Digital Transformation Technology (Digitech) | e-ISSN : 2807-9000
Volume 3, **Number** 1, Maret 2023
https://doi.org/10.47709/digitech.v3i1.2311

Penerapan Kemanan *Data Text* menggunakan Metode Kriptografi *Vigener Chiper* Berbasis Web

Salsabila Azura[1*], Muhlis Tahir[2], Anggun Dwi Lestari[3], Alvi Sakia Mardiana[4], Auliya Turrofifah[5], Khairunnisa Nur Susanti[6], Moch Shobibur Rohman[7]
[1,2,3,4,5,6,7]Pendidikan Informatika, Fakultas Ilmu Pendidikan, Universitas Trunojoyo Madura, Indonesia
[1]salsabilaazura54154@gmail.com, [2]muhlis.tahir@trunojoyo.ac.id, [3]anggundwilestari221@gmail.com, [4]sakiaalvi@gmail.com, [5]auliyatrrffh@gmail.com , [6]nichauti@gmail.com, [7]mochshobiburrohman@gmail.com

Histori Artikel:
Diajukan: 14 Maret 2023
Disetujui: 18 Maret 2023
Dipublikasi: 19 Maret 2023

Kata Kunci:
Teknologi, kriptografi, vigenere chipper, web dan PHP

Abstrak

Pesatnya perkembangan zaman, semakin pesat pula kemajuan teknologi, dimana sangat mempermudah seseorang dalam berkomunikasi. Salah satu hal yang sangat sering dilakukan yaitu berkomunikasi menggunakan komputer, sedangkan suatu jaringan komputer dibutuhkan untuk mengamankan suatu informasi atau pesan. Diiringi dengan adanya peningkatnya pada sebuah ancaman terhadap teknologi termasuk juga keamanan dan kerahasiaan pesan atau informasi. Saat melakukan pertukaran data, kerahasiaan dan keamanan adalah sesuatu hal yang sangat penting dalam komunikasi data, baik untuk tujuan privasi ataupun individu, maupun untuk keamanan bersama. Salah satu cara agar keamanan dan kerahasiaan pesan atau informasi dapat terjaga yaitu dengan menggunakan teknik kriptografi. Kriptografi merupakan salah satu metode pengamanan data yang dapat dipergunakan untuk menjaga sebuah kerahasiaan data, keaslian data dan juga keaslian pengirim, data yang telah terkirim akan dirubah menjadi sebuah kode tertentu dan hanya dapat dibuka oleh penerima yang mempunyai kunci untuk merubah sebuah kode itu kembali sehingga kerahasian pesan atau informasi tetap dapat terjaga. Dalam pembuatan web kriptografi ini, peneliti menggunakan metode Vigenere Cipher, dimana Vigener Chiper merupakan salah satu metode untuk mengenkripsi teks alfabet dengan menggunakan serangkaian caesar cipher yang berbeda berdasarkan huruf dari kata kunci dan merupakan salah satu bentuk subtitusi polyalphabetic yang sangat sederhana. Pembuatan web ini menggunakan bahasa pemrograman PHP dan diharapkan dengan adanya aplikasi ini dapat mengatasi dari permasalahan tersebut.

PENDAHULUAN

Perkembangan teknologi dalam sistem keamanan untuk menjamin kerahasiaan informasi data yang sudah berkembang dengan pesat saat ini. Teknik seperti steganografi dan kriptografi dikembangkan untuk menjaga kerahasiaan informasi. Penerapan yang dilakukan tidak hanya pada satu teknik pengamanan data, melainkan bisa juga dengan melakukan kombinasi atau modifikasi algoritma (Ginting, 2020). Sebagai jaringan publik, Internet sangat rentan terhadap pencurian data. Kemudian salah satu cara yang dapat digunakan untuk melindungi data adalah dengan seni kriptografi.

Salah satu metode keamamanan informasi yaitu dengan menggunakan sistem kriptografi dengan menyediakan isi informasi (plaintext) tersebut menjadi isi yang tidak dapat dipahami ketika melalui proses enkripsi, dan melakukan proses dekripsi, yang meliputi penggunaan kunci yang benar, untuk mendapatkan kembali informasi aslinya. Dalam bidang kriptografi, Sandi Vigenère Chiper merupakan metode menyandikan sebuah teks alfabet dengan menggunakan deretan sandi Caesar berdasarkan huruf-huruf pada kata kunci. Sandi Vigenère adalah bentuk sederhana dari sebuah sandi substitusi polialfabetik. Kelebihan sandi ini dibanding sandi Caesar dan sandi monoalfabetik lainnya yaitu sandi ini tidak begitu rentan terhadap metode pemecahan sandi (Arfandy et al., 2022)

Berdasarkan penelitian yang dilakukan oleh Gunadhi & Sudrajat dengan judul "Pengamanan Data Rekam Medis pasien menggunakan Kriptografi *Vigenere Chiper*" tahun 2021. Pada penelitian tersebut penulis menggambarkan alur kerja serta tahapan-tahapan proses penelitian menggunakan *work breakdown structure*, dimana dapat disimpulakn bahwa penggunakaan Kriptografi *Vigenere Chiper* dapat mengakomodasikan kebutuhan penggunaan sistem untuk meningkatkan keamanan data pasien yang ada dalam aplikasi rekam medis

sehingga data lebih aman dari serangan *kriptanalis*.

Selain itu terdapat penelitian yang dilakukan oleh Riski, Kamsyakawuni, & Zianul pada tahun 2018 dengan judul "Implementasi Vigenere Cipher Pada Pengamanan Data Medis". Dimana dalam penelitian tersebut peneliti merancang penggunaan suatu metode yang akan digunakan untuk mengamankan data medis yang berupa citra, peneliti menggunakan algortima kriptografi vigenere cipher. Setelah peneliti merancang dan megimplementasikan, hasil yang diperoleh yaitu 100% NPCR, nilai rata-rata UACI citra RGB sebesar 20% dan citra biner sebesar 43%. Selanjutnya penelitian yang dilkukan oleh Aditya Permana pada tahun 2018 dengan judul "Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigene Cipher Berbasis Android" peneliti berhasil membuat aplikasi berbasis android, dimana peneliti mengenkripsikan pesan teks menjadi sebuah pesan yang rahasia yang selanjutnya pesan tersebut diteruskan kepada aplikasi android seperti SMS dan sebagainya sehingga. Dengan aplikasi tersebut dapat memberikan keamanan Ketika ingin bertukar informasi dengan mengirimkan pesan teks terenkripsi menggunakan aplikasi berbasis android. Oleh karena itu peneliti yang akan dilakukan bertujuan untuk menerapkan sebuah keamanan data text dengan menggunakan metode algoritma Vigenere Chiper. Produk yang dikembangkan diharapkan dapat membantu para pengguna dalam melakukan kemanan data text.

STUDI LITERATUR

A. Kriptogtafi

Kriptografi adalah sebuah seni dan ilmu yang berguna untuk menjaga data atau informasi yang dikirim, dengan cara mengubah data tersebut menjadi kode-kode tertentu. Data tersebut hanya akan dikirimkan ke orang yang mempunyai kunci, dimana kunci tersebut berfungsi untuk mengubah kembali kode-kode tersebut menjadi data atau informasi awal yang dikirimkan (Amrulloh & Ujianto, 2019).Terdapat beberapa istilah dalam ilmu kriptografi, diantaranya adalah sebagai berikut:

1. Pesan, *Plainteks*, dan *Ciphertek*s
   Pesan merupakan sebuah informasi yang bisa dipahami arti atau maknanya. Pesan dapat juga disebut sebagai *plainteks* atau *clear text*.
2. Pengirim dan Penerima
   Komunikasi data biasanya melibatkan pertukaran informasi antara dua pihak, yaitu pengirim dan penerima. Pengirim merupakan pihak yang mengirim informasi kepada pihak lainnya. Sedangkan untuk pihak Penerima pihak yang menjadi sasaran atas pesan atau informasi yang dikirim oleh sumber (pengirim) (Oktavia, 2016).
3. Enkripsi dan dekripsi
   Menurut Budi Raharjo dalam (Primartha, 2011) enkripsi merupakan sebuah proses yang dilakukan dengan tujuan untuk mengamankan plainteks, dimana plainteks tersebut diubah menjadi disebut ciphertext. Sedangkan dekripsi merupakan sebuah proses kebalikan dari enkripsi yaitu mengubah chipertext menjadi plainteks kembali.
4. Cipher dan kunci
   Chiper merupakan algoritma atau aturan untuk melakukan proses enkripsi dan dekripsi. Kriptografi dalam mengatasi masalah keamanan sebuah data dilakukan dengan menggunkan kunci (Pabokory, Astuti, & Kridalaksana, 2016).

B. Vigenere Cipher

Vigenere cipher merupakan sebuah metode untuk mengenkripsi teks alfabet dengan menggunakan serangkaian caesar cipher yang berbeda berdasarkan huruf dari kata kunci dan merupakan bentuk subtitusi polyalphabetic yang sederhana (Amrulloh & Ujianto, 2019). Menurut Halim dalam (Efrandi, Asnawati, & Yupiyanti, 2014) Vigenere cipher termasuk pada kriptografi klasik yang telah ada sejak tahun 1986 dan dipublikasikan oleh Blaise de Vigenere. Cara kerja dari Vigenère cipher hampir mirip dengan algoritma Caesar cipher, yaitu dalam proses enkripsi plainteks pada pesan dilakukan dengan cara menggeser huruf pada pesan tersebut sejauh nilai kunci pada deret alphabet. Vigenère cipher merupakan salah satu algoritma kriptografi klasik yang menggunakan metode substitusi abjad majemuk. Substitusi abjad-majemuk mengenkripsi setiap huruf yang ada menggunakan kunci yang berbeda, tidak seperti Caesar cipher yang menerapkan metode substitusi abjad-tunggal yang semua huruf disuatu pesan dienkripsi menggunakan kunci yang sama (Irawan, 2017).

Berikut ini adalah tabel Vigenere Cipher

	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 Algoritma Vigenere Chiper

C. Keamanan

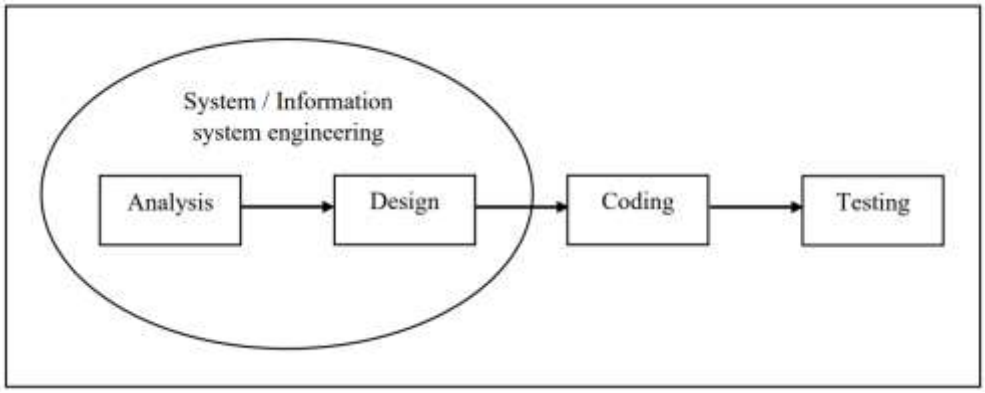
Menurut Santoso & Fakhriza dalam (Arfandy, Simanjuntak, & Pasaribu, 2022) Keamanan merupakan sebuah keadaan bebas dari bahaya. Istilah keamanan dapat digunakan untuk segala bentuk hubungan terhadap segala bentuk kejahtan atau kecelakaan. Keamanan adalah sebuah topik yang luas misalnya disini hal-hal yag termasuk contoh dari keamanan adalah keamanan negara terhadap teroris, keamanan sebuah komputer terhadap hacker, keamanan supermarket terhadap maling dan lain sebagainya. Dalam hal ini host pada sebuah komputer yang terhubung ke internet, memiliki ancaman keamanan data lebih besar daripada host komputer yang tidak tersambung kemanapun. Berikut merupakan beberapa aspek dalam keamanan informasi yaitu Privacy, Confidentiality (kerahasiaan), Integrity (integritas), dan Availability (ketersediaan) (Betty Yel & M Nasution, 2022).

D. PHP

PHP yang kepanjanganya adalah *Personal Home Page*. PHP adalah sebuah bahasa pemrograman yang *open source*, biasanya bahasa ini difungsikan untuk membuat situs web yang dinamis dan powerful. PHP mempunyai beberapa keunggulan, diantaranya adalah mempunyai tingkat akses yang cepat, mempunyai level lifecycle yang cepat sehingga PHP selalu mengikuti *update* trkait perkembangan teknologi internet, PHP dapat berjalan pada beberapa server contohnya Apache, Microsoft IIS, dan lain sebagainya, selain itu PHP mampu berjalan di Linux, dan PHP juga *support* pada beberapa database yang ada, serta PHP juga bersifat gratis sehingga memudahkan semua orang untuk dapat menggunakannya (Amrulloh & Ujianto, 2019). PHP adalah bahasa pemrograman berjenis server-side. PHP akan diproses oleh server dimana hasil dari PHP dikirimkan kembali ke browser. Maka dari itu, salah satu tool yang harus ada sebelum mulai membuat sebuah program dengan menggunakan bahasa PHP adalah server (Abdurrahman, Ahmad, Rusidi, & Saadulloh, 2022). PHP adalah bahasa pemrograman yang bekerja didalam sebuah dokumen HTML (*Hypertext Markup Language*), dimana hal ini berfungsi agar dapat menghasilkan isi atau tampilan dari halaman web yang sesuai permintaan (Mubarak, 2019).

METODE

Menurut Pressman dalam (Supandi et al., 2019) Metode *waterfall* merupakan sebuah metode yang menggambarkan pendekatan sistematis dan berurutan yang biasanya digunakan dalam pengembangan perangkat lunak. Dimana tahapan dari metode ini dimulai dengan spesifikasi kebutuhan pengguna lalu tahap perencanaan, pemodelan, konstruksi, serta penyerahan *system* ke pengguna, dan terkahir ialah *support* terkait perangkat lunak yang dikembangkan. Model *Waterfall* merupakan salah satu model SDLC yang sering digunakan dalam pengembangan sistem informasi atau perangkat lunak. Tahapan dari model berurutan dan sistematis dimulai dari perencanaan sampai dengan pengelolaan (Wahid, 2020). Berikut merupakan penjelasan lebih detail dari tahapan metode *waterfall* (Hakim, 2020):



Gambar 2 Alur *Waterfall*, Sumber: (Hakim, 2020)

1. *Analysis* (Analisis)
   Pada tahap ini dilakukan pendalaman terkait informasi tentang produk atau sistem dengan melakukan analisis kebutuhan dari sebuah produk atau sistem tersebut.
2. *Design* (Desain)
   Tahap ini berisi rancangan desain dari *system* atau perangkat lunak yang akan dibuat.
3. *Coding* (Kode Progran)
   Penulis menuliskan kode program untuk membuat produk atau sistem web.

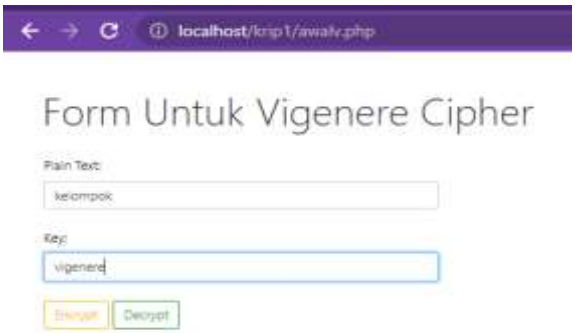
4. *Testing* (Pengujian)
   Sistem yang telah dikembangkan dilakukan uji coba atau pengujian guna memastikan bahwa produk dan sistem telah berhasil dibuat dan menguji keamanan data text.

HASIL

1. *Analysis* (Analisis)
   Pada tahap ini penulis mencari data dan informasi terkait keamanan data text yang menggunakan vigenere chiper dengan melalui beberapa jurnal yang dijadikan acuan pada penelitian ini, Produk yang akan dikembangkan adalah berupa web atau kalkulator berhitung menggunakan metode vigere chiper adapun analisis kebutuhan untuk mengembangkan produk tersebut adalah dengan menggunakan software Visual Studio dan Xampp lalu bahasa yang digunakan adalah bahasa PHP dan HTML.
2. *Design* (Desain)
   Pada tahapan ini penulis membuat sketsa tampilan produk web dengan beberapa tombol untuk melakukan proses sistem enkripsi dan deskripsi, berikut adalah sketsa produk web algoritma vigenere cipher :

Gambar 3 Sketsa Desain Produk Vigenere Cipher

Setelah membuat sketsa desain produk langkah selanjutnya adalah membuat tampilan produk dalam bentuk web dengan menggunakan software visual studio, xampp dan menggunakan bahasa program HTML dan PHP, berikut ini adalah tampilan desain produk :



Gambar 4 Tampilan web vigenere cipher

3. *Coding* (Kode Progran)

Setelah membuat desain maka tahapan selanjutnya adalah membuat kode program dengan menggunakan bahasa PHP dan HTML, berikut ini adalah tampilan kode program proses deskripsi dan enkripsi untuk pembuatan produk web vigenere cipher :

```
function doCrypt(isDecrypt) {
if (document.getElementById("key").value.length == 0) {
alert("Key is empty");
return;
}
var key = filterKey(document.getElementById("key").value);
if (key.length == 0) {
alert("Key has no letters");
return;
}
if (isDecrypt) {
for (var i = 0; i < key.length; i++)
key[i] = (26 - key[i]) % 26;
}
var textElem = document.getElementById("text");
textElem.value = crypt(textElem.value, key);
}
```

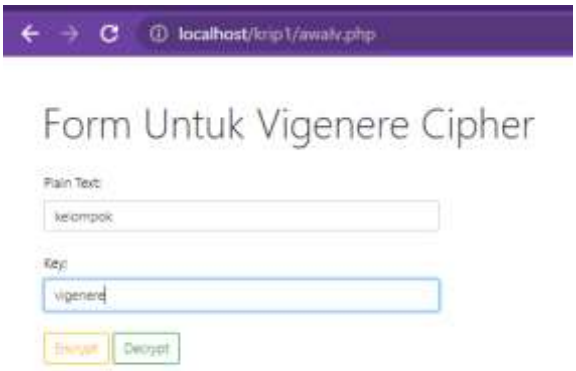
Gambar 5 Kode Program Proses Deskripsi

```
function crypt(input, key) {
var output = "";
for (var i = 0, j = 0; i < input.length; i++) {
var c = input.charCodeAt(i);
if (isUppercase(c)) {
output += String.fromCharCode((c - 65 + key[j % key.length]) % 26 + 65);
j++;
} else if (isLowercase(c)) {
output += String.fromCharCode((c - 97 + key[j % key.length]) % 26 + 97);
j++;
} else {
output += input.charAt(i);
}
}
return output;
}
```

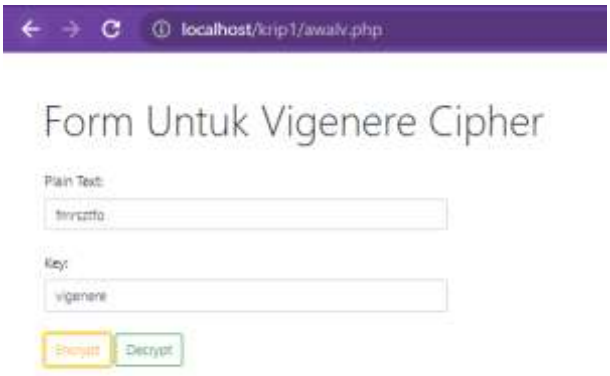
Gambar 6 Kode Program Proses Enkripsi

4. *Testing* (Pengujian)

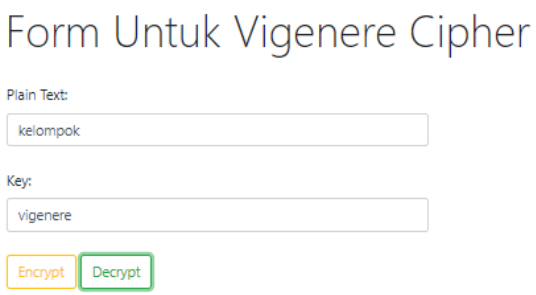
Tahapan selanjutnya adalah pengujian, dari hasil pengembangan aplikasi menggunakan bahasa pemrograman PHP dan metode kriptografi menggunakan sandi vigenere cipher diperoleh hasil berupa form enkripsi dan dekripsi.



Gambar 7 Tampilan Memasukan Plaintext Untuk Enkripsi

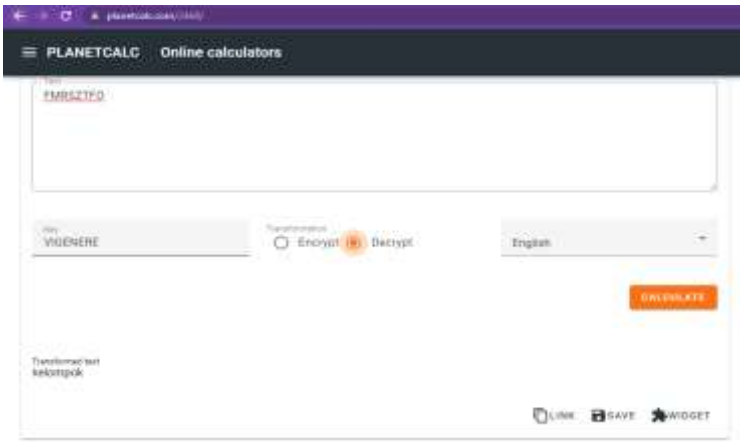


Gambar 8 Tampilan Memasukan Chipertext Untuk Deskripsi



Gambar 9 Tampilan Hasil Deskripsi Chipertext

Dari pengujian pengembangan vigenere tersebut menggunakan plaintext KELOMPOK dan kunci VIGENERE diperoleh cipertext FMRSZTFO. Berdasarkan pengujian produk perhitungan vigenere cipher yang dikembangkan pada gambar 6, 7, 8 dengan menggunakan plaintext dan kunci yang sama keduanya menghasilkan cipertext yang sama. Proses enkripsi pada produk yang dikembangkan adalah menggunakan model matematika dari enkripsi pada algoritma vigenere. Dari uji coba yang sudah dilakukan mendapatkan hasil cipertext FMRSZTFO dari plaintext KELOMPOK dan kunci VIGENERE. Lalu dilakukan uji coba menggunakan aplikasi online yang sudah ada dengan menggunakan ciphertext FMRSZTFO dan kunci VIGENERE sehingga mendapatkan hasil sebagai berikut:



Gambar 10 Tampilan Website Online Perhitungan Vigenere Chiper

PEMBAHASAN

Pada produk pengembangan yang sudah dikembangkan berupa Kemanan Data Text dengan Metode Algoritma Vigenere Chiper menghasilkan perhitungan yang sesuai dengan perhitungan yang sudah dilakukan pada poin hasil perhitungan, perhitungan dilakukan dengan menggunakan rumus yang sudah ditentukan yaitu rumus untuk mencari chipertext adalah $Ci = (Pi + Ki)\ mod\ 26$ dan rumus untuk mencari plaintext adalah $Pi = (Ci - Ki)\ mod\ 26$. Produk yang sudah dikembangkan berupa website hasil dari produk yang sudah dikembangkan diujicoba dan dibandingkan dengan website online lain dan hasil yang sudah dilakukan ujicoba mendapatkan bahwa hasil sama dan dapat dikatakan bahwa website yang buat berhasil melakukan perhitungan dengan metode viogenere chiper. P-erhitungan yang dilakukan adalah dengan menggunakan abjad dan angka, abjad A-Z dan angka 0-25 lalu setelah mengkonversi dilakukan perjumlahan ataupun pengurangan sehingga mendapatkan hasil yang sudah dilakukan.

Pada proses enkripsi pada produk yang dikembangkan dengan menggunakan model matematika dari enkripsi pada algoritma vigenere cipher adalah dengan cara mengkoneversi huruf alfabet dari A-Z menjadi 0-25.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Tabel 1 Konversi Abjad ke Angka

Untuk proses enkripsi menggunakan rumus:

$$\boldsymbol{Ci = (Pi + Ki)\ mod\ 26}$$

Sebagai contoh
Plaintext = KELOMPOK
Kunci = VIGENERE
Perhitungan sebagai berikut :

C1 = K + V Mod 26
= 10 + 21 Mod 26
= 5 = F

C2 = E + I Mod 26
= 4 + 8 Mod 26
= 12 = M

C3 = L + G Mod 26
= 11 + 6 Mod 26
= 17 = R

C4 = O + E Mod 26

= 14 + 4 Mod 26
= 18 = S

C5 = M + N Mod 26
= 12 + 13 Mod 26
= 25 = Z

C6 = P + E Mod 26
= 15 + 4 Mod 26
= 19 = T

C7 = O + R Mod 26
= 14 + 17 Mod 26
= 5 = F

C8 = K + E Mod 26
= 10 + 4 Mod 26
= 14 = O

Pada perhitungan diatas Plaintext dan Kunci dikonversi menjadi angka, kemudian hasil konversi dari plaintext dan kunci dijumlahkan, hasil dari penjumlahan kemudian dikonversi lagi menjadi huruf alfabet menggunakan tabel vigenere cipher sehingga menghasilkan *Cipertext*. Apabila hasil penjumlahan lebih dari 25 hasil penjumlahan harus dikurangi 26. Sedangkan untuk dekripsi menggunakan rumus :

$$\boldsymbol{Pi = (Ci - Ki)\ mod\ 26}$$

Sebagai contoh :
Chipertext = FMRSZTFO
Kunci = VIGENERE
Perhitungan sebagai berikut :

P1 = F - V Mod 26
= 5 - 21 Mod 26
= 10 = K

P2 = M - E Mod 26
= 12 - 8 Mod 26
= 4 = E

P3 = R - G Mod 26
= 17 - 6 Mod 26
= 11 = L

P4 = S - E Mod 26
= 18 - 4 Mod 26
= 14 = O

P5 = Z - N Mod 26
= 25 - 13 Mod 26
= 10 = M

P6 = T - E Mod 26
= 19 - 4 Mod 26
= 15 = P

P7 = F - R Mod 26
= 5 - 17 Mod 26
= 14 = O

P8 = O - E Mod 26
= 14 - 4 Mod 26

= 10 = K

Pada perhitungan *Cipertext* dan Kunci dikonversi menjadi angka, kemudian hasil konversi dari Cipertext dan kunci dijumlahkan, hasil dari penjumlahan kemudian dikonversi lagi menjadi huruf alfabet menggunakan tabel vigenere cipher sehingga menghasilkan *Plaintext*. Apabila hasil penjumlahan lebih kecil dari 0 hasil penjumlahan harus ditambah 26.

KESIMPULAN

Setelah penulis melakukan tahap pengembangan dan implementasi web yang dibuat, maka dapat ditarik kesimpulan bahwa: 1) Web yang dibuat untuk melakukan proses enkripsi dan dekripsi text dapat berjalan dengan baik; 2) Perbandingan hasil dari proses enkripsi maupun dekripsi text dengan menggunakan web yang dikembangkan dan web yang sudah ada menghasilkan hasil yang sama; 3) Web yang dikembangkan menggunakan algoritma vignere chiper dan bahasa pemrograman PHP serta HTML; 4) Pada penggunaan web untuk keamanan text, sebelumnya diperlukan kunci dan plainteks (teks yang akan disembunyikan) dalam proses enkripsi maupun dekripsi.

REFERENSI

Aditya Permana, A. (2018). Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android. *Jurnal AL-AZHAR INDONESIA SERI SAINS DAN TEKNOLOGI*, *4*(3), 110–115.

Abdurrahman, H., Ahmad, Y., Rusidi, & Saadulloh. (2022). JTIM : Jurnal Teknik Informatika Mahakarya. *JTIM: Jurnal Teknik Informatika Mahakarya*, *03*(2), 37–44.

Amrulloh, A., & Ujianto, E. I. H. (2019). Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher. *Jurnal CoreIT*, *5*(2), 71–77.

Arfandy, D., Simanjuntak, M., & Pasaribu, T. (2022). Penerapan Metode Vigenere Cipher Untuk Mengamankan Data Text. *JUKI : Jurnal Komputer Dan Informatika*, *4*(1), 48–54.

Betty Yel, M., & M Nasution, M. K. (2022). Keamanan Informasi Data Pribadi Pada Media Sosial. *Jurnal Informatika Kaputama (JIK)*, *6*(1), 92–101.

Efrandi, Asnawati, & Yupiyanti. (2014). Aplikasi Kriptografi Pesan Menggunakan Algoritma. *Jurnal Media Infotama*, *10*(2), 120–128.

Ginting, V. S. (2020). Penerapan Algoritma Vigenere Cipher dan Hill Cipher Menggunakan Satuan Massa. *Jurnal Teknologi Informasi*, *4*(2), 241–246. https://doi.org/10.36294/jurti.v4i2.1365

Gunadhi, E., & Sudrajat, A. (2017). Pengamanan Data Rekam Medis Pasien Menggunakan Kriptografi Vigènere Cipher. *Jurnal Algoritma*, *13*(2), 295–301. https://doi.org/10.33364/algoritma/v.13-2.295

Hakim, R. R. Al, Rusdi, E., & Setiawan, M. A. (2020). Android Based Expert System Application for Diagnose COVID-19 Disease: Cases Study of Banyumas Regency. *Journal of Intelligent Computing and Health Informatics*, *1*(2), 26. https://doi.org/10.26714/jichi.v1i2.5958

Irawan, M. D. (2017). Implementasi Kriptografi Vigenere Cipher Dengan Php. *Jurnal Teknologi Informasi*, *1*(1), 11. https://doi.org/10.36294/jurti.v1i1.21

Mubarak, A. (2019). Rancang Bangun Aplikasi Web Sekolah Menggunakan Uml (Unified Modeling Language) Dan Bahasa Pemrograman Php (Php Hypertext Preprocessor) Berorientasi Objek. *JIKO (Jurnal Informatika Dan Komputer)*, *2*(1), 19–25. https://doi.org/10.33387/jiko.v2i1.1052

Oktavia, F. (2016). Upaya Komunikasi Interpersonal Kepala Desa Borneo Sejahtera Dengan Masyarakat Desa Long Lunuk. *Ilmu Komunikasi*, *4*(1), 239–253.

Pabokory, F. N., Astuti, I. F., & Kridalaksana, A. H. (2016). Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. *Informatika Mulawarman : Jurnal Ilmiah Ilmu Komputer*, *10*(1), 20. https://doi.org/10.30872/jim.v10i1.23

Primartha, R. (2011). Penerapan Enkripsi dan Dekripsi File Menggunakan Data Encryption Standard (DES). *ISNN : 2355-4614 / Universitas Sriwijaya*, *3*(2), 371–387.

Riski, A., Kamsyakawuni, A., & Zianul, A. M. (2018). Implementasi Vigenere Cipher Pada Pengamanan Data Medis. *Jurnal Riset Dan Aplikasi Matematika (JRAM)*, *2*(1), 23. https://doi.org/10.26740/jram.v2n1.p23-30

Supandi, F., Desta P, W., Ambar S, Y., & Sudir, M. (2019). Analisis Resiko Pada Pengembangan Perangkat Lunak Yang Menggunakan Metode Waterfall Dan Prototyping. *Prosiding Seminar Nasional Dinamika Informatika 2018 (SENADI 2018)*, *2*(1), 83–86. http://prosiding.senadi.upy.ac.id/index.php/senadi/article/view/86

Wahid, A. A. (2020). Analisis Metode Waterfall Untuk Pengembangan Sistem Informasi. *Jurnal Ilmu-Ilmu Informatika Dan Manajemen STMIK*, *November*, 1–5.