Penerapan *Vigenere Cipher* Untuk Aksara Arab

Prisyafandiafif Charifa (13509081)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
prisyafandiafif.charifa@gmail.com

ABSTRAK

***Vigenere Cipher* adalah sebuah algoritma kriptografi (*cipher*) yang bersifat simetris, *polyalphabetic*, dan substitusi. Ini artinya, dengan *Vigenere Cipher* ini, suatu pesan yang berupa teks akan dienkripsi dengan melakukan pemetaan huruf dengan angka untuk kemudian ditambahkan ke suatu *plaintext* sehingga didapatkan *ciphertext*-nya. Teks yang dimaksudkan untuk *Vigenere Cipher* ini pada penerapannya umumnya adalah teks berupa aksara Latin, yaitu berupa A hingga Z. Karena implementasinya yang cukup sederhana yaitu pada 26 huruf aksara Latin, maka keamanan dari *Vigenere Cipher* ini juga dianggap kurang. Karena itulah, telah dilakukan cukup banyak modifikasi pada *Vigenere Cipher* sehingga keamanannya bertambah, yaitu dengan memodifikasi kunci ataupun *plaintext*-nya. Terkadang, timbul juga pertanyaan, bagaimana *Vigenere Cipher* dapat digunakan untuk aksara selain aksara latin? Sebagai contoh adalah aksara Arab. Atas dasar itulah, pada makalah ini penulis mencoba penerapan algoritma *Vigenere Cipher* ini pada aksara Arab. Aksara Arab adalah salah satu dari ratusan bahasa di dunia yang menggunakan aksara sendiri selain aksara Latin dan terkenal karena keindahan dan beberapa ciri khasnya. Aksara yang terkenal di Asia Timur akan kerumitan dan keindahan aksaranya selain aksara Arab adalah aksara Kanji dari negara Jepang dan aksara Cina dari negeri Cina. Aksara Arab juga terkenal karena merupakan satu-satunya aksara di Asia yang ditulis dan dibaca terbalik yaitu dari kanan ke kiri. Mengingat dominasi yang cukup besar pula akan aksara Arab di dunia, maka akan cukup menarik untuk mencoba menerapkan algoritma *Vigenere Cipher* ini pada aksara Arab yang total berjumlah 28 huruf, dengan 225 huruf yang akan bertambah pada implementasinya karena adanya kombinasi.**

***Kata Kunci*—aksara Arab, *Vigenere Cipher*, *plaintext*, *ciphertext*, enkripsi, dekripsi.**

I. PENDAHULUAN

Kriptografi adalah seni dan dan ilmu yang digunakan untuk menyembunyikan pesan yang memiliki beberapa terminologi dasar[1]. Terminologi dasar tersebut di antaranya adalah pengirim pesan, penerima pesan, pesan itu sendiri, *plaintext*, *ciphertext*, enkripsi, dekripsi, dan kunci.

Salah satu algoritma klasik dari Kriptografi adalah *Vigenere Cipher*, yang pastinya memiliki delapan terminologi dasar tersebut. Algoritma *Vigenere Cipher* juga termasuk ke dalam golongan algoritma enkripsi substitusi karena dalam algoritma *Vigenere Cipher* ini, setiap huruf akan diganti dengan huruf lain. Disebut juga algoritma klasik karena selain penemuannya yang sudah cukup lama, juga karena algoritma *Vigenere Cipher* ini dapat didekripsi dengan cukup cepat tanpa menggunakan bantuan mesin atau komputer. Seperti yang sudah diutarakan sebelumnya, algoritma *Vigenere Cipher* ini umumnya menggunakan aksara Latin dalam penerapannya, yaitu huruf A sampai dengan Z.

Dalam makalah ini akan dibahas mengenai penerapan algoritma *Vigenere Cipher* dalam aksara Arab, yang memiliki keunikan tersendiri yaitu jumlahnya yang mencapai 28 huruf (dengan tambahan beberapa kombinasi, akan menjadi 225 huruf), dan penulisan serta pembacaannya adalah dari kanan ke kiri. Aksara Arab ini dalam kenyataannya ditulis tanpa menggunakan tanda baca atau *tajwid*, berbeda dengan aksara Arab yang ada di dalam kitab suci agama Islam yaitu Al-Qur'an. Aksara Arab ini jika di dalam *unicode*, ada pada rentang 0x0600 sampai dengan 0x06FF[2].

II. DASAR TEORI

II.1 *Monoalphabetic Substitution Cipher*

Monoalphabetic substitution cipher adalah metode dalam suatu algoritma kriptografi yang dalam proses enkripsinya adalah dengan mengganti satu karakter dalam *plaintext* dengan karakter lain dalam susunan suatu aksara[3].

Sebagai contoh, terdapat suatu *plaintext* dalam aksara Latin yang diberikan pada tabel *cipher* 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
X	D	G	S	Z	A	N	Y	O	B	T	M	J	C	E	V	F	H	K	W	P	L	Q	U	R	I

Gambar 1. Contoh Tabel *Monoalphabetic Substitution Cipher* [3]

Pada tabel di atas, diasumsikan semua karater dari *plaintext* bukanlah huruf kapital, di mana baris pertama merepresentasikan karakter-karakter yang mungkin ada di dalam *plaintext*, dan baris kedua merepresentasikan karakter-karakter pengganti (substitusi). Dengan kata lain, jika ada *plaintext* yaitu "ayah", maka *ciphertext*-nya adalah XRXY. Berikut adalah rumus dari *Monoalphabetic*

Substitution Cipher ini:

$$C_n = (a * P_n + m) \bmod 26$$

$$P_n = (a * C_n - m) \bmod 26$$

Gambar 2. Rumus *Monoalphabetic Substitution Cipher* untuk Aksara Latin [4]

Di mana C adalah *ciphertext*, P adalah *plaintext*, n adalah jumlah karakter dari *plaintext* atau *ciphertext*, dan m adalah jumlah pergeseran karakter untuk *ciphertext* dari aksara tersebut.

II.2 *Caesar Cipher*

Caesar Cipher yang juga sering dikenal sebagai *Caesar's Cipher* atau *Caesar's Shift*, adalah salah satu pengembangan dari *Monoalphabetic Substitution Cipher* dan merupakan salah satu dari metode enkripsi dalam kriptografi yang cukup sederhana [5]. Secara singkat, *Caesar's Cipher* adalah *Monoalphabetic Substitution Cipher* dengan nilai m adalah 3 dalam proses enkripsinya. Sesuai dengan namanya, metode ini pertama kali digunakan oleh Julius Cesar, seorang Kaisar Romawi yang mengirimkan pesan pada seseorang[1]. Sebagai contoh adalah sebagai berikut:

```
Plain:    ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher:   XYZABCDEFGHIJKLMNOPQRSTUVW
```

Gambar 3. Contoh Tabel *Caesar Cipher* [5]

Sehingga untuk suatu *plaintext* "IBU", maka *ciphertext*-nya adalah "FYR". Dalam kenyataannya, metode *Monoalphabetic Substitution Cipher* ataupun *Caesar Cipher* ini dianggap keamanannya cukup lemah, karena *ciphertext*-nya hanyalah berupa karakter yang dipetakan satu-satu dengan *plaintext*-nya, maka dengan metode analisis frekuensi ataupun pencarian secara *brute force* pada *ciphertext*-nya, dapat ditemukan dengan mudah *plaintext*-nya. Apalagi mengingat kemampuan mesin atau komputer saat ini yang sudah semakin maju. Untuk itulah, dikembangkan *Polyalphabetic Substitution Cipher* yang merupakan perkembangan dari *Monoalphabetic Substitution Cipher*.

II.3 *Polyalphabetic Substitution Cipher*

Sesuai dengan namanya, *Polyalphabetic substitution cipher* adalah metode dalam suatu algoritma kriptografi yang dalam proses enkripsinya adalah dengan mengganti lebih dari satu karakter dalam *plaintext* dengan karakter lain dalam susunan suatu aksara[6]. Metode ini pertama kali digunakan oleh Leon Battista Alberti pada tahun 1467 Masehi, namun pertama kali diciptakan pada kisaran abad 8 Masehi oleh seorang kriptanalis dari negara Arab bernama Al-Kindi. *Polyalphabetic Substitution Cipher* ini dibangun dari sejumlah *Monoalphabetic Substitution Cipher*, namun dengan menggunakan kunci yang berbeda-beda untuk setiap abjadnya. *Vigenere Cipher* adalah salah satu algoritma kriptografi klasik yang menerapkan *Polyalphabetic Substitution Cipher*.

II.4 *Vigenere Cipher*

Vigenere Cipher adalah salah satu metode enkripsi teks dengan menggunakan serangkaian *Caesar Cipher* yang berbeda[6] dan merupakan salah satu penerapan dari metode *Polyalphabetic Substitution Cipher*.

Vigenere Cipher sudah mengalami beberapa perkembangan sebelumnya. Metode ini ditemukan pada tahun 1552 oleh Giovan Battista Bellaso dalam bukunya yang berjudul *La cifra del. Sig. Giovan Battista Bellaso*. Metode ini terkenal karena cukup mudah untuk dimengerti dan diterapkan, dan mempunyai tingkat keamanan yang cukup tinggi karena cukup sukar dipecahkan secara manual. Akibatnya, metode ini mendapat julukan "chiffre indechiffrable" dalam bahasa Prancis yang artinya adalah "*Cipher* yang tidak bisa dipecahkan". Banyak orang sudah mencoba untuk memecahkan *Vigenere Cipher* ini dengan membuat skema-skema enkripsi tertentu, namun baru berhasil 300 tahun kemudian[7].

Metode ini berhasil dipecahkan pada tahun 1863 oleh Friedrich Kasiski, dan mempublikasikannya, sehingga metode kriptanalisis untuk Vigenere Cipher disebut sebagai Metode Kasiski. Metode Kasiski ini menggunakan beberapa kelemahan dalam *Vigenere Cipher*, yaitu di mana ada banyak kemungkinan untuk suatu karakter dienkripsi menggunakan karakter kunci yang sama. Contohnya adalah sebagai berikut:

```
Key:        ABCDABCDABCDABCDABCDABCDABCD
Plaintext:  CRYPTOISSHORTFORCRYPTOGRAPHY
Ciphertext: CSASTPKVSIQUTGQUCSASTPIUAQJB
```

Gambar 4. Contoh *Ciphertext* dengan Karakter Berulang pada *Vigenere Cipher*[7]

Dapat dilihat pada contoh di atas, serangkaian karakter "CSASTP" terlihat berulang pada *ciphertext*. Ini tentunya akan memudahkan suatu *ciphertext* untuk dipecahkan dengan Metode Kasiski. Metode ini tidak akan dibahas lebih lanjut karena tidak menjadi fokus dalam makalah ini.

Dalam penerapan *Vigenere Cipher*, digunakan tabel *Vigenere* untuk melakukan enkripsi. Kolom menyatakan *plaintext*, dan baris menyatakan kunci. Setiap baris dari persegi menyatakan *ciphertext* yang akan diperoleh dengan *Caesar Cipher*, yang mana pergeseran hurufnya ditentukan dari nilai desimal karakter kuncinya. Berikut adalah tabel *Vigenere* untuk aksara Latin:

Gambar 5. Tabel *Vigenere* Aksara Latin [8]

Tabel *Vigenere* digunakan untuk memperoleh karakter *ciphertext*. Sebagai contoh, diketahui kunci untuk enkripsi dengan *Vigenere Cipher* adalah "PYRAMID" dan *plaintext*-nya adalah "ATTACKATSUNDOWN". Dalam hal ini, jika panjang karakter kunci kurang dari panjang karakter *plaintext*, maka karakter kunci akan diulang secara periodik seperti pada contoh berikut ini:

Key letters:	P	Y	R	A	M	I	D	P	Y	R	A	M	I	D	P
Plaintext:	A	T	T	A	C	K	A	T	S	U	N	D	O	W	N

Gambar 6. Contoh Kunci dan *Plaintext* untuk *Vigenere Cipher* [9]

Dari contoh di atas, maka dengan mencocokkan satu persatu karakter-karakter dari kunci dengan karakter-karakter dari *plaintext*, maka diketahui bahwa huruf "A" dari *plaintext* akan diganti dengan huruf "P", huruf "T" dari *plaintext* akan diganti dengan huruf "R", dst. Untuk lebih jelasnya adalah sebagai berikut:

Gambar 7. Contoh Penggunaan Tabel *Vigenere*

Dapat dilihat pada gambar di atas bahwa huruf "C" pada *plaintext* yang berpasangan dengan huruf "M" pada kunci, akan menghasilkan huruf "O" untuk *ciphertext*-nya. Langkah ini diulangi terus hingga semua karakter dalam *plaintext* tersubstitusi dan dihasilkanlah *ciphertext* yaitu "PRKAOSDIQLNPWZC".

Untuk rumus matematis dari enkripsi *Vigenere Cipher* adalah sebagai berikut:

$$C_n = (P_n + K_n) \bmod 26 \quad \text{--> } P_n + K_n < 26$$

$$C_n = ((P_n + K_n) - 26) \bmod 26 \text{ --> } P_n + K_n > 26$$

Gambar 8. Rumus Matematis Enkripsi *Vigenere Cipher*[9]

Di mana C_n adalah nilai desimal suatu karakter ke-n dalam *ciphertext*, P_n adalah nilai desimal suatu karakter ke-n dalam *plaintext*, dan K_n adalah nilai desimal suatu karakter ke-n dalam kunci.

II.5 Aksara Arab

Aksara Arab adalah aksara yang digunakan untuk menuliskan bahasa Arab. Aksara Arab ditulis dan dibaca dari arah kanan ke kiri, dalam gaya *curscive*, dan mencakup 28 huruf (dapat menjadi 225 huruf dengan kombinasinya).

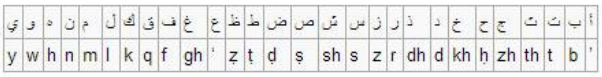
Dua puluh delapan huruf dalam aksara Arab diadaptasi dari berbagai naskah Arab untuk berbagai bahasa, seperti Persia, Ottoman, Sindhi, Urdu, Malay, dsb. Dalam aksara Arab, tidak ada perbedaan antara huruf kapital dan tidak.

Banyak huruf dalam aksara Arab terlihat sama, namun sebenarnya dibedakan dengan adanya sejenis titik pada bagian atas atau bawah suatu alfabet yang disebut sebagai *rasm*. Titik-titik ini dapat disebut sebagai bagian yang terpadu dengan huruf-huruf dalam aksara Arab, karena titik-titik ini membedakan huruf-huruf yang mempunyai bunyi berbeda. Sebagai contoh, pada aksara Arab, huruf yang pada aksara Latin adalah b dan t, sebenarnya mempunyai bentuk yang sama, namun b mempunyai satu titik di bawah huruf Arab-nya, dan t mempunyai dua titik di atas huruf Arab-nya.

Terdapat dua susunan utama dalam huruf Arab, yaitu susunan *abjadī* asli dan susunan *hijā'ī* atau *'alifbā'ī*. Susunan *abjadī* asli diturunkan dari huruf *Phoenician* seperti huruf *Hebrew*, sedangkan susunan *hijā'ī* atau *'alifbā'ī* digunakan saat sekumpulan nama atau kata diurutkan, seperti pada buku telepon, kamus, dsb. Berikut adalah susunan yang paling umum dari *abjadī* asli:

Gambar 9. Susunan Paling Umum *abjadī* Asli [10]

Sedangkan berikut ini adalah susunan *hijā'ī* terbaru:



Gambar 10. Susunan ***hijā'ī*** **T**erbaru **[11]**

III. IMPLEMENTASI DALAM PROGRAM

Aksara Arab dalam implementasinya melalui program komputer adalah menggunakan *unicode*, bukan ASCII seperti aksara Latin. *Unicode* untuk aksara Arab ada di antara rentang 0x0600 sampai dengan 0x06FF[2] dengan jumlah 225 karakter. Untuk mengimplementasikan *Vigenere Cipher* pada aksara Arab ini, idenya tidak jauh berbeda dengan aksara Latin yang memiliki 26 karakter, yaitu dengan melakukan *encode* setiap karakter ke bilangan integer dan desimal untuk kemudian disubstitusi ke dalam rumus matematis dari *Vigenere Cipher* dengan aksara Arab ini.

Karena representasi aksara Arab adalah dengan *unicode*, maka pertama-tama dilakukan konversi dari *unicode* tersebut ke integer dengan menggunakan fungsi toInt. Berikut adalah algoritma untuk fungsi toInt:

```
function toInt (input : char, output :
integer)
{
      konversi : integer
      konversi <- input
      if (konversi >= 0x0600 &&
konversi <= 0x06FF) then
      {
            output <- konversi -
0x0600
            return output
      }
      else
      {
            return -1
      }
}
```

Pada algoritma di atas, terdapat fungsi toInt yang berguna untuk mengkonversi karakter-karakter dalam aksara Arab ke integer. Fungsi toInt akan menerima sebuah masukan yaitu nilai *unicode* dari aksara Arab yang berada dalam rentang 0x0600 sampai dengan 0x06FF. Dalam program ini, *unicode* dari aksara Arab yang berada dalam rentang 0x0600 sampai dengan 0x06FF tersebut akan dikonversikan ke angka 0 sampai dengan 224. Jika masukan bukan berupa nilai *unicode* yang berada dalam rentang 0x0600 sampai dengan 0x06FF, maka fungsi akan mengeluarkan nilai integer -1.

Setelah itu dilakukan proses enkripsi dengan menggunakan konsep *Vigenere Cipher* pada umumnya tetapi tentunya dengan rumus matematis yang berbeda, karena aksara Arab memiliki 225 karakter dengan kombinasinya sedangkan aksara Latin yang biasa digunakan untuk *Vigenere Cipher* biasa hanya memiliki 26 karakter. Berikut adalah rumus matematis dari *Vigenere Cipher* dengan aksara Arab:

$$C_n = (P_n + K_n) \bmod 225$$

Gambar 11. Rumus Matematis Enkripsi *Vigenere Cipher* pada Aksara Arab

Dengan nilai desimal yang berada dalam rentang 0 sampai dengan 224. Setelah itu, dapat dibuat programnya dengan berdasar pada rumus matematis tersebut dengan algoritma sebagai berikut:

```
function encryptarab (input : string,
inputkunci : string, output : string)
{
      hasilenkrip : string
      i : integer
      hasilkonversiinput : integer
      hasilkonversikunci : integer
      temp : integer

      i <- 0
      hasilenkrip <- ""
      hasilkonversiinput <- 0
      hasilkonversikunci <- 0
      temp <- 0

      for i=0 to i < input.length() do
      {
            hasilkonversiinput <-
toInt(input.charAt(i))

            if (hasilkonversiinput = -
1) then
            {
                  output <- ""
            }

            hasilkonversikunci <-
toInt(inputkunci.charAt(i mod
key.lenght()))

            temp <-
(hasilkonversiinput +
hasilkonversikunci) mod 225

            if (temp <= 224) then
            {
                  output <-
toChar(temp + 0x0600)
            }
      }
      return output
```

```
}
```

Fungsi encryptarab ini berfungsi untuk mengenkripsi karakter-karakter dalam aksara Arab dengan rumus matematis enkripsi *Vigenere Cipher* yang sudah dibahas sebelumnya. Panjang kunci dan *plaintext* bebas. Masukan dari fungsi ini adalah string, dan keluarannya juga adalah string. String masukannya adalah string yang mewakili *plaintext* dan string yang mewakili kunci. Pertama-tama, setiap karakter *plaintext* dan kunci akan dikonversi ke integer dengan fungsi toInt yang sudah dijelaskan sebelumnya. Setelah itu, hasil yang berupa integer tersebut akan dimasukkan ke dalam rumus matematis enkripsi *Vigenere Cipher* untuk aksara Arab untuk perhitungannya. Dari perhitungan tersebut, didapatkanlah suatu integer yang merepresentasikan setiap karakter *ciphertext*-nya. Tentunya saat ditampilkan, bukanlah *ciphertext* dalam bentuk desimal, melainkan harus dalam bentuk aksara Arab lagi. Oleh karena itu, dilakukan konversi ulang dari integer ke karakter aslinya dengan menggunakan fungsi bawaan toChar. Jika nilai integer dari karakter *ciphertext*-nya adalah lebih kecil atau sama dengan 224 (karena 225 adalah jumlah karakter aksara Arab dalam *unicode*), maka nilai integer *ciphertext* tersebut akan ditambahkan dengan 0x0600 dahulu sebelum dikonversi ke karakter aslinya.

Untuk proses dekripsinya, juga tidak berbeda jauh dengan proses dekripsi pada *Vigenere Cipher* biasa, namun tentunya rumus matematisnya akan lain, yaitu sebagai berikut:

$$P_n = (C_n - K_n) \bmod 225$$

Gambar 12. Rumus Matematis Dekripsi *Vigenere Cipher* pada Aksara Arab

Dengan nilai desimal yang berada dalam rentang 0 sampai dengan 224. Setelah itu, sama dengan proses enkripsi, dapat dibuat programnya dengan berdasar pada rumus matematis tersebut dengan algoritma sebagai berikut:

```
function decryptarab (input : string,
inputkunci : string, output : string)
{
      hasildekrip : string
      i : integer
      hasilkonversiinput : integer
      hasilkonversikunci : integer
      temp : integer

      i <- 0
      hasildekrip <- ""
      hasilkonversiinput <- 0
      hasilkonversikunci <- 0
      temp <- 0

      for i=0 to i < input.length() do
      {
            hasilkonversiinput <-
toInt(input.charAt(i))

            if (hasilkonversiinput = -
1) then
            {
                  output <- ""
            }

            hasilkonversikunci <-
toInt(inputkunci.charAt(i mod
key.lenght()))

            temp <-
(hasilkonversiinput -
hasilkonversikunci) mod 225

            if (temp <= 224) then
            {
                  output <-
toChar(temp + 0x0600)
            }
      }
      return output
}
```

Fungsi decryptarab ini berfungsi untuk mendekripsi karakter-karakter *ciphertext* dalam aksara Arab dengan rumus matematis dekripsi *Vigenere Cipher* yang sudah dibahas sebelumnya. Masukan dari fungsi ini adalah string, dan keluarannya juga adalah string.. Dalam hal ini, input adalah *ciphertext* dan inputkey adalah kuncinya. Pertama-tama, setiap karakter *ciphertext* dan kunci akan dikonversi ke integer dengan fungsi toInt yang sudah dijelaskan sebelumnya. Setelah itu, hasil yang berupa integer tersebut akan dimasukkan ke dalam rumus matematis dekripsi *Vigenere Cipher* untuk aksara Arab untuk perhitungannya. Dari perhitungan tersebut, didapatkanlah suatu integer yang merepresentasikan setiap karakter *plaintext*-nya. Tentunya saat ditampilkan, bukanlah *plaintext* dalam bentuk desimal atau integer, melainkan harus dalam bentuk aksara Arab lagi. Oleh karena itu, dilakukan konversi ulang dari integer ke karakter aslinya dengan menggunakan fungsi bawaan toChar. Jika nilai integer dari karakter *plaintext*-nya adalah lebih kecil atau sama dengan 224 (karena 225 adalah jumlah karakter aksara Arab dalam *unicode*), maka nilai integer *plaintext* tersebut akan ditambahkan dengan 0x0600 dahulu sebelum dikonversi ke karakter aslinya.

Dalam program ini dan algoritma sebelumnya, dapat diketahui juga bahwa program tidak akan menerima masukan string *plaintext* selain aksara Arab. Ini terbukti pada bagian berikut:

```
if (hasilkonversiinput = -1) then
      {
            output <- ""
      }
```

Dengan begitu, karakter selain aksara Arab akan dienkripsi menjadi karakter kosong pada *ciphertext*-nya.

Pengujian dari progam implementasi *Vigenere Cipher* untuk aksara Arab dilakukan dengan *plaintext* berikut:

دطج كحمدطج كحمدطج كحمدطج كحمدطج كحمدطج كحمدطج كحم

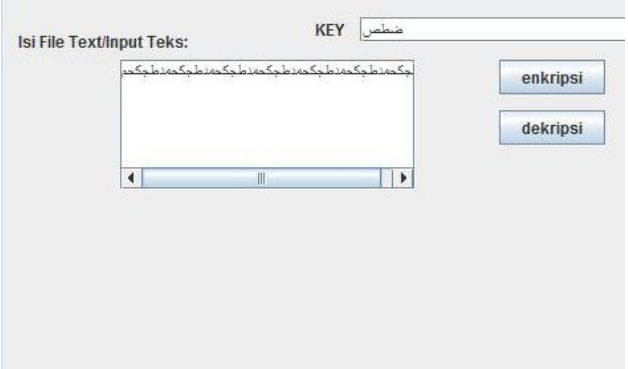
dan dengan kunci sebagai berikut:

ضطص

Maka didapatkan keluarab *ciphertext* sebagai berikut:

ت٣و٦ب٥ت٣و٦ب٥ت٣و٦ب٥ت٣و٦ب٥ت٣و٦ب٥ت٣و٦ب٥ت٣و٦ب

Berikut adalah *screenshot* dari program *Vigenere Cipher* untuk aksara Arab ini:



IV. SIMPULAN

Dari berbagai pembahasan di atas mengenai penerapan *Vigenere Cipher* dengan aksara Arab, dapat diambil beberapa simpulan sebagai berikut :

a. *Vigenere Cipher* untuk aksara Latin menggunakan ASCII, sedangkan *Vigenere Cipher* untuk aksara Arab menggunakan *unicode*
b. *Vigenere Cipher* untuk aksara Arab pada dasarnya memiliki prinsip yang sama dengan *Vigenere Cipher* biasa yang digunakan untuk aksara Latin, perbedannya hanya pada karakter yang diproses, rentang, dan rumus matematisnya
c. Kelemahan yang ada pada *Vigenere Cipher* dengan aksara Arab sedikit bertambah karena aksara Arab memiliki 225 karakter total dengan kombinasinya, yang mana *Vigenere Cipher* untuk aksara Latin hanya 26 karakter

V. DAFTAR PUSTAKA

[1] Munir, Rinaldi. 2006. Kriptografi. Bandung: Informatika.
[2] http://www.unicode.org/charts/PDF/U0600.pdf
Tanggal Akses : 23 Maret 2013
[3] http://www.imxcited.com/cp05_secret_writings/010_mono_cipher.html
Tanggal Akses : 23 Maret 2013
[4] http://www.srcf.ucam.org/~bgr25/cipher/monoalph.php
Tanggal Akses : 23 Maret 2013
[5] http://www.murky.org/blg/category/cryptography/
Tanggal Akses : 24 Maret 2013
[6] http://www.math.cornell.edu/~mec/2003-2004/cryptography/polyalpha/polyalpha.html
Tanggal Akses : 24 Maret 2013
[7] Gaines, Helen Fouche. 1939. "The Gronsfeld, Porta and Beaufort Ciphers". Cryptanalysis a Study of Ciphers and Their Solutions. Dover Publications. pp. 117–126. ISBN 0-486-20097-3.
[8] http://www.math.cornell.edu/~mec/2003-2004/cryptography/polyalpha/vigenere.html
Tanggal Akses : 25 Maret 2013
[9] http://hem.passagen.se/tan01/poly.html
Tanggal Akses : 26 Maret 2013
[10] http://www.saudiaramcoworld.com/issue/198102/arabic.and.the.art.of.printing-a.special.section.htm
Tanggal Akses : 26 Maret 2013

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, 26 Maret 2013

Prisyafandiafif Charifa
(13509081)