BAB III

ANALISIS DAN DESAIN SISTEM

III.1. Analisa Masalah

Hasil dari penelitian ini sendiri berupa proses Enkripsi dengan menggunakan metode gabungan seperti Algoritma *Vigenere Cipher* dan Algoritma *Hill Cipher* dapat dilakukan dan Menggabungkan dua metode atau lebih dapat membuat pesan semakin sulit dimengerti bagi orang lain. Dengan menggunakan Algoritma *Hill Cipher* dan Algoritma *Vigenere Cipher*, penulis mengharapkan dapat mengamankan serta dapat membantu dalam menyandikan teks.

Berdasarkan analisis yang telah penulis kemukanan diatas, dapat diambil kesimpulan bahwa mengidentifikasi permasalahan-permasalahan yang ada pada sistem serta menyelesaikan permasalahan tersebut. Menggunakan keamanan seperti Algoritma *Hill Cipher* dan Algoritma *Vigenere Cipher* diharapkan menjadi media yang lebih baik dalam melakukan Enkripsi dan Dekripsi.

III.2. Starategi Pemecahan Masalah

Beberapa strategi pemecahan masalah dalam perancangan Penyandian Text dengan menggunakan algoritma *Hill Cipher* dan *Vigenere Cipher* ini adalah sebagai berikut:

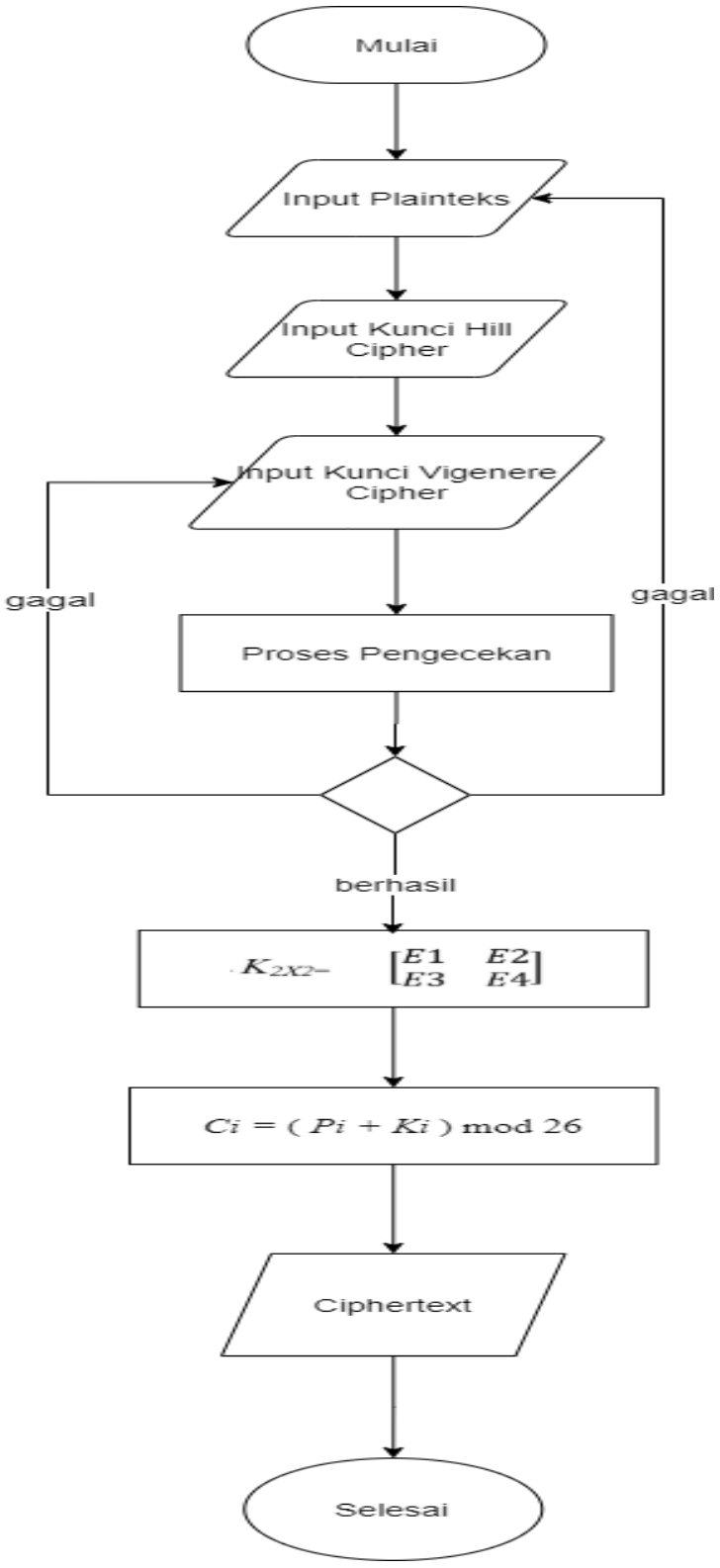
1. Sistem penyandian teks ini dapat digunakan pada semua perangkat yang telah support menggunakan Web browser.

2. Sistem yang dibangun ini digunakan untuk penyandian teks dengan menggunakan *Hill Cipher* yang telah disandikan isinya dan menggunakan algoritma affine cipher.

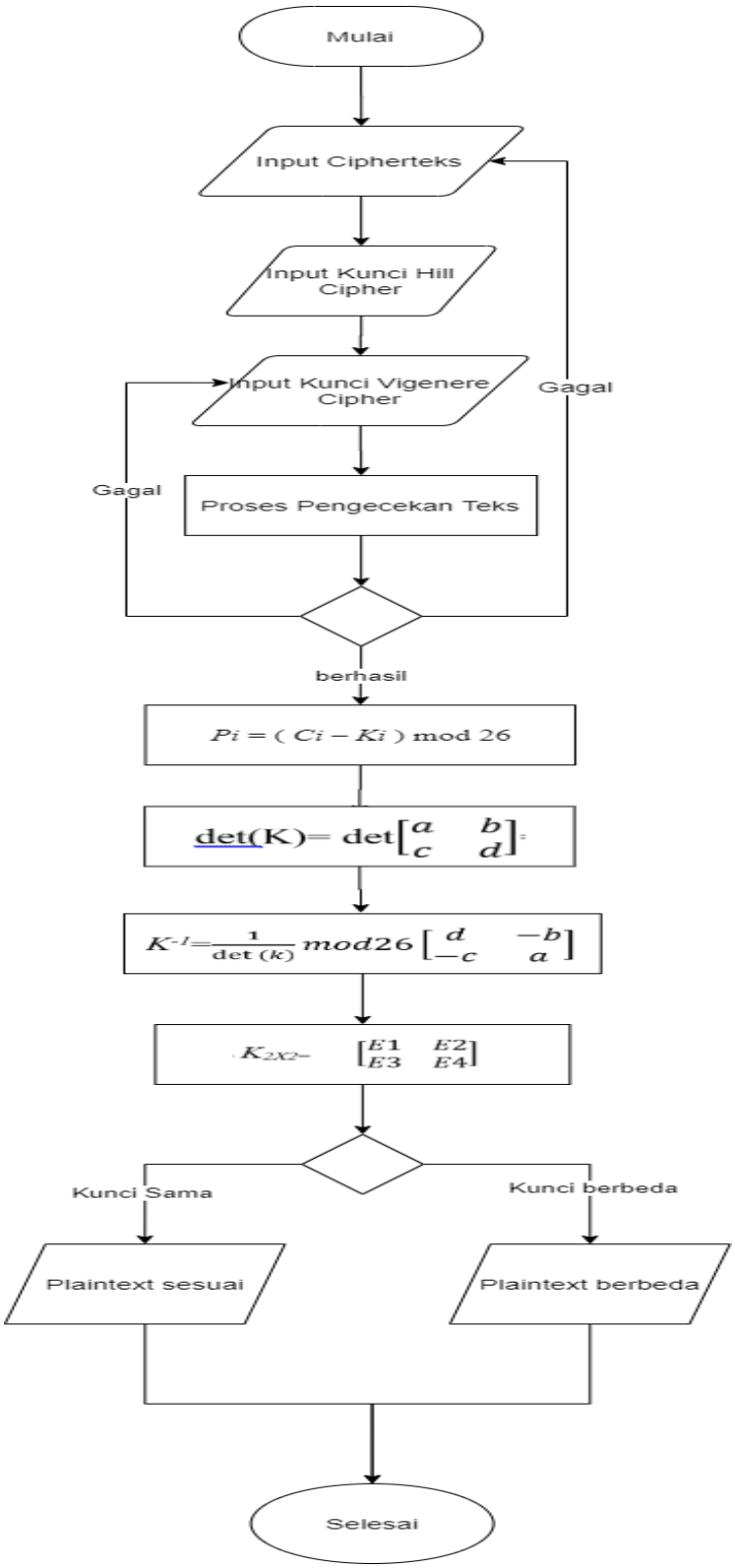
3. Sistem yang dibangun nantinya akan memiliki sebuah aplikasi khusus untuk penyandian teks.

III.3. *Flowchart*

Berikut ini adalah *Flowchart* Enkripsi dan Dekripsi pada Algoritma *Hill Cipher* dan *Vigenere Cipher* dapat dilihat pada gambar berikut:



Gambar III.1. *Flowchart* Enkripsi *Hill Cipher* dan *Vigenere Cipher*



Gambar III.2. *Flowchart* Dekripsi *Hill Cipher* dan *Vigenere Cipher*

III.4. Skenario Sistem

User akan diberikan link untuk menguji suatu teks pada Aplikasi berbasis Website. Di Halaman utama website, user akan mendapatkan suatu tampilan yang dimana terdapat pilihan menu Enkripsi dan Dekripsi. Untuk tampilan menu Enkripsi terdapat kolom pengisian *plaintext*, kolom pengisian *key*, button enkripsi dan kolom hasil enkripsi atau *ciphertext*. Sementara untuk tampilan menu Dekripsi terdapat kolom pengisian *ciphertext*, kolom pengisian *key*, button enkripsi dan kolom hasil dekripsi atau *plaintext.* Ketika user memasukkan *plaintext* ataupun *ciphertext* beserta key-nya, selanjutnya tinggal menekan button enkrispi ataupun dekripsi. Maka akan muncul hasilnya di Kolom hasil Enkripsi ataupun Dekripsi. Jika user memasukkan selain Karakter berupa abjad A - Z, maka sistem langsung menolak. Jadi setiap user di haruskan menggukan karakter abjad A-Z.

III.5. Algoritma *Hill Cipher*

Algoritma *Hill Cipher* merupakan algoritma kriptografi kunci simetris yang mempunyai berbagai kelebihan dalam mengenkripsi data). *Hill Cipher* ialah penerapan aritmatika modulo pada kriptografi. Teknik kriprografi ini menggunakan matrik persegi sebagai kunci yang nantinya digunakan untuk melakukan enkripsi dan dekripsi.

Dasar dari teknik *hill cipher* adalah aritmatika modulo terhadap matriks. Dalam penerapannya, *hill cipher* menggunakan teknik perkalian matriks dan teknik invers terhadap matriks. Kunci pada *hill cipher* adalah matriks *n* x *n* dengan *n*

merupakan ukuran blok. Pengugunakn block disini 2x2 dikarekan sebagai dasar pengujian suatu matriks. Jika matriks kunci disebut dengan *K*, maka matriks *K* adalah sebagai berikut :

$K_{nXn} = K_{2X2=}$ $\begin{bmatrix} E1 & E2 \\ E3 & E4 \end{bmatrix}$

Matriks *K* yang menjadi kunci ini harus merupakan matriks yang *invertible*, yaitu memiliki *multiplicative inverse K*-1 sehingga :

K : Kunci Matriks

E : Elemen (Nilai Karakter)

K^{-1} *: Inverse* Matriks

K . K-1 = 1

Persamaan Enkrisi: C=E(K,C)=K P mod 26..... (1)

Persamaan Dekripsi: P=D(K,P)=K^{-1} C mod 26..... (2)

Dengan :

E= Enkripsi

D= Dekripsi

C= Ciphertext

K= Key

P= Plaintext

Untuk nilai dari setiap elemen, akan di buat tabel sebagai berikut:

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*	*19*	*20*	*21*	*22*	*23*	*24*	*25*

Tabel III.I. Elemen Karakter

III.5.1. Proses Ekripsi Algoritma *Hill Cipher*

Pilih *plaintext* dengan beberapa karakter yang ukuran kunci matriks 2x2. Untuk itu, bagi *plaintext* menjadi beberapa blok, dengan tiap bloknya berisi 2 karakter.

P: KRIPTO

K: DBFE = $\begin{bmatrix}3 & 1\\5 & 4\end{bmatrix}$

Tentukan *Ciphertext* nya :

Indeks untuk setiap karakter yang diblok $\begin{bmatrix}K\\R\end{bmatrix} = \begin{bmatrix}10\\17\end{bmatrix}, \begin{bmatrix}I\\P\end{bmatrix} = \begin{bmatrix}8\\15\end{bmatrix}, \begin{bmatrix}T\\O\end{bmatrix} = \begin{bmatrix}19\\14\end{bmatrix}$

Lakukan Perkalian matiks antara kunci dan blok plaintext

$$\begin{bmatrix}3 & 1\\5 & 4\end{bmatrix}\begin{bmatrix}10\\17\end{bmatrix} = \begin{bmatrix}(3x10)+ & (1x17)\\(5x10)+ & (4x17)\end{bmatrix} = \begin{bmatrix}47\\118\end{bmatrix}(mod26) = \begin{bmatrix}21\\14\end{bmatrix}$$

$$\begin{bmatrix}3 & 1\\5 & 4\end{bmatrix}\begin{bmatrix}8\\15\end{bmatrix} = \begin{bmatrix}(3x8)+ & (1x15)\\(5x8)+ & (4x15)\end{bmatrix} = \begin{bmatrix}39\\100\end{bmatrix}(mod26) = \begin{bmatrix}13\\22\end{bmatrix}$$

$$\begin{bmatrix}3 & 1\\5 & 4\end{bmatrix}\begin{bmatrix}19\\14\end{bmatrix} = \begin{bmatrix}(3x19)+ & (1x14)\\(5x19)+ & (4x14)\end{bmatrix} = \begin{bmatrix}71\\151\end{bmatrix}(mod26) = \begin{bmatrix}19\\21\end{bmatrix}$$

Ubah hasil perhitungan ke dalam bentuk karakter:

$$\begin{bmatrix}21\\14\end{bmatrix} = \begin{bmatrix}V\\O\end{bmatrix}, \begin{bmatrix}13\\22\end{bmatrix} = \begin{bmatrix}N\\W\end{bmatrix}, \begin{bmatrix}19\\21\end{bmatrix} = \begin{bmatrix}T\\V\end{bmatrix}$$

Sehingga *Ciphertext* yang dihasilkan adalah VONWTV.

III.5.2. Proses Dekripsi Algoritma Hill Cipher

Untuk melakukan dekrispi diperlukan untuk menghitung nilai determinan dari matriks kunci (*K*) dan menghitung Invers Matriks Kunci (K^{-1}).

det(K)= det$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$= det$\begin{bmatrix} 3 & 1 \\ 5 & 4 \end{bmatrix}$= ((a*d)-(b*c)=((3*4)-(5*1))= 12-5= 7

$K^{-1}=\frac{1}{\det(k)} mod 26 \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

$K^{-1}=\frac{1}{7} mod 26 \begin{bmatrix} 4 & -1 \\ -5 & 3 \end{bmatrix}$

$K^{-1}=15 \begin{bmatrix} 4 & -1 \\ -5 & 3 \end{bmatrix}= \begin{bmatrix} 60 & -15 \\ -75 & 45 \end{bmatrix} mod 26= \begin{bmatrix} 8 & 11 \\ 3 & 21 \end{bmatrix}$

Maka $K^{-1}=\begin{bmatrix} 8 & 11 \\ 3 & 21 \end{bmatrix}$

Setelah di temukannya K^{-1}, dekripsi dapat dilakukan yang dimana

C: VONWTV

$K^{-1}=\begin{bmatrix} 8 & 11 \\ 3 & 21 \end{bmatrix}$

Lakukan Perkalian matiks antara kunci dan blok *plaintext.*

$$\begin{bmatrix} 8 & 11 \\ 3 & 21 \end{bmatrix} \begin{bmatrix} 21 \\ 14 \end{bmatrix} = \begin{bmatrix} (8x21) + & (11x14) \\ (3x21) + & (21x14) \end{bmatrix} = \begin{bmatrix} 322 \\ 357 \end{bmatrix} (mod 26) = \begin{bmatrix} 10 \\ 17 \end{bmatrix}$$

$$\begin{bmatrix} 8 & 11 \\ 3 & 21 \end{bmatrix} \begin{bmatrix} 13 \\ 22 \end{bmatrix} = \begin{bmatrix} (8x13) + & (11x22) \\ (3x13) + & (21x22) \end{bmatrix} = \begin{bmatrix} 346 \\ 501 \end{bmatrix} (mod 26) = \begin{bmatrix} 8 \\ 15 \end{bmatrix}$$

$$\begin{bmatrix}8 & 11\\3 & 21\end{bmatrix}\begin{bmatrix}19\\21\end{bmatrix} = \begin{bmatrix}(8x19) + & (11x21)\\(3x19) + & (21x21)\end{bmatrix} = \begin{bmatrix}383\\519\end{bmatrix}(mod26) = \begin{bmatrix}19\\14\end{bmatrix}$$

Maka *plaintext* yang dihasilkan sama seperti sebelumnya yaitu KRIPTO

III.6. Algoritma *Vigenere Cipher*

Metode *Vigenere Cipher* adalah suatu metode penyandian teks alfabet menggunakan deretan sandi *Caesar* berdasarkan huruf pada kunci. Sandi *Vigenere* merupakan bentuk sederhana dari substitusi. Kelebihan sandi dibanding sandi Caesar dan sandi monoalfabetik lain adalah sandi yang tidak rentan terhadap metode pemecahan sandi.

Enkripsi (penyandian) dengan sandi *Vigenère* juga dapat dituliskan secara matematis, dengan menggunakan penjumlahan dan operasi modulus, yaitu:

$Ci = (Pi + Ki)$ mod 26. ..... (3)

Sedangkan proses dekripsi dengan sandi *Vigenere* dituliskan secara matematis sebagai berikut,

$Pi = (Ci – Ki)$ mod 26..... (4)

Ci = nilai ascii dari karakter *ciphertext* ke-*i*

Pi = nilai ascii dari karakter *plaintext* ke-*i*

Ki = nilai ascii dari karakter kunci ke-i

III.6.1. Proses Enkripsi Algoritma *Vigenere Cipher*

Pilih plaintext dengan beberapa karakter begitu juga dengan *key* nya.

P: KRIPTOGRAFI

K: BIRU

Selanjutnya kunci diperluas sampai ukurannya sama dengan *plaintext*.

K: BIRUBIRUBIR

(K+B)mod 26 = (10+1) mod 26 = 11 mod 26 = 11 = L

(R+I)mod 26 = (17+8) mod 26 = 25 mod 26 = 25 = Z

(I+R)mod 26 = (8+17) mod 26 = 25 mod 26 = 25 = Z

(P+U)mod 26 = (15+20) mod 26 = 35 mod 26 = 9 = J

(T+B)mod 26 = (19+1) mod 26 = 20 mod 26 = 20 = U

(O+I)mod 26 = (14+8) mod 26 = 22 mod 26 = 22 = W

(G+R)mod 26 = (6+17) mod 26 = 23 mod 26 = 23 = X

(R+U)mod 26 = (17+20) mod 26 = 37 mod 26 = 11 = L

(A+B)mod 26 = (0+1) mod 26 = 1 mod 26 = 1 = B

(F+I)mod 26 = (5+8) mod 26 = 13 mod 26 = 13 = N

(I+R)mod 26 = (8+17) mod 26 = 25 mod 26 = 11 = Z

Maka *Ciphertext* yang dihasilkan ialah LZZJUWXLBNZ

III.6.2 Proses Dekripsi *Vigenere Cipher*

C: LZZJUWXLBNZ

K: BIRUBIRUBIR

(L-B)mod 26 = (11-1) mod 26 = 10 mod 26 = 10 = K

(Z-I)mod 26 = (25-8) mod 26 = 17 mod 26 = 17 = R

(Z-R)mod 26 = (25-17) mod 26 = 8 mod 26 = 8 = I

(J-U)mod 26 = (9-20) mod 26 = -11+26 mod 26 = 15 = P

(U-B)mod 26 = (20-1) mod 26 = 19 mod 26 = 19 = T

(W-I)mod 26 = (22-8) mod 26 = 14 mod 26 = 14 = O

(X-R)mod 26 = (23-17) mod 26 = 6 mod 26 = 6 = G

(L-U)mod 26 = (11-20) mod 26 = -9+26 mod 26 = 17 = R

(B-B)mod 26 = (1-1) mod 26 = 0 mod 26 = 0 = A

(N-I)mod 26 = (13-8) mod 26 = 5 mod 26 = 5 = F

(Z-R)mod 26 = (25-17) mod 26 = 8 mod 26 = 8 = I

III.7. Penggabungan Metode Hill Cipher dan Vigenere Cipher

III.7.1. Studi Kasus

Jika Plaintext terdari 6 karakter yaitu KRIPTO dengan *key* DBFE maka tentukan *Ciphertext* nya dengan melakukan penggabungan enkripsi dengan *Hill Cipher* dan *Vigenere Cipher*.

P: KRIPTO

K: DBFE = $\begin{bmatrix}3 & 1\\5 & 4\end{bmatrix}$

Indeks untuk setiap karakter yang diblok $\begin{bmatrix}K\\R\end{bmatrix} = \begin{bmatrix}10\\17\end{bmatrix}, \begin{bmatrix}I\\P\end{bmatrix} = \begin{bmatrix}8\\15\end{bmatrix}, \begin{bmatrix}T\\O\end{bmatrix} = \begin{bmatrix}19\\14\end{bmatrix}$

Lakukan Perkalian matiks antara kunci dan blok plaintext

$$\begin{bmatrix}3 & 1\\5 & 4\end{bmatrix}\begin{bmatrix}10\\17\end{bmatrix} = \begin{bmatrix}(3x10)+ & (1x17)\\(5x10)+ & (4x17)\end{bmatrix} = \begin{bmatrix}47\\118\end{bmatrix}(mod26) = \begin{bmatrix}21\\14\end{bmatrix}$$

$$\begin{bmatrix}3 & 1\\5 & 4\end{bmatrix}\begin{bmatrix}8\\15\end{bmatrix} = \begin{bmatrix}(3x8)+ & (1x15)\\(5x8)+ & (4x15)\end{bmatrix} = \begin{bmatrix}39\\100\end{bmatrix}(mod26) = \begin{bmatrix}13\\22\end{bmatrix}$$

$$\begin{bmatrix}3 & 1\\5 & 4\end{bmatrix}\begin{bmatrix}19\\14\end{bmatrix} = \begin{bmatrix}(3x19)+ & (1x14)\\(5x19)+ & (4x14)\end{bmatrix} = \begin{bmatrix}71\\151\end{bmatrix}(mod26) = \begin{bmatrix}19\\21\end{bmatrix}$$

Ubah hasil perhitungan ke dalam bentuk karakter:

$$\begin{bmatrix}21\\14\end{bmatrix} = \begin{bmatrix}V\\O\end{bmatrix}, \begin{bmatrix}13\\22\end{bmatrix} = \begin{bmatrix}N\\W\end{bmatrix}, \begin{bmatrix}19\\21\end{bmatrix} = \begin{bmatrix}T\\V\end{bmatrix}$$

Sehingga *Ciphertext* yang dihasilkan adalah VONWTV.

Selanjutnya kunci diperluas sampai ukurannya sama dengan *plaintext*.

K: DBFEDB

(V+D)mod 26 = (21+3) mod 26 =24 mod 26 = 24 = Y

(O+B)mod 26 = (14+1) mod 26 =15 mod 26 = 15 = P

(N+F)mod 26 = (13+5) mod 26 =18 mod 26 = 18 = S

(W+E)mod 26 = (22+4) mod 26 =26 mod 26 = 0 = A

(T+D)mod 26 = (19+3) mod 26 =22 mod 26 = 22 = W

(V+B)mod 26 = (21+1) mod 26 =22 mod 26 = 22 = W

Dari Penjabaran diatas, hasil *ciphertext* penggabungan enkripsi antara *hill cipher* dan *vigenere cipher* ialah YPSAWW.

Untuk mengubah kembali karakter YPSAWW ke dalam bentuk *plaintext* maka dibutuhkan enkripsi gabungan antara *vigenere cipher* dengan *hill cipher*. Kunci yang digunakan masih sama seperi sebulumnya yaitu DBFE.

P: YPSAWW

K: DBFE

Selanjutnya kunci diperluas sampai ukurannya sama dengan *ciphertext* nya.

K: DBFEDB

(Y-D)mod 26 = (24-3) mod 26 =21 mod 26 = 21 = V

(P-B)mod 26 = (15-1) mod 26 =14 mod 26 = 14 = O

(S-F)mod 26 = (18-5) mod 26 =13 mod 26 = 13= N

(A-E)mod 26 = (0-4) mod 26 =22 mod 26 = 22 = W

(W=D)mod 26 = (22-3) mod 26 =19 mod 26 = 19 = T

(W-B)mod 26 = (22-1) mod 26 =21 mod 26 = 21 = V

Hasil Plaintextnya ialah VONWTV.

Untuk melakukan tahap dekrispi selanjutnya diperlukan untuk menghitung nilai determinan dari matriks kunci (*K*) dan menghitung Invers Matriks Kunci (K^{-1}).

det(K)= det$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$= det$\begin{bmatrix} 3 & 1 \\ 5 & 4 \end{bmatrix}$= ((a*d)-(b*c)=((3*4)-(5*1))= 12-5= 7

$K^{-1}=\frac{1}{\det(k)} mod 26 \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

$K^{-1}=\frac{1}{7} mod 26 \begin{bmatrix} 4 & -1 \\ -5 & 3 \end{bmatrix}$

$K^{-1}=15 \begin{bmatrix} 4 & -1 \\ -5 & 3 \end{bmatrix}= \begin{bmatrix} 60 & -15 \\ -75 & 45 \end{bmatrix} mod 26= \begin{bmatrix} 8 & 11 \\ 3 & 21 \end{bmatrix}$

Maka $K^{-1}=\begin{bmatrix} 8 & 11 \\ 3 & 21 \end{bmatrix}$

Setelah di temukannya K^{-1}, dekripsi dapat dilakukan yang dimana

C: VONWTV

$K^{-1}=\begin{bmatrix} 8 & 11 \\ 3 & 21 \end{bmatrix}$

Lakukan Perkalian matiks antara kunci dan blok *plaintext.*

$$\begin{bmatrix} 8 & 11 \\ 3 & 21 \end{bmatrix} \begin{bmatrix} 21 \\ 14 \end{bmatrix} = \begin{bmatrix} (8x21) + & (11x14) \\ (3x21) + & (21x14) \end{bmatrix} = \begin{bmatrix} 322 \\ 357 \end{bmatrix} (mod 26) = \begin{bmatrix} 10 \\ 17 \end{bmatrix}$$

$$\begin{bmatrix} 8 & 11 \\ 3 & 21 \end{bmatrix} \begin{bmatrix} 13 \\ 22 \end{bmatrix} = \begin{bmatrix} (8x13) + & (11x22) \\ (3x13) + & (21x22) \end{bmatrix} = \begin{bmatrix} 346 \\ 501 \end{bmatrix} (mod 26) = \begin{bmatrix} 8 \\ 15 \end{bmatrix}$$

$$\begin{bmatrix} 8 & 11 \\ 3 & 21 \end{bmatrix} \begin{bmatrix} 19 \\ 21 \end{bmatrix} = \begin{bmatrix} (8x19) + & (11x21) \\ (3x19) + & (21x21) \end{bmatrix} = \begin{bmatrix} 383 \\ 519 \end{bmatrix} (mod 26) = \begin{bmatrix} 19 \\ 14 \end{bmatrix}$$

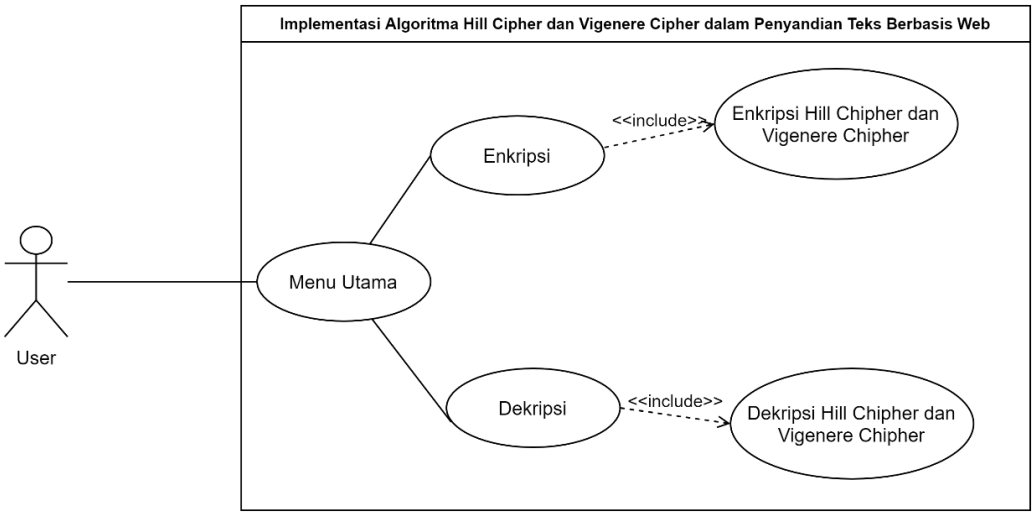
Maka *plaintext* yang dihasilkan dari penggabungan *vigenre cipher* dengan hill *cipeher* kembali seperti sebelumnya yaitu KRIPTO.

III.8. Desain Sistem

Pada tahap ini dirancang sebuah desain dari rancang aplikasi Penyandian Tesk. Bagaimana desain yang akan digunakan pada antarmuka perangkat berbasis *Web*. Dengan merancang sistem menggunakan Bahasa pemodelan Unified Modeling Language (UML).

III.8.1 *Use Case Diagram*

Use case menjelaskan suatu alur proses sistem yang akan di bangun. Maka dibuatlah suatu bentuk diagram *Use Case* dapat dilihat pada gambar sebagai berikut:

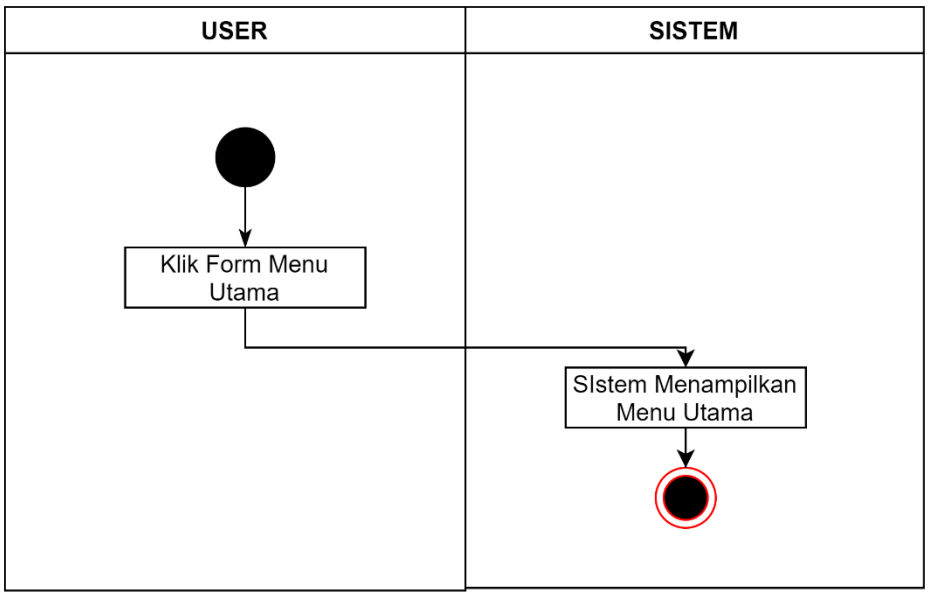


Gambar III.1. *Use Case Diagram* Penyandian Teks

III.8.2 *Activity Diagram*

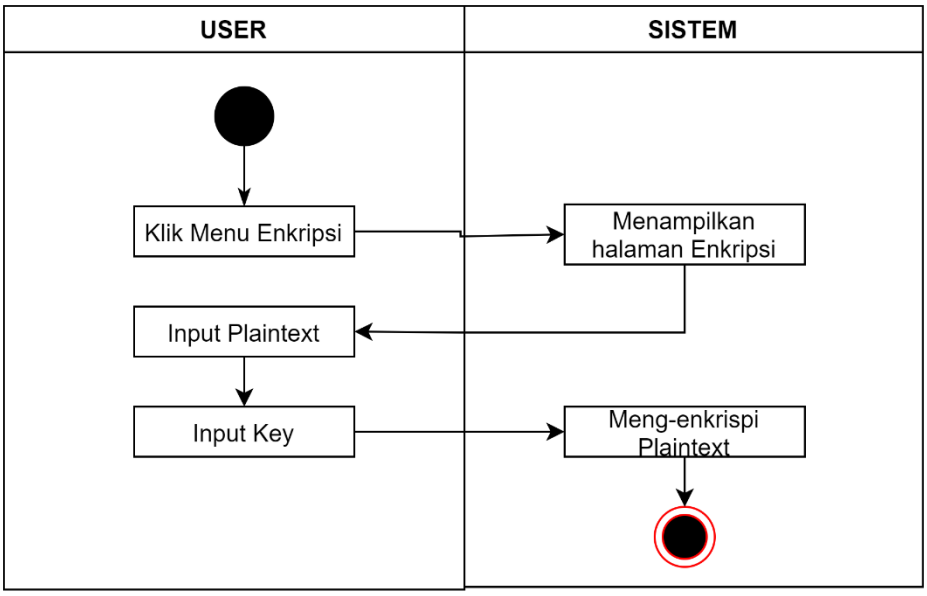
Activity diagram menggambarkan berbagai alir aktivitas dalam sistem yang sedang dirancang, bagaimana masing-masing alir berawal, *decision* yang mungkin terjadi, dan bagaimana mereka berakhir. *Activity diagram* yang terdapat pada aplikasi yaitu sebagai berikut:

III.8.2.1. *Activity Diagram* Menu Utama



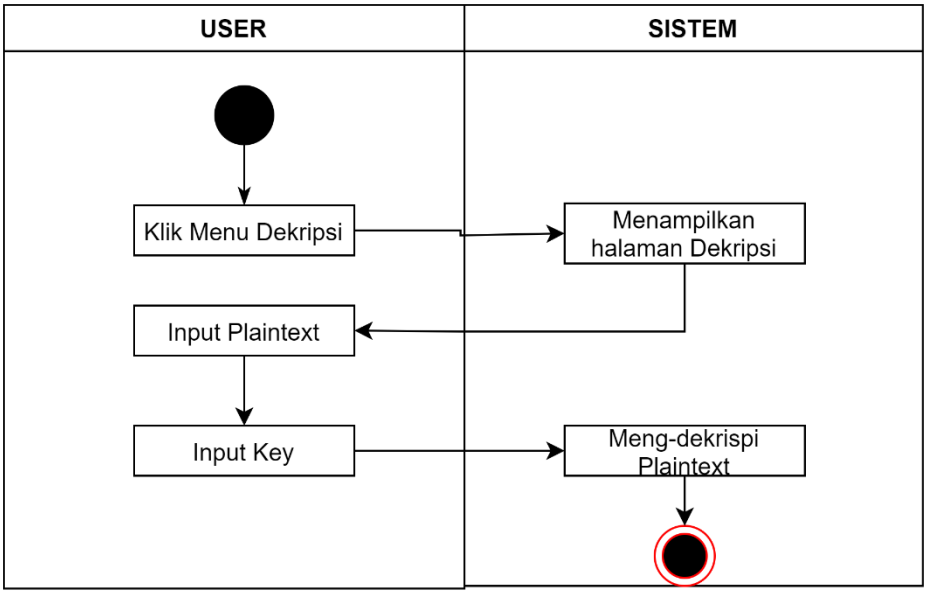
Gambar III.2. Activity Diagram Menu Utama

III.8.2.2. *Activity Diagram* Enkripsi *Hill Cipher* dan *Vigenere Cipher*



Gambar III.3. *Activity Diagram* Enkripsi *Hill Cipher* dan *Vigenere Cipher*

III.8.2.3. *Activity Diagram* Dekripsi *Hill Cipher* dan *Vigenere Cipher*

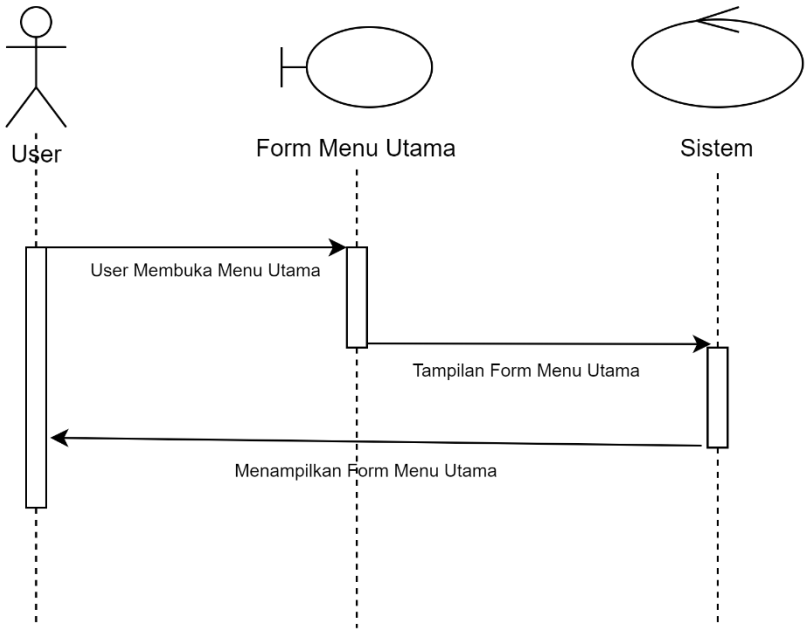


Gambar III.4. *Activity Diagram* Dekripsi *Hill Cipher* dan *Vigenere Cipher*

III.8.3 *Sequence Diagram*

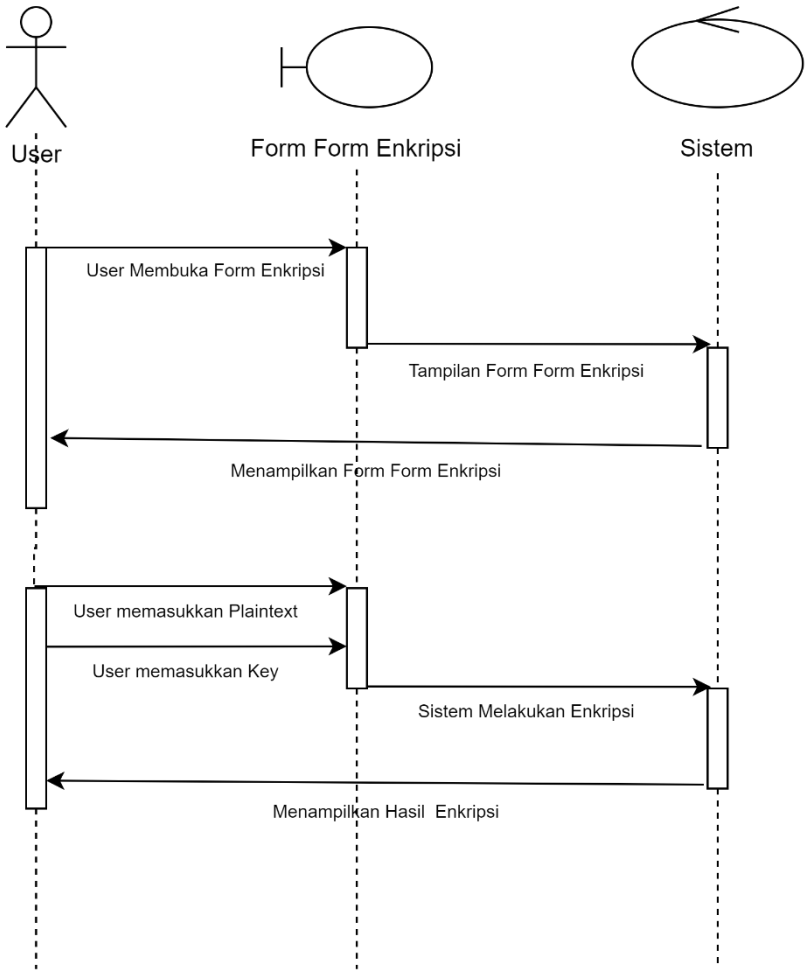
Gambaran *Sequence Diagram* dibuat pendefinisian *Use Case* yang memiliki proses sendiri atau yang penting semua *Use Case* yang telah didefinisikan interaksi jalannya sudah dicakup pada *Sequence Diagram*.

III.8.3.1. *Sequence Diagram* Menu Utama



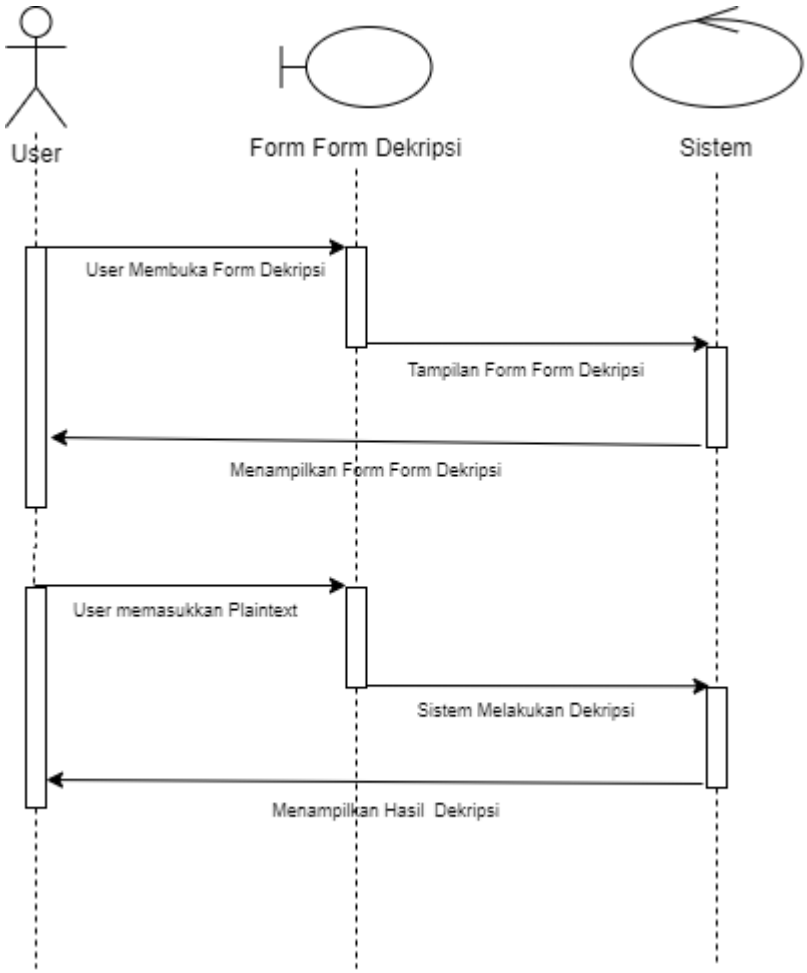
Gambar III.5. *Sequence Diagram* Menu Utama

III.8.3.2. *Sequence Diagram* Enrkipsi *Hill Cipher* dan *Vigenere Cipher*



Gambar III.6. *Sequence Diagram* Enkripsi *Hill Cipher* dan *Vigenere Cipher*

III.8.3.3. *Sequence Diagram* Dekripsi *Hill Cipher* dan *Vigenere Cipher*

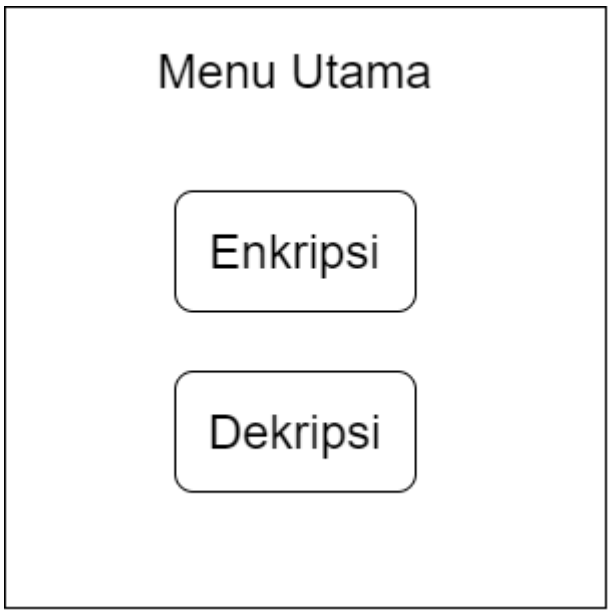


Gambar III.7. *Sequence Diagram* Dekripsi *Hill Cipher* dan *Vigenere Cipher*

III.9. Desain *Interface*

III.9.1. Perancangan *Form* Menu Utama

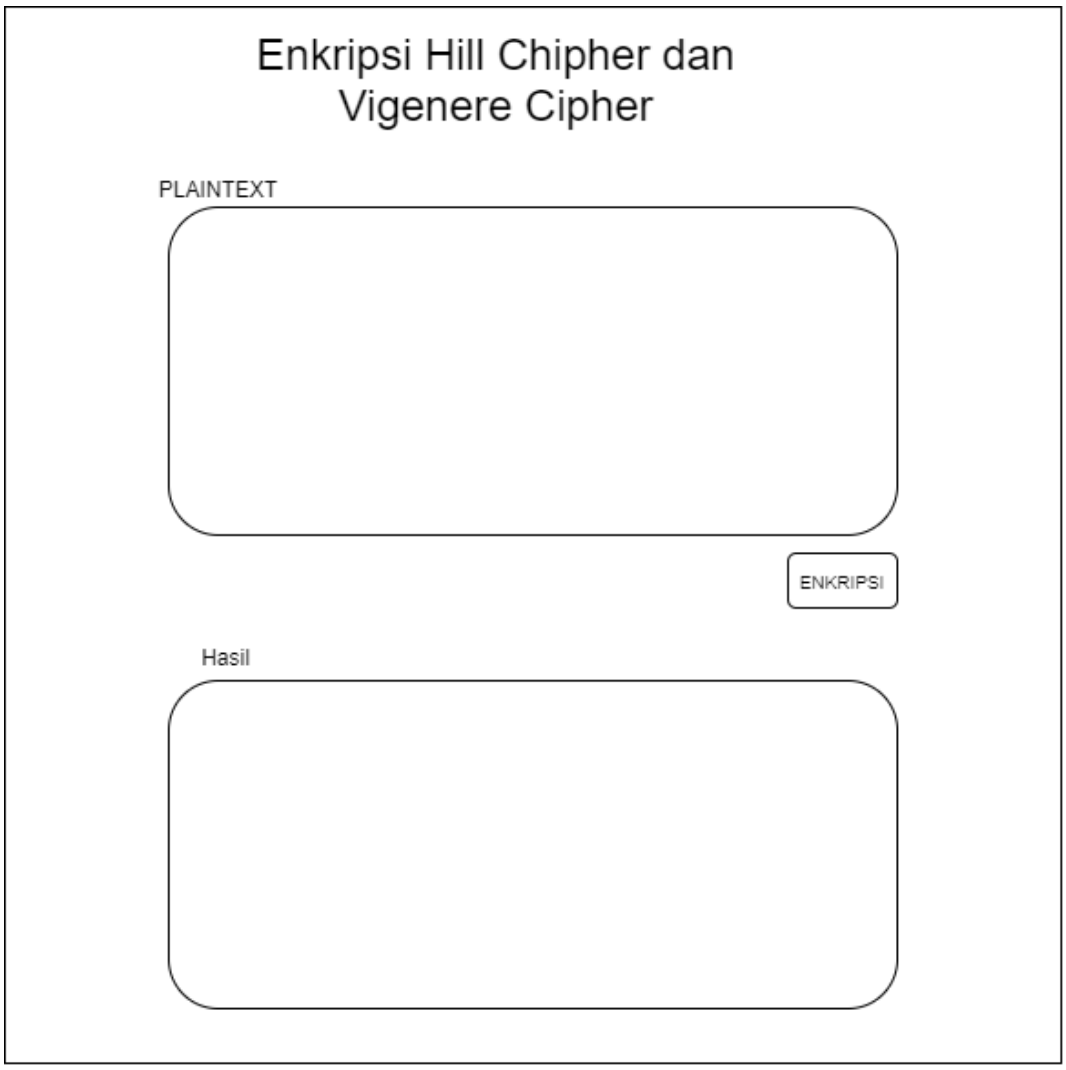
Pada tampilan *form* Utama ini terdiri dari 2 buah *buttom* akses, yaitu *button* Enrkripsi dan Dekrispi. Untuk lebih jelasnya, perancangan *form* Utama dapat dilihat pada Gambar III.9 sebagai berikut:



Gambar III.8. Perancangan *Form* Menu Utama

III.9.2. Perancangan *Form* Enkrispi *Hill Cipher* dan *Vigenere Cipher*

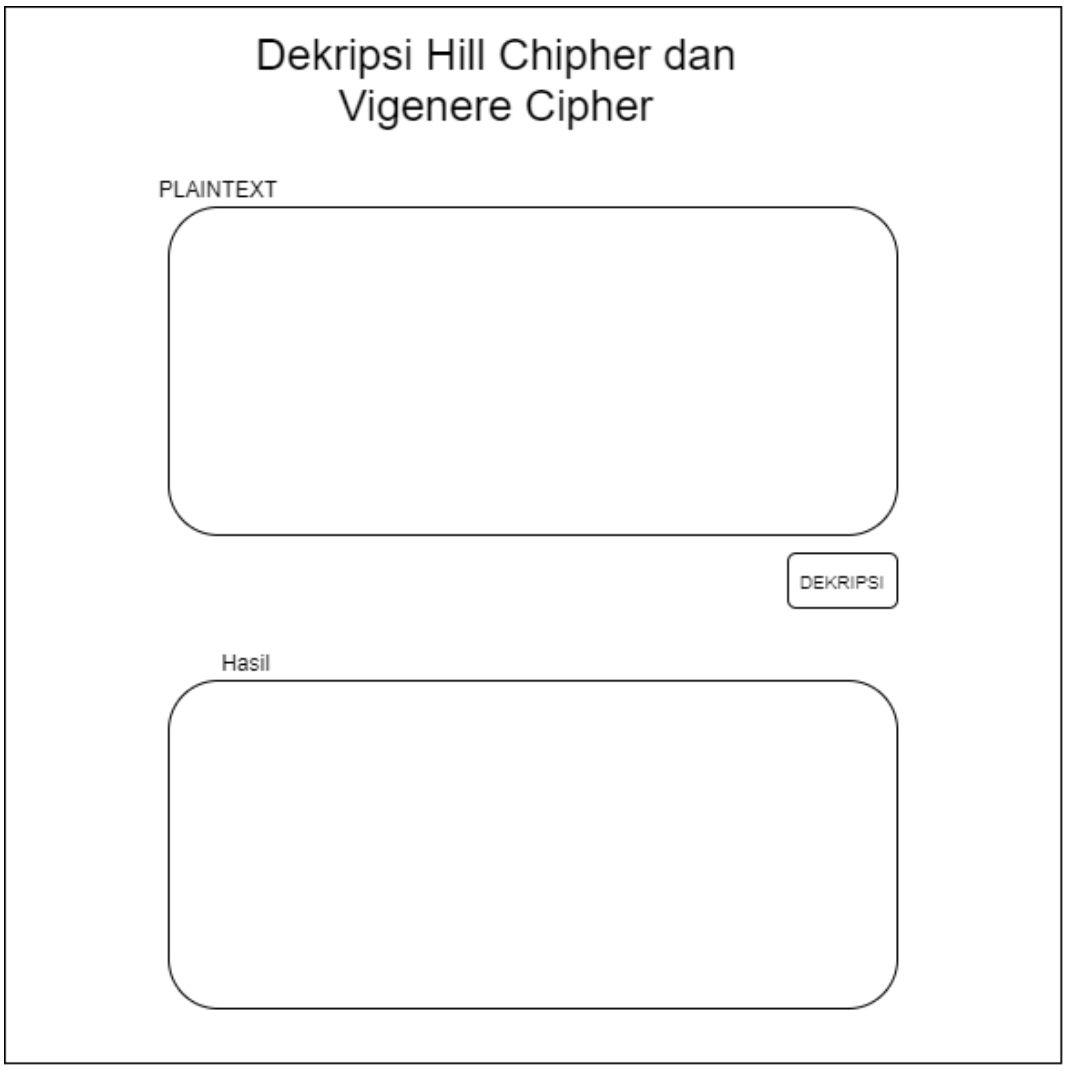
Pada *form* Enrkripsi *Hill Cipher* dan *Vigenere Cipher* menampilkan tampilan untuk mengisi *plaintext* yang ingin di enkripsi. Untuk lebih jelasnya, perancangan *form* Utama dapat dilihat pada Gambar III.10 sebagai berikut:



Gambar III.9. Perancangan *Form* Enkripsi *Hill Cipher* dan *Vigenere Cipher*

III.9.3. Perancangan *Form* Dekrispi *Hill Cipher* dan *Vigenere Cipher*

Pada *form* Derkripsi *Hill Cipher* dan *Vigenere Cipher* menampilkan tampilan untuk mengisi *Ciphertext* yang ingin di dekripsi. Untuk lebih jelasnya, perancangan *form* Utama dapat dilihat pada Gambar III.11 sebagai berikut:



Gambar III.9. Perancangan *Form* Enkripsi *Hill Cipher* dan *Vigenere Cipher*