Jurnal CoreIT, Vol.5, No.2, Desember 2019
ISSN 2460-738X (Print)
ISSN 2599-3321 (Online)

Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher

Arif Amrulloh[1], EIH.Ujianto[2]
[1]Program Magister Teknologi Informasi, Universitas Teknologi Yogyakarta
[2]Universitas Teknologi Yogyakarta (UTY)
[1,2]Jl.Siliwangi (Ringroad Utara),Jombor, Sleman,D.I. Yogyakarta 55285
arif.amrulloh@student.uty.ac.id[1], erik.iman@uty.ac.id[2]

***Abstrak* – Keamanan informasi pada sebuah aplikasi sangatlah penting, sistem keamanan sangat diperlukan pada sebuah aplikasi karena di sebagian perusahaan atau bahkan di suatu negara membutuhkan keamanan informasi , dan informasi penting yang tidak boleh di akses oleh sembarangan penerima pesan harus di amankan. Untuk megamankan informasi tersebut dibutuhkan suatu algoritma yang dapat menyamarkan pesan penting agar tidak bisa dibaca oleh pihak yang tidak memiliki hak untuk menerima informasi tersebut. Kriptografi merupakan salah satu cara yang bisa digunakan untuk memproteksi pengiriman data, data yang dikirim akan dirubah menjadi kode tertentu dan hanya bisa dibuka oleh penerima yang memiliki kunci untuk merubah kode itu kembali sehingga kerahasian pesan atau informasi tetap dapat dijaga, dan untuk mempermudah pemrosesan data diperlukan sebuah aplikasi, aplikasi kriptografi berbasis web bisa dibangun dan digunakan untuk mempermudah pemrosesan data, selain itu aplikasi berbasis web dapat di akses dari mana saja.**

Kata Kunci – Kriptografi, Vigenere Cipher, PHP.

PENDAHULUAN

Dewasa ini dengan makin pesatnya perkembangan teknologi, banyak organisasi dan perusahaan berusaha mengadopsi teknologi informasi terbaru untuk membantu kelancaran bisnis, Pentingnya keamanan informasi kadang terabaikan dan baru disadari setelah terjadi bencana [1]. Di Kazakhstan Keamanan informasi dipertimbangkan dalam tiga aspek yaitu teknis, sosial dan politik. Menurut konsep tersebut, aspek teknis meliputi perlindungan sistem informasi nasional, informasi dan infrastruktur telekomunikasi dari akses yang tidak sah, penggunaan, pengungkapan, pelanggaran, perubahan, membaca, memeriksa, merekam, atau memusnahkan untuk memastikan integritas, kerahasiaan dan ketersediaan informasi [2]. Ada beberapa cara untuk melakukan pengamanan data ataupun pesan, diantaranya dengan menggunakan teknik penyamaran data yang disebut dengan kriptografi dan teknik penyembunyian data yang disebut dengan steganografi [3] .

Kriptografi adalah proses linguistik, matematika, dan representasional yang berbeda dari komputasi, dilihat dari fakta sejarah menyatakan bahwa sebagian besar kriptografi dilakukan dengan kertas , tinta, dan kemudian, telegraf [4]. Kriptografi adalah salah satu cara untuk mencegah kebocoran data yang bersifat rahasia, Secara umum ada dua jenis kriptografi, yaitu kriptografi klasik dan kriptografi modern, Kriptografi klasik (simetrik) adalah suatu algoritma yang menggunakan satu kunci untuk mengamankan data. Dua teknik dasar yang biasa dilakukan adalah substitusi dan transposisi. Sedangkan kriptografi modern (asimetrik) adalah algoritma yang lebih kompleks dari pada algoritma klasik, hal ini disebabkan algoritma ini menggunakan komputer [5].

Dalam pembuatan aplikasi ini akan menggunakan kriptografi klasik. Secara umum kriptografi klasik dikelompokkan dalam dua model yaitu menggunakan teknik substitusi dan transposisi. Teknik substitusi dilakukan dengan mengganti salah satu karakter yang ada dalam sebuah teks menggunakan karakter yang lain. Teknik yang termasuk dalam kategori substitusi adalah kriptografi Caesar [6]. Kemudian ada sandi vigenere yang merupakan pengembangan dari sandi caesar. Pada sandi caesar, setiap huruf teks terang digantikan dengan huruf lain yang memiliki perbedaan tertentu pada urutan alfabet. Misalnya pada sandi caesar dengan geseran 3, A menjadi D, B menjadi E and dan seterusnya. Sandi vigenere terdiri dari beberapa sandi caesar dengan nilai geseran yang berbeda. Untuk menyandikan suatu pesan, digunakan sebuah tabel alfabet yang disebut tabel vigenere, tabel vigenere berisi alfabet yang dituliskan dalam 26 baris, masing-masing baris digeser satu urutan ke kiri dari baris sebelumnya membentuk ke-26 kemungkinan sandi caesar. Setiap huruf disandikan dengan menggunakan baris yang berbeda-beda sesuai kata kunci yang diulang. Sandi ini dikenal luas karena cara kerjanya mudah di-mengerti dan dijalankan, dan bagi para pemula sulit dipecahkan [7].

METODOLOGI PENELITIAN

A. Metodologi Penelitian

Metode Penelitian yang digunakan dalam penelitian ini adalah metode analisis dan pengembangan sistem.

Adapun langkah-langkahnya adalah sebagai berikut:

1. Pembuatan Aplikasi berbasis web menggunakan PHP dengan algoritma vigenere cipher.

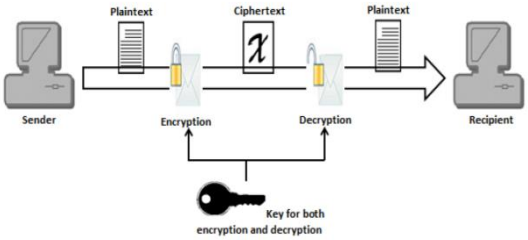
2. Implementasi dan pengujian sistem dengan melakukan pengujian aplikasi yang telah dibuat dan membandingkan dengan aplikasi yang sudah ada.

B. Kriptografi

Kriptografi merupakan seni dan ilmu untuk memproteksi pengiriman data dengan mengubahnya menjadi kode tertentu dan hanya ditujukan untuk orang yang hanya memiliki sebuah kunci untuk mengubah kode itu kembali yang berfungsi dalam menjaga kerahasiaan data atau pesan. Dalam kriptografi, data atau pesan yang dikirimkan melalui jaringan akan disamarkan sedemikian rupa. Sehingga seandainya data tersebut bisa diperoleh dan dibaca oleh orang lain, maka pihak yang tidak berhak atau berwenang tersebut tidak akan bisa mengerti arti dari data tersebut.

Dalam bidang kriptografi terdapat dua konsep yang sangat penting atau utama yaitu enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi atau data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal. Sebuah pesan atau data yang masih asli dan belum mengalami penyandian dikenal dengan istilah plaintext. Kemudian setelah disamarkan dengan suatu cara penyandian, maka plaintext ini disebut sebagai chipertext. Proses penyamaran dari plaintext ke ciphertext disebut enkripsi (encryption), dan proses pengembalian dari ciphertext menjadi plaintext kembali disebut dekripsi (decryption) [3]. Dalam algoritma simetris kunci yang digunakan untuk mengenkripsi dan mendekripsi data adalah sama. Ada banyak algoritma simetris seperti Blowfish, DES, AES dan sebagainya. Setiap algoritma menggunakan metode yang berbeda untuk mengenkripsi dan mendekripsi data, Adapun komponen enkripsi simetris adalah seperti berikut [8]:

1. Plaintext: adalah data asli yang akan dikirm ke penerima tertentu. Data-data ini akan menjadi input ke algoritma enkripsi.
2. Algoritma enkripsi: adalah serangkaian proses yang akan dieksekusi ke dalam plaintext dengan bantuan kunci rahasia untuk menghasilkan ciphertext.
3. Kunci rahasia: adalah nilai yang digunakan untuk menggabungkan plaintext dan mengubahnya menjadi ciphertext.
4. Ciphertext: adalah output dari plaintext asli yang dimasukkan ke algoritma enkripsi.
5. Algoritma dekripsi: adalah sekumpulan proses yang akan dieksekusi menjadi ciphertext dengan bantuan kunci rahasia untuk menghasilkan teks asli atau plaintext.



Gambar 1. Proses enkripsi kriptografi simetris

C. Vigenere Cipher

Vigenere cipher adalah metode mengenkripsi teks alfabet dengan menggunakan serangkaian caesar cipher yang berbeda berdasarkan huruf dari kata kunci dan merupakan bentuk substitusi polyalphabetic yang sederhana. Karakter yang digunakan dalam Vigenere Cipher yaitu A, B, C, ..., Z dan dikonversi kedalam angka 0, 1, 2, ..., 25. Proses enkripsi dilakukan dengan menulis kunci berulang kali sesuai dengan panjang karakter pada pesan [9]. Jika pada Caesar cipher kuncinya hanya satu nilai saja, maka pada Vigenere cipher kunci yang digunakan berbentuk deretan huruf. Kunci yang berbetuk deretan kata tersebut akan memung-kinkan setiap huruf plainteks untuk dienkripsi dengan kunci yang berbeda. Jika panjang kunci yang digunakan lebih pendek dari panjang plainteks maka kunci akan diulang sampai panjang kunci sama dengan panjang plainteks. Algoritma ini akan meminimalkan kemungkinan dipecahkannya ci-pherteks jika satu huruf plainteks diketahui [7].

Proses Enkripsi dan Dekripsi pada Vigenere Cipher bekerja dengan membaca kata per karakter, dimana apabila pesan yang dikirim melebihi panjang kunci yang digunakan, maka kunci akan diulang kembali sampai pesan yang dikirim tersebut mendapatkan kunci masing-masing, Vigenere Cipher juga dapat menggunakan sebuah tabel untuk menengkripsikan sebuah plaintext yang mana tabel tersebut terdiri dari 26 baris dan kolom alphabet, dan tiap barisnya akan digeser satu huruf ke kiri [10]. Model matematika dari enkripsi dan dekripsi pada algoritma vigenere cipher adalah seperti berikut :

$Ci = (Pi + Ki) \bmod 26$

Sedangkan untuk proses dekripsi adalah :

$Pi = (Ci - Ki) \bmod 26$ jika $Ci-Ki > 0$

$Pi = ((Ci - Ki)+26) \bmod 26$ jika $Ci-Ki < 0$

Keterangan :

C = Ciphertext (Pesan Acak)

P = Plaintext (Pesan Asli)

K = Kunci

	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 2. Tabel vigenere cipher

D. PHP

PHP(Personal Home Page) merupakan bahasa scripting yang open source dan digunakan untuk membuat situs web yang dinamis dan powerful. PHP pertama kali dibuat oleh Rasmus Lerdorf pada tahun 1995. Pada waktu itu PHP bernama FI (Form Interpreted). Pada saat tersebut PHP adalah sekumpulan script yang digunakan untuk mengolah data form dari web. Perkembangan selanjutnya adalah Rasmus melepaskan kode sumber tersebut dan menamakannya PHP/FI, pada saat tersebut
kepanjangan dari PHP/FI adalah Personal Home Page/Form Interpreter. Dengan pelepasan kode sumber ini menjadi open source, maka banyak programmer yang tertarik untuk ikut mengembangkan PHP. Pada November 1997, dirilis PHP/FI 2.0. Pada rilis ini interpreter sudah diimplementasikan dalam C [11]. Bahasa PHP banyak digunakan sebagai bahasa server side yang populer. Banyak situs web perusahaan menggunakan PHP karena dapat menghasilkan produktivitas perangkat lunak yang tinggi. Selain itu, PHP secara resmi menawarkan dukungan SOAP dalam versi 5. Dengan demikian, dukungan ini membantu meningkatkan penyebaran luas layanan web berbasis pada SOAP [12].

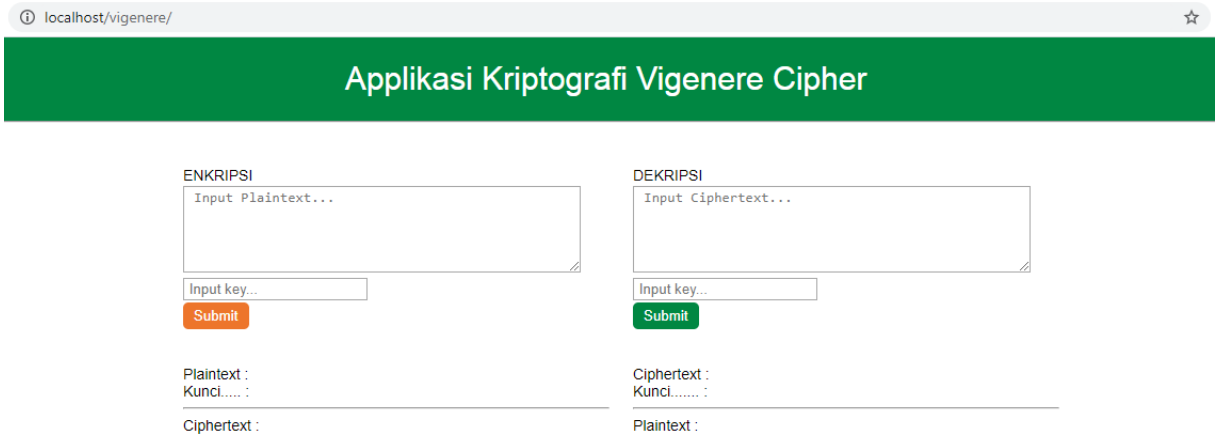
Beberapa keunggulan dari PHP adalah :

1. Memiliki tingkat akses yang lebih cepat.
2. Memiliki tingkat lifecycle yang cepat sehingga selalu mengikuti perkembangan teknologi internet;
3. Memiliki tingkat keamanan yang tinggi.
4. Mampu berjalan di beberapa server yang ada, misalnya Apache, Microsoft IIS, PWS, AOLserver, phttpd, httpd, dan Xitami.
5. Mampu berjalan di Linux sebagai platform sistem operasi utama bagi PHP.
6. Mendukung ke beberapa database yang sudah ada.
7. Bersifat gratis.

HASIL DAN PEMBAHASAN

A. Enkripsi

Dari hasil pengembangan aplikasi menggunakan bagasa pemrograman PHP dan metode kriptografi menggunakan sandi vigenere cipher diperoleh hasil berupa form enkripsi dan dekripsi.

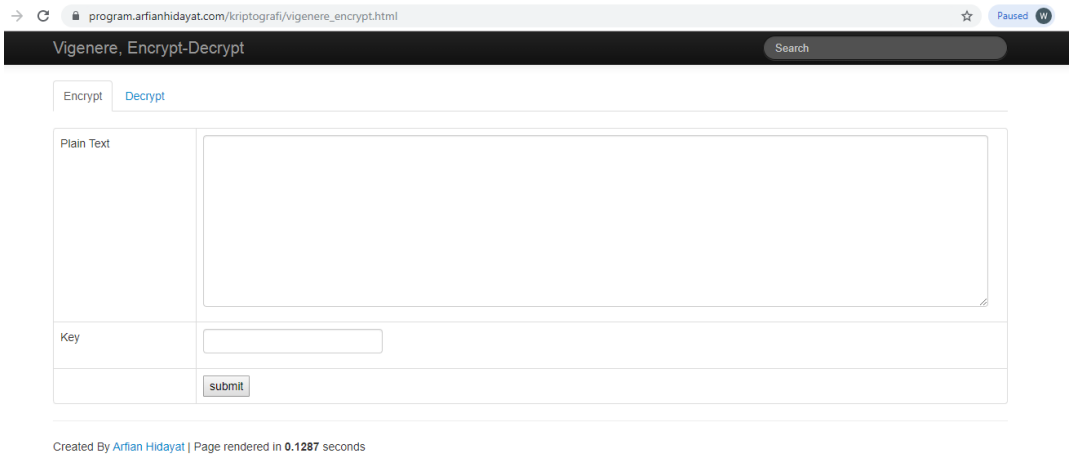


Gambar 3. Tampilan Aplikasi Kriptografi Vigenere Cipher

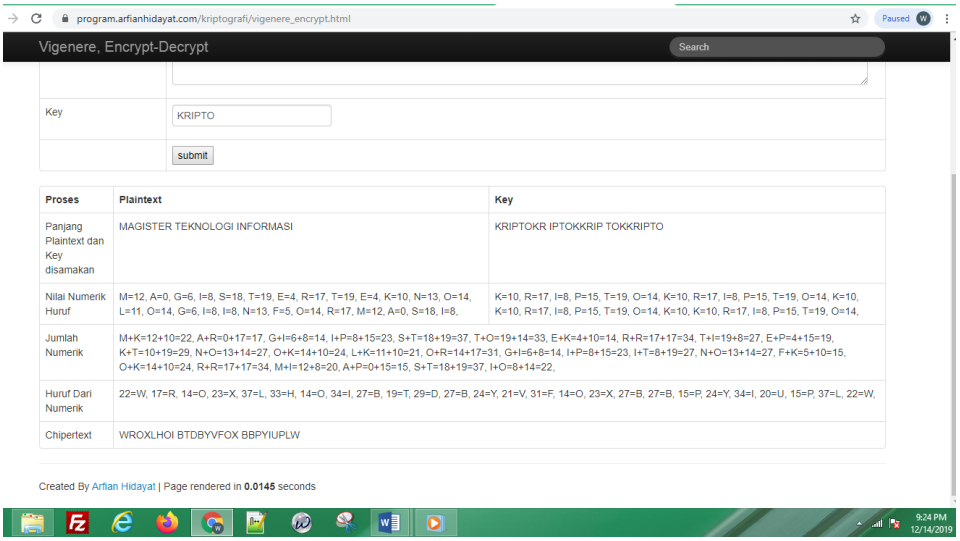
Gambar 4. Hasil enkripsi di aplikasi

Dari pengujian pada Gambar 4 menggunakan plaintext MAGISTER TEKNOLOGI INFORMASI dan kunci KRIPTO menghasilkan cipertext : WROXLHOI BTDBYCWVB WXWWGFOCZ

Kemudian dilakukan uji coba menggunakan aplikasi online yang sudah ada dengan alamat https://program.arfianhidayat.com/kriptografi/vigenere_encrypt.html



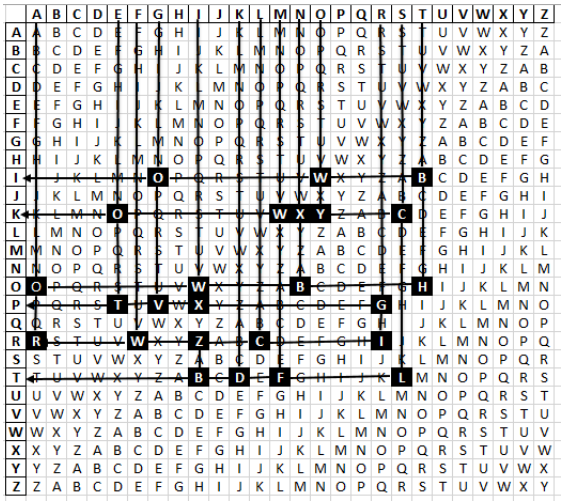
Gambar 5. Tampilan aplikasi online



Gambar 6. Hasil enkripsi aplikasi online

Dari pengujian aplikasi online pada Gambar 6 menggunakan plaintext MAGISTER TEKNOLOGI INFORMASI dan kunci KRIPTO diperoleh cipertext WROXLHOI BTDBYVFOX BBPYIUPLW. Uji coba aplikasi online pada saat artikel ini ditulis dilakukan pada tanggal 12 Desember 2019.

Berdasarkan pengujian aplikasi yang dikembangkan (Gambar 4) dan aplikasi online (Gambar 6) menggunakan plaintext dan kunci yang sama keduanya menhgasilkan cipertext yang berbeda. Kemudian untuk menguji dan mengetahui aplikasi mana yang paling mendekati kesesuaian sesuai dengan metode vigenere cipher maka dilakukan pengecekan manual menggunakan tabel vigenere cipher dengan tools microsoft excel.



Gambar 7. Pemetaan menggunakan excel

Plaintext	M	A	G	I	S	T	E	R		T	E	K	N	O	L	O	G	I		I	N	F	O	R	M	A	S	I
Kunci	K	R	I	P	T	O	K	R		I	P	T	O	K	R	I	P	T		O	K	R	I	P	T	O	K	R
Cipertext	W	R	O	X	L	H	O	I		B	T	D	B	Y	C	W	V	B		W	X	W	W	G	F	O	C	Z

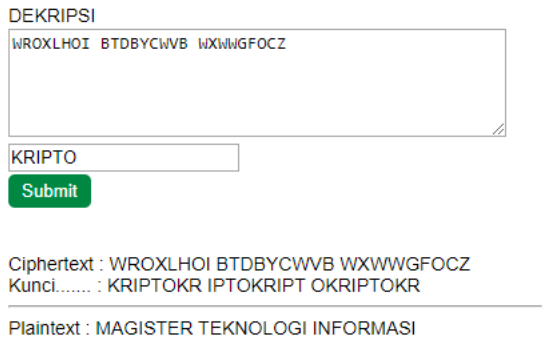
Gambar 8. Hasil pemetaan pada excel

Hasil pengecekan manual menggunakan microsoft excel diperoleh hasil
P : MAGISTER TEKNOLOGI INFORMASI
K : KRIPTOKR IPTOKRIPT OKRIPTOKR
C : WROXLHOI BTDBYCWVB WXWWGFOCZ

Berdasarkan semua uji coba diketahuai bahwa cipertext dari aplikasi yang dikembangkan memiliki kesamaan dengan cipertext manual dari excel, sedangkan hasil dari aplikasi online memiliki perbedaan pada kata kedua dan kata ketiga.

B. Dekripsi

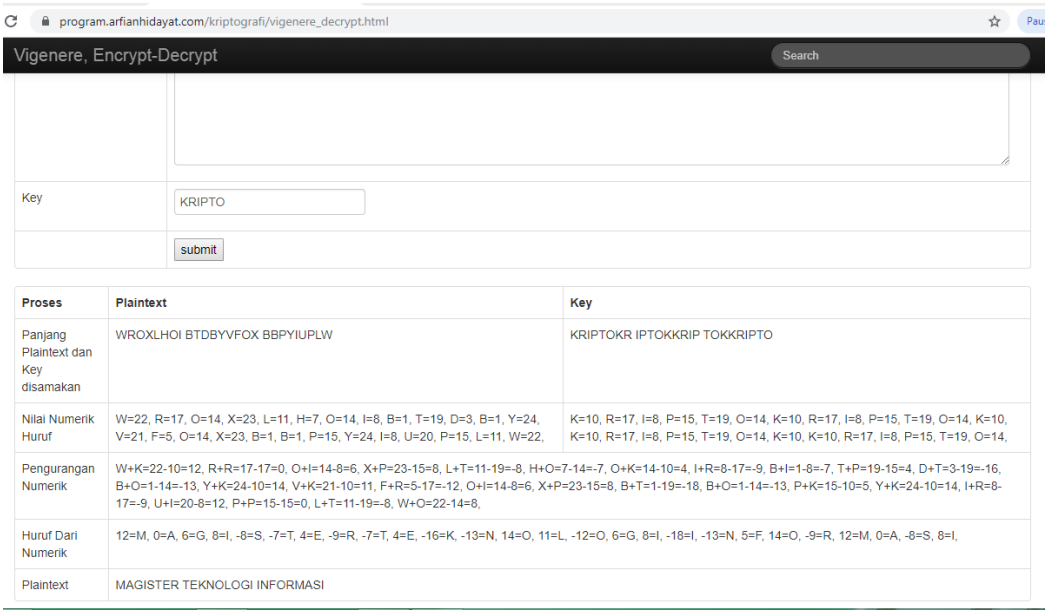
Setelah mendapatkan cipertext dari hasil enkripsi kemudian dilakukan proses dekripsi yaitu mengembalikan cipertext menjadi plaintext dengan menggunakan kunci yang sama. Dekripsi yang di uji coba pertama adalah aplikasi pengembangan dengan cipertext WROXLHOI BTDBYCWVB WXWWGFOCZ dan kunci KRIPTO



Gambar 9. Form dekripsi hasil pengembangan

Dari uji coba dekripsi pada Gambar 9 menggunakan cipertext :
WROXLHOI BTDBYCWVB WXWWGFOCZ
dan kunci KRIPTO menghasilkan plaintext MAGISTER TEKNOLOGI INFORMASI.

Kemudian dilakukan uji coba menggunakan aplikasi online yang sudah ada dengan cipertext WROXLHOI BTDBYVFOX BBPYIUPLW
dan kunci KRIPTO



Proses	Plaintext	Key
Panjang Plaintext dan Key disamakan	WROXLHOI BTDBYVFOX BBPYIUPLW	KRIPTOKR IPTOKKRIP TOKKRIPTO
Nilai Numerik Huruf	W=22, R=17, O=14, X=23, L=11, H=7, O=14, I=8, B=1, T=19, D=3, B=1, Y=24, V=21, F=5, O=14, X=23, B=1, B=1, P=15, Y=24, I=8, U=20, P=15, L=11, W=22,	K=10, R=17, I=8, P=15, T=19, O=14, K=10, R=17, I=8, P=15, T=19, O=14, K=10, K=10, R=17, I=8, P=15, T=19, O=14, K=10, K=10, R=17, I=8, P=15, T=19, O=14,
Pengurangan Numerik	W+K=22-10=12, R+R=17-17=0, O+I=14-8=6, X+P=23-15=8, L+T=11-19=-8, H+O=7-14=-7, O+K=14-10=4, I+R=8-17=-9, B+I=1-8=-7, T+P=19-15=4, D+T=3-19=-16, B+O=1-14=-13, Y+K=24-10=14, V+K=21-10=11, F+R=5-17=-12, O+I=14-8=6, X+P=23-15=8, B+T=1-19=-18, B+O=1-14=-13, P+K=15-10=5, Y+K=24-10=14, I+R=8-17=-9, U+I=20-8=12, P+P=15-15=0, L+T=11-19=-8, W+O=22-14=8,	
Huruf Dari Numerik	12=M, 0=A, 6=G, 8=I, -8=S, -7=T, 4=E, -9=R, -7=T, 4=E, -16=K, -13=N, 14=O, 11=L, -12=O, 6=G, 8=I, -18=I, -13=N, 5=F, 14=O, -9=R, 12=M, 0=A, -8=S, 8=I,	
Plaintext	MAGISTER TEKNOLOGI INFORMASI	

Gambar 10. Hasil dekripsi aplikasi online

Hasil dekripsi pada Gambar 10 dengan cipertext WROXLHOI BTDBYVFOX BBPYIUPLW dan kunci KRIPTO menghasilkan plaintext MAGISTER TEKNOLOGI INFORMASI.

C. Pembahasan

Proses enkripsi pada aplikasi yang dikembangkan adalah menggunakan model matematika dari enkripsi pada algoritma vigenere cipher yaitu 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

Gambar 11. Konversi huruf menjadi angka

Untuk proses enkripsi menggunakan rumus :
Ci = (Pi + Ki) mod 26

Sebagai contoh

Plaintext	M	A	G	I	S	T	E	R		T	E	K	N	O	L	O	G	I
Konversi	12	0	6	8	18	19	4	17		19	4	10	13	14	11	14	6	8
Kunci	K	R	I	P	T	O	K	R		I	P	T	O	K	R	I	P	T
Konversi	10	17	8	15	19	14	10	17		8	15	19	14	10	17	8	15	19
Hasil Konversi	22	17	14	23	37	33	14	34		27	19	29	27	24	28	22	21	27
Cipertext	W	R	O	X	L	H	O	I		B	T	D	B	Y	C	W	V	B

Gambar 12. Proses enkripsi

Pada Gambar 12. 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 :
Pi = (Ci – Ki)mod26 jika Ci-Ki > 0
Pi = ((Ci - Ki)+26)mod26 jika Ci-Ki < 0

Sebagai Contoh

Cipertext	W	R	O	X	L	H	O	I		B	T	D	B	Y	C	W	V	B
Konversi	22	17	14	23	11	7	14	8		1	19	3	1	24	2	22	21	1
Kunci	K	R	I	P	T	O	K	R		I	P	T	O	K	R	I	P	T
Konversi	10	17	8	15	19	14	10	17		8	15	19	14	10	17	8	15	19
Hasil Konversi	12	0	6	8	-8	-7	4	-9		-7	4	-16	-13	14	-15	14	6	-18
Plaintext	M	A	G	I	S	T	E	R		T	E	K	N	O	L	O	G	I

Gambar 13. Proses Dekripsi

Pada Gambar 13. 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.

Perbedaan antara aplikasi yang dikembangkan dengan aplikasi online berada pada perulangan kata kunci. Setelah dilakukan uji coba beberapa kali pada aplikasi online diketahui bahwa pada kata kedua dan setelahnya selalu tidak sama jika dicocokan dengan tabel vigenere cipher.

Sebagai contoh plaintext MAGISTER TEKNOLOGI INFORMASI dengan kunci KRIPTO apabila di enkripsi menggunakan tabel vigenere cipher menghasilkan kunci :
KRIPTOKR IPTOKRIPT OKRIPTOKR
sedangkan pada aplikasi online hasilnya :
KRIPTOKR IPTOKKRIP TOKKRIPTO

Dari semua uji coba diketahui bahwa perbedaan antara aplikasi yang dikembangkan, aplikasi online dan enkripsi manual menggunakan tabel vigenere cipher berada pada perulangan kata kunci.

KESIMPULAN DAN SARAN

Dari hasil uji coba menggunakan aplikasi yang dikembangkan dan aplikasi online yang sudah ada dapat diketahui bahwa aplikasi hasil pengembangan memiliki kesesuaian dengan hasil test manual menggunakan tabel vigenere cipher sedangkan pada aplikasi online ditemukan ketidaksesuaian pada perulangan kata kunci dan cipertext.

Saran dari peneliti dalam melakukan pengembangan aplikasi diperlukan testing implentasi sistem untuk memastikan aplikasi berjalan dengan baik, dan jika diperlukan, hasil dari aplikasi dibandingkan dengan hasil perhitungan manual atau testing menggunakan cara manual.

REFERENSI

[1] N. Mona Permatasari Mokodompit, "Evaluasi Keamanan Sistem Informasi Akademik," *Jurnal Sistem Informasi Bisnis*, vol. 2, pp. 97-104, 2016.

[2] A. P. Pernebekova, "Information Security and the Theory of Unfaithful Information," *Journal of Information Security*, vol. 6, pp. 265-272, 2015.

[3] F. N. Pabokory, "IMPLEMENTASI KRIPTOGRAFI PENGAMANAN DATA PADA PESAN TEKS, ISI FILE DOKUMEN, DAN FILE DOKUMEN MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD," *Jurnal Informatika Mulawarman*, vol. 10, no. 1, pp. 20-31, 2015.

[4] N. Hamlin, "Number in Mathematical Cryptography," *Open Journal of Discrete Mathematics*, vol. 7, pp. 13-31, 2017.

[5] M. Natsir, "Pengembangan Prototype Sistem Kriptografi Untuk Enkripsi Dan Dekripsi Data Office Menggunakan Metode Blowfish Dengan Bahasa Pemrograman Java," *Jurnal Format*, vol. 6, no. 1, pp. 87-105, 2017.

[6] M. M. Amin, "IMPLEMENTASI KRIPTOGRAFI KLASIK PADA KOMUNIKASI BERBASIS TEKS," *Jurnal Pseudocode*, vol. 3, no. 2, pp. 129-136, 2016.

[7] Efrandi, "APLIKASI KRIPTOGRAFI PESAN MENGGUNAKAN ALGORITMA VIGENERE CIPHER," *Jurnal Media Infotama*, vol. 10, no. 2, pp. 120-128, 2014.

[8] M. U. Bokhari, "A Review on Symmetric Key Encryption Techniques in Cryptography," *International Journal of Computer Applications*, vol. 147, no. 10, pp. 43-48, 2016.

[9] E. H. A. Mendrofa, "Collaborative Encryption Algorithm Between Vigenere Cipher, Rotation of Matrix (ROM), and One Time Pad (OTP) Algoritma," *Advances in Science, Technology and Engineering Systems Journal*, vol. 2, no. 5, pp. 13-21, 22017.

[10] M. R. Darmawan, "IMPLEMENTASI ALGORITMA KRIPTOGRAFI VIGENER CIPHER DAN AFFINE CIPHER UNTUK MENGAMANKAN PESAN PADA APLIKASI CHATTING BERBASIS ANDROID," *SKANIKA*, vol. 1, no. 2, pp. 583-590, 2018.

[11] M. Muslim, "PENGEMBANGAN SISTEM INFORMASI JURUSAN BERBASIS WEB UNTUK MENINGKATKAN PELAYANAN DAN AKSES INFORMASI," *Jurnal MIPA*, vol. 35, no. 1, pp. 91-98, 2012.

[12] T. Suzumura, "Performance Comparison of Web Service Engines in PHP, Java, and C," *IEEE Computer Society*, pp. 385-392, 2008.