Journal of Computer Science and Information Systems (JCoInS)
Program Studi Sistem Informasi, Fakultas Sains & Teknologi, Universitas Labuhanbatu
Volume: 2, Nomor: 3, Agustus 2021, Pages. 124-132
e-ISSN: 2747-2221

Perancangan Aplikasi Enkripsi Menggunakan Algoritma *Vigenere Cipher* Berbasis Web

Rohani

Manajemen Informatika, Fakultas Sains & Teknologi, Universitas Labuhanbatu

Email: hanihime206@gmail.com

Corresponding Author : hanihime206@gmail.com

Abstract

Security and privacy is needed when exchanging important information in the era of information and communication technology today. One way that can be used to make an important information can not be understood by unauthorized people is encrypt information so that the information is difficult and can not even be understood by others. Encryption cryptography is used to convert key information into ciphers to encrypt the required sentence want encrypted and memelurkan key. One way to encrypt important information by using the method vigenere cipher algorithm, encryption is a way to produce by processing the original text letters into numbers using mathematical operations. The key used vigenere cipher algorithm that is shaped, in the form of a row of letter keys that will allow each original text to be encrypted. Results of encryption using methods vigenere cipher that can encrypt important information by means of encrypting the data into a code that can not be read by unauthorized people and this application can also restore data that has been encrypted into data that can be read by means of decrypting data has been encrypted.

Keywords: Encryption Algorithm Vigenere Cipher, PHP.

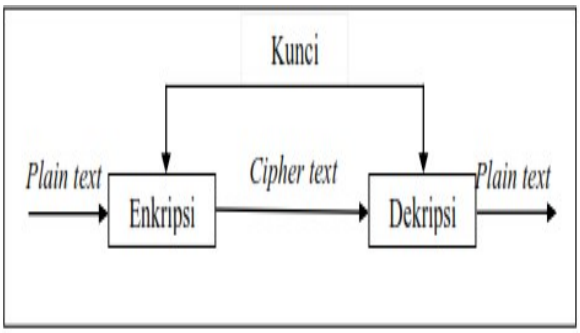
1. Pendahuluan

Keamanan dan privasi sangat dibutuhkan saat melakukan pertukaran informasi penting pada era teknologi informasi dan komunikasi saat ini. Pada seiring perkembangan teknologi yang semakin pesat maka semakin besar pula penyadapan informasi penting yang bersifat privasi dengan melalui berbagai macam perantara media sosial. Salah satu teknik pengamanan informasi yang bisa dipelajari dan dikembangkan adalah kriptografi dengan metode vigenere cipher.

Kriptografi adalah ilmu yang mempelajari keamanan untuk merahasiakan informasi penting dan meng-enkripsikannya. Enkripsi digunakan untuk menyandikan informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak. Dengan enkripsi informasi disandikan (*encrypted*) dengan menggunakan sebuah kunci (*key*). Untuk membuka (*decrypt*) informasi tersebut digunakan juga sebuah kunci yang sama dengan kunci untuk mengenkripsi.

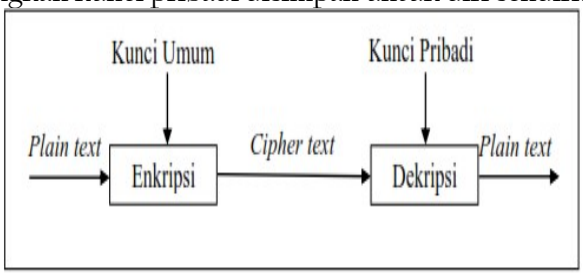
Algoritma dalam kriptografi dibagi menjadi dua, yaitu :

Algoritma simentris atau sering disebut algoritma kriptografi konvensional adalah algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan proses dekripsi. Algoritma kriptografi simentris dibagi menjadi dua kategori yaitu algoritma aliran (*stream cipher*) dan algoritma blok (*block cipher*).



Gambar 1. Proses Enkripsi dan Dekripsi Algoritma Simetris.

Algoritma asimentris adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsi. Dimana kunci enkripsi dapat disebarkan kepada umum dan dinamakan kunci publik (*public key)*, sedangkan kunci dekripsi disimpan untuk digunakan sendiri dan dinamakan kunci pribadi (*private key)*. Oleh karena itu, kriptografi ini dikenal dengan nama kriptografi kunci publik (*public key cryptography)*. Kriptografi asimentris, dimana setiap pelaku publik informasi akan memiliki sepasang kunci, yaitu kunci publik dan kunci pribadi dimana kunci publik di distribusikan kepada umum sedangkan kunci pribadi disimpan untuk diri sendiri.



Gambar 2. Proses Enkripsi Dan Dekripsi Algoritma Asimetris

Vigenere cipher adalah salah satu algoritma kriptografi klasik yang diperkenalkan pada abad 16 atau kira-kira pada tahun 1986. Cara kerja dari vigenere cipher ini mirip dengan caesar cipher, yaitu mengenkripsikan plainteks pada pesan dengan cara menggeser huruf pada pesan tersebut sejauh nilai kunci pada deret *alphabet*. Model matematika dari enkripsi pada algoritma vigenere cipher ini adalah seperti berikut:

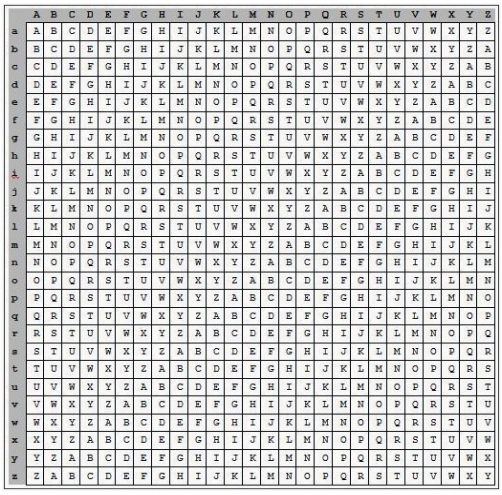
$C_i = E_k (M_i) = (M_i + K_i) \bmod 26$

Dan model matematika untuk dekripsinya adalah :

$M_i = D_k (C_i) = (C_i - K_i) \bmod 26$

Dengan C memodelkan cipherteks, M memodelkan plainteks, dan K memodelkan kunci.

Pergeseran huruf-huruf ini bisa dipetakan dalam bentuk 26x26 yang memetakan antara huruf pada plainteks dengan huruf pada kunci seperti yang di perlihatkan pada gambar dibawah ini :



	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 3. Tabel Pemetaan Vigenere Cipher.

Pengertian aplikasi menurut para ahli adalah sebagai berikut:

1. Menurut Jogiyanto adalah pengguna dalam suatu komputer, intruksi (*instruction)* atau pernyataan *(statement)* yang disusun sedemikian rupa sehingga komputer dapat memproses *input* menjadi *output.*
2. Menurut Rachmad Hakim S, adalah perangkat lunak yang digunakan untuk tujuan tertentu, seperti mengolah dokumen, mengatur Windows, dan permainan *(game)*, dan sebagainya.
3. Menurut Harip Santoso, adalah suatu kelompok *file (from, class, report)* yang bertujuan untuk melakukan aktivitas tertentu yang saling terkait, misalnya aplikasi *payroll*, aplikasi *fixed asset.*

Website adalah lokasi di internet yang menyajikan kumpulan informasi sehubungan dengan profil pemilik situs. Website adalah suatu halaman yang memuat situs-situs *web page* yang berada di internet yang berfungsi sebagai media penyampai informasi, komunikasi, atau transaksi.

3. Metode Penelitian

Metode Pengumpulan Data

Metode pengumpulan data salah satu cara yang dilakukan untuk mengumpulkan data yang diperlukan untuk menyusun tugas akhir, dalam penelitian ini data yang digunakan merupakan data sekunder. Penulis memperoleh data dari telaah pustaka dan artikel-artikel yang penulis dapat dari pustaka yang mendukung, informasi dari internet, dan jurnal-jurnal.

4. Hasil dan Pemabahasan

Metode Perancangan Sistem

Metode perancangan sistem berisi rancangan yang digunakan dalam membangun sistem, diantaranya membangun rancangan *input*, rancangan proses, rancangan *output*, rancangan sistem dan rancangan *interface*.

Rancangan bertujuan untuk memberikan gambaran umum dari sistem yang akan berjalan kepada setiap pengguna. Perancangan adalah sekumpulan aktivitas yang menggambarkan secara rinci begaimana sistem akan berjalan. Hal itu bertujuan untuk menghasilkan produk perangkat lunak yang sesuai dengan kebutuhan pengguna *(user)*.

Tahapan perancangan sistem merupakan tahap lanjutan dalam pengembangan sistem, yang dilakukan setelah selesai tahap analisa sistem. Tujuan dari tahapan ini untuk memberikan gambaran kepada *user* tentang bagaimana sistem baru yang diusulkan akan bekerja dan memberikan ilustrasi dan penjelasan yang lengkap kepada *programmer* dalam mengimplementasikan rancangan sistem ke dalam sebuah program aplikasi atau bahasa pemrograman. *UML (Unified Modelling Language)* adalah tahapan-tahapan pekerjaan yang dilakukan oleh analisis sistem dan *programmer* dalam membangun sebuah sistem. Metode-metode *UML* yang digunakan antara lain *use case diagram*, *activity diagram*, *sequence diagram*, dan *component diagram.*

```
<?php
// berfungsi untuk mengenkripsikan teks yang diberikan
function encrypt($pswd, $text)
{
// merubah kunci menjadi huruf kecil
	$pswd = strtolower($pswd);
// menginisialkan variabel
	$code = "";
	$ki = 0;
	$kl = strlen($pswd);
	$length = strlen($text);
// mengulangi setiap baris dalam teks
	for ($i = 0; $i < $length; $i++)
	{
// jika hurufnya alfa, ENKRIPSI TEKS
	if (ctype_alpha($text[$i]))
	{
// huruf besar
	if (ctype_upper($text[$i]))
	{
	text[$i] = chr(((ord($pswd[$ki]) - ord("a") + ord($text[$i]) - ord("A")) % 26) +
ord("A"));
				}
// huruf kecil
				else
				{
$text[$i] = chr(((ord($pswd[$ki]) - ord("a") + ord($text[$i]) - ord("a")) % 26) +
ord("a"));
				}
// pembaharuan indeks kunci
				$ki++;
				if ($ki >= $kl)
				{
					$ki = 0;
				}
			}
	}
// mengembalikan kode terenkripsi
```

```
        return $text;
}
// berfungsi untuk mendekripsikan teks yang diberikan
function decrypt($pswd, $text)
{
// merubah kunci menjadi huruf kecil
        $pswd = strtolower($pswd);
        // menginisialkan variabel
        $code = "";
        $ki = 0;
        $kl = strlen($pswd);
        $length = strlen($text);
// mengulangi setiap baris dalam teks
        for ($i = 0; $i < $length; $i++)
        {
// jika hurufnya alfa, DEKRIPSI TEKS
                if (ctype_alpha($text[$i]))
                {
// huruf besar
                        if (ctype_upper($text[$i]))
                        {
        $x = (ord($text[$i]) - ord("A")) - (ord($pswd[$ki]) - ord("a"));
        if ($x < 0)
                                {
        $x += 26;
                                }
        $x = $x + ord("A");
        $text[$i] = chr($x);
                        }

// huruf kecil
                        else
                        {
                $x = (ord($text[$i]) - ord("a")) - (ord($pswd[$ki]) - ord("a"));
                if ($x < 0)
                                {
                $x += 26;
                                }

                $x = $x + ord("a");

                $text[$i] = chr($x);
                        }
// memperbaharui indeks kunci
                $ki++;
                if ($ki >= $kl)
                        {
                $ki = 0;
```

```
                    }
                }
        }
// mengembalikan kode dekripsi
        return $text;
}
?>
```

Penjelasan dari *source code:*

Karakter huruf yang diinputkan dengan menggunakan huruf besar atau huruf kecil akan disesuaikan dengan tabel ASCII. Untuk mengenkripsikan dengan proses jika password (key) yang diinputkan akan diubah menjadi huruf alphabet ditambah dengan teks yang diinputkan akan diubah menjadi huruf alphabet dengan proses menyesuasikan modul dari inputan password (key) ditambah teks dengan jumlah 26 huruf alphabet.

Untuk mendekripsikan data enkripsi jika data enkripsi karakter teks yang diinputkan akan dirubah ke huruf alphabet dikurang dengan password (key) yang diinputkan, jika data enkripsi lebih kecil dari 0 maka data enkripsi akan disesuaikan dengan 26 huruf dari alphabet. Data enkripsi akan ditambah dengan huruf karakter yang sudah dirubah dan menghasilkan teks sama dengan karakter huruf yang diinputkan sebelumnya,

Implementasi

Tahapan implementasi sistem merupakan tahap penterjemah perancangan berdasarkan hasil analisis ke dalam suatu bahasa pemrograman tertentu serta penerapan perangkat lunak yang dibangun dengan keadaan sebenarnya. Adapun pembahasan implementasi terdiri dari perangkat lunak pembangun, perangkat keras pembangun, dan implementasi antar muka. Penggunaan vigenere cipher berbasis web adalah untuk mempermudah *user* dalam melakukan enkripsi dan dekripsi menggunakan metode kriptografi vigenere cipher.

Pengujian

Pengujian dilakukan dengan menguji proses *use case* diagram dan kemungkinan kesalahan yang terjadi untuk setiap proses. Pengujian ini dilakukan secara *black box*, yaitu dilakukan dengan memperhatikan masukan sistem dan keluaran dari sistem. Sesuai dengan material pengujian maka akan dilaksanakan pengujian sebagai berikut :

Rancangan Pengujian Enkripsi

Proses ini berfungsi untuk mengenkripsikan plainteks dan *key*, langkah-langkah yang dilakukan *user* dalam proses ini adalah sebagai berikut :

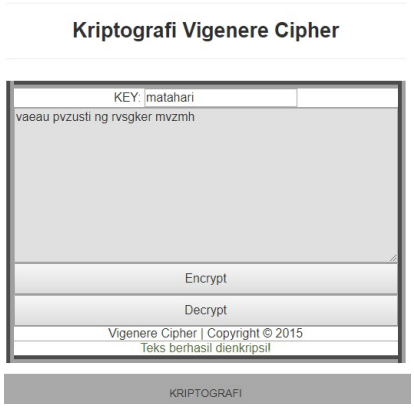
1. *Input key*
   User diminta untuk menginputkan *key* yang berisikan alfabet sebelum mengenkripsikannya.
2. *Input* plainteks
   User diminta untuk menginputkan plainteks yang berisikan alfabet sebelum mengenkripsikannya.
3. Tombol *button encrypt* dan Tombol *button decrypt*

Pada tombol *button encrypt* dapat mengenkripsikan *key* dan plainteks yang telah di masukkan oleh *user*, pada tombol *button decrypt* dapat mendekripsikan kembali plainteks dan *key* atau mendekripsikan data enkripsi dan *key* yang sama pada saat *user* mengenkripsikan.

Gambar 4. Rancangan Pengujian Enkripsi

Pada gambar 4 rancangan pengujian enkripsi menjelaskan bahwa *user* menginputkan *key* dan menginputkan data plainteks. Pada *form* ini *user* menginputkan *key* dengan kata "matahari" dan menginputkan data plainteks dengan kalimat "jalan perisai gg anggrek merah".

Hasil Rancangan Pengujian Enkripsi



Gambar 5. Hasil Rancangan Pengujian Enkripsi

Pada gambar 5 rancangan hasil pengujian enkripsi adalah tampilan hasil dari data plainteks dan *key* yang berhasil di enkripsikan oleh sistem. Pada *form* ini terlihat hasil dari plainteks dan *key* yang menghasilkan data enkripsi, plainteks yang diinputkan dengan kalimat "jalan perisai gg anggrek merah" dan *key* yang diinputkan dengan kata "matahari" menghasilkan data enkripsi "vaeau pvzusti ng rvsgker mvzmh".

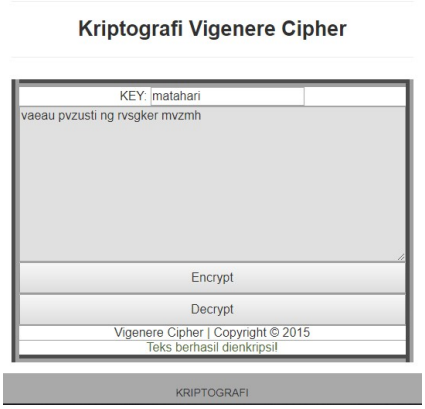
Rancangan Pengujian Dekripsi

Proses ini berfungsi untuk mendekripsikan data enkripsi dan *key* yang telah diterima oleh *user*, langkah-langkah yang dilakukan *user* untuk mendekripsikan data enkripsi adalah sebagai berikut :

1. *Input* data enkripsi

User diminta untuk menginputkan data enkripsi yang telah diterimanya.

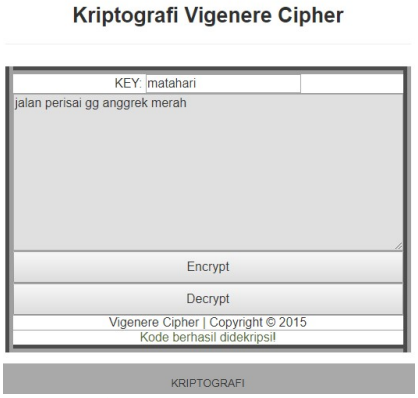
2. *Input key*
   User diminta untuk menginputkan *key* yang sama saat sebelum dienkripsikannya plainteks.



Gambar 6. Rancangan Pengujian Dekripsi

Pada gambar 6 rancangan pengujian dekripsi, pada *form* ini menjelaskan bahwa *user* menginputkan data enkripsi dan *key*, untuk mendekripsikan data enkripsi yang diterima *user* harus menginputkan data enkripsi dan *key* yang sama dikarena ketika *user* menginputkan *key* yang salah maka data dekripsi yang didapatkan tidak akan sesuai ataupun salah sehingga data dekripsi tidak dapat dibaca oleh pendekripsi dan data tidak akan bisa terbaca serta ketika *user* menginputkan data enkripsi yang salah hasil dari dekripsi tidak akan bisa dibaca dan dimengerti.

Hasil Rancangan Pengujian Dekripsi



Gambar 7. Hasil Rancangan Pengujian Dekripsi

Pada gambar 7 hasil rancangan pengujian dekripsi adalah tampilan dari hasil pengujian dekripsi yang berhasil di dekripsikan oleh sistem, pada *form* ini menjelaskan bahwa hasil yang diinputkan dengan plainteks "vaeau pvzusti ng rvsgker mvzmh" dan menginputkan *key* yang sama yaitu "matahari" menghasilkan kalimat yang dapat dibaca dan dimengerti oleh *user*. Pada *form* ini menjelaskan bahwa data enkripsi yang didekripsikan kembali ke kalimat yang tidak dapat dibaca dan dimengerti sebelumnya dapat menghasilkan data dekripsi yang dapat dibaca dan dimengerti oleh *user*.

5. Kesimpulan

Dari hasil perancangan dan implementasi aplikasi kriptografi dengan metode algoritma vigenere cipher, maka didapatkan kesimpulan sebagai berikut :

1. Aplikasi kriptografi ini dapat disimpulkan bahwa dengan menggunakan aplikasi algoritma vigenere cipher dapat menyandikan data penting dengan cara mengenkripsikan data tersebut menjadi sandi-sandi yang tidak dapat dibaca oleh orang yang tidak berhak.
2. Aplikasi kriptografi ini juga dapat mengembalikan data yang telah dienkripsikan menjadi data yang dapat dibaca dengan cara mendekripsikan data enkripsi tersebut.

6. Daftar Pustaka

A. R. R. Hasan Abdurahman, "Perancangan Aplikasi E-Canteen Berbasis Android Dengan Menggunakan Metode Object Oriented Analysis & Design (OOAD)," J. Penelit. Komun. dan Opini Publik, vol. 20, no. 1, pp. 83–92, 2014.

Efrandi, Asnawati, and Yupiyanti, "Aplikasi Kriptografi Pesan Menggunakan Algoritma Vigenere Chiper," J. Media Infotama, vol. 10, no. 2, pp. 120–128, 2014.

Muhammad Dedi Irawan, "IMPLEMENTASI KRIPTOGRAFI VIGENERE CIPHER DENGAN PHP," J. Teknol. Inf., vol. 1, no. 1, pp. 12–23, 2017.

Rulia Puji Hastanti; Bambang Eka Purnama; Indah Uly Wardati, "Sistem Penjualan Berbasis Web (E-Commerce) Pada Tata Distro Kabupaten Pacitan," J. Bianglala Inform., vol. 3, no. 2, pp. 1–10, 2015.