Vigenere Cipher Untuk Aksara Korea (Hangul)

Ignatius Ronaldo Galman Kurniawan - 13509074
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
ignatius.ronaldo@students.itb.ac.id

***Abstrak*—*Vigenere Cipeher* adalah salah satu algoritma kriptografi klasik yang menarik dan terkenal. Algoritma ini umumnya menggunakan alfabet Latin (a,b,c,...,x,y,z) dan bahasa Inggris dalam penerapannya. Algoritma ini juga sudah mengalami banyak modifikasi agar menambah keamanannya sehingga dapat memperkuat penggunaan algoritma ini dalam perannya menyampaikan pesan. Modifikasi yang dilakukan bisa dengan memodifikasi kunci ataupun plainteksnya. Akan tetapi semua itu masih dilakukan dalam alfabet Latin. Pada makalah ini penulis mencoba penerapan algoritma *Vigenere Cipher* ini pada aksara Korea (Hangul). Aksara Korea merupakan salah satu dari 100 bahasa di dunia yang menggunakan aksaranya sendiri dalam penerapannya. Aksara yang terkenal di Asia Timur akan kerumitan dan keindahan aksaranya selain Hangul adalah aksara China (Hanja), aksara Jepang (Kanji). Oleh karena itu akan sangat menarik untuk menerapkan *Vigenere Cipher* ke dalam aksara Korea yang memiliki sangat banyak kombinasi (11268 kombinasi) sehingga akan membuat bilangan mod dari yang sebelumnya hanya berjumlah 26 menjadi 11268. Dengan demikian walaupun Algoritma ini masih bisa dipecahkan dengan metode Kasiski, akan tetapi dengan bilangan mod yang sangat besar 11268, tentunya bukan perkara mudah untuk memecahkan algoritma ini relatif terhadap algoritma *Vigenere Cipher* standar yang hanya memiliki bilangan mod sejumlah 26.**

***Kata Kunci*—*exhaustive search*, Hangul, Hanja, Kanji, *Vigenere Cipher*.**

I. PENDAHULUAN

Kriptogtafi merupakan seni dan ilmu yang digunakan untuk menyembunyikan pesan yang memiliki beberapa terminologi dasar[1]. Terminologi dasar yang penting diantaranya adalah pengirim pesan, penerima pesan, pesan, plainteks, cipherteks, enkripsi, dekripsi dan kunci.

Demikian juga dengan *Vigenere Cipher* merupakan sebuah Algoritma Kriptografi klasik yang memiliki 8 elemen tersebut. Disebut algoritma klasik karena algoritma ini tergolong algoritma dasar karena menggunakan algoritma berbasis karakter dan dapat dipecahkan tanpa menggunakan komputer. Akan tetapi algoritma ini tentunya bisa diimplementasikan ke dalam program komputer. Umumnya algoritma *Vigenere Cipher* ini menggunakan alfabet Latin dan bahasa Inggris sebagai penerapannya.

Dalam makalah ini akan dibahas penerapan dan implementasi algoritma ini dalam aksara Korea (Hangul) yang memiliki struktur alfabet yang sama sekali berbeda dengan aksara Latin. Dalam Hangul ada terdapat 11268 kemungkinan kombinasi yang terdapat dalam *unicode* dengan interval 0x3130 - 0x318F dan 0xAC00 - 0xD7A3.[2] Jumlah yang sangat berbeda jauh apabila dibandingkan aksara Latin yang direpresentasikan dalam kode *ASCII* yang tentunya membuat implementasi Hangul ke dalam *Vigenere Cipher* menjadi semakin menarik untuk diimplementasikan ke dalam program komputer.

II. DASAR TEORI

***Monoalphabetic* dan *Polyalphabetic Substitution* Cipher[1][3][4]**

Monoalphabetic substitution cipher adalah metode yang mengganti setiap karakter dengan karakter lain dalam susunan alfabet.
Sebagai contoh :
Tiap huruf di plainteks disubstitusi dengan huruf kedua dari susunan abjad yang menyebabkan pergeseran huruf sejauh 1.

Tabel Substitusi

P :	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
C :	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 a

dengan P : plainteks, C : cipherteks

artinya a diganti dengan b, b diganti dengan c, dst.

Rumus Matematis

$$c_i = E(p_i) = (p_i + k) \mod 26$$

$$p_i = D(c_i) = (c_i - k) \mod 26$$

dengan P_i = plainteks, C_i = cipherteks, k = kunci

Dan Caesar Cipher merupakan kasus khusus dari *monoalphabetic* cipher dengan pergeseran sejauh 3 yang membuat tabel susbstitusi menjadi seperti ini :

P : 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
C :d e f g h i j k l m n o p q r s t u v w x y z a b c

Rumus matematis Caesar Cipher adalah rumus matematis *monoalphabetic substitution* cipher dengan nilai k = 3.

Metode ini pertama kali digunakan oleh Julius Cesar, seorang Kaisar Romawi yang mengirimkan pesan kepada para gubernurnya dengan menggunakan pesan yang sudah terenkripsi [1].
Akan tetapi algoritma jenis ini sangatlah lemah, banyak lubang keamanan yang ada pada metode ini, dikarenakan satu karakter di plainteks dipetakan satu-ke-satu ke cipherteksnya sehingga dengan teknik *exhaustive* key *search*, algoritma ini bisa dibongkar, apalagi dengan kemampuan komputasi dewasa ini mungkin hanya dalam hitungan detik kunci/pergeseran huruf dapat ditemukan.

Polyalphabetic Substitution Cipher adalah metode yang pertama kali digunakan oleh Leon Battista Alberti kira-kira tahun 1467. Akan tetapi sumber lain mengatakan bahwa penemu *polyalphabetic* cipher adalah seorang kriptanalis Arab, Al Kindi, 600 tahun sebelum Alberti[3]. *Polyalphabetic Substitution* Cipher adalah metode yang berdasarkan substitusi, dan menggunakan cipher substitusi ganda, yang menggunakan kunci yang berbeda-beda. Cipher ini dibangun dari sejumlah cipher *monoalphabetic*, akan tetapi dengan kunci yang berbeda-beda untuk setiap alfabetnya. Metode ini menyempurnakan metode *monoalphabetic*, karena dengan penggunaan kunci yang berbeda-beda untuk setiap abjadnya, metode *exhaustive search* tidak mungkin digunakan untuk memecahkan algoritma ini, oleh karena itu dewasa ini cara ini masih sering diterapkan dengan berbagai macam modifikasi pada algoritma maupun kuncinya agar metode ini tidak mudah dipecahkan walaupun kemampuan komputasi saat ini sangat membuka kemungkinan untuk memecahkan algoritma kriptografi yang kuat sekalipun.
Contoh terkenal dari terapan metode *polyalphabetic* adalah *Vigenere Cipher*.

***Vigenere Cipher*[1][5]**
Vigenere Cipher adalah metode enkripsi teks alfabet dengan menggunakan deretan Caesar Cipher berdasarkan huruf - huruf pada kunci. *Vigenere Cipher* ditemukan oleh Blaise de Vigenere dari Prancis pada tahun 1586. Walaupun metode ini sudah ditemukan sebelum Vigenere, yaitu oleh Giovan Batista Belaso pada tahun 1553, akan tetapi Vigenere lah yang menyempurnakan metode ini sehingga Vigenere lebih dihormati dan algoritma ini dinamai *Vigenere Cipher*.
Metode ini sangat terkenal karena kemudahan untuk digunakan bagi semua orang dan sulit untuk dipecahkan bagi pemula pada zamannya.
Metode ini baru bisa dipecahkan pada abad ke-19 oleh Charles Babbage, seorang matematikawan dari Inggris. Dan Friedrich Kasiski mempublikasikan cara memecahkan *Vigenere Cipher*, sehingga metode ini dinamakan tes Kasiski.
Penggunaan *Vigenere Cipher* adalah oleh Tentara Konfederasi pada saat Perang Sipil Amerika. Perang ini meletus setelah *Vigenere Cipher* berhasil dipecahkan.

Cara Kerja *Vigenere Cipher* adalah menggunakan tabel Vigenere untuk melakukan enkripsi. Kolom paling kiri menyatakan kunci, sedangkan bagian atas menyatakan plainteks.
Setiap baris dari bujur sangkar menyatakan cipherteks yang diperoleh dengan Caesar Cipher, yang pergeseran huruf ditentukan nilai desimal oleh huruf kunci. (a=0, b=1, ..., y = 24, z = 25).
Berikut adalah Tabel Vigenere:

	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Gambar 1 Tabel Vigenere

Tabel Vigenere digunakan untuk memperoleh cipherteks dengan menggunakan kunci yang sudah tetap dengan panjang tertentu. Jika panjang kunci kurang dari plainteks, maka penggunaan kunci akan dilakukan secara periodik.
Contoh:

Plainteks	: saya ganteng
Kunci	: asda sdasdas

Perhatikan bahwa kunci asd diulang sampai sejauh plainteks. Setiap huruf di plainteks akan dienkripsi dengan kunci di bawahnya.
Cara enkripsi adalah dengan menarik garis vertikal huruf plainteks ke bawah dan menarik garis horizontal huruf kunci ke kanan. Dengan demikian perpotongan kedua garis ini akan menghasilkan sebuah huruf yang merupakan sebuah cipherteks.
Misalkan plainteks huruf G dengan Kunci S, maka dengan tabel Vigenere akan dihasilkan perpotongan huruf G dan S yaitu huruf Y.
Ilustrasi seperti gambar di bawah:

	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Gambar 2 Ilustrasi Penggunaan Tabel Vigenere

Dan Cipherteks dari “saya ganteng” dengan kunci “asd” adalah:

Plainteks	:	saya ganteng
Kunci	:	asda sdasdas
Cipherteks	:	ssba ydnlhny

Rumus Matematis dari *Vigenere Cipher* adalah sebagai berikut:

Rumus Enkripsi:

$C_i = (P_i + K_i) \bmod 26$	$P_i+K_i < 26$
$C_i = ((P_i + K_i) - 26) \bmod 26$	$P_i+K_i > 26$

Rumus Dekripsi:

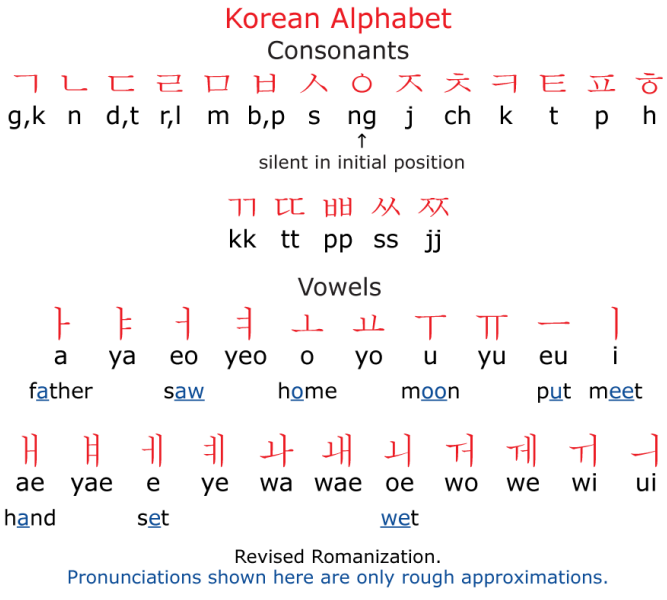
$P_i = (C_i-K_i) \bmod 26$	$C_i-K_i > 0$
$P_i = ((C_i-K_i) + 26) \bmod 26$	$C_i-K_i < 0$

Dengan :
P_i : nilai desimal karakter plainteks ke-i
C_i : nilai desimal karakter cipherteks ke-i
K_i : nilai desimal karakter kunci ke-i

Nilai desimal karakter adalah :
A = 0, B = 1, C = 2, D = 3, . . . , Z = 25.

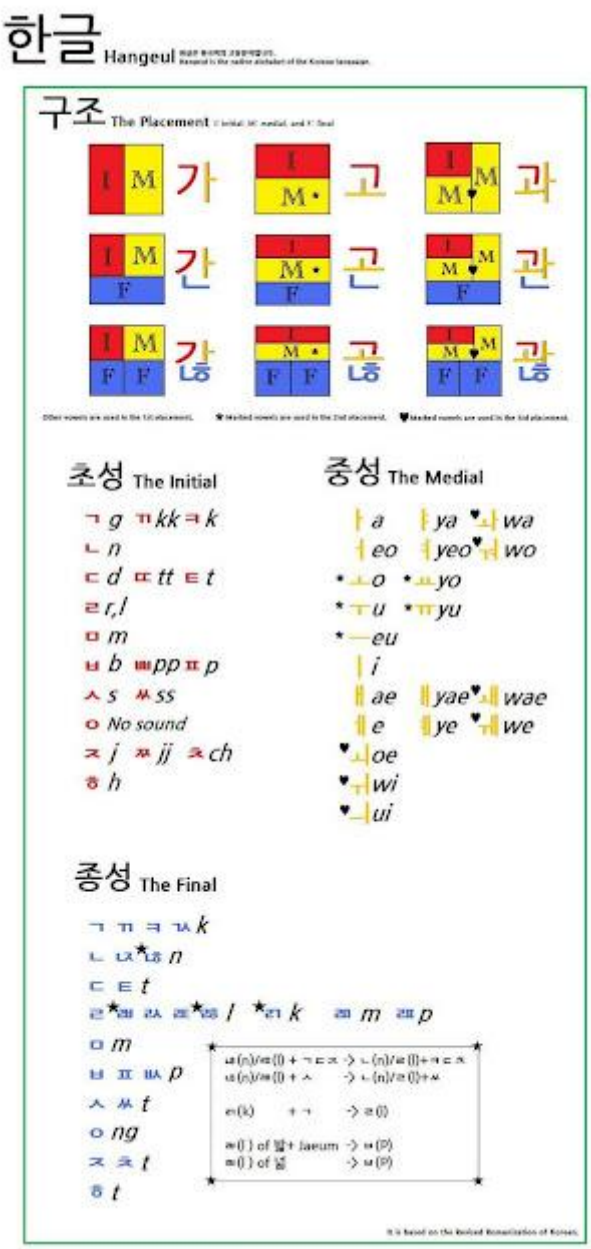
Huruf Hangul[6][7][8][9][10]
Hangul adalah tulisan dasar/aksara Korea Selatan. Kata Hangul (한글) adalah nama dari Korea Selatan. Sedangkan di Korea Utara dikenal sebagai Chosŏn'gŭl (조선글).
Pada zaman dulu kala rakyat Korea menggunakan tulisan Hanja, yang mana identik dengan tulisan Cina kuno. Tulisan Hanja itu termasuk logograf (ideograf), yang mana tiap hurufnya melambangkan suatu kata atau morfem. Untuk fasih membaca dan menulis tulisan Hanja, rakyat Korea perlu menghafal banyak sekali bentuk huruf, akibatnya hanya kaum terpelajar saja yang melek huruf. Lalu, pada pertengahan abad ke-15, Sejong The Great (세종대왕), raja yang memerintah dinasti Joseon di Korea saat itu, memiliki ide bagaimana meningkatkan tingkat literasi rakyat Korea, yaitu dengan cara menciptakan featural alphabet yang mudah dipelajari, Hangul.
Berbeda dari penulisan huruf hiragana, ataupun katakana yang memiliki konsonan tersendiri. Huruf Jepang tak bisa berdiri sendiri. Setiap konsonan dan vokal memiliki 1 huruf yang berlainan. Lain halnya dengan Hangul. Jika di deretkan, huruf Hangul memiliki lebih dari 11.000 kombinasi yang mungkin terpakai.

Hangul terdiri dari 14 Konsonan dasar dan 5 turunannya, dan juga 10 Vokal dasar dan 11 turunannya. Jadi seluruhnya ada 40 alfabet dasar dalam Hangul.
Sebuah karakter Hangul disusun dari 2 atau lebih unit. Unit tersebut terdiri dari beberapa konsonan dan vokal, yaitu:



Gambar 3 Alfabet Korea

Cara penyusunan unit-unit tersebut umumnya atas→bawah, atau atas→kanan→bawah. Seperti yang ditunjukkan pada gambar di bawah ini:



Gambar 4 Sistem Penyusunan Satu Karakter Hangul

III. IMPLEMENTASI DALAM PROGRAM DAN ANALISIS

Aksara Hangul dalam representasinya di komputer memiliki keunikan, yakni tidak menggunakan *ASCII* seperti alfabet Latin, akan tetapi menggunakan *unicode*. *Unicode* untuk hangul memiliki batasan antara 0x3130 - 0x318F (jumlahnya 96 karakter) dan 0xAC00 - 0xD7A3(11172) yang apabila dijumlahkan adalah 11268.

Ide awal adalah mirip dengan membuat *Vigenere Cipher* untuk sistem alfabet 26 karakter, yaitu dengan melakukan encode setiap karakter ke bilangan integer untuk kemudian disubstitusi ke dalam rumus matematisnya.

Demikian juga dengan *Vigenere Cipher* untuk Hangul ini, algoritma yang digunakan untuk melakukan encode karakter *Unicode* ke dalam integer adalah dengan menggunakan fungsi toInteger.

Program *Vigenere Cipher* untuk Hangul ini dibuat penulis menggunakan bahasa pemrograman Java dengan kakas IDE NetBeans 7.0.1.

Implementasi fungsinya adalah sebagai berikut:

```
       public static int toInteger(char input)
       {
            int value = input;
            if (value >= 0x3130 && value <=
0x318F)
            {
                return input - 0x3130;
            }
            else if (value >= 0xAC00 && value <=
0xD7A3)
            {
                return input - 0xAC00 + 96;
            }
            else return -1;
     }
```

Penjelasan:

Fungsi toInteger adalah fungsi untuk mengkonversikan karakter Hangul ke nilai integer.

Fungsi toInteger menerima sebuah masukan yakni nilai *Unicode* Hangul, yaitu dalam interval 0x3130 - 0x318F dan 0xAC00 - 0xD7A3. Ada 2 kelompok interval, dimana jika masukan berupa *Unicode* 0x3130 - 0x318F akan dikonversikan ke angka 0 – 95, dan jika masukan berupa *Unicode* 0xAC00 - 0xD7A3 akan dikonversikan ke angka

96 – 11267. Dengan demikian jika fungsi menerima masukan karakter Hangul akan otomatis dikonversi ke sebuah bilangan antara 0 – 11267 bergantung pada nilai *Unicode* masukan. Apabila masukan bukan berupa aksara Hangul, maka fungsi akan mengembalikan nilai -1. Ini juga menjadi batasan program, bahwa program hanya menerima masukan berupa karakter Hangul.

Kemudian proses enkripsi dan dekripsi juga masih memakai konsep *Vigenere Cipher* standar akan tetapi tentunya *Vigenere Cipher* Hangul memiliki rumusan matematis yang berbeda dibandingkan dengan *Vigenere Cipher* standar yang hanya memiliki 26 karakter berbanding dengan jumlah kombinasi karakter Hangul yang mencapai 11268 karakter.

Rumus Matematika untuk *Vigenere Cipher* Hangul:

Enkripsi

$$C_i = (P_i + K_i) \bmod 11268$$

Dekripsi

$P_i = (C_i-K_i) \bmod 11268$
$P_i = ((C_i-K_i) + 11268) \bmod 11268$

Dengan
P_i : nilai desimal karakter plainteks ke-i
C_i : nilai desimal karakter cipherteks ke-i
K_i : nilai desimal karakter kunci ke-i

Nilai karakter desimal adalah:

□ = 0, . . . , 힣 = 11267

Dan fungsi Enkripsi yang diimplementasi adalah sebagai berikut :

```
  public static String encript(String input, String
key)
  {
   String result = "";
   for (int i = 0; i < input.length(); i++)
    {
     int                    value                    =
HangulCiphers.toInteger(input.charAt(i));
     if (value == -1) continue;
     int                  keyValue                   =
HangulCiphers.toInteger(key.charAt(i%key.length()));
     int temp = (value + keyValue)%(11172+96);
     if  (temp  <  96)  result  +=  (char)  (temp  +
0x3130);
     else result += (char) (temp - 96 + 0xAC00);
    }
    return result;
}
```

Penjelasan:
Fungsi ini menerima masukan berupa plainteks dan kunci dengan panjang bebas. Kemudian baik plainteks maupun kunci akan di encode dengan fungsi toInteger. Setelah itu maka plainteks dan kunci yang sudah terkonversi akan dimasukkan ke dalam rumus matematis untuk enkripsi seperti yang telah disebutkan di atas. Kemudian setelah dilakukan perhitungan, maka didapatlah sebuah angka, yakni angka untuk cipherteks. Agar dapat ditampilkan ke layar, maka angka tersebut di decode kembali ke *unicode*nya, yakni jika angka tersebut kurang dari 96, maka angka tersebut ditambah 0x3130, karena karakter tersebut berada pada interval 0x3130 - 0x318F, dan jika lebih dari 96, maka angka tersebut akan dikurangi 96 sebelum ditambahkan 0xAC00, karena angka tersebut berada di *unicode* interval 0xAC00 - 0xD7A3.

Sedangkan untuk fungsi dekripsinya juga memiliki prinsip yang sama dengan *Vigenere Cipher* standar, implementasinya adalah sebagai berikut:

```
  public static String decript(String input, String key)
  {
   String result = "";
   for (int i = 0; i < input.length(); i++)
    {
     int                    value                    =
HangulCiphers.toInteger(input.charAt(i));
     if (value == -1) continue;
     int                  keyValue                   =
HangulCiphers.toInteger(key.charAt(i%key.length()));

     int temp=0;
     temp = (value - keyValue + 11172 + 96)%(11172+96);
     if (temp < 96) result += (char) (temp + 0x3130);
     else result += (char) (temp - 96 + 0xAC00);
     }
    return result;
}
```

Penjelasan:
Fungsi ini menerima masukan berupa cipherteks dan kunci dengan panjang bebas. Kemudian baik cipherteks maupun kunci akan di encode dengan fungsi toInteger. Setelah itu maka cipherteks dan kunci yang sudah terkonversi akan dimasukkan ke dalam rumus matematis untuk dekripsi seperti yang telah disebutkan di atas. Kemudian setelah dilakukan perhitungan, maka didapatlah sebuah angka, yakni angka untuk plainteks. Agar dapat ditampilkan ke layar, maka angka tersebut di decode kembali ke *unicode*nya, yakni jika angka tersebut kurang dari 96, maka angka tersebut ditambah 0x3130, karena karakter tersebut berada pada interval 0x3130 - 0x318F, dan jika lebih dari 96, maka angka tersebut akan dikurangi 96 sebelum ditambahkan 0xAC00, karena angka tersebut berada di *unicode* interval 0xAC00 - 0xD7A3.

Sebagai catatan, jika input bukan berupa karakter Hangul, maka fungsi ini tidak akan memprosesnya, dengan demikian berarti program tidak akan menangani masukan yang bukan berupa Hangul.
Ini tercermin dari pernyataan

```
  if (value == -1) continue;
```

baik dalam fungsi enkripsi maupun dekripsi program *Vigenere Cipher* Hangul ini.

Hasil pengujian program adalah sebagai berikut :

Input:
Berupa teks lagu[11] yang memiliki campuran antara bahasa Inggris dan Korea.

[Taeyeon]
세상 어느 곳에 그대 숨더라도
나는 그댈 찾아낼 수가 있어요
그대가 없다면
그대가 없다면
내 심장은 뛰지 않으니까

사랑이라 굳이 말하지 않아도
마음으로 나는 알 수가 있죠
그대만 있다면
그대만 있다면
아무것도 난 필요 없는데

You are my everything to me
You are my everything to me
하늘의 별처럼 환하게 비춰주리
그대는 나만의 사랑
영원한 나만의 사랑
우리 사랑해요
그대 하나면 난 충분해요

[The One]
그 무엇과 비교할 수 있을까요
그 무엇과 바꿀 수가 있나요
그대의 사랑을
그대의 마음을
그 누가 대신 할 수 있나요

You are my everything to me
You are my everything to me
하늘의 별처럼 환하게 비춰주리
그대는 나만의 사랑
영원한 나만의 사랑
우리 사랑해요
그대 하나면 나 충분해요

이별하는 일 없을거에요
그대에게 상처주는 일
눈물 흘리게 할일 나 없도록

[Taeyeon]
You are my everything to me
You are my everything to me

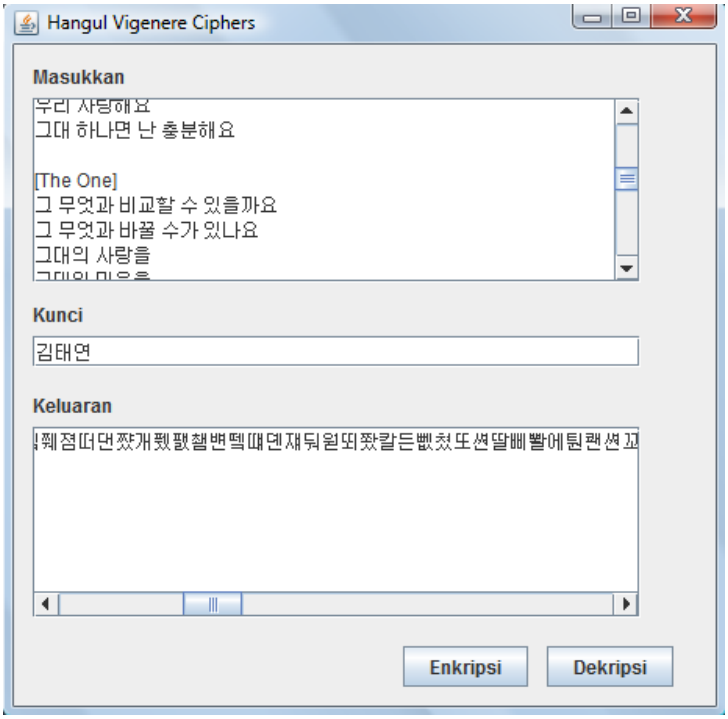
[The One]
우리 변치마요
세월이 흐른대도
그대는 나만의 사랑
영원한 나만의 사랑

[Together]
우리 사랑해요
슬픔 없는 세상에서 우리…

Kunci :
김태연

Output:
며꼍뻬첨툯된괤쵐뭠춤매과대ㅜ나걀컞빼쬌뭐왐샀됀줴졈떠턼젮개퓄괤쵐꺼됒떄덴더넸쨍쁀릐싸쟎쁴촘냬썌냉뗀매잧쨔쫰풍싸쟎빼츔대뗬짜놔대ㅜ쟬끤꺼뗔쮀졈떠댄쨨개퓄괤쵐밴뗔떄덴쟤둬윋뙤쫬칼든뻢쳤또쎤딸삐뽤에퉌쾐쎤꼬겐큐숴폼괤쵐딴쫨밴삐쌔냉좡쀈쎨헔퐜째껸먱듼뱌껸먱캬든괤쵐캐쫨봔쫬웡ㅠ감뿌졈둬됒꾜겐꿰캘쒸뗔짤펈든괤뷔뻿음때쨐뭐왐샀쫨줴졈떠삐썌냉떐괤쵐째쫨짬쁼나챔꺠쵐얀쎬뭐쨨헔든캐쳨째훽켸넴곴캐웜라민쮜다나갸쳤헔퐜째껸먱둍쥰캔대댄떤매봵뿎폼매봵감뿌나갸풍헔퓄헔큉뛴쏀줴쨔뗄쎤딴뗈뻢떐꼐뼈든괤쵐조퇈썡에띈딴뗈흄햌킐폼꼬쎬쨜쫨뻢츔뫽듼뱌휐탸대든며딙쨔앤반갸츔괤쵐딴쫨밴삐썌냉좡쀈쎨헔퐜째껸먱둼뱌껸먱캬든믤썠뻢쳤며꼍조메쥐다

Screenshot:



Gambar 5 Screenshot Program Hangul *Vigenere Cipher*

Dari hasil pengujian didapatkan bahwa program hanya akan menerima masukan berupa Hangul, dan semua tulisan yang bukan Hangul tidak akan diproses.

IV. KESIMPULAN

Vigenere Cipher untuk Hangul memiliki prinsip yang sama dengan *Vigenere Cipher* standar, yang membedakan hanyalah pada karakter yang diproses dan intervalnya. Pada *Vigenere Cipher* standar menggunakan karakter *ASCII*, sedangkan pada Hangul *Vigenere Cipher* menggunakan *unicode*.

Kelemahan yang ada pada *Vigenere Cipher* standar pun masih ada di Hangul *Vigenere Cipher* ini, akan tetapi tingkat keamanannya tentu saja bertambah, dikarenakan alfabet Latin hanya memiliki 26 karakter, sedangkan karakter Hangul memiliki 11268 karakter. Untuk memecahkan algoritma ini pun butuh usaha yang lebih banyak, sehingga dapat diambil kesimpulan bahwa algoritma untuk Hangul ini lebih aman dibandingkan dengan sistem alfabet 26 karakter.

REFERENSI

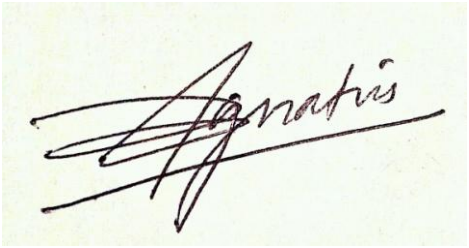
[1] Munir, Rinaldi. 2006. Kriptografi. Bandung: Informatika.
[2] http://www.*unicode*map.org/.
[3] http://en.wikipedia.org/wiki/*Polyalphabetic*_cipher.
[4] http://en.wikipedia.org/wiki/*Monoalphabetic*_*substitution*_cipher.
[5] http://id.wikipedia.org/wiki/Sandi_Vigen%C3%A8re.
[6] http://thinkzone.wlonk.com/Language/Korean.htm.
[7] http://en.wikipedia.org/wiki/Hangul.
[8] http://id.wikipedia.org/wiki/Tabel_konsonan_dan_vokal_Hangeul
[9] http://id.wikipedia.org/wiki/Hangeul
[10] http://anggriawan.web.id/2011/01/belajar-tulisan-korea-hangul.html
[11] http://rieriefanfictions.wordpress.com/2011/10/03/lyric-like-a-star-tayeon-feat-the-one-hangul-romanization-eng-indo-translation/

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 18 Maret 2012

ttd



Ignatius Ronaldo Galman Kurniawan - 13509074