Jurnal Informasi Komputer Logika
Volume 1, Nomor 4, Oktober 2020
ISSN 2955-7002
Available Online http://ojs.logika.ac.id/index.php/jikl

Algoritma Vigenere Cipher Untuk Penyandian Record Informasi Pada Database

Tomy Satria Alasi[1], Ahmad Taufik Al Afkari Siahaan[2]
[1]Teknik Informatika, STMIK Logika, Medan
[2] Sains Dan Teknologi, Ilmu Komputer, Universitas Islam Negeri Sumatera Utara Medan, Medan
Email: [1]tomysatriaaalasi@live.com, [2]siahaan.taufik.alafkari@gmail.com

Abstrak – Penelitian ini menghasilkan penyandian record database dengan algoritma vigenere cipher. Jika penggunaan database semakin berkembang maka perlu program untuk penyandian. Penyandian record database merupakan mengamankan rekaman data pada database. Database adalah kumpulan data yang terorganisir yang disimpan dan diakses secara elektronik dari sistem komputer. Database sangat kompleks bahkan semakin hari semakin di kembangkan. Semakin banyak data pada database maka semakin banyak informasi yang harus di amankan. Pengamanan informasi tersebut dapat dilakukan dengan ilmu kriftografi. Kriptografi atau yang sering dikenal dengan sebutan ilmu penyandian data adalah suatu bidang ilmu dan seni yang bertujuan untuk menjaga kerahasiaan suatu informasi yang berupa data-data dari pihak lain yang tidak berhak, sehingga tidak menimbulkan kerugian, salah satu algoritma sederhana kriftografi adalah algoritma vigenere cipher. Algoritma viginere cipher adalah metode enkripsi abjad teks dengan menggunakan serangkaikan terjalin berdasarkan kata kunci. Algoritma viginere cipher dapat dimanfaatkan untuk penyandian record informasi dalam database berdasarkan penguncian oleh pengguna dalam sebuah aplikasi.

Kata Kunci: Algoritma Viginere Cipher, Penyandian, Record Informasi, Database

Abstract−This research resulted in the encryption of MySQL database records using the vigenere cipher algorithm. If the use of databases is growing, a program for encryption is needed. Database record encoding is to secure data records in the database. A database is an organized collection of data that is stored and accessed electronically from a computer system. The database is very complex and is increasingly being developed. The more data in the database, the more information that must be secured. Safeguarding this information can be done with cryptography. Cryptography or what is often known as the science of encoding data is a field of science and art that aims to maintain the confidentiality of information in the form of data from other unauthorized parties, so that it does not cause losses, one of the simple cryptography algorithms is the vigenere cipher algorithm. The viginere cipher algorithm is a method of encrypting text alphabets by using interwoven series based on keywords. The viginere cipher algorithm can be used to encode information records in the database based on user locking in an application.

Keywords: Vigenere Cipher Algorithm, Encoding, Record Information, Database

1. PENDAHULUAN

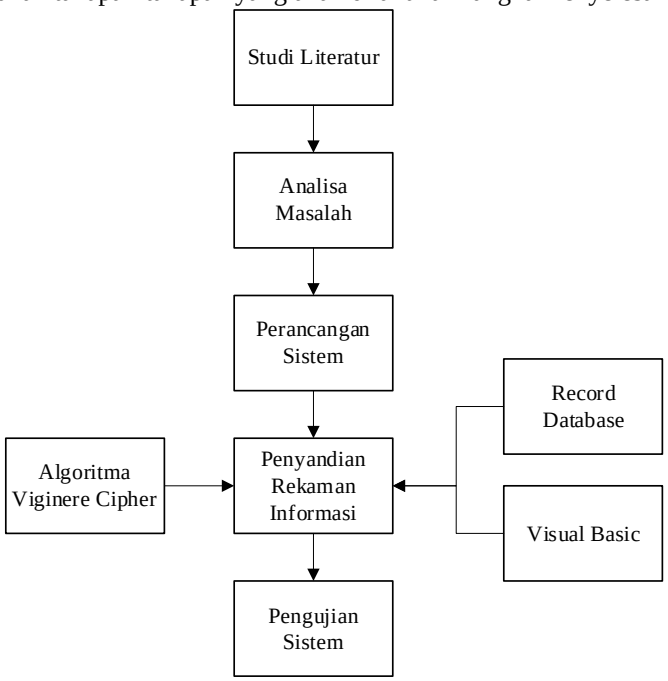
Setiap saat penggunaan database semakin berkembang pesat. Hampir semua aplikasi Online menggunakan database. Bayangkan jika data dibajak dan dimanfaatkan oleh orang yang tidak berkepentingan maka akan sangat merugikan suatu organisasi. Suatu sistem yang terpenting adalah keamanan sistem itu sendiri. Berbagai hal terus dilakukan untuk meningkatkan sebuah keamanan data. Data yang sudah disimpan di dalam database dinamakan record atau rekaman. Pengamanan rekaman data dapat dilakukan dengan kriftografi. Kriftografi dapat mengamankan data berdasarkan aturan sehingga data tidak mudah dibaca oleh pihak yang tidak berkepentingan[1]. Kriptografi digunakan untuk menjaga keamanan pesan atau informasi[2], baik informasi yang ditransmisikan melalui saluran komunikasi maupun informasi disimpan di dalam media penyimpanan[3]. Algoritma viginere cipher adalah salah satu algoritma kriptografi standar yang mencegah penyerang selama transmisi[4]. Kebutuhan akan informasi yang cepat, tepat, dan akurat sangat penting. Berbagai instansi berusaha mengembangkan usahanya dengan melakukan banyak perubahan dengan memanfaatkan teknologi yang canggih seperti Komputer sebagai pengganti tenaga kerja manusia[5]. Penyimpanan informasi sering dilakukan di dalam database. Database adalah tempat penyimpanan data yang dapat di relasi kan dan dimanfaatkan dengan mudah dan cepat. Sistem elektronik berbasis setiap hari selalu dimanfaatkan[6]. Pada intinya sebuah informasi tidak baik jika tidak menggunakan keamanan jika informasi tersebut menggunakan database maka informasi yang ada harus diamankan di dalam database. Aplikasi yang digunakan dalam pengujian ini adalah visual basic. Microsoft visual basic (sering disingkat sebagai VB saja) merupakan sebuah bahasa pemrograman yang menawarkan *integrated development environment* (IDE) visual untuk membuat program perangkat lunak berbasis sistem operasi Microsoft Windows dengan menggunakan model pemrograman[7]. Pengujian ini dilakukan langsung mengambil record database dan mengunci record menggunakan aplikasi yang di bangun dengan microsoft visual basic.

Jurnal Informasi Komputer Logika
Volume 1, Nomor 4, Oktober 2020
ISSN 2955-7002
Available Online http://ojs.logika.ac.id/index.php/jikl

2. METODE PENELITIAN

2.1 Metode Penelitian

Metode penelitian merupakan tahapan-tahapan yang akan dilakukan rangka menyelesaikan masalah dibahas.



Gambar 1. Metode Penelitian

Uraian dari kerangka kerja penelitian yang digambarkan pada sebagai berikut :

1. Studi Literatur
   Tahap ini merupakan tahap pembelajaran konsep tentang penyandian record informasi, kriftografi, algoritma viginere cipher, database, MySQL, konsep pemrograman.
2. Analisa masalah
   menentukan masalah yang berhubungan dengan bahan penelitian. Studi mengenai teori algoritma viginere cipher dan cara penyandian data dengan kriftografi.
3. Penyandian Rekaman Informasi
   hasil dari perancangan aplikasi yang menggunakan pemrograman Microsoft Visual Basic yang meliputi tampilan hasil enkripsi dan deskripsi untuk penyandian rekaman informasi dengan algoritma viginere cipher data diambil dari record database .
4. Pengujian Sistem
   Pengujian sistem dilakukan untuk melihat implementasi dari algoritma viginere cipher ke dalam sebuah aplikasi. dilakukan uji coba sistem yang telah selesai dirancang, proses uji coba ini diperlukan untuk memastikan bahwa aplikasi yang telah dibuat sudah benar, sesuai dengan karakteristik yang ditetapkan.

2.2 Algoritma Viginere Cipher

Algoritma adalah urutan langkah-langkah logis penyelesaian masalah yang disusun secara sistematis[8]. Algoritma viginere cipher adalah salah satu algoritma kriptografi standar yang mencegah penyerang selama transmisi[4]. Algoritma ini menggunakan tabel untuk penyandian data. Mirip dengan caesar cipher yaitu teknik yang sederhana[1]. Cipher menggunakan hasil teks yang sudah di sandi atau enkripsi. Algoritma Viginere cipher dipublikasikan pada tahun 1586, tetapi algoritma tersebut baru dikenal luas 200 tahun kemudian yang oleh penemunya cipher tersebut dinamakan viginere cipher. Cipher ini berhasil dipecahkan oleh Babbage dan Kasiski pada pertengahan abad 19. Rumus penyandian dan pengembalian dari sandi dengan algoritma viginere cipher adalah sebagai berikut:

$$C_i = (P_i + K_i) mod\ 26 \qquad (1)$$

$$P_i = (P_i + K_i) \text{mod } 26 \qquad (2)$$

Keterangan :

Jurnal Informasi Komputer Logika
Volume 1, Nomor 4, Oktober 2020
ISSN 2955-7002
Available Online http://ojs.logika.ac.id/index.php/jikl

Ci = nilai desimal karakter ciphertext ke-i
Pi = nilai desimal karakter plaintext ke-i
Ki = nilai desimal karakter kunci ke-i

2.3 Penyandian Record Informasi Pada Database

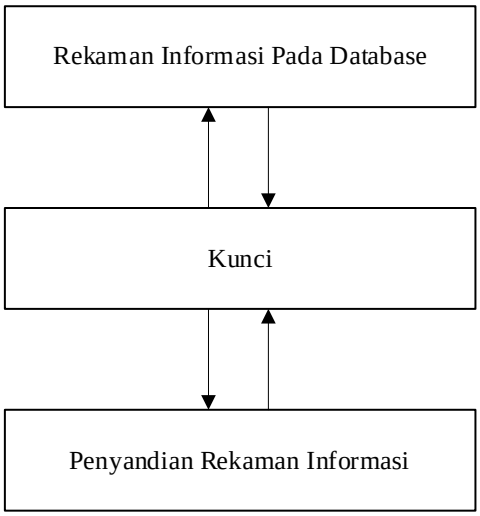
Penyandian record informasi pada database yaitu pengamanan semua data-data yang telah diolah dengan tujuan untuk menghasilkan informasi-informasi yang dibutuhkan oleh para pengguna. Hal ini selaras dengan tujuan database itu sendiri yaitu suatu pengorganisasian sekumpulan data yang saling terkait sehingga memudahkan aktivitas untuk memperoleh informasi. Penyandian tersebut bertujuan sebagai keamanan database sehingga adanya proteksi terhadap perusakan data dan pemakaian data oleh pemakai yang tidak punya kewenangan. Hal yang dihasilkan dari penyandian record database adalah :

1. *Interuption*
   Merupakan sumber daya basis data dirusak atau menjadi tidak dapat dipakai (ancaman terhadap *availability*).
2. *Interception*
   Merupakan pemakai atau bagian yang tidak berhak mengakses sumber daya basis data (ancaman *secrety*).
3. *Modification*
   Merupakan pemakai atau bagian yang tidak berhak tidak hanya mengakses tapi juga merusak sumber daya sistem komputer (ancaman *integrity*).
4. *Fabrication*
   Merupakan pemakai atau bagian yang tidak berhak menyisipkan objek palsu ke dalam sistem (ancaman *integrity*).

Ada banyak aplikasi yang dapat digunakan untuk menciptakan sebuah database. Salah satu aplikasi yang sering digunakan adalah *structured query language* (SQL). SQL adalah database yang telah dibuat dapat diintegrasikan dengan aplikasi-aplikasi yang baru dibuat dengan tujuan dapat mendukung pemrosesan informasi yang dibutuhkan. SQL biasanya di atur lebih mudah dengan manajemen database yang dikenal dengan MySQL. MySQL adalah sebuah database *management system* (manajemen basis data) menggunakan perintah dasar SQL

3. HASIL DAN PEMBAHASAN

Dewasa ini masih banyak *record database* yang digunakan pada sistem informasi masih sama persis seperti informasi yang sebenarnya. Hal ini telah memberikan kemudahan bagi orang-orang yang tidak berhak mengakses database sebuah sistem informasi untuk mengerti dan memahami setiap *record* yang ada. Akibat dari kemudahan tersebut juga dapat melahirkan kejadian-kejadian yang tidak dinginkan seperti pencurian informasi, pencurian database ataupun hal-hal lain yang justru merugikan pihak-pihak pemilik database itu sendiri. Tahapan dilakukan secara struktur, model database serta proses penyandian *record* informasi pada *database*, dapat diuraikan seperti berikut.

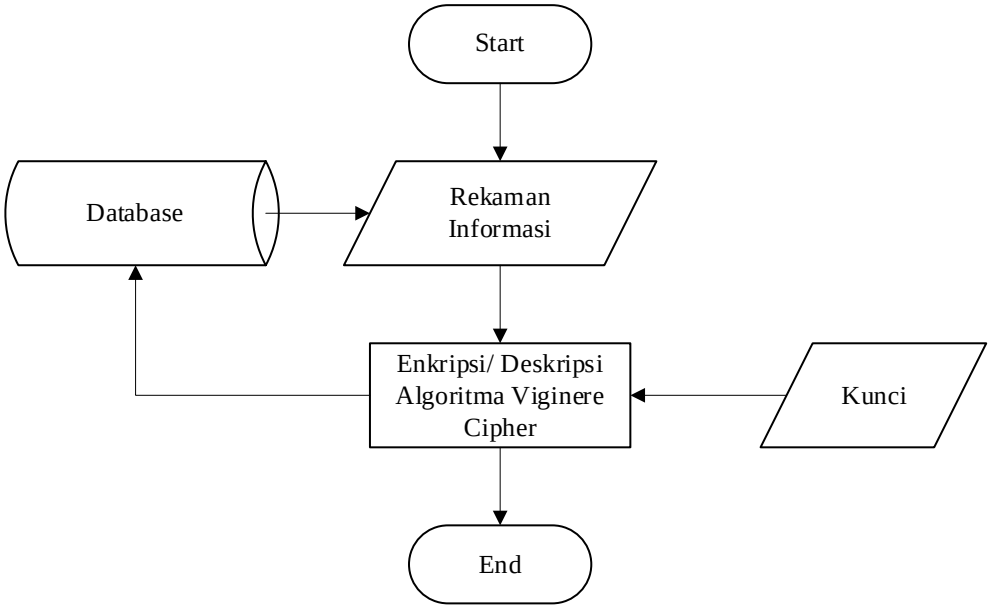


Gambar 2. Alur Penyandian

Rekaman informasi pada database diambil kemudian di kunci dengan algoritma viginere cipher. Kemudian hasil dari penguncian menghasilkan penyandian rekaman informasi.

Jurnal Informasi Komputer Logika
Volume 1, Nomor 4, Oktober 2020
ISSN 2955-7002
Available Online http://ojs.logika.ac.id/index.php/jikl

Salah satu teknik penyandian yang dapat digunakan dalam penyandian record rekaman informasi adalah menerapkan algoritma viginere cipher yang mengadopsi teknik penyandian caesar, di mana dapat melakukan substitusi setiap karakter yang akan disandikan secara berurutan berdasarkan nilai kunci dan faktor-faktor pengali yang terbentuk.



Gambar 3. Alur Penyandian Rekaman Informasi

Sebagai analisis akan dilakukan pengujian data teks dengan nilai "Data Penting" dan akan di kunci dengan teks "kunci". Algoritma viginere cipher menggunakan tabel 26 × 26 dengan A sampai Z sebagai judul baris dan judul kolom.

	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

Sehingga informasi teks "Data Penting" yang tersimpan di database di sandikan menjadi "*Nugc Xohgkvq*".

Tabel 1. Hasil Perhitungan Penyandian

Plain	D	a	t	a		P	e	n	t	i	n	g
Key	K	u	n	c	i	K	u	n	c	i	K	u
Cipher	N	u	g	c		X	o	h	g	k	v	q

Tabel diatas menunjukkan teknik penyandian informasi dengan algoritma viginere cipher.

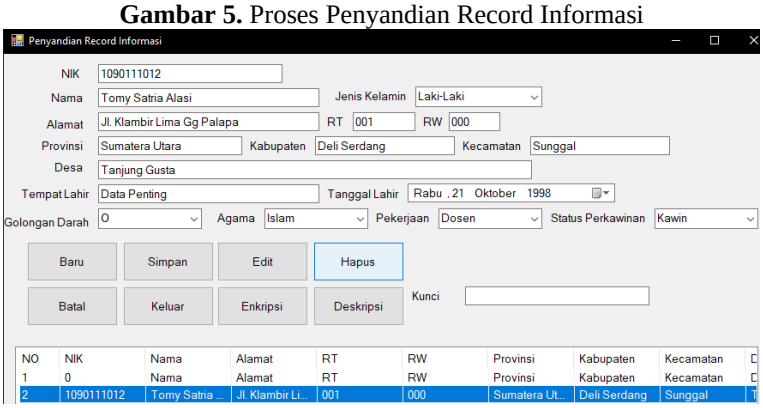
Gambar 4. Record Informasi Pada Database

nik	nama	alamat	rt	rw	provinsi	Kabupaten	kecamatan	desa	tmptlahir	tgllahir	jnskelamin	goldarah
0	Nama	Alamat	RT	RW	Provinsi	Kabupaten	Kecamatan	Desa	Tempat Lahir	2020-10-05	Jenis Kelami	Go
1090111012	Tomy Satria Alasi	Jl. Klambir Lima Gg Palapa	001	000	Sumatera Utara	Deli Serdang	Sunggal	Tanjung Gusta	Kutacane	1998-10-21	Laki-Laki	O

Jurnal Informasi Komputer Logika
Volume 1, Nomor 4, Oktober 2020
ISSN 2955-7002
Available Online http://ojs.logika.ac.id/index.php/jikl

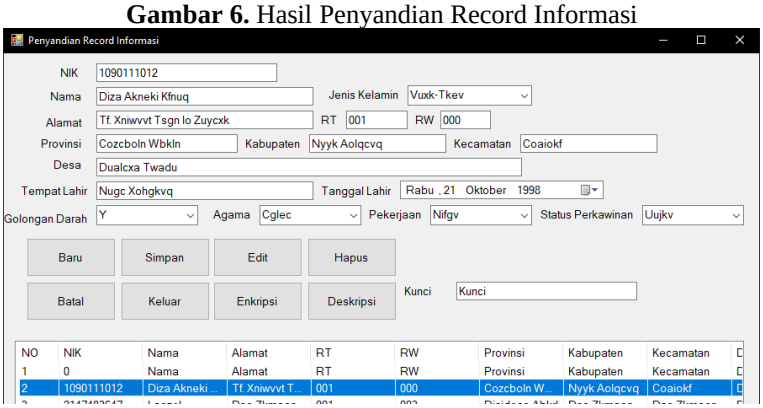
Record informasi pada *database* biasa dilihat dengan aplikasi phpmyadmin. Phpmyadmin sering dimanfaatkan developer untuk pengolahan *database*.

Gambar 5. Proses Penyandian Record Informasi



Penyandian record informasi dibuat sederhana. Dengan menyimpan data baru kemudian melakukan penyandian *record* database.

Gambar 6. Hasil Penyandian Record Informasi



Hasil Penyandian record database langsung dapat dilihat setelah menambahkan kunci dan disimpan langsung dalam *record database*. Penguncian dilakukan dengan algoritma viginere *cipher*.

Gambar 7. Penyandian Tersimpan Ke dalam *Database*

Informasi yang telah disandikan akan disimpan dalam *database* MySQL. Adapun program yang digunakan menghasilkan penyandian record informasi sebagai berikut:

```
Function Vigenere_Cipher(ByVal Text As String, ByVal key As String, ByVal Encrypt As Boolean)
    Dim Result As String = ""
    Dim temp As String = ""
    Dim j As Integer = 0
    For i As Integer = 0 To Text.Length - 1
      If j = key.Length Then
        j = 0
      End If
      If Char.IsLetter(key(j)) Then
        If Text(i) <> " " And Char.IsLetter(Text(i)) Then
          temp += key(j)
          j += 1
        Else
          temp += Text(i)
        End If
      Else
        j += 1
        If j >= key.Length Then
```

```
            j = 0
          End If
          i -= 1
        End If
      Next
      For i As Integer = 0 To Text.Length - 1
        Dim N As Integer
        Dim NewAscii As Integer
        If Char.IsLetter(Text(i)) Then
          If Char.IsLower(temp(i)) Then
            N = Asc(temp(i)) - Asc("a")
          ElseIf Char.IsUpper(temp(i)) Then
            N = Asc(temp(i)) - Asc("A")
          End If
          If Encrypt Then
            NewAscii = N + Asc(Text(i))
          Else
            NewAscii = 26 - N + Asc(Text(i))
          End If
          If (NewAscii > Asc("z") And Char.IsLower(Text(i))) Or (NewAscii > Asc("Z") And
Char.IsUpper(Text(i))) Then
            NewAscii -= 26
          End If
        Else
          NewAscii = Asc(Text(i))
        End If
        Result += Chr(NewAscii)
      Next
      Return Result
    End Function
```

Penyandian record informasi pada database dilakukan dengan cara perulangan dengan fungsi *loop* pada konsep pemrograman.

4. KESIMPULAN

Setelah melakukan analisa terhadap penerapan algoritma vigenere cipher untuk penyandian *record* informasi pada database, maka penulis dapat menarik beberapa kesimpulan sebagai berikut :

1. Algoritma viginere cipher melakukan proses penyandian pada setiap record dari tabel database yang telah dipilih sebanyak sekali kali (secara sederhana) dengan nilai subtitusi setiap karakter record tergantung pada nilai hasil perkalian kunci dengan bilangan faktor pengali yang terbentuk. Hasil akhir yang digunakan adalah hasil proses pengamanan dengan kunci hasilnya tidak memiliki kemiripan dengan record asli. Pembentukan kunci berdasarkan keputusan pengguna. Perlu diperhatikan bahwa kunci tidak boleh lupa.
2. Implementasi pengamanan vigenere cipher untuk penyandian *record* informasi pada database diawali dengan penentuan kunci dan data yang memiliki record yang disandikan.
3. Pengujian dilakukan dalam bahasa pemrograman *visual basic* dapat berjalan sesuai analisa.

UCAPAN TERIMAKASIH

Terima kasih disampaikan kepada pihak-pihak yang telah mendukung terlaksananya penelitian ini.

REFERENCES

[1] T. S. Alasi, “IMPLEMENTASI KRIPTOGRAFI DENGAN ALGORITMA CEASAR CIPHER UNTUK KEAMANAN DATA MICROSOFT OFFICE WORD DAN EXCEL.” Accessed: Oct. 02, 2020. [Online]. Available: http://ojs.logika.ac.id/index.php/jikl/article/download/26/26.

[2] P. Fitriani and T. S. Alasi, “Pengamanan Pesan Dengan Teknik Steganografi Menggunakan Metode Least Significant Bit Pada Citra Digital,” *J. Inf. Komput. Log.*, vol. 1, no. 2, 2019.

[3] R. Munir, “Kriptografi,” in *2*, 2019.

[4] K. Nahar and P. Chakraborty, “A Modified Version of Vigenere Cipher using 95$\times$ 95 Table,” *Int. J. Eng. Adv. Technol.*, vol. 9, no. 5, pp. 1144–1148, 2020.

[5] H. Kurniawan, W. Apriliah, I. Kurnia, and D. Firmansyah, "Penerapan Metode Waterfall Dalam Perancangan Sistem Informasi Penggajian Pada SMK Bina Karya Karawang," *J. Interkom J. Publ. Ilm. Bid. Teknol. Inf. dan Komun.*, vol. 14, no. 4, pp. 13–23, 2020.

[6] M. Asrori and A. Z. Falani, "IMPLEMENTASI PENENTUAN PEMBERIAN TUNJANGAN PENDIDIK & TENAGA KEPENDIDIKAN BERBASIS FUZZY DATABASE MODEL TAHANI," *Insa. Comtech Inf. Sci. Comput. Technol. J.*, vol. 4, no. 2, 2019.

[7] P. Fitriani and T. S. Alasi, *Sistem Pendukung Keputusan dengan Metode WASPAS, COPRAS dan EDAS: Menentukan Judul Skripsi Mahasiswa*. Yayasan Kita Menulis, 2020.

[8] T. S. Alasi, "Penerapan Algoritma Algoritma Boyer Moore untuk Penyaringan Pesan dan Algoritma Hill Cipher dalam Keamanan Pesan Teks Berbasis Web Chat," *KAKIFIKOM Kumpul. Artik. Karya Ilm. Fak. Ilmu Komput.*, vol. 1, no. 2, pp. 73–79, 2019.