KRIPTANALISIS HILL CIPHER TERHADAP KNOWN PLAINTEXT ATTACK MENGGUNAKAN METODE DETERMINAN MATRIKS BERBASIS ANDROID

Wafiqah Yasmin Azhar
Teknik Informatika
STMIK Kharisma Karawang
Email: yasminwafiqah@gmail.com

Supriyadi
Teknik Informatika
STMIK Kharisma Karawang
Email: supriyadistmikkharisma@yahoo.com

Yessy Yanitasari
Teknik Informatika
STMIK Kharisma Karawang
Email: yanitasari@yahoo.com

ABSTRAK

Saat ini teknik kriptografi Hill *Cipher* telah diimplementasikan untuk beberapa aplikasi. Dalam implementasinya ada saja kesalahan atau kecerobohan seperti kunci matriks yang digunakan pada proses enkripsi hilang karena tidak disimpan atau bahkan lupa. Oleh sebab itu diperlukan teknik kriptanalisis untuk mendapatkan kembali kunci yang hilang tersebut. Teknik kriptanalisis pada kriptografi Hill *Cipher* yang telah diketahui adalah dengan menggunakan persamaan linier dan menggunakan perkalian matriks. Pada persamaan linier, nilai dari masing-masing variabel matriks kunci dapat diketahui, namun proses pencarian nilai pada tiap variabel tersebut tidak dapat dilakukan dalam waktu yang singkat. Sedangkan pada perkalian matriks proses pencarian variabel matriks kunci hanya dapat dilakukan jika matriks yang merepresentasikan *plaintext* memiliki invers atau nilai determinannya sama dengan satu. Nilai determinan yang didapatkan dari suatu matriks dapat dioperasikan untuk mencari nilai suatu variabel dari operasi aljabar linear yang telah direpresentasikan kedalam bentuk matriks. Masing-masing variabel tersebut dapat melakukan proses pencarian determinan secara bersamaan. Dalam penelitian ini telah dikembangkan suatu sistem untuk mencari nilai pada variabel matriks kunci berdasarkan perhitungan determinan matriks menggunakan paradigma *System Development Life Cycle* (SDLC) *Waterfall* dan diimplementasikan pada sistem operasi berbasis Android

Kata kunci: determinan matriks, hill *cipher*, *known plaintext attack*, kriptanalisis, SDLC *waterfall*.

ABSTRACT

Nowadays Hill Cipher cryptography technique has been implemented for several applications. In the implementation, there are mistakes or carelessness such as key matrix used in the encryption process is lost because it is not kept or forgotten. Therefore necessary cryptanalysis techniques to getting back the lost key. Cryptanalysis techniques in cryptography Hill Cipher already known is to use linear equations and use matrix multiplication. In the linear equation, the value of each variable key matrix can be known, but the process of finding value in each of these variables can not be done in a short time. While the matrix multiplication, the process of finding key matrix variables can only be done if the matrix representing the plaintext has an inverse or determinant value is equal to one. Value of the determinant of a matrix can be operated to find the value of a variable of linear algebra operations that have been represented into the matrix. Each of these variables can make the search process determinants at the same time. In research has been develop a system to find the value in the variable key matrix based on the calculation of the determinant of the matrix using the paradigm of System Development Life Cycle (SDLC) Waterfall and implemented on an operating system based on Android.

Keywords: *cryptanalysis, hill cipher, known plaintext attack , matrix determinant, SDLC waterfall.*

1. PENDAHULUAN

Kriptografi adalah ilmu yang menggunakan matematika untuk mengenkripsi dan mendekripsi datanya. Kriptografi dapat digunakan untuk menyimpan informasi yang bersifat sensitif yang akan dikirimkan kepada penerima melalui media yang tidak aman (seperti *internet*) sehingga tidak dapat dibaca oleh siapapun kecuali si penerima pesan yang dimaksud [1]. Namun bukan berarti tidak ada celah untuk membobol pesan sandi *(ciphertext)* untuk mengetahui isi pesan aslinya *(plaintext)*. Ada tiga hal yang paling umum yang dapat dilakukan untuk mendapatkan *ciphertext* kembali menjadi *plaintext* [2]. Pertama dengan melakukan pencurian, membeli, bahkan menyuap untuk mendapatkan kunci. Kedua ceroboh dalam implementasinya, seperti *ciphertext* yang dikirim beserta dengan kuncinya. Ketiga dengan menggunakan kriptanalisis. Kriptanalisis adalah ilmu untuk mengamankan, menganalisis dan membobol keamanan kriptografi [3]. Kriptanalisis dapat melakukan serangan terhadap pesan yang dienkripsi berdasarkan ketersediaan data yang ada, salah satunya dengan *known plaintext attack* atau dengan mengetahui sebagian atau potongan *plaintext* dari pesan tersebut [4]. Salah satu kriptografi yang mudah dipecahkan dengan teknik *known plaintext attack* adalah kriptografi Hill *Cipher* [5]. Hill *Cipher* merupakan kriptografi kunci simetris klasik yang diciptakan oleh Lester S. Hill pada tahun 1929. Saat ini teknik kriptografi Hill *Cipher* telah diimplementasikan untuk beberapa aplikasi, seperti enkripsi data *Short Messege Service* (SMS) berbasis Android [6] dan enkripsi pada *database* inventaris [7].

Dalam implementasiannya ada saja kesalahan atau kecerobohan pada saat melakukan enkripsi, seperti kunci matriks yang digunakan pada proses enkripsi hilang karena tidak disimpan atau bahkan lupa. Oleh sebab itu diperlukan teknik kriptanalisis untuk mendapatkan kembali kunci yang hilang tersebut. Ada dua teknik kriptanalisis untuk pencarian variabel matriks kunci pada kriptografi Hill *Cipher* yang telah diketahui, yaitu dengan menggunakan persamaan linier dan menggunakan perkalian matriks [5]. Pada persamaan linier, nilai dari masing-masing variabel matriks kunci dapat diketahui, namun tiap variabel matriks kuncinya memiliki keterkaitan antara satu variabel dengan variabel lainnya. Sehingga nilai dari setiap variabel matriks kunci tersebut tidak dapat diketahui pada waktu yang bersamaan, sehingga proses pencarian nilai pada tiap variabel tersebut tidak dapat dilakukan dalam waktu yang singkat. Sedangkan pada perkalian matriks, proses pencarian variabel matriks kunci hanya dapat dilakukan jika matriks yang merepresentasikan *plaintext* memiliki invers. Jika matriks yang merepresentasikan *plaintext* tidak memiliki invers maka pencarian kunci tidak dapat dilakukan. Hal tersebut disebabkan karena nilai determinan pada matriks yang merepresentasikan *plaintext* tidak sama dengan satu.

Determinan matriks adalah selisih antara perkalian elemen-elemen pada diagonal utama dengan perkalian elemen-elemen pada diagonal sekunder [8]. Nilai determinan yang didapatkan dari suatu matriks dapat dioperasikan untuk mencari nilai suatu variabel dari operasi aljabar linear yang telah direpresentasikan kedalam bentuk matriks. Langkah awal yang dilakukan untuk mencari nilai pada variabel-variabel tersebut adalah melakukan proses penentuan nilai determinan tiap variabel dan nilai determinan keseluruhan. Selanjutnya nilai determinan masing-masing variabel tersebut dioperasikan dengan operasi pembagian terhadap nilai determinan keseluruhan, sehingga nilai tiap masing-masing variabel tersebut dapat ditemukan. Masing-masing variabel tersebut dapat melakukan proses operasi pembagian secara bersamaan, sehingga waktu yang digunakan untuk pencarian nilai dari masing-masing variabel dapat dilakukan dalam waktu yang singkat. Oleh karena itu dalam penelitian ini penulis akan mengembangkan suatu sistem untuk mencari nilai pada variabel matriks kunci berdasarkan perhitungan determinan matriks yang diperoleh dari operasi perkalian matriks yang direpresentasikan ke dalam bentuk operasi aljabar linear. Sistem tersebut dikembangkan menggunakan paradigma *System Development Life Cycle* (SDLC) *Waterfall* [9] dan diimplementasikan pada sistem operasi berbasis Android.

2. METODOLOGI PENELITIAN

Berikut merupakan metode penelitian yang digunakan dalam penelitian ini.

2.1 Bahan Penelitian

Bahan penelitian yang digunakan dalam penelitian adalah dengan cara melakukan studi literatur dari buku, *e-book,* jurnal ilmiah, serta *internet*.

2.2 Alat Penelitian

Alat yang digunakan dalam penelitian ini meliputi perangkat keras dan perangkat lunak yang disajikan dalam Tabel 1 dan Tabel 2.

Tabel 1. Rincian perangkat keras

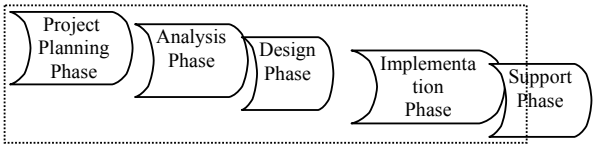
No	*Perangkat Keras*	*Spesifikasi*
1.	*Notebook*	Processor Core i3-4005U, RAM 2GB, VGA Graphics 4400, Hardisk 500GB.
2.	*Smartphone*	Android 5.0.1 Lollipop, RAM 2GB, CPU Exynos 5 Octa 5410, GPU PowerVR SGX 544MP

Tabel 2. Rincian perangkat lunak

No	*Perangkat Lunak*	*Fungsi*
1.	Zorin Ubuntu 14.04 64-bit	Sistem Operasi Linux *Based.*
2.	Eclipse 3.8.1	*Platform* untuk membuat aplikasi Android.
3.	JDK 8	*Runtime Development* untuk Eclipse.
4.	Android SDK 24	*Software Development Kit* yang menyediakan *library* untuk Android.
5.	LibreOffice 4.2.8.2	Aplikasi *Word Processing* dan *Presentation.*
6.	Gaphor	Pembuatan *Unified Modelling Language*.
7.	Dia Diagram 0.97.2	Pembuatan *flowchart* dan desain tampilan.

2.3 Alat Penelitian

Metode penelitian yang digunakan untuk membangun sistem adalah metode SDLC *Waterfall* [9] yang terdiri dari lima tahapan. Namun pada penelitian ini penulis hanya akan menggunakan empat tahapan dari kelima tahapan tersebut, seperti yang terdapat pada Gambar 1.



Gambar 1. SDLC *Waterfall*

2.3.1 Project Planning Phase

Tahap perencanaan yang dilakukan adalah menganalisis pencarian nilai determinan dari variabel kunci matriks Hill *Cipher,* serta mengidentifikasi kebutuhan-kebutuhan yang diperlukan dalam pembuatan aplikasi. Rincian *Project Planning Phase* dijelaskan pada Tabel 3.

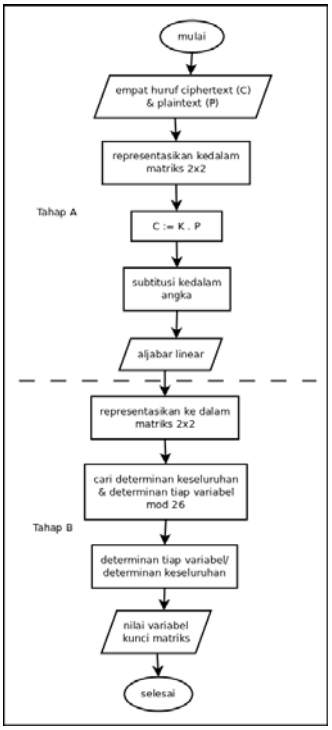
Tabel 3. Rincian *project planning phase*

No	*Tahapan*	*Deskripsi*
1.	Identifikasi Masalah	1. Bagaimana menganalisis pencarian nilai variabel matriks kunci berdasarkan determinan variabel kunci. 2. Bagaimana mengembang-kan sistem untuk mencari nilai variabel matriks kunci berbasis Android.
2.	Pengumpulan Data	Melakukan studi literatur melalui buku, *e-book,* jurnal, serta internet.
3.	Menganalisis Teori	Teori mengenai : 1. Kriptografi Hill *Cipher* 2. Kriptanalisis Kriptografi Hill *Cipher* 3. Determinan matriks 4. SDLC *Waterfall* 5. *Software Testing* 6. Android 7. Eclipse
4.	Pembuatan Jadwal	Membuat rancangan berjangka dan target pembuatan aplikasi
5.	Mencari Solusi	Menentukan teori dan sistem yang sesuai untuk pencarian nilai variabel matriks kunci berdasarkan determinan variabel kunci Hill *Cipher*.
6.	Mendefinisikan Kebutuhan	Menentukan *tools* yang dibutuhkan baik *hardware* maupun *software.*

2.3.2 Analysis Phase

a) Analisis Pencarian Nilai Determinan Kunci Matriks Hill *Cipher*

Berikut merupakan analisis pencarian nilai determinan kunci matriks Hill *Cipher* yang dijelaskan pada Gambar 2.



Gambar 2. Analisis Pencarian Nilai Determinan Matriks

b) Analisis Sistem

Pada tahap ini dilakukan analisis sistem pada pembuatan aplikasi dengan menggunakan *Object Oriented Analysis* (OOA), yaitu:

1) *System Activities (Actor Description and Use Case Description, Use Case Diagram, Scenario Use Case)*
2) *Class Diagram (Class Definition, Class Relation)*
3) *Object Interaction (Sequence Diagram)*
4) *Object Behavior (Activity Diagram)*

2.3.3 *Design Phase*

Pada tahap ini dilakukan analisis terhadap desain aplikasi untuk membuat aplikasi menggunakan *Object Oriented Design* (OOD), seperti :

a) Desain proses, yaitu rancangan logika pemrosesan data yang akan disajikan menggunakan *flowchart.*
b) Desain antarmuka, yaitu rancangan tampilan masukan dan keluaran yang akan di operasikan oleh *user.*

2.3.4 Implementation Phase

Pada Tahapan ini dilakukan beberapa tahapan setelah dilakukan penulisan kode program dilakukan dengan *Object Oriented Programming* (OOP), seperti :

a) Instalasi sistem, yaitu menjelaskan tahapan-tahapan mengenai proses instalasi aplikasi di dalam *smartphone*.

b) Pelatihan prosedural, yaitu pelatihan tata cara penggunaan aplikasi yang telah diinstal di dalam *smartphone*.
c) Pengujian Terhadap Sistem
   1) Pengujian *white box,* yaitu pengujian yang dilakukan pada *syntax* dan algoritme aplikasi.
   2) Pengujian *black box*, yaitu pengujian yang dilakukan oleh *user* untuk menguji setiap fungsi di dalam aplikasi.

3. HASIL DAN PEMBAHASAN

3.1 Project Planning Phase

Tahapan Project Planning Phase menghasilkan rincian setiap aktivitas yang dilakukan pada metode penelitian yang dijelaskan pada Tabel 4.

Tabel 4. Hasil *project planning phase*

No	*Tahapan*	*Hasil*
1.	Identifikasi Masalah	1. Menghasilkan nilai variabel matriks kunci berdasarkan determinan variabel kunci. 2. Menghasilkan aplikasi pencarian nilai variabel matriks kunci berbasis Android.
2.	Pengumpulan Data	1. Kunci matriks Hill *Cipher* berupa angka 2. *Plaintext* dan *ciphertext* berupa huruf
3.	Menganalisis Teori	Menghasilkan : 1. Teknik kriptografi Hill *Cipher* 2. Teknik kriptanalisis Kriptografi Hill *Cipher* 3. Nilai determinan matriks 4. Langkah-langkah pem-buatan sistem dengan SDLC *Waterfall* 5. Langkah-langkah untuk melakukan pengujian sis-tem. 6. Arsitektur Android 7. Tools yang terdapat pada Eclipse
4.	Pembuatan Jadwal	Jadwal terinci selama enam bulan, dan tahapannya sesuai dengan metode pengembangan sistem SDLC *Waterfall.*
5.	Mencari Solusi	Dapat mencari nilai variabel matriks kunci berdasarkan determinan variabel kunci Hill *Cipher*.
6.	Mendefinisikan Kebutuhan	Laptop untuk pengetikan kode program dengan kebutuhan *software* : Zorin Ubuntu 14.04 64-bit, Eclipse 3.8.1, Java Development Kit 8, Android SDK 24, LibreOffice 4.2.8.2, Gaphor, dan Dia Diagram 0.97.2. *Smartphone* Android untuk proses instalasi *software* dengan spesifikasi : minimal sistem operasi Gingerbread 2.3.3.

3.2 Analysis *Phase*

a) Analisis Pencarian Nilai Determinan Kunci Matriks Hill Cipher

Tahap A :

1) Mendefinisikan empat huruf ciphertext dan plaintext.

Y B H K U B = T E K N I K

2) Representasikan *ciphertext* dan *plaintext* kedalam matriks 2 x 2.

$$Ciphertext \quad : \quad \begin{bmatrix} Y & H \\ B & K \end{bmatrix}$$

$$Plaintext \quad : \quad \begin{bmatrix} T & K \\ E & N \end{bmatrix}$$

3) Masukan matriks *ciphertext* dan *plaintext* kedalam rumus Hill *Cipher*.

Dimana : C = K . P
C = *Ciphertext*
P = *Plaintext*
K = Kunci Matriks

Anggap kunci : $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$

$$\begin{bmatrix} Y & H \\ B & K \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} T & K \\ E & N \end{bmatrix}$$

4) Subtitusi matriks ciphertext dan plaintext kedalam bentuk angka.

$$\begin{bmatrix} 24 & 7 \\ 1 & 10 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 19 & 10 \\ 4 & 13 \end{bmatrix}$$

5) Menghasilkan aljabar linear

24 = 19a + 4b
7 = 10a + 13b
1 = 19c + 4d
10 = 10c + 13d

Tahap B :

1) Representasikan pada matriks 2 x

Det $= \begin{bmatrix} 19 & 4 \\ 10 & 13 \end{bmatrix}$ Det c $= \begin{bmatrix} 1 & 4 \\ 10 & 13 \end{bmatrix}$

Det a $= \begin{bmatrix} 24 & 4 \\ 7 & 13 \end{bmatrix}$ Det d $= \begin{bmatrix} 1 & 19 \\ 10 & 10 \end{bmatrix}$

Det b $= \begin{bmatrix} 24 & 19 \\ 7 & 10 \end{bmatrix}$

2) Cari determinan keseluruhan dan determinan tiap variabel, modulus 26
(Rule : Det b dan Det d tidak ditukar posisinya)

Det $= \begin{bmatrix} 19 & 4 \\ 10 & 13 \end{bmatrix}$ Tukar Posisi $= \begin{bmatrix} 4 & 19 \\ 13 & 10 \end{bmatrix}$ 40 – 247 = -207 mod 26 = 1

Det a $= \begin{bmatrix} 24 & 4 \\ 7 & 13 \end{bmatrix}$ Tukar Posisi $= \begin{bmatrix} 4 & 24 \\ 13 & 7 \end{bmatrix}$ 28 – 312 = -284 mod 26 = 2

Det b $= \begin{bmatrix} 24 & 19 \\ 7 & 10 \end{bmatrix}$ 40 – 133 = 107 mod 26 = 3

Det c $= \begin{bmatrix} 1 & 4 \\ 10 & 13 \end{bmatrix}$ Tukar Posisi $= \begin{bmatrix} 4 & 1 \\ 13 & 10 \end{bmatrix}$ 40 – 13= 27 mod 26 = 1

$$\text{Det d} = \begin{bmatrix} 1 & 19 \\ 10 & 10 \end{bmatrix} 10 - 190 = -180 \bmod 26 = 2$$

3) Determinan tiap variabel dibagi determinan keseluruhan

$$a = \frac{Deta}{Det} = \frac{2}{1} = 2 \qquad c = \frac{Detc}{Det} = \frac{1}{1} = 1$$

$$b = \frac{Detb}{Det} = \frac{3}{1} = 3 \qquad d = \frac{Detd}{Det} = \frac{2}{1} = 2$$

4) Menghasilkan nilai variabel kunci matriks.

$$K = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}$$

$$K^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} 2 & -3 \\ -1 & 2 \end{bmatrix}$$

b) Analis Sistem

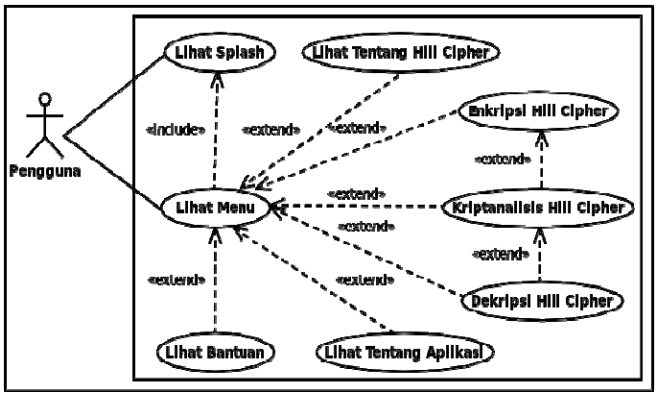
1) *System Activities*

a. Actor Description

Aktor pada aplikasi ini terdiri dari satu aktor yang disebut pengguna.

b. Use Case Diagram

Berikut merupakan *Use Case Diagram* yang dijelaskan pada Gambar 3.



Gambar 3. ***Use Case Diagram***

c. Skenario Use Case

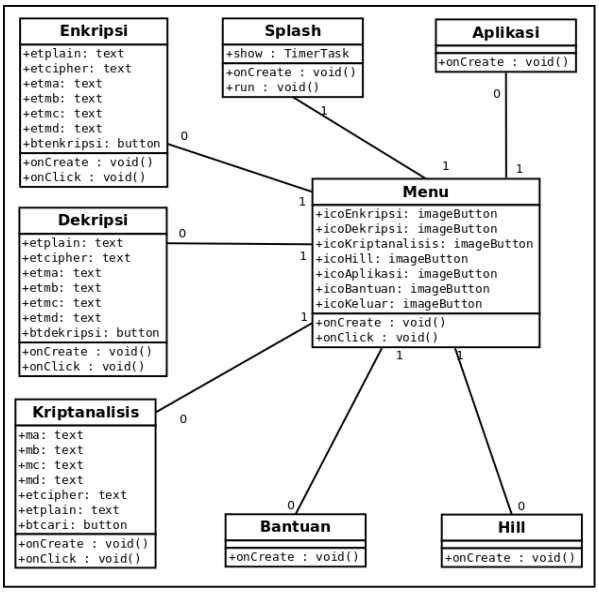
Terdiri dari delapan skenario yaitu Lihat Splash, Lihat Menu, Lihat Tentang Hill *Cipher*, Enkripsi Hill *Cipher*, Kriptanalisis Hill *Cipher*, Dekripsi Hill *Cipher*, Lihat Tentang Aplikasi, dan Lihat Bantuan. Berikut adalah skenario kriptanalisis Hill *Cipher* yang dijelaskan pada **Tabel 5**.

Tabel 5. Skenario kriptanalisis hill *cipher*

Nama Use Case	***Kriptanalisis Hill Cipher***	
Skenario	Masuk kedalam menu Kriptanalisis Hill *Cipher*	
Pemicu Hal	Aktor ingin melakukan kriptanalisis Hill *Cipher*	
Deskripsi Singkat	Jika aktor ingin melakukan kriptanalisis Hill *Cipher*, maka aktor harus masuk pada menu Kriptanalisis Hill *Cipher*	
Aktor	Pengguna	
Use Case Terkait	Lihat Menu, Enkripsi Hill *Cipher*, Dekripsi Hill *Cipher*.	
Stakeholder	Pengguna	
Kondisi Sebelum	Aktor ingin melakukankriptanalisis Hill *Cipher*	
Kondisi Setelah	Aktor berhasil melakukan kriptanalisis Hill *Cipher*	
Alur Aktivitas	***Aktor***	***Sistem***
	1. Membuka aplikasi 2. Menekan tombol Kriptanalisis Hill *Cipher* 3. Menekan tombol Cari Kunci	2.1 Menampilkan halaman untuk kriptanalisis Hill *Cipher*. 3.1 Menampilkan kunci matriks dekripsi Hill *Cipher.*
Kondisi Pengecualian	3.1 Jika kunci tidak muncul, periksa *plaintext* dan *ciphertext*	

2) Class Diagram

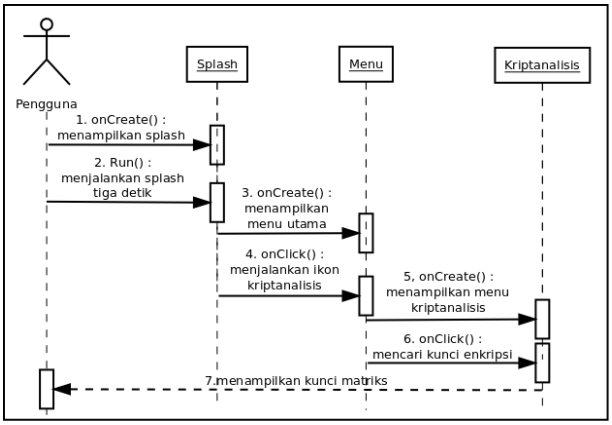
Berikut merupakan *Class Diagram* yang dijelaskan pada Gambar 4.



Gambar 4. *Class Diagram*

3) Object Interaction (Sequence Diagram)

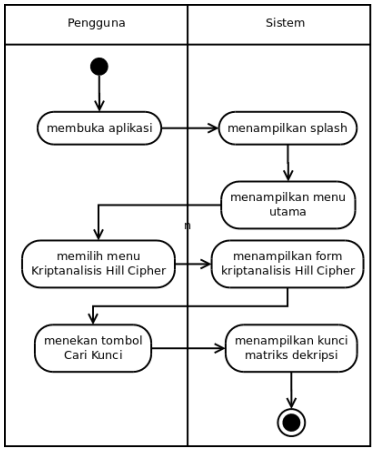
Terdiri dari delapan *sequence* yaitu Lihat Splash, Lihat Menu, Enkripsi Hill *Cipher*, Dekripsi Hill *Cipher*, Kriptanalisis Hill *Cipher*, Lihat Tentang Aplikasi, Lihat Tentang Hill *Cipher*, dan Lihat Bantuan. Berikut merupakan *sequence* Kriptanalisis Hill *Cipher* yang dijelaskan pada Gambar 5.



Gambar 5. *Sequence* Kriptanalisis Hill *Cipher*

4) Object Behavior (Activity Diagram)

Terdiri dari delapan *activity* yaitu Lihat Splash, Lihat Menu, Enkripsi Hill *Cipher*, Dekripsi Hill *Cipher*, Kriptanalisis Hill *Cipher*, Lihat Tentang Aplikasi, Lihat Tentang Hill *Cipher*, Lihat Bantuan. Berikut adalah *activity diagram* yang dijelaskan pada Gambar 6**.**

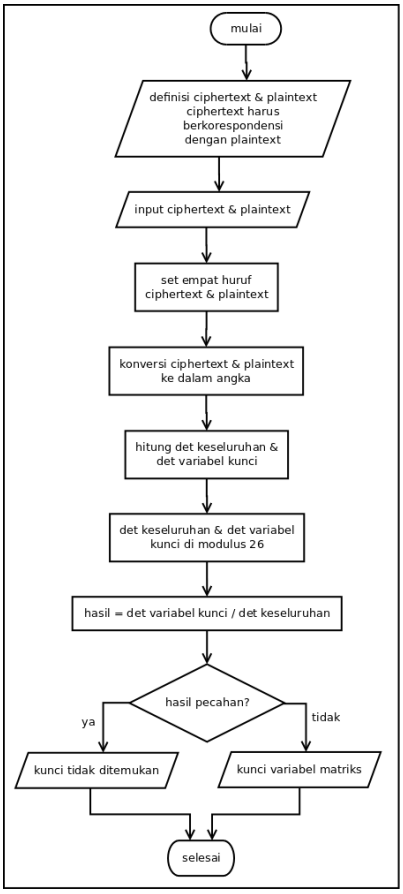


Gambar 6. *Activity* Kriptanalisis Hil *Cipher*

3.3 Design Phase

a) Desain Proses

Berikut adalah alur desain proses yang dijelaskan pada Gambar 7**.**

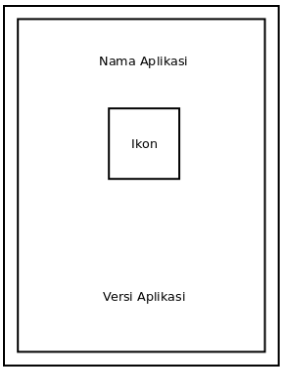


Gambar 7. Desain Proses

b) Desain Antarmuka

1) Tampilan Splash

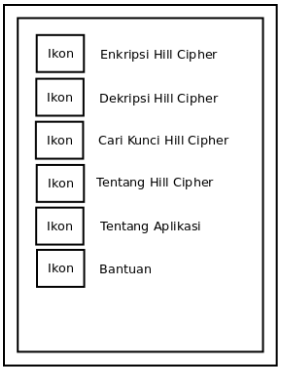
Berikut adalah desain tampilan splash yang dijelaskan pada Gambar 8**.**



Gambar 8. Desain Tampilan Splash

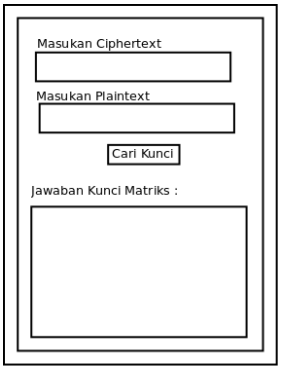
2) Tampilan Menu

Berikut adalah desain tampilan menu yang dijelaskan pada Gambar 9.



Gambar 9. Desain Tampilan Menu

3) Tampilan Kriptanalisis Hill *Cipher*
Berikut adalah desain tampilan kriptanalisis Hill *Cipher* yang dijelaskan pada **Gambar 10.**



Gambar 10. Desain Tampilan Kriptanalisis Hill *Cipher*

3.4 Implementation Phase

a) Tampilan Aplikasi Kriptanalisis
Berikut adalah tampilan kriptanalisis Hill *Cipher* yang dijelaskan pada Gambar 11**.**

Gambar 11. Tampilan Kriptanalisis Hill *Cipher*

b) Instalasi Sistem

1) Instalasi Perangkat Keras
Smartphone dengan RAM dengan kapasitas minimum 8192 Mb dan *Internal Storage* dengan kapasitas minimum 2 Gb instalasi.
2) Instalasi Perangkat Lunak

Smartphone/tablet dengan minimal spesifikasi Sistem Operasi minimum *Android Gingerbread* 2.3.3 dan *Google Play* Market untuk proses instalasi.

c) Pelatihan Prosedural : Berisi tata cara penggunaan aplikasi.

1) Membuka Splash dengan cara buka aplikasi kemudian menampilkan splash
2) Membuka Menu dengan cara buka aplikasi kemudian menampilkan menu
3) Menu Enkripsi Hill *Cipher* dengan cara buka aplikasi, tekan ikon "Enkripsi Hill *Cipher*", masukan *plaintext* kedalam kolom yang disediakan, tekan tombol "Enkripsi" dan menampilkan *ciphertext*
4) Menu Dekripsi Hill *Cipher* dengan cara buka aplikasi, tekan ikon "Dekripsi Hill *Cipher*", masukan *ciphertext* kedalam kolom yang disediakan, tekan tombol "Dekripsi" dan menampilkan *plaintext*
5) Menu Kriptanalisis Hill *Cipher* dengan cara buka aplikasi, tekan ikon "Kriptanalisis Hill *Cipher",* masukan *ciphertext* dan *plaintext* kedalam kolom (minimal empat huruf), tekan tombol Cari Kunci", menampilkan kunci matriks.
6) Menu Tentang Hill *Cipher* dengan cara buka aplikasi, tekan ikon "Tentang Hill *Cipher"* dan menampilkan informasi Hill *Cipher*.
7) Menu Tentang Aplikasi dengan cara buka aplikasi, tekan ikon "Tentang Aplikasi*"* dan menampilkan informasi Aplikasi.
8) Menu Bantuan dengan cara buka aplikasi, tekan ikon "Bantuan*"* dan menampilkan informasi penggunaan Aplikasi.

d) Pengujian Terhadap Sistem

1) *Blackbox*

Dengan kriteria Ketepatan, keandalan, efisiensi, keutuhan, kegunaan, portabilitas dan reusabilitas. Berikut adalah tabel pengujian *Blackbox* yang dijelaskan pada Tabel 6**.**

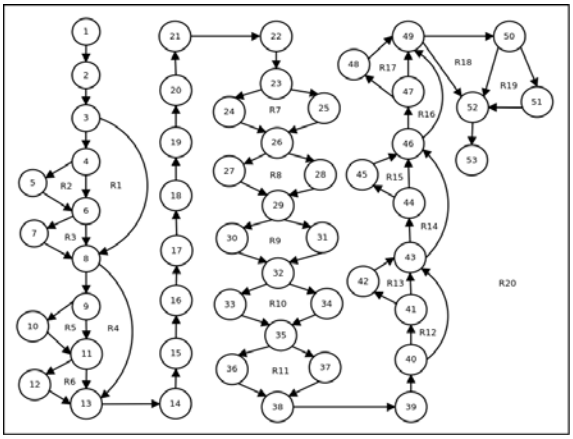
Tabel 6. Pengujian *blackbox*

No	*Nama Kasus Uji*	*Kesimpulan*
1.	Lihat Splash	Teruji
2.	Lihat Menu	Teruji
3.	Enkripsi Hill *Cipher*	Teruji
4.	Dekripsi Hill *Cipher*	Teruji
5.	Kriptanalisis Hill *Cipher*	Teruji
6.	Lihat Tentang Hill *Cipher*	Teruji
7.	Lihat Tentang Aplikasi	Teruji
8.	Lihat Bantuan	Teruji

2) *Whitebox*

a. *Flowgraph* Kriptanalisis Hill *Cipher*

Berikut adalah gambar *flowgraph* kriptanalisis Hill *Cipher* yang dijelaskan pada Gambar 12**.**



Gambar 12. *Flowgraph* Kriptanalisis Hill *Cipher*

b. Cyclomatic *Complexity* V(G) Kriptanalisis Hill *Cipher*

1. V(G) = R
   = 20
2. V(G) = E – N + 2
   = 71 – 53 + 2 = 20
3. V(G) = P + 1
   = 19 + 1 = 20

c. Independent *Path*
Berikut adalah tabel *Independent Path* yang dijelaskan pada Tabel 7.

Tabel 7. *Independen path*

No	*Path*
1.	1-2-3-8-13-14-15-16-17-18-19-20-21-22-23-24-26-27-29-30-32-33-35-36-38-39-40-43-46-49-52-53
2.	1-2-3-4-5-6-7-8-13-14-15-16-17-18-19-20-21-22-23-24-26-27-29-30-32-33-35-36-38-39-40-43-46-49-52-53
3.	1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-16-17-18-19-20-21-22-23-24-26-27-29-30-32-33-35-36-38-39-40-43-46-49-52-53
4.	1-2-3-8-13-14-15-16-17-18-19-20-21-22-23-25-26-28-29-31-32-34-35-37-38-39-40-43-46-49-52-53
5.	1-2-3-4-5-6-7-8-13-14-15-16-17-18-19-20-21-22-23-25-26-28-29-31-32-34-35-37-38-39-40-43-46-49-52-53
6.	1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-16-17-18-19-20-21-22-23-25-26-28-29-31-32-34-35-37-38-39-40-43-46-49-52-53
7.	1-2-3-8-13-14-15-16-17-18-19-20-21-22-23-25-26-28-29-31-32-34-35-37-38-39-40-41-42-43-46-49-52-53
8.	1-2-3-4-5-6-7-8-13-14-15-16-17-18-19-20-21-22-23-25-26-28-29-31-32-34-35-37-38-39-40-41-42-43-46-49-52-53
9.	1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-16-17-18-19-20-21-22-23-25-26-28-29-31-32-34-35-37-38-39-40-41-42-43-46-49-52-53
10.	1-2-3-8-13-14-15-16-17-18-19-20-21-22-23-25-26-28-29-31-32-34-35-37-38-39-40-43-44-45-46-49-52-53
11.	1-2-3-4-5-6-7-8-13-14-15-16-17-18-19-20-21-22-23-25-26-28-29-31-32-34-35-37-38-39-40-43-44-45-46-49-52-53
12.	1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-16-17-18-19-20-21-22-23-25-26-28-29-31-32-34-35-37-38-39-40-43-44-45-46-49-52-53
13.	1-2-3-8-13-14-15-16-17-18-19-20-21-22-23-25-26-28-29-31-32-34-35-37-38-39-40-43-46-47-48-49-52-53
14.	1-2-3-4-5-6-7-8-13-14-15-16-17-18-19-20-21-22-23-25-26-28-29-31-32-34-35-37-38-39-40-43-46-47-48-49-52-53
15.	1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-16-17-18-19-20-21-22-23-25-26-28-29-31-32-34-35-37-38-39-40-43-46-47-48-49-52-53
16.	1-2-3-8-13-14-15-16-17-18-19-20-21-22-23-25-26-28-29-31-32-34-35-37-38-39-40-43-46-49-50-52-53
17.	1-2-3-4-5-6-7-8-13-14-15-16-17-18-19-20-21-22-23-25-26-28-29-31-32-34-35-37-38-39-40-43-46-49-50-52-53
18.	1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-16-17-18-19-20-21-22-23-25-26-28-29-31-32-34-35-37-38-39-40-43-46-49-50-52-53
19.	1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-16-17-18-19-20-21-22-23-24-26-27-29-30-32-33-

No	*Path*
	35-36-38-39-40-41-42-43-44-45-46-47-48-49-50-51-52-53
20.	1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-16-17-18-19-20-21-22-23-25-26-28-29-31-32-34-35-37-38-39-40-41-42-43-44-45-46-47-48-49-50-51-52-53

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, maka dapat ditarik kesimpulan :

a) Aplikasi ini dapat menganalisis pencarian nilai variabel matriks kunci berdasarkan determinan variabel kunci.
b) Aplikasi ini dapat mencari nilai variabel matriks kunci dengan kriptanalisis Hill *Cipher* berbasis Android.

5. SARAN

Berdasarkan kesimpulan di atas, aplikasi tersebut masih dapat dikembangkan lagi seperti :

a) Aplikasi untuk mencari nilai dari variabel dari suatu determinan matriks kunci Hill *Cipher* dapat dikembangkan dengan matriks ordo 3 x 3 atau lebih.
b) Jumlah *plaintext* yang diperlukan pada proses pencarian kunci matriks Hill *Cipher* kurang dari empat huruf.
c) Diperlukan manajemen waktu yang lebih disiplin dan sumber daya manusia yang berkualitas.

DAFTAR PUSTAKA

[1] [NA : Network Associates, Inc.] US. 1999. *An Introduction to Cryptography*. Santa Clara. United States of America.
[2] Schaefer, Edward. 2010. *An Introduction to Cryptography and Cryptanalysis*. Santa Clara University, United States of America.
[3] Ayushi. 2010. *A Symmetric Key Cryptographic Algorithm. International Journal of Computer Applications* (0975 – 8887) Volume 1 – No. 15. Lecturer, Hindu College of Engineering.
[4] Keliher, Liam., Delaney, Anthony Z. 2013. *Cryptanalysis of the Toorani-Falahati Hill Ciphers*. IEEE. Department of Mathematics and Computer Science, Mount Allison University, Sackville, New Brunswick, Canada.
[5] Munir, Rinaldi. 2006. *Kriptografi*. Informatika, Bandung.
[6] Cahyono, Murti. 2014. *Implementasi Algoritma Hill Cipher Pada Aplikasi Sms Berbasis Android*. Teknik Informatika Amikom Yogyakarta, Yogyakarta.
[7] Santosa. Edgar Dika. 2015. *Implementasi Algoritma Caesar Cipher Dan Hill Cipher Pada Database Sistem Inventori Tb Mita Jepara*. Teknik Informatika Universitas Dian Nuswantoro, Semarang.
[8] Howard, A. 1991. *Aljabar Linear Elementer*. Edisi 6. Erlangga. Jakarta.
[9] Satzinger, John W, Jackson, Robert B, dan Burd, Stephen D. 2010. *Systems Analysis and Design in a Changing World, Fifth Edition*. Course Technology, Boston.