BAB III
METODOLOGI PENELITIAN

3.1. Analisa Masalah

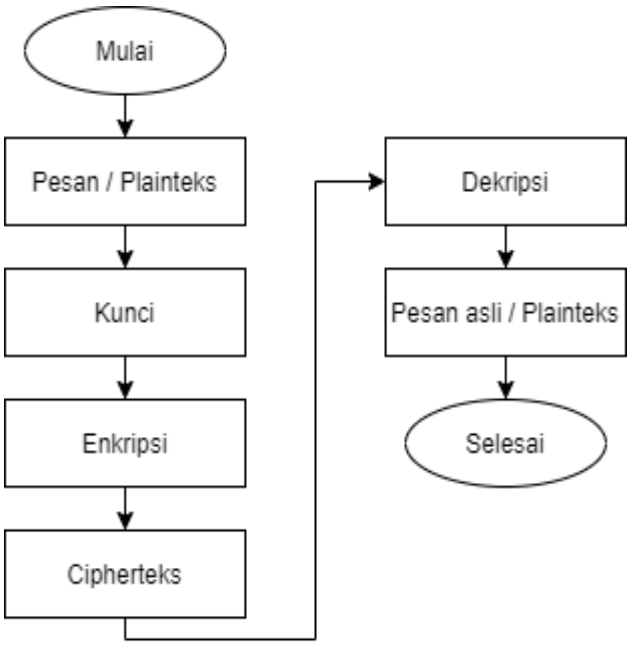
Keamanan informasi merupakan aspek penting dalam pengiriman suatu informasi. Seringkali terjadi penyadapan atau pencurian informasi oleh pihak yang tidak bertanggung jawab. Dalam hal ini diperlukan suatu penyandian pesan agar informasi yang disampaikan tidak mudah dibaca oleh orang lain.

Proses enkripsi pesan yang telah banyak dilakukan yaitu enkripsi pesan dari pesan alfabet ke dalam bentuk alfabet dimana karakter pada enkripsi tersebut mudah ditebak dan sudah biasa diterapkan. Terdapat juga proses enkripsi pesan dalam tulisan Korea ke dalam bentuk tulisan Korea menggunakan algoritma *Vigenere Cipher* dan algoritma *Enigma Cipher* dengan menggunakan rotor. Namun algortima yang digunakan tersebut belum cukup kuat.

Pada penelitian ini dilakukan enkripsi pesan alfabet ke dalam huruf Korea dengan pengimplementasian *finite automata* untuk menentukan pola suku kata. Pesan alfabet yang dienkripsi tidak termasuk karakter angka dan tanda baca. Pola suku kata yang diterima oleh *finite automata* adalah pola KV dan KVK. Dimana K merupakan konsonan dan V merupakan Vokal. Penentuan pola tersebut disesuaikan dengan aturan huruf Korea yang terdiri dari huruf konsonan sebagai awalan, huruf vokal sebagai penengah dan huruf vokal sebagai akhiran. Jika diakhir pola suku kata terdapat pola yang kosong maka akan dilakukan *padding*, yaitu penyisipan huruf acak. Proses enkripsi pesan alfabet menggunakan pembangkit kunci dari sebuah kalimat yang panjang. Pada kalimat kunci tersebut huruf yang berulang akan dihilangkan. Hasil dari kunci akan ditambahkan huruf yang belum terdaftar kemudian kunci tersebut dipartisi ke dalam dua himpunan. Pembangkit kunci tersebut juga digunakan untuk menentukan konversi alfabet ke dalam huruf Korea.

3.2. Rancangan Sistem

Rancangan sistem pada penelitian digambarkan menggunakan diagram alir *(flowchart)* yang menjelaskan mengenai tahapan proses sistem. Pada Gambar 3.1 merupakan diagram alir tahapan proses sistem.



Gambar 3. 1 Flowchart Proses Sistem

Pada alur proses diatas, tahapan yang paling utama adalah proses enkripsi dan dekripsi pada pesan. Proses enkripsi dan dekripsi membutuhkan sebuah kunci untuk dapat mengubah pesan tersebut menjadi sebuah cipherteks atau dari cipherteks menjadi pesan asli. Pembangkit kunci untuk proses enkripsi dan dekripsi yaitu dari sebuah kalimat yang cukup panjang dan dibangkitkan menggunakan konsep cipher subtitusi abjad tunggal *(monoalphabetic cipher)*. Pada kunci yang diinputkan tidak memiliki batas maksimal karakter. Hal ini dikarenakan dalam kalimat tersebut huruf yang berulang akan dihilangkan sehingga huruf awal yang telah memenuhi susunan alfabet tidak akan diproses. Namun semakin panjang kunci yang diinputkan akan memengaruhi waktu komputasi. Berdasarkan hasil pembangkit kunci akan dilakukan penyusunan kunci menjadi dua himpunan. Tiap himpunan kunci terdiri dari 13 huruf dari kalimat tersebut. Berikut proses pembentukan kunci :

a. Kunci yang diinputkan dapat menggunakan kombinasi huruf besar dan huruf kecil. Contoh kunci yang ditentukan :

   ‘Enkripsi Huruf Alfabet ke Dalam Huruf Korea’

b. Menghilangkan huruf yang berulang dan karakter diubah menjadi huruf kecil seluruhnya :

‘enkripshufalbtdmo’

c. Menambahkan huruf yang belum ada pada daftar susunan alfabet :
‘enkripshufalbtdmocgjqvwxyz’

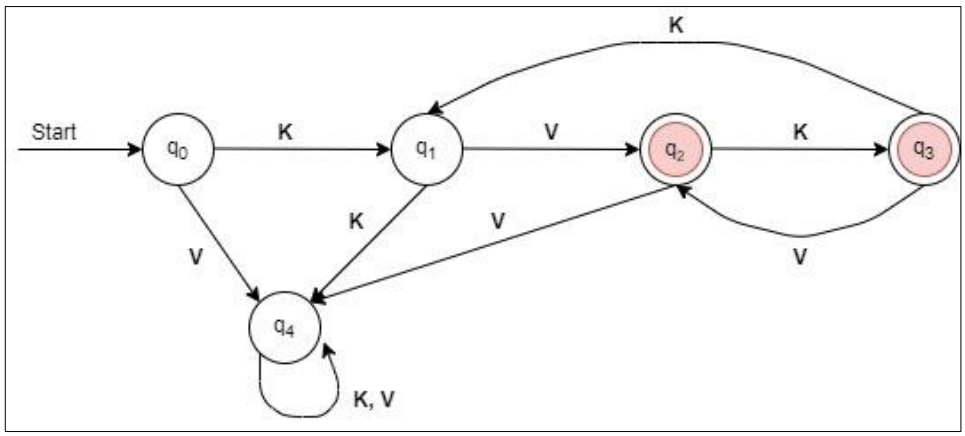
d. Mempartisi huruf ke dalam dua himpunan kunci :

Tabel 3. 1 Himpunan Kunci

Class 1	E	K	I	S	U	A	B	D	O	G	Q	W	Y
Class 2	N	R	P	H	F	L	T	M	C	J	V	X	Z
Urutan ke-*n*	1	2	3	4	5	6	7	8	9	10	11	12	13

Daftar himpunan kunci di atas digunakan untuk menentukan huruf Korea sebagai hasil enkripsi dari pesan alfabet. Pesan alfabet merupakan tulisan yang tersusun dari beberapa huruf abjad. Untuk dapat melakukan enkripsi pesan alfabet ke dalam huruf Korea harus mengetahui pola penulisan huruf Korea berdasarkan aturannya. Dalam penulisan huruf Korea, hangul tersusun atas jamo atau pembentuk tulisan yang umumnya terdiri dari tiga elemen yaitu awalan *(initial)*, penengah *(medial)*, penutup *(final)*. Ketentuan penulisan pada hangul antara lain elemen awalan harus ada dan harus berupa bunyi konsonan, elemen penengah harus ada dan harus berupa bunyi vokal serta elemen penutup tidak harus selalu ada.

Berdasarkan aturan penulisan tersebut, maka dibentuk state diagram yang mengikuti prinsip *Deterministic Finite Automata* (DFA) dimana seluruh transisi dari satu state ke state yang lain dituliskan dengan tegas dan tidak memberikan ruang transisi epsilon. Transisi epsilon merupakan sebuah transisi dimana sistem tidak akan menerima suatu inputan apapun saat terjadi perubahan state [7]. Dalam hal ini dibentuk dua pola suku kata yang dapat dikenali oleh sistem yaitu pola KV dan KVK. Dimana K merupakan konsonan dan V merupakan vokal. Pola suku kata yang dibentuk ini memperhatikan kaidah penulisan huruf Korea. Pada Gambar 3.2 merupakan rancangan diagram FSA untuk pengenalan pola suku kata.



Gambar 3. 2 Rancangan Diagram FSA

Pada rancangan diagram FSA di atas, pada state q_0 akan dikenali pola K dan V. Jika pola awal yang dikenali adalah V, maka akan menuju pada state q_4. Dimana state q_4 tidak akan pernah bisa menuju pada *final state* yang berarti pola tersebut tidak diterima oleh FSA. Jika pola awal yang dikenali adalah K maka akan menuju pada state q_1. State q_1 akan mengenali pola V yang menuju state q_2 sebagai *final state* pertama yang berarti pola tersebut dapat diterima oleh FSA sebagai pola KV. Jika pada state q_2 dikenali pola K, maka akan menuju state q_3 sebagai *final state* kedua yang berarti pola tersebut dapat diterima oleh FSA sebagai pola KVK. Oleh karena itu, dalam hal ini pola KV dan KVK dapat dikenali dan dapat diterima oleh FSA.

Dalam pengimplementasian *finite automata* untuk menentukan pola suku kata, maka harus ditentukan huruf vokal dan konsonan hangul yang digunakan untuk mengubah pesan alfabet menjadi cipherteks hangul. Penentuan huruf Korea sesuai dengan banyaknya himpunan kunci yang telah dibentuk yaitu sebanyak 13 buah. Terdapat satu buah huruf vokal dan konsonan yang digunakan sebagai huruf penentu pada penyisipan pola suku kata. Huruf vokal tersebut yaitu ㅖ *(ye)* dan huruf konsonan yaitu ㅇ *(-ng)*. Penyisipan pola dilakukan karena terdapat dua kelas himpunan kunci, dimana setiap satu karakter hangul vokal maupun konsonan dapat digunakan untuk dua karakter kunci huruf alfabet dan satu karakter huruf alfabet pada kunci dapat dikonversi ke dalam dua karakter hangul. Penyisipan digunakan sebagai penanda bahwa satu karakter sebelum huruf ㅖ *(ye)*

dan ㅇ*(-ng)* merupakan karakter kunci himpunan kelas kedua. Berikut merupakan huruf vokal dan konsonan Hangul yang ditentukan untuk konversi cipherteks.

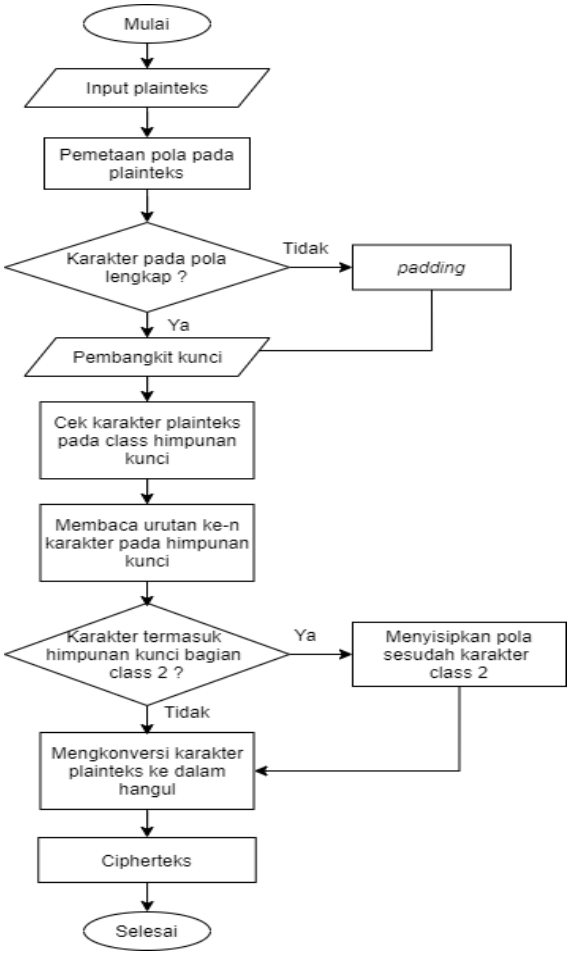
Tabel 3. 2 Huruf Vokal dan Konsonan Hangul

n	V	K
1	ㅏ	ㄱ
2	ㅑ	ㄴ
3	ㅓ	ㄷ
4	ㅕ	ㄹ
5	ㅗ	ㅁ
6	ㅛ	ㅂ
7	ㅜ	ㅅ
8	ㅠ	ㅈ
9	ㅡ	ㅊ
10	ㅣ	ㅋ
11	ㅐ	ㅌ
12	ㅒ	ㅍ
13	ㅖ	ㅎ

3.2.1. Enkripsi

Proses enkripsi pesan alfabet ke dalam huruf Korea dilakukan dengan menyesuaikan pola suku kata pada pesan. Pola tersebut akan dipetakan pada karakter pesan alfabet yang di masukan. Karakter pesan alfabet tersebut akan di cek pada dua himpunan kunci yang telah ditentukan. Jika terdapat huruf alfabet yang masuk dalam kategori kunci himpunan kedua, maka akan disisipkan pola

setelah karakter. Jika pola V pada kategori kelas kedua maka akan disisipkan pola KV, jika pola K pada kategori kedua maka akan disisipkan pola VK. Pola yang disisipkan akan dikonversi menggunakan huruf Korea yang berbeda, untuk karakter V ditetapkan dengan huruf （ㅐ）dan untuk karakter K ditetapkan dengan huruf（ㅇ）. Jika pada akhir pola suku kata terdapat satu huruf yang kosong, maka akan di isi huruf secara acak atau *padding*. Penentuan huruf Korea berdasarkan dengan pola yang telah dipetakan pada pesan alfabet, apakah huruf tersebut masuk pada kategori pola KV atau KVK. Jika semua karakter telah dipetakan dalam huruf Korea, maka karakter tersebut akan dituliskan berdasarkan aturan penulisan huruf Korea. Pada Gambar 3.3 merupakan flowchart proses enkripsi pesan.



Gambar 3. 3 Flowchart Proses Enkripsi

Berikut merupakan penyelesaian proses enkripsi pesan alfabet menjadi huruf Korea.

1. Menginputkan plainteks. Plainteks yang diinputkan dapat menggunakan kombinasi huruf besar dan huruf kecil alfabet dan tidak memiliki batas maksimal karakter. Namun semakin banyak karakter plainteks yang diinputkan maka akan semakin lama proses komputasi. Hasil plainteks yang diinputkan akan diubah menjadi huruf kecil seluruhnya.
   Plainteks yang diinputkan : Jangan Lupa Menggunakan Masker
   Hasil plainteks : janganlupamenggunakanmasker

2. Memetakan pola. Karakter alfabet akan dipetakan pola dengan susunan pola KVK dan KV. Satu karakter alfabet dapat dipetakan pola K (konsonan) atau pola V (vokal). Susunan pola yaitu dengan mempartisi setiap tiga karakter plainteks kemudian memetakan karakter tersebut dengan pola KVK sebanyak karakter plainteks yang telah dipartisi. Jika diakhir karakter terdapat satu karakter tersisa, maka akan dilakukan *padding* atau penyisipan karakter secara acak untuk memenuhi susunan pola dan diberikan pola KV.
   Partisi plainteks : jan-gan-lup-ame-ngg-una-kan-mas-ker
   Hasil pemetaan pola : kvk kvk kvk kvk kvk kvk kvk kvk kvk

3. Mengecek karakter plainteks pada himpunan kunci pada Tabel 3.1.
   Plainteks : janganlupamenggunakanmasker
   Kelas kunci : [2, 2, 2, 1, 2, 2, 1, 2, 2, 2, 2, 1, 2, 1, 1, 2, 2, 2, 1, 2, 2, 2, 2, 1, 1, 1, 2]

4. Mengecek urutan karakter alfabet sesuai dengan karakter pada himpunan kunci pada Tabel 3.1.
   Plainteks : janganlupamenggunakanmasker
   Urutan karakter : [9, 3, 0, 9, 3, 0, 4, 7, 2, 3, 6, 0, 0, 9, 9, 7, 0, 3, 1, 3, 0, 6, 3, 3, 1, 0, 1]

5. Melakukan penyisipan pola pada karakter yang termasuk himpunan kunci bagian 2. Jika karakter tersebut berpola K maka akan disisipkan pola VK setelahnya. Dan jika karakter tersebut berpola V maka akan disisipkan pola KV setelahnya.
   Plainteks : janganlupamenggunakanmasker

Pola awal : kvk kvk kvk kvk kvk kvk kvk kvk kvk

Kelas kunci : [2, 2, 2, 1, 2, 2, 1, 2, 2, 2, 2, 1, 2, 1, 1, 2, 2, 2, 1, 2, 2, 2, 2, 1, 1, 1, 2]

Penyisipan pola :

k(vk)v(kv)k(vk)kv(kv)k(vk)kv(kv)k(vk)k(vk)v(kv)kk(vk)vkk(vk)v(kv)k(vk)kv(kv)k(vk)k(vk)v(kv)kkvk(vk)

Hasil penyisipan pola :

kvkvkvkvkkvkvkvkkvkvkvkkvkvkvkkvkvkkvkvkvkkvkvkvkkvkvkvkkvkvk

6. Mengonversi karakter alfabet ke dalam huruf Korea. Karakter hangul yang dikonversi sesuai dengan urutan karakter dan pola pada Tabel 3.2. Sebelum mengubah ke dalam huruf Korea, hasil penyisipan pola akan dicek menggunakan *finite automata* apakah pola yang dihasilkan sudah sesuai dengan ketentuan penulisan huruf Korea. Jika hasil pengecekan *True* maka karakter dapat dikonversi ke dalam huruf Korea. Jika *False* maka proses tidak dapat dilakukan karena pola hangul tidak sesuai dengan kaidah penulisan.

   Urutan karakter : [9, 3, 0, 9, 3, 0, 4, 7, 2, 3, 6, 0, 0, 9, 9, 7, 0, 3, 1, 3, 0, 6, 3, 3, 1, 0, 1]

   Pola :[k,v,k,v,k,v,k,v,k,k,v,k,v,k,v,k,k,v,k,v,k,v,k,v,k,k,v,k,v,k,v,k,k,v,k,v,k,k,v,k,v,k,v,k,v,k,v,k,k,v,k,v,k,v,k]

   kvkvk

   Hasil konversi :

   ㅋ ㅖ ㅇ ㅕ ㅇ ㅖ ㄱ ㅖ ㅇ ㅋ ㅕ ㅇ ㅖ ㄱ ㅖ ㅇ ㅁ ㅠ ㅇ ㅖ ㄷ ㅖ ㅇ ㄹ ㅖ ㅇ ㅜ ㅇ ㅖ ㄱ ㄱ ㅖ ㅇ ㅣ

   ㅋ ㅈ ㅖ ㅇ ㅏ ㅇ ㅖ ㄹ ㅖ ㅇ ㄴ ㅕ ㅇ ㅖ ㄱ ㅖ ㅇ ㅅ ㅖ ㅇ ㅕ ㅇ ㅖ ㄹ ㄴ ㅏ ㄴ ㅖ ㅇ

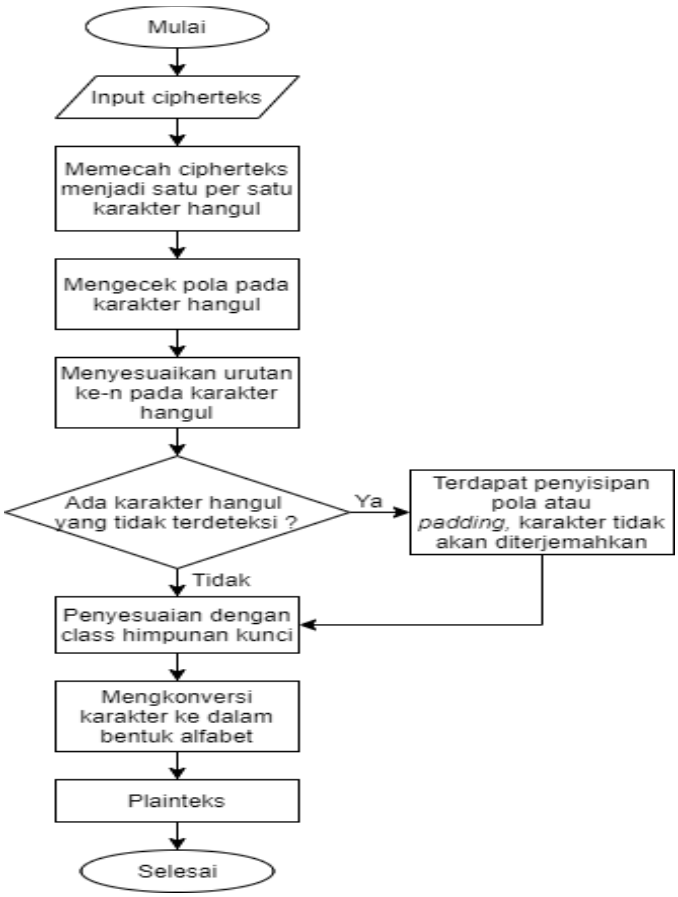
7. Menulis hasil enkripsi (cipherteks) sesuai dengan aturan penulisan huruf Korea.

   Cipherteks : 케여예곙켜예곙뮤예뗑례우옉계잌졔아예렝녀예곙셰여옐나넹

3.2.2. Dekripsi

Proses enkripsi pesan alfabet ke dalam huruf Korea dilakukan dengan memecah cipherteks hangul menjadi susunan karakter huruf yang ditulis satu per satu. Huruf Korea yang telah dipecah akan disesuaikan dengan urutan huruf yang

ada pada daftar huruf vokal dan konsonan. Hasil dari daftar karakter tersebut dapat digunakan untuk menentukan pola suku kata KV atau KVK yang sesuai. Kemudian inputan kunci dapat digunakan untuk melakukan dekripsi cipherteks menjadi pesan asli atau plainteks. Namun pada proses dekripsi ini harus memperhatikan pola suku kata yang telah disisipkan. Jika pada proses dekripsi menemukan huruf hangul berupa ㅖ *(ye)* dan ㅇ *(-ng)* maka huruf tersebut merupakan pola suku kata yang disisipkan yang berarti tidak memiliki arti dari pesan yang disampaikan dan digunakan sebagai penanda karakter yang termasuk dalam kelas himpunan kunci kedua. Pada Gambar 3.4 merupakan flowchart proses dekripsi pesan.



Gambar 3. 4 Flowchart Proses Dekripsi

Berikut merupakan penyelesaian proses dekripsi pesan dalam bentuk cipherteks Hangul ke dalam pesan asli.

1. Menginputkan cipherteks. Cipherteks yang diinputkan harus dalam bentuk tulisan huruf Korea.

Cipherteks : 켸여예곙켜예곙뮤예뎽례우옉계잌졔아예롕녀예곙셰여옐나벵

2. Memecah cipherteks huruf Korea menjadi karakter huruf yang ditulis satu per satu. Pemecahan cipherteks sesuai dengan aturan penulisan Hangul yaitu terdapat tiga susunan huruf. Huruf bagian atas kiri merupakan awalan, huruf bagian atas kanan merupakan penengah dan huruf bagian bawah merupakan akhiran. Adapun susunannya yaitu atas→bawah atau atas→kanan→bawah.

   켸 → ㅋㅖ

   여 → ㅇㅕ

   예 → ㅇㅖ

   곙 → ㄱㅖㅇ

   켜 → ㅋㅕ

   …

   …

   나 → ㄴㅏ

   벵 → ㄴㅖㅇ

   Hasil pemecahan cipherteks :

   ㅋㅖㅇㅕㅇㅖㄱㅖㅇㅋㅕㅇㅖㄱㅖㅇㅁㅠㅇㅖㄷㅖㅇㄹㅖㅇㅜㅇㅖㄱㄱㅖㅇㅣ

   ㅋㅈㅖㅇㅏㅇㅖㄹㅖㅇㄴㅕㅇㅖㄱㅖㅇㅅㅖㅇㅕㅇㅖㄹㄴㅏㄴㅖㅇ

3. Mengecek pola pada karakter hangul sesuai dengan Tabel 3.2.
   Pola : kvkvkvkvkkvkvkvkkvkvkvkkvkvkvkkvkvkkvkvkvkkvkvkvkkvkvk
   vkkvkvk

4. Menyesuaikan urutan karakter pada pola sesuai dengan Tabel 3.2. Jika terdapat karakter yang tidak terdeteksi maka karakter tersebut merupakan karakter penyisipan. Karakter yang digunakan untuk penyisipan adalah karakter ㅇ dan ㅖ. Berikut hasil urutan dengan karakter penyisipan :

   [9, x, x, 3, x, x, 0, x, x, 9, 3, x, x, 0, x, x, 4, 7, x, x, 2, x, x, 3, x, x, 6, x, x, 0, 0, x,

x, 9, 9, 7, x, x, 0, x, x, 3, x, x, 1, 3, x, x, 0, x, x, 6, x, x, 3, x, x, 3, 1, 0, 1, x, x]

Maka hasil urutan tanpa karakter penyisipan :

[9, 3, 0, 9, 3, 0, 4, 7, 2, 3, 6, 0, 0, 9, 9, 7, 0, 3, 1, 3, 0, 6, 3, 3, 1, 0, 1]

5. Penyesuaian dengan himpunan kunci pada Tabel 3.1

   Kelas kunci :

   [2, 2, 2, 1, 2, 2, 1, 2, 2, 2, 2, 1, 2, 1, 1, 2, 2, 2, 1, 2, 2, 2, 2, 1, 1, 1, 2]

6. Mengonversi karakter huruf Korea ke dalam huruf Alfabet sesuai dengan kelas kunci dan urutan karakter pada Tabel 3.1.

   Plainteks : **janganlupamenggunakanmasker**

3.3. Rancangan Pengujian

Rancangan pengujian yang akan digunakan pada penelitian ini yaitu menggunakan jenis pengujian sistem analisis frekuensi, *recovery testing* dan pengujian terhadap serangan.

3.3.1. Analisis Frekuensi

Dalam pengujian analisis frekuensi dilakukan untuk mengetahui dan membandingkan sebaran karakter huruf yang sering muncul baik karakter dalam pesan alfabet (plainteks) ataupun huruf Korea (cipherteks). Pada pengujian analisis frekuensi akan digunakan plainteks dengan dua teks bahasa yang berbeda yaitu bahasa Inggris dan bahasa Indonesia.

Pada teks bahasa Inggris berjumlah 828 karakter dan diperoleh dari teks cerita fiksi yang terdapat pada website http://textfiles.com/stories/ dengan judul “Saturday Night at The Shindar Encampment” oleh Lucillus. Sedangkan untuk teks bahasa Indonesia berjumlah 861 karakter dan merupakan potongan cerita pendek bahasa Indonesia yang terdapat pada website http://cerpenmu.com/cerpen-motivasi/ dengan judul “Di Bawah Sinar Mentari”. Pembangkit kunci enkripsi yang akan digunakan adalah kalimat ‘teknik informatika’ yang memiliki panjang 17 karakter.

Pada pengujian analisis frekuensi ini juga akan ditentukan nilai variansi dari plainteks dan cipherteks pada masing-masing teks bahasa Inggris maupun bahasa

Indonesia. Nilai variansi digunakan untuk mengetahui variasi karakter yang muncul. Jika nilai variansi pada cipherteks lebih besar dari nilai variansi plainteks, maka hasil tersebut baik karena karakter cipherteks lebih banyak variasinya dibandingkan karakter plainteks. Hal ini akan menyulitkan kriptanalisis untuk menebak pesan tanpa mengetahui kunci nya. Adapun rumus yang akan digunakan untuk menentukan nilai variansi adalah :

$$s^2 = \frac{n\sum_{i=1}^{n} x_i^2 - (\sum_{i=1}^{n} x_1)^2}{n(n-1)}$$

Keterangan :

s^2 : variansi
xi : nilai *x* ke-*i*
n : ukuran sampel

3.3.2. *Recovery Testing*

Dalam pengujian *recovery testing* digunakan untuk mengevaluasi hasil dekripsi cipherteks apakah hasil dekripsi tersebut sesuai dengan pesan asli (plainteks) atau sebaliknya. Pengujian ini dilakukan untuk mengetahui integritas dan keefektifan dari sistem.

Pada rancangan pengujian *recovery* akan digunakan delapan plainteks dengan panjang kunci yang berbeda untuk masing-masing plainteks. Plainteks yang digunakan pada pengujian juga memiliki panjang karakter yang berbeda, mulai dari pesan yang berukuran pendek sampai dengan pesan yang berukuran panjang. Plainteks tersebut diperoleh dari teks cerita fiksi yang terdapat pada website http://textfiles.com/stories/. Berikut daftar delapan plainteks yang akan digunakan :

1. Saturday Night at The Shindar Encampment
2. The Horse and The Donkey
3. The Snow Maiden
4. Jack and The Beanstalk
5. The Tree
6. The Greedy Dog
7. Narcissus
8. The Sleeping Princess

2.3.3. Pengujian Terhadap Serangan

Pengujian ini dilakukan untuk mengetahui ketahanan dari informasi yang disampaikan terdahap serangan dari pihak luar yang ingin mengetahui pesan rahasia secara tidak sah. Bahkan pihak luar tersebut ada juga yang ingin mengubah isi pesan rahasia yang diberikan oleh pengirim demi keuntungan pribadi. Terdapat dua jenis serangan yang dilakukan yaitu serangan secara aktif dan pasif. Pada penelitian ini dilakukan pengujian serangan secara aktif, dimana penyerang dapat mengubah aliran pesan seperti menghapus sebagian cipherteks, mengubah cipherteks, menyisipkan potongan cipherteks palsu, mengubah informasi yang tersimpan dan lain sebagainya [16].

Pengujian serangan dilakukan menggunakan cipherteks dari hasil enkripsi yaitu **‘켸여예곙켜예곙뮤예뎽례우옉계잌제아예렝녀예곙셰여옐나넹’.** Adapun pesan asli dari cipherteks tersebut adalah ‘jangan lupa menggunakan masker’ dan digunakan kunci ‘enkripsi pesan alfabet ke dalam huruf korea’.