

Kriptografi untuk Huruf Hiragana

Nabilah Shabrina
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
if8087@if.itb.ac.id

Abstraksi – Kriptografi pada umumnya digunakan untuk mengenkripsi huruf alphabet yang terdiri dari huruf a hingga z. Namun tidak semua huruf di dunia ini menggunakan huruf alphabet. Salah satunya adalah huruf hiragana, yang merupakan salah satu huruf di Jepang. Mereka memiliki bentuk huruf sendiri. Namun pada dasarnya proses encoding dan decoding yang dilakukan sama, yang berbeda hanya dalam bentuk representasi datanya. Bila dengan huruf alphabet biasa digunakan ASCII, maka pada huruf hiragana ini menggunakan Unicode.

Huruf hiragana secara garis besar berjumlah 46, namun bila ditambah dengan huruf-huruf tambahan lainnya bisa mencapai angka 80. Pada makalah ini akan ditampilkan proses kriptografi dengan menggunakan salah satu algoritma, yaitu caesar cipher.

Konsep algoritma caesar cipher cukup sederhana, yaitu dengan menggeser beberapa huruf saja tergantung kunci yang dimasukkan oleh user. Bila dalam kriptografi yang menggunakan alphabet akan memakai bilangan 26 untuk proses mod, maka pada hiragana akan digunakan bilangan 80, sebagai representasi jumlah hiragana.

Namun, algoritma ini memiliki kelemahan yaitu mudah dipecahkan dengan exhaustive search karena jumlah kuncinya sangat sedikit, yaitu berjumlah 80. Namun caesar cipher dengan menggunakan hiragana lebih susah dipecahkan daripada dengan alphabet karena jumlah huruf yang harus dicoba-coba lebih banyak, yaitu 80 dibandingkan dengan 26.

Index—katakana, caesar cipher, unicode.

I. PENDAHULUAN

1.1 Kriptografi

Kriptografi, secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita. Selain pengertian tersebut terdapat pula pengertian ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Namun, tidak semua aspek keamanan informasi ditangani oleh kriptografi.

Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu :

1. Kerahasiaan. Kerahasiaan merupakan layanan yang digunakan untuk menjaga isi dari informasi dari siapapun, kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.
2. Integritas data, yaitu hal yang berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.
3. Autentikasi, merupakan hal yang berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diperiksa keaslian, isi datanya, waktu pengiriman, dan lain-lain.
4. Non-repudiasi., atau nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat.

2. Algoritma Caesar Cipher

Ada beberapa macam jenis algoritma yang ada, salah satunya adalah algoritma caesar cipher. Pada algoritma ini, konsepnya sangat sederhana, yaitu dengan menggeser beberapa huruf sesuai dengan kunci masukan oleh user.

Misalkan, $A = 0,$
 $B = 1,$
 $C = 2,$
 \dots
 $Z = 25$

maka, Caesar Cipher dirumsukan secara matematis:

Enkripsi: $c_i = E(p_i) = (p_i + 3) \bmod 26$

Dekripsi: $p_i = D(c_i) = (c_i - 3) \bmod 26$

Ket: p_i = karakter plaintext ke- i

c_i = karakter ciphertext ke- i

Jika pergeseran huruf sejauh k , maka:

Enkripsi: $c_i = E(p_i) = (p_i + k) \bmod 26$

Dekripsi: $p_i = D(c_i) = (c_i - k) \bmod 26$

k = kunci rahasia

Untuk 256 karakter ASCII, maka:

Enkripsi: $c_i = E(p_i) = (p_i + k) \bmod 256$

Dekripsi: $p_i = D(c_i) = (c_i - k) \bmod 256$

k = kunci rahasia

1.3 Huruf Hiragana

Jepang memakai tiga jenis huruf dalam kehidupan sehari-harinya. Huruf hiragana, katakana, dan kanji. Hiragana dan katakana adalah suatu cara penulisan bahasa Jepang dan mewakili sebutan sukukata. Hiragana digunakan untuk menulis kata-kata asli bahasa Jepang. Katakana biasanya digunakan untuk menulis kata-kata yang berasal dari bahasa asing yang sudah diserap ke dalam bahasa Jepang. Sedangkan kanji merupakan huruf yang diadopsi dari negara Cina, yang memiliki arti dalam satu huruf.

Huruf hiragana merupakan salah satu huruf Jepang yang memiliki jumlah secara garis besar yaitu 46 huruf. Berikut merupakan tabel yang menampilkan huruf-huruf hiragana.

Basic hiragana syllables					Additional sounds					平 仮 名		
あ	い	う	え	お	が	ぎ	ぐ	げ	ご			
a	i	u	e	o	ga	gi	gu	ge	go			
か	き	く	け	こ	ざ	じ	ず	ぜ	ぞ			
ka	ki	ku	ke	ko	だ	ぢ	づ	で	ど			
さ	し	す	せ	そ	da	ji	zu	de	do			
た	ち	つ	て	と	ば	び	ぶ	べ	ぼ			
ta	chi	tsu	te	to	ぱ	ぴ	ぷ	ぺ	ぽ			
な	に	ぬ	ね	の	きゃ	きゅ	きょ	ぎゃ	ぎゅ		ぎょ	
na	ni	nu	ne	no	kya	kyu	kyo	gya	gyu		gyo	
は	ひ	ふ	へ	ほ	にゃ	にゅ	にょ	ひゃ	ひゅ	ひょ		
ha	hi	fu	he	ho	nya	nyu	nyo	hya	hyu	hyo		
ま	み	む	め	も	びゃ	びゅ	びょ	ぴゃ	ぴゅ	ぴょ		
ma	mi	mu	me	mo	mya	myu	myo	rya	ryu	ryo		
や		ゆ		よ	みゃ	みゅ	みょ	りゃ	りゅ	りょ		
ya		yu		yo	mya	myu	myo	rya	ryu	ryo		
ら	り	る	れ	ろ	じゃ	じゅ	じょ	ちゃ	ちゅ	ちょ		
ra	ri	ru	re	ro	ja	ju	je	jo	cha	chu		
わ				を	ちゃ	ちゅ	しゃ	しゅ	しゅ	しゅ		
wa				wo	che	cho	sha	shu	she	sho		
ん	ひらがな											
n	Hiragana											

Dalam proses kriptografi ini, hiragana diubah terlebih dahulu menjadi bentuk unicode hexadecimal, baru dilakukan proses kriptografi dengan menggunakan caesar cipher. Berikut ini merupakan tabel unicode

U+3041	あ	HIRAGANA LETTER SMALL A
U+3042	あ	HIRAGANA LETTER A
U+3043	い	HIRAGANA LETTER SMALL I
U+3044	い	HIRAGANA LETTER I
U+3045	う	HIRAGANA LETTER SMALL U
U+3046	う	HIRAGANA LETTER U
U+3047	え	HIRAGANA LETTER SMALL E
U+3048	え	HIRAGANA LETTER E
U+3049	お	HIRAGANA LETTER SMALL O
U+304A	お	HIRAGANA LETTER O
U+304B	か	HIRAGANA LETTER KA
U+304C	か	HIRAGANA LETTER GA
U+304D	き	HIRAGANA LETTER KI
U+304E	ぎ	HIRAGANA LETTER GI
U+304F	く	HIRAGANA LETTER KU
U+3050	く	HIRAGANA LETTER GU
U+3051	け	HIRAGANA LETTER KE
U+3052	げ	HIRAGANA LETTER GE
U+3053	こ	HIRAGANA LETTER KO
U+3054	こ	HIRAGANA LETTER GO
U+3055	さ	HIRAGANA LETTER SA
U+3056	ざ	HIRAGANA LETTER ZA
U+3057	し	HIRAGANA LETTER SI
U+3058	じ	HIRAGANA LETTER ZI
U+3059	す	HIRAGANA LETTER SU
U+305A	ず	HIRAGANA LETTER ZU
U+305B	せ	HIRAGANA LETTER SE
U+305C	ぜ	HIRAGANA LETTER ZE
U+305D	そ	HIRAGANA LETTER SO
U+305E	ぞ	HIRAGANA LETTER ZO
U+305F	た	HIRAGANA LETTER TA
U+3060	だ	HIRAGANA LETTER DA
U+3061	ち	HIRAGANA LETTER TI
U+3062	ち	HIRAGANA LETTER DI
U+3063	っ	HIRAGANA LETTER SMALL TU
U+3064	つ	HIRAGANA LETTER TU
U+3065	づ	HIRAGANA LETTER DU
U+3066	て	HIRAGANA LETTER TE
U+3067	で	HIRAGANA LETTER DE
U+3068	と	HIRAGANA LETTER TO
U+3069	ど	HIRAGANA LETTER DO
U+306A	な	HIRAGANA LETTER NA
U+306B	に	HIRAGANA LETTER NI
U+306C	ぬ	HIRAGANA LETTER NU
U+306D	ね	HIRAGANA LETTER NE
U+306E	の	HIRAGANA LETTER NO
U+306F	は	HIRAGANA LETTER HA
U+3070	ば	HIRAGANA LETTER BA
U+3071	ぱ	HIRAGANA LETTER PA
U+3072	ひ	HIRAGANA LETTER HI
U+3073	び	HIRAGANA LETTER BI
U+3074	ぴ	HIRAGANA LETTER PI
U+3075	ふ	HIRAGANA LETTER HU
U+3076	ぶ	HIRAGANA LETTER BU
U+3077	ぷ	HIRAGANA LETTER PU
U+3078	へ	HIRAGANA LETTER HE
U+3079	べ	HIRAGANA LETTER BE
U+307A	ぺ	HIRAGANA LETTER PE
U+307B	ほ	HIRAGANA LETTER HO
U+307C	ぼ	HIRAGANA LETTER BO
U+307D	ぽ	HIRAGANA LETTER PO
U+307E	ま	HIRAGANA LETTER MA
U+307F	み	HIRAGANA LETTER MI
U+3080	む	HIRAGANA LETTER MU
U+3081	め	HIRAGANA LETTER ME
U+3082	も	HIRAGANA LETTER MO
U+3083	や	HIRAGANA LETTER SMALL YA

U+3084	や	HIRAGANA LETTER YA
U+3085	ゆ	HIRAGANA LETTER SMALL YU
U+3086	ゆ	HIRAGANA LETTER YU
U+3087	よ	HIRAGANA LETTER SMALL YO
U+3088	よ	HIRAGANA LETTER YO
U+3089	ら	HIRAGANA LETTER RA
U+308A	り	HIRAGANA LETTER RI
U+308B	る	HIRAGANA LETTER RU
U+308C	れ	HIRAGANA LETTER RE
U+308D	ろ	HIRAGANA LETTER RO
U+308E	わ	HIRAGANA LETTER SMALL WA
U+308F	わ	HIRAGANA LETTER WA
U+3090	ゐ	HIRAGANA LETTER WI
U+3091	ゑ	HIRAGANA LETTER WE
U+3092	を	HIRAGANA LETTER WO
U+3093	ん	HIRAGANA LETTER N
U+3094	ゝ	HIRAGANA LETTER VU
U+3095	か	HIRAGANA LETTER SMALL KA
U+3096	け	HIRAGANA LETTER SMALL KE

II. CAESAR CIPHER DALAM HIRAGANA

Seperti yang telah disebutkan di awal, akan dilakukan proses enkripsi teks hiragana dengan menggunakan algoritma caesar cipher.

Algoritma ini akan mengenkripsi teks dengan menggeser plan teks sebanyak kuncinya

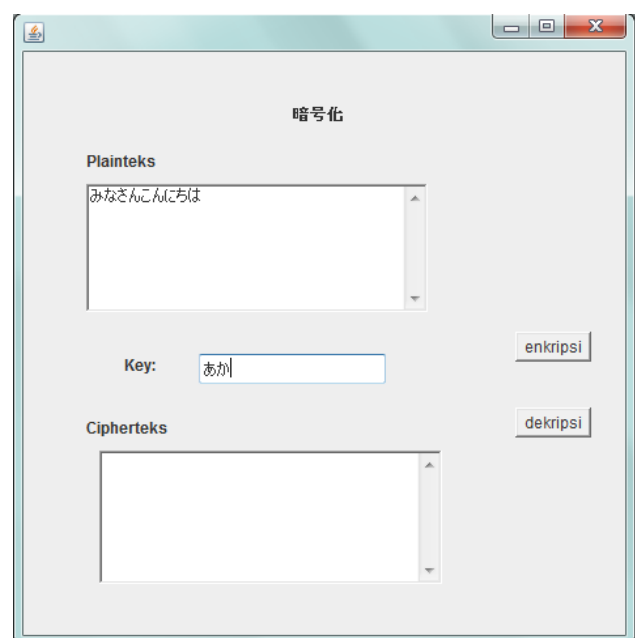
Untuk kasus kriptografi dengan menggunakan huruf hiragana, maka yang digunakan adalah:

$$\text{Enkripsi: } c_i = E(p_i) = (p_i + k) \bmod 80$$

$$\text{Dekripsi: } p_i = D(c_i) = (c_i - k) \bmod 80$$

k = kunci rahasia

contoh tampilan antarmuka untuk aplikasi ini adalah sebagai berikut :



Pertama, input hiragana harus di-convert dulu menjadi bentuk unicode heksadesimal dalam bentuk string. Setelah itu, digunakan prosedur berikut untuk melakukan enkripsi.

Misal inputan user adalah みなさんこんにちは, maka Unicode heksadesimal yang akan dihasilkan adalah "\u307f\u306a\u3055\u3093\u3001\u3053\u3093\u306b\u3061\u306f".

Dalam aplikasi ini, fungsi kunci adalah sebagai jumlah pergeseran. Caranya adalah dengan menjadikan u3041 sebagai representasi huruf あ dinilai sebagai angka 0, u3042 sebagai representasi huruf あ sebagai angka 1, dan seterusnya. Kemudian, semua angka ini ditambah dan dimod dengan 80, sehingga menghasilkan angka untuk jumlah pergeseran dari plainteks.

Sebelumnya, string dari plainteks diconvert terlebih dahulu menjadi array of string, yang masing-masing kolom dari array merupakan satu buah huruf dalam bentuk representasi hexadecimal.

Kemudian digunakan fungsi enkripsi sebagai berikut

```
public String[] Enkripsi (String[] input, int
kunci)
{
    int[] temp = new String [500];
    int[] hasil =new int[100];
    int[] teksInt =new int[100];
    int m=0;

//mengubah ke dalam bentuk integer
for(int i=0;i<input.length();i++)
{
    m= Integer.parseInt(str,16);
    teksInt[i]=m;
}

//Melakukan pergeseran dengan kunci
for(int i=0;i<input.length();i++)
{
    hasil[i] = (teksInt[i]+kunci)%80;
}

//menggunakan fungsi untuk mengubah dari array
of integer menjadi string yang berisi Unicode
heksadesimal

temp=ArrayInttoStringUnicode(hasil);

return temp;
}
```

Sedangkan fungsi dekripsi merupakan kebalikan dari fungsi enkripsi, adalah sebagai berikut:

```
public String[] Dekripsi (String[] input, int
kunci)
{
    int[] temp = new String [500];
    int[] hasil =new int[100];
    int[] teksInt =new int[100];
    int m=0;
```

```
//mengubah ke dalam bentuk integer
for(int i=0;i<input.length();i++)
{
    m= Integer.parseInt(str,16);
    teksInt[i]=m;
}

//Melakukan pergeseran dengan kunci
for(int i=0;i<input.length();i++)
{
    hasil[i] = (teksInt[i]-kunci)%80;
}

//menggunakan fungsi untuk mengubah dari array
of integer menjadi string yang berisi Unicode
heksadesimal

temp=ArrayInttoStringUnicode(hasil);

return temp;
}
```

Berikut ini merupakan contoh dari kode untuk menerjemahkan dari bentuk string of Unicode menjadi bentuk hiragana:

```
import java.io.PrintStream;
import java.io.UnsupportedEncodingException;

public class Test {
    public static void main (String[] argv) throws
UnsupportedEncodingException {
        String unicodeMessage =

"\u7686\u3055\u3093\u3001\u3053\u3093\u306b\u3061\u306f";

        PrintStream out = new PrintStream(System.out, true,
"UTF-8");
        out.println(unicodeMessage);
    }
}
```

Hasil dari kode ini adalah campuran hiragana dan katakana yaitu “皆さん、こんにちは”.

III. KESIMPULAN

Caesar Cipher, sebagaimana yang telah diterapkan dalam algoritma ini, merupakan algoritma yang sangat sederhana untuk diterapkan. Keunggulan algoritma ini adalah mudah diterapkan di berbagai teks karena hanya menggeser urutan huruf saja. Namun Caesar cipher juga memiliki kekurangan, yaitu kurang aman digunakan, karena *Caesar cipher* mudah dipecahkan dengan *exhaustive key search*. Hal itu disebabkan jumlah kuncinya sangat sedikit.

Namun caesar cipher yang diterapkan pada huruf

hiragana memiliki tingkat keamanan yang relatif lebih tinggi karena berbeda dengan huruf alfabet yang hanya memiliki 26 huruf, hiragana secara keseluruhan, ditambah huruf tambahan, memiliki jumlah huruf sebanyak 80. Hal itu mengakibatkan *exhaustive key search* yang akan dilakukan akan semakin banyak memerlukan usaha untuk memecahkannya. Berbeda dengan huruf alfabet yang menggunakan ASCII dalam melakukan pengkodean, hiragana menggunakan unicode, lebih tepatnya dalam aplikasi ini dengan UTF-8.

REFERENCES

- [1] Slide IF 3058, Kriptografi, Rinaldi Munir
- [2] Wikipedia.org/ (tanggal akses: 22/03/2011)
- [3] digilibs.its.ac.id/ (tanggal akses: 22/03/2011)
- [4] <http://hints.macworld.com/article.php?story=20050208053951714>(tanggal akses: 22/03/2011)
- [5] <http://www.utf8-chartable.de/unicode-utf8-table.pl> (tanggal akses: 22/03/2011)

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, 23 Maret 2011



Nabilah Shabrina
13508087