan alat mekanik sederhana untuk membantu enkripsi dan dekripsi tanpa menggunakan komputer. Kriptografi klasik dalam melakukan proses enkripsi dan dekripsi adalah berbasis karakter yaitu proses yang dilakukan secara satu persatu karakter pesan dengan metode subtitusi (penggantian karakter) dan/atau metode transposisi (pertukaran tempat) [6].
2. Kriptografi Modern
   Kriptografi modern adalah kriptografi yang sudah memakai perhitungan yang sangat kompleks sehinggah diperlukan komputer untuk memprosesnya dan pemakaian mode bit (bahasa mesin) daripada mode karakter sehinggah diperlukan komputer untuk memprosesnya [7].

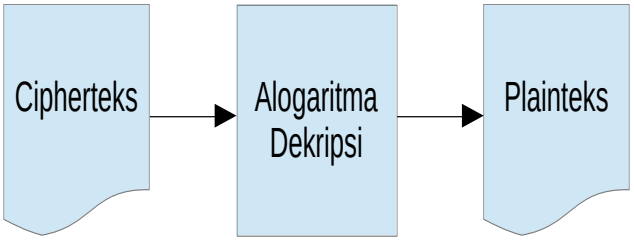
2.4 Enkripsi dan Dekripsi

1. Enkripsi
   Enkripsi adalah kumpulan algoritma matematika yang bertugas untuk melakukan proses pengacakan plainteks menjadi cipherteks.



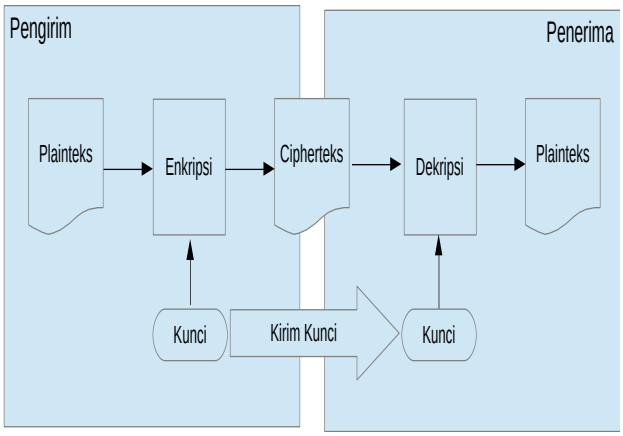
Gambar 1 Alur Enkripsi

2. Dekripsi
   Dekripsi adalah kumpulan algoritma matematika untuk melakukan proses pengembalian cipherteks menjadi plainteks.



Gambar 2: Alur Dekripsi

Konsep matematis yang mendasari algoritma kriptografi adalah relasi antara dua buah himpunan yang berisi elemen-elemen plainteks dan himpunan yang berisi cipherteks. Enkripsi dan dekripsi merupakan sebuah fungsi yang memetakan elemen-elemen antara kedua himpunan tersebut.



Gambar 3: Alur Algoritma Kriptografi Kunci

2.5 Teknik Menemukan Kunci

Pada serangan ini bertujuan untuk mencari kunci untuk mendekripsikan cipherteks, serangan ini terbagi menjadi 2 serangan yaitu :

1. Exhaustive attack atau brute force attack
   Serangan untuk menemukan kunci dekripsi pada cipherteks ini dengan cara untuk mencoba semua kunci kemungkinan yang ada. Teknik ini menerapakan cara mendekripsikan cipherteks dengan mencoba kunci secara satu-satu, bila tidak ditemukan plainteks yang tidak mengandung arti maka gunakan kunci lain sampai menemukan plainteks tersebut mengandung arti, maka kunci juga berhasil ditemukan.
2. Analytical attack
   Pada serangan ini tidak dilakukan semua mencoba semua kunci kemungkinan. Tetapi menganalisa kelemahan sebuah kriptografi untuk mengurangi kunci yang tidak mungkin ada, lalu mencoba kunci yang telah kita pilih untuk mendekripsikan cipherteks menjadi plainteks.

2.6 Hill Chpher

Hill Cipher adalah algoritma kriptografi yang menggunakan perhitungan perkalian matriks sebagai enkripsi dan dekripsi dalam kriptografi. Hill Cipher dikembangkan oleh Lester Hill pada tahun 1929. Hill Cipher merupakan jenis kunci kriptografi simetri [8]. Cara kerja Hill Cipher yaitu mengganti satu karakter dengan karakter lainnya atau disebut dengan metode subtitusi. Kunci pada Hill Cipher disebut dengan matriks K dengan ukuran n x n (berbentuk bujur sangkar). Matriks K harus memiliki invers matriks itu bertujuan untuk proses dekripsi yang mengembalikan cipherteks ke plainteks

Tabel 1 Konversi Alfabet ke Angka Hill Cipher

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

1. Teknik Enkripsi Algoritma Hill Cipher
   Teknik enkripsi alogartima *Hill Cipher* akan dijelaskan dengan sebuah contoh yaitu, pengiriman sebuah pesan yang berisi "KELVIN" dengan kunci matriks berordo 2X2 $K = \begin{bmatrix} 3 & 2 \\ 9 & 1 \end{bmatrix}$. Pertama mengubah pesan ke dalam bentuk angka dengan anggapan dengan table angka pada tabel 1, Jadi K=10, E=4, L=11, V=21, I=8, N=13. Lalu membagikan pesan tersebut menjadi beberapa blok plainteks dan dalam satu blok berisi 2 karakter pesan $P_{1,2} = \begin{bmatrix} 10 \\ 4 \end{bmatrix}$, jadi terbagi menjadi 3 blok plainteks dengan isi masing-masing blok adalah 2 karakter. Blok plainteks yang telah dibagi kemudian dienkripsi mengunakan kunci untuk menghasilkan cipherteks (C).

$$C_{1,2} = \begin{bmatrix} 3 & 2 \\ 9 & 1 \end{bmatrix}\begin{bmatrix} 10 \\ 4 \end{bmatrix} = \begin{bmatrix} (3 \times 10) + (2 \times 4) \\ (9 \times 10) + (1 \times 4) \end{bmatrix} = \begin{bmatrix} 38 \\ 94 \end{bmatrix}$$

$$C_{3,4} = \begin{bmatrix} 3 & 2 \\ 9 & 1 \end{bmatrix}\begin{bmatrix} 11 \\ 21 \end{bmatrix} = \begin{bmatrix} (3 \times 11) + (2 \times 21) \\ (9 \times 11) + (1 \times 21) \end{bmatrix} = \begin{bmatrix} 75 \\ 120 \end{bmatrix}$$

$$C_{5,6} = \begin{bmatrix} 3 & 2 \\ 9 & 1 \end{bmatrix}\begin{bmatrix} 8 \\ 13 \end{bmatrix} = \begin{bmatrix} (3 \times 8) + (2 \times 13) \\ (9 \times 8) + (1 \times 13) \end{bmatrix} = \begin{bmatrix} 50 \\ 85 \end{bmatrix}$$

   Dihasilkan angka yang tidak memiliki korespondensi dengan huruf-huruf, maka hasil perhitungan akan dimodulokan sebanyak 26. Sehinggah $C_{1,2}$ menjadi $C_{1,2} = \begin{bmatrix} 38 \\ 94 \end{bmatrix} = \begin{bmatrix} 12 \\ 16 \end{bmatrix} mod\ 26$. Maka didapatkan huruf yang berkorespondensi dengan angka yaitu M dan Q. Blok yang telah dimodulokan menghasilkan cipherteks yaitu C = 12, 16, 23, 16, 24, 7 dan dikonversikan ke huruf maka C = MQXQYH.

2. **Teknik Dekripsi Algoritma *Hill Cipher***
   Untuk mendekripsikan kembali chipherteks ke plainteks, alogartima *Hill Cipher* mengubah matriks kunci menjadi invers matriks. Lalu mengkalikan invers matriks dengan cipherteks untuk mendapatkan plainteks. Ini akan dijelaskan ke sebuah contoh yang dilanjutkan contoh cipherteks yang dihasilkan enkripsi yang diatas. Cipherteks yaitu C = MQXQYH dan kunci akan melakukan dekripsi untuk mendapatkan plainteks. Kunci akan diubah ke dalam bentuk invers

$$K = \begin{bmatrix} 3 & 2 \\ 9 & 1 \end{bmatrix}, \det(K) = (3 \cdot 1) - (9 \cdot 2) = -15 \ \therefore\ -15\ (mod\ 26)$$
$$= 11$$

   Untuk mendapatkan nilai kebalikan dari determinan dengan mod 26 maka disertakan tabel dibawah ini

Tabel 2 Nilai Kebalikan dari Mod 26

Determinan	1	3	5	7	9	11	15	17	19	21	23	25
Nilai kebalikan mod 26	1	9	21	15	3	19	7	23	11	5	17	25

Dengan menggunakan tabel 2.2 maka nilai kebalikan dari mod 26 pada determinan *K* yaitu 19, maka det(*K*) = 19, lalu kunci diubah ke adjoin matriks

$$adj(K) = \begin{bmatrix} 1 & -2 \\ -9 & 3 \end{bmatrix}$$

pencarian kunci invers dengan melakukan perkalian det (K) dengan adjoin (K)

$$K^{-1} = \frac{1}{\det(K)} \cdot adj(K) = 19 \begin{bmatrix} 1 & -2 \\ -9 & 3 \end{bmatrix} = \begin{bmatrix} 19 & -38 \\ -171 & 57 \end{bmatrix}$$
$$= \begin{bmatrix} 19 & 14 \\ 11 & 5 \end{bmatrix} (mod\ 26)$$

Konversi cipherteks menjadi angka sesuai dengan tabel 2.1 C = MQXQYH menjadi C = 12 16 23 16 24 7, lalu membagi angka tersebut ke dalam blok-blok $\begin{bmatrix} 12 \\ 16 \end{bmatrix}, \begin{bmatrix} 23 \\ 16 \end{bmatrix}, \begin{bmatrix} 24 \\ 7 \end{bmatrix}$. Setelah itu melakukan perkalian dengan kunci invers matriks untuk mendapatkan plainteks (*P*).

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

$$P_{1,2} = \begin{bmatrix} 19 & 14 \\ 11 & 5 \end{bmatrix} \begin{bmatrix} 12 \\ 16 \end{bmatrix} = \begin{bmatrix} (19 \cdot 12) + (14 \cdot 16) \\ (11 \cdot 12) + (5 \cdot 16) \end{bmatrix} = \begin{bmatrix} 452 \\ 212 \end{bmatrix}$$
$$= \begin{bmatrix} 10 \\ 4 \end{bmatrix} (mod\ 26)$$

$$P_{3,4} = \begin{bmatrix} 19 & 14 \\ 11 & 5 \end{bmatrix} \begin{bmatrix} 23 \\ 16 \end{bmatrix} = \begin{bmatrix} (19 \cdot 23) + (14 \cdot 16) \\ (11 \cdot 23) + (5 \cdot 16) \end{bmatrix} = \begin{bmatrix} 661 \\ 333 \end{bmatrix}$$
$$= \begin{bmatrix} 11 \\ 21 \end{bmatrix} (mod\ 26)$$

$$P_{5,6} = \begin{bmatrix} 19 & 14 \\ 11 & 5 \end{bmatrix} \begin{bmatrix} 24 \\ 7 \end{bmatrix} = \begin{bmatrix} (19 \cdot 24) + (14 \cdot 7) \\ (11 \cdot 24) + (5 \cdot 7) \end{bmatrix} = \begin{bmatrix} 554 \\ 299 \end{bmatrix}$$
$$= \begin{bmatrix} 8 \\ 13 \end{bmatrix} (mod\ 26)$$

Didapat plainteks yaitu *P* = 10 4 11 21 8 13, lalu dikonversikan ke alfabet menggunakan tabel 2.1 maka plainteks menjadi P = KELVIN.

3. Analisa Alogaritma *Hill Cipher*

Algortima *Hill Cipher* memiliki metode subtitusi yang menghasilkan frekuensi yang tidak sama sehinggah dengan metode serangan *ciphertext only attack* akan sulit dilakukan. Kelemahan utama pada *Hill Cipher* jika serangan mengunakan metode *know plaintext attack*. Pada serangan ini jika penyerang dapat mengumpulkan sepasang plainteks dan sepasang cipherteks yang menggunakan kunci yang sama maka bisa didapatkan kunci yang digunakan dalam *Hill Cipher* dengan menggunakan persamaan linear. Sebagai contoh untuk membuktikannya maka akan digunakan

contoh plainteks dan cipherteks pada proses enkripsi dan dekripsi *Hill Cipher* yaitu memakai plainteks
P = KELVIN dan cipherteks *C* = MQXQYH
Konversikan alfabet menjadi angka
P = 10 4 11 21 8 13 *C* = 12 16 23 16 24 7
dan membagi *P* dan *C* ke dalam blok-blok dengan 1 blok berisi 2 angka dari karakter yang telah dikonversikan

$$P_{1,2} = \begin{bmatrix}10\\4\end{bmatrix}, P_{3,4} = \begin{bmatrix}11\\21\end{bmatrix}, P_{5,6} = \begin{bmatrix}8\\13\end{bmatrix}$$
$$C_{1,2} = \begin{bmatrix}12\\16\end{bmatrix}, C_{3,4} = \begin{bmatrix}23\\16\end{bmatrix}, C_{5,6} = \begin{bmatrix}24\\7\end{bmatrix}$$

$C = \begin{bmatrix}23 & 24\\16 & 7\end{bmatrix}$Memilih $P_{3,4}$ dan $P_{5,6}$, pemilihan kedua matriks karena menghasilkan invers matriks. Pemilihan kedua matriks *P* maka *C* memilih $C_{3,4}$ dan $C_{5,6}$yang merupakan hasil cipherteks dari plainteks. Dan menggabungkan masing-masing *P* ke dalam satu matriks, demikian matriks *C*.

$$P = \begin{bmatrix}11 & 8\\21 & 13\end{bmatrix}$$

Untuk mendapatkan kunci menggunakan persamaan linear digunakan persamaan kriptografi *C* = *K*.*P* dengan susunan matriks $K = \begin{bmatrix}a & b\\c & d\end{bmatrix}$

$$C = K.P$$
$$\begin{bmatrix}23 & 24\\16 & 7\end{bmatrix} = \begin{bmatrix}a & b\\c & d\end{bmatrix}\begin{bmatrix}11 & 8\\21 & 13\end{bmatrix}$$

$11a + 21b = 23$ [i]
$8a + 13b = 24$ [ii]
$11c + 21d = 16$ [iii]
$8c + 13b = 7$ [iv]
Selesaikan persamaan [i] dan [ii] dengan metode subtitusi, lalu selesaikan persamaan [iii] dan [iv] dengan metode yang sama
$11a + 21b = 23$ [i]

$$21b = 23 - 11a$$
$$b = (23 - 11a)5$$
$$b = (115 - 55a)mod 26$$

$b = 11 + 23a$ [i]

$8a + 13b = 24$ [ii]
$8a + 13(11 + 23a) = 24$
$8a + 143 + 299a = 24$
$307a = -119$
$(-307a = 119)mod\ 26$
$5a = 15, a = 3$ [ii]

Maka

$b = 11 + 23a$ [i]

$$b = 11 + 23(3)$$
$$b = (80)mod\ 26$$

$b = 2$ [i]
Didapat nilai a dan b yaitu 3 dan 2, melanjutkan persamaan tiga dan empat

$11c + 21d = 16$ [iii]
$21d = 16 - 11c$
$d = (16 - 11c)5$
$d = (80 - 55c)mod\ 26$
$d = 2 + 23c$ [iii]

$8c + 13d = 7$ [iv]
$8c + 13(2 + 23c) = 7$
$8c + 26 + 299c = 7$
$(-307c = 19)mod\ 26$

Maka

$$d = 2 + 23c \text{ [iii]}$$
$$d = 2 + 23(9)$$
$$d = 2 + 207$$
$$d = 209 \bmod 26$$
$$d = 1 \text{ [iii]}$$

$$5c = 19$$
$$c = (19)21, 5^{-1} = 21$$
$$c = (399) mod\ 26$$

$c = 9$ [iv]

Didapatkan c dan d yaitu 9 dan 1, dan jika digabungkan maka matriks kunci $K = \begin{bmatrix} 3 & 2 \\ 9 & 1 \end{bmatrix}$. Dan matriks kunci tersebut sama dengan matriks kunci yang dipakai pada enkripsi dan dekripsi.

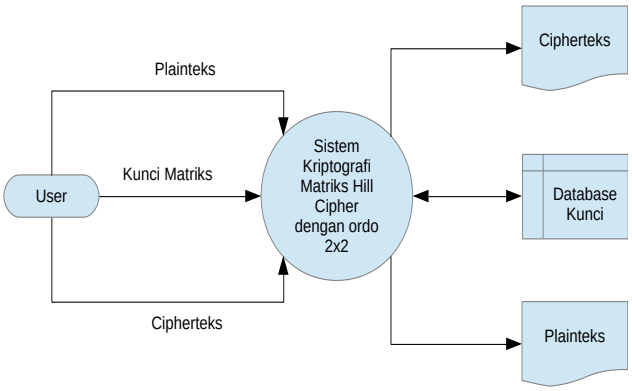
2.7 Android

Android adalah sistem operasi yang berbasis pada kernel linux yang dibuat untuk perangakat mobile seperti smartphone, pc tablet, dll. Android merupakan sistem operasi terbuka atau *open source*, sehinggah para pengembang bebas untuk mengembangkan aplikasi yang mereka inginkan. Android dibeli oleh Google dan untuk mengembangkan sistem operasi android Google membentuk *Open Handset Alliance*, ini merupakan gabungan 34 perusahaan yang terdiri dari perusahaan perangkat keras, peranti lunak, dan telekomunikasi yang termasuk didalamnya adalah Google, HTC, Intel, Motorola, Qualcomm, T-Mobile, dan Nividia[9].

PEMBAHASAN

1. **Perancangan Sistem Kriptografi *Hill Cipher***

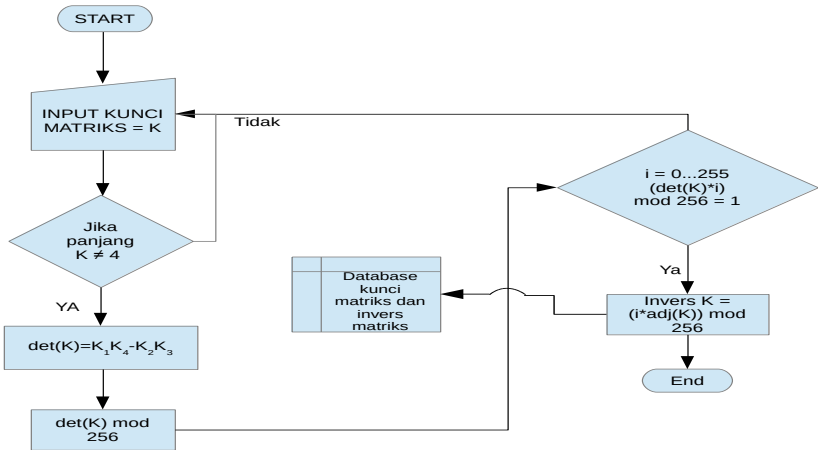
   Sistem adalah kumpulan beberapa perintah yang membentuk satu kesatuan untuk mencapai sebuah tujuan. Sistem kriptografi *Hill Cipher* adalah kumpualn perintah untuk menjalankan proses kriptografi dengan metode *Hill Cipher*.



Gambar 4 Flowchart Sistem Kriptografi Hill Cipher

2. **Flowchart Perhitungan Kunci Matriks**

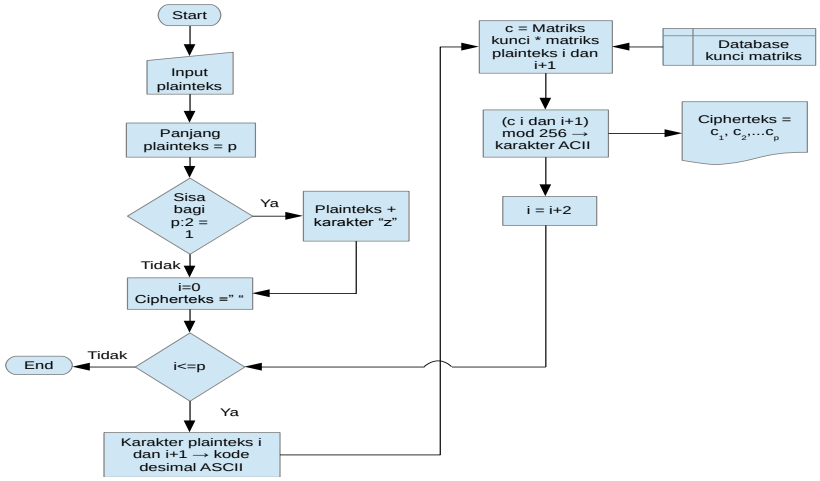
   Dalam Hill Cipher penentuan sebuah kunci matriks adalah utama dalam proses enkripsi dan dekripsi, jika kunci matriks tidak mempunyai matriks invers maka proses dekripsi pada sebuah cipherteks tidak akan mendapatkan kembali plainteks (pesan asli) meskipun pesan tersebut dapat terenkripsi. Proses pencarian kunci matriks invers dari kunci matriks (K) berordo 2×2



Gambar 5 Flowchart Perhitungan Kunci Matriks

3. Proses *Flowchart* Perhitungan Enkripsi

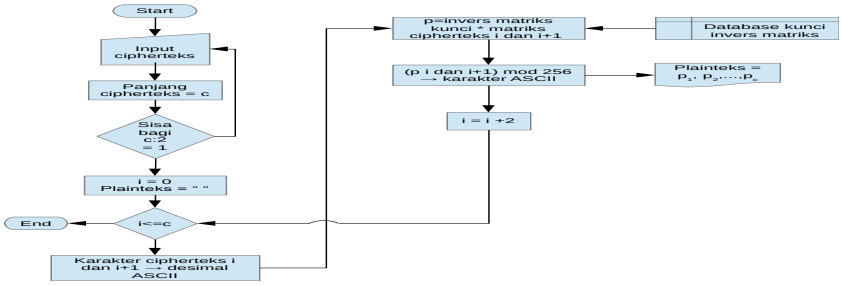
Proses enkripsi pada *Hill Cipher* menggunakan teknik perkalian matriks antara matriks kunci dengan plainteks untuk mendapatkan cipherteks.



Gambar 6 Flowchart Proses Enkripsi Hill Cipher

4. Proses Flowchart Perhitungan Dekripsi

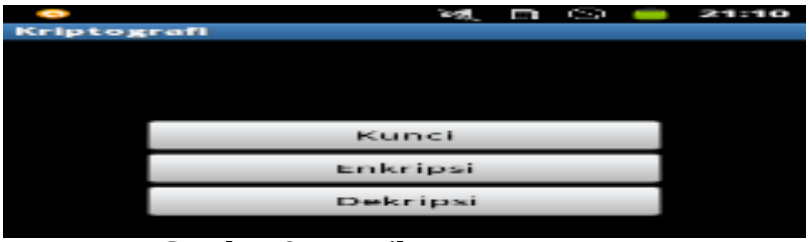
Proses dekripsi pada *Hill Cipher* menggunakan teknik perkalian matriks antara kunci matriks invers dengan cipherteks untuk mendapatkan plainteks.



Gambar 7 Flowchart Proses Dekripsi Hill Cipher

Perancangan User Interface Kriptografi Hill Cipher

User interface adalah tampilan halaman sebuah program. User interface utama pada kriptografi Hill Cipher terbagi menjadi beberapa bagian yaitu bagian kunci, enkripsi, dan dekripsi. Gambar 3.5 merupakan tampilan utama program krpitografi Hill Cipher.



Gambar 8 Tampilan Utama Program

Gambar 9 Tampilan Enkripsi Data

Gambar 10 Tampilan Deskripsi Data

SIMPULAN DAN SARAN

Simpulan

1. Hasil cipherteks dari algoritma *Hill Cipher* adalah metode subtitusi yaitu menggantikan karakter satu dengan karakter lainnya.
2. Karakter cipherteks yang dihasilkan tidak akan memiliki kesamaan satu dengan yang lainnya meskipun karakter plainteks tersebut sama. Sebagai contoh karakter “a” pada plainteks maka karakter cipherteks adalah “x” dan untuk karakter kedua dari “a” bisa saja “p”, “x” ataupun yang lainnya.
3. Panjang karakter akan mempengaruhi hasil cipherteks pada algoritma *Hill Cipher*. Sebagai contoh dua yaitu kalimat “ada tiga rumah” dan “itu tiga rumah” memiliki panjang karakter yang sama yaitu empat belas karakter ,maka cipherteks yang dihasilkan akan sama yaitu dimulai dari kalimat “tiga rumah” sedangakan empat karakter yang didepannya yang dihasilkan tidak sama. Jika sebuah kalimat “dari tiga rumah” maka hasil cipherteks yang dihasilkan ini tidak akan sama dengan dua kalimat diatas.

4. Penggunaan algoritma untuk pengacakan pesan dapat dilakukan secara berulang-ulang yaitu pesan yang telah terenkripsi dapat kembali dienkripsi kembali. Dan untuk mengembalikan pesan asli maka harus dilakukan dua kali dekripsi.
5. Alogaritma matriks *Hill Cipher* memiliki kelemahan terhadap serangan know plaintext attack, dimana dapat dipecahkan untuk mendapatkan kunci yaitu menggunakan persamaan linear dengan syarat mendapatkan kumpulan plainteks dan cipherteks yang menggunakan kunci yang sama.

Saran

1. Penggunaan kode *Unicode* dengan tujuan karakter yang diproses lebih banyak lagi.
2. Penggabungan alogaritma lain dengan alogaritma *Hill Cipher* untuk meningkatkan tingkat keamanan data atau pesan.
3. Pemberian kunci yang lebih banyak tidak hanya 4 digit nomor tetapi 9 digit nomor untuk meningkatkan kesulitan pemecahan kode *Hill Cipher*.
4. Pengembangan lebih lanjut ke perangkat lain seperti ios, windows phone dan blackberry.

DAFTAR RUJUKAN

[1] Munir, Rinaldi. 2006. *Kriptografi*. Bandung : Informatika.

[2] Sadikin, Rifki. 2012. *Kriptografi untuk Keamanan Jaringan*. Yogyakarta : Andi.

[3] Muis, Saludin.2013. *Pengantar Kriptografi Kuantum Teknik Enkripsi Masa Depan.* Yogyakarta : Graha Ilmu.

[4] Imrona, Mahmud. 2013. *Aljabar Linear Dasar*, Edisi Kedua. Jakarta : Erlangga.

[5] Kadir, Abdul. 2012. *Alogaritma & Pemrograman menggunakan Java*. Yogyakarta : Andi.

[6] Safaat.H, Nazruddin. 2012. *Android: Pemrograman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android*, Edisi Revisi. Bandung : Informatika.

[7] Wahana Komputer. 2013. *Step by Step menjadi Programmer Android*. Yogyakarta : Andi.

[8] Wahana Komputer. 2013. *Android Programming With Eclips*. Yogyakarta : Andi.

[9] Ariyus, Doni. 2008. Pengantar Ilmu Kriptografi. Yogyakarta : Andi Offset.