PENGGUNAAN KRIPTOGRAFI KLASIK ENKRIPSI DESKRIPSI MENGGUNAKAN METODE VIGNERE CIPHER BERBASIS WEBSITE

Isti'anatul Mazidah[1], Muhlis Tahir[2], Soleha[3], Hamdani[4], Yogi Rifansyah Ramadhan[5]

[1,2,3,4,5]Universitas Trunojoyo Madura
Jl. Raya Telang, Perumahan Telang Inda, Telang, Kec. Kamal, Kabupaten Bangkalan, Jawa Timur 69162

Email : [1]210631100025@student.trunojoyo.ac.id, [2]muhlis.tahir@trunojoyo.ac.id, [3]210631100036@student.trunojoyo.ac.id , [4]210631100030@student.trunojoyo.ac.id, [5]210631100015@student.trunojoyo.ac.id

ABSTRAK

Sebagaimana perkembangan zaman, kemajuan teknologi juga sangat mempermudah seseorang dalam berkomunikasi. Salah satu hal yang paling umum dilakukan adalah menggunakan komputer untuk berkomunikasi, sementara jaringan komputer diperlukan untuk mentransmisikan data atau informasi. Ketika melakukan pengumpulan data, keamanan dan privasi adalah dua aspek yang sangat penting dari komunikasi data, baik untuk tujuan pribadi atau untuk keamanan data kelompok. Salah satunya cara yang paling efektif untuk memastikan keamanan dan integritas data adalah menggunakan teknik kriptografi dengan menggunakan metode Vigenere Cipher, Vigenere Cipher adalah teknik yang dapat digunakan untuk mengenkripsi teks sehingga informasi tidak dapat dibaca atau disalahgunakan oleh mereka yang tidak diminta untuk menerima teks. Tujuan penelitian ini untuk mempermudah proses enkripsi dan deskripsi metode vigenere cipher dengan menggunakan websate. Penelitian ini menggunakan metode studi literatur berdasarkan berbagai jurnal dan eksperimen, termasuk implementasi sistem dan teknik perancangan. Hasil pengujian terhadap website yang dibuat dengan pemetaan manual menunjukkan hasil yang sama. Keduanya menghasilkan enkripsi dan deskripsi yang sesuai

Keywords: *Vignere Cipher, Kriptografi, Keamanan.*

ABSTRACT

As time goes by, advances in technology also make it easier for people to communicate. One of the most common things to do is use computers to communicate, while computer networks are needed to transmit data or information. When collecting data, security and privacy are two very important aspects of data communication, whether for personal purposes or for group data security. One of the most effective ways to ensure data security and integrity is to use cryptographic techniques using the Vigenere Cipher method. Vigenere Cipher is a technique that can be used to encrypt text so that information cannot be read or misused by those who are not asked to receive the text. The aim of this research is to simplify the encryption process and description of the vigenere cipher method using websate. This research uses a literature study method based on various journals and experiments, including system implementation and design techniques. Test results on websites created using manual mapping show the same results. Both produce appropriate encryption and plaintext.

Keywords: *Vignere Cipher, Cryptography, Security*

1. PENDAHULUAN

Pesatnya perkembangan teknologi telah memudahkan setiap orang dalam mengakses berbagai sumber data dan informasi nasional maupun internasional, namun hal tersebut tidak menghilangkan kemungkinan terjadinya pencurian data oleh pihak yang tidak bertanggung jawab, menjaga keamanan data pribadi atau perusahaan sangat penting untuk melindungi keutuhan data dari kerusakan dan pencurian oleh pihak – pihak yang tidak bertanggung jawab sesuai dengan data yang disimpan dan informasi aslinya[1]. Keamanan informasi di kazhakstan merupakan suatu hal yang penting yang dimana di pertimbangkan dalam tiga aspek yaitu teknis, sosial dan politik. Oleh karena itu pada aspek teknis melibatkan perlindungan sistem infomasi nasional, kemudian informasi dan infrastruktur

telekomunikasi dari akses yang tidak sah, penggunaan, pengungkapan, pelanggran, perubahan, membaca, memeriksa, merekam, atau memusnahkan dengan maksud untuk memastikan integritas, kerahasiaan, dan ketersediaan infomasi[2]. Data seringkali sangat sensitif dan harus dibatasi hanya untuk pihak yang berwenang. Oleh karna itu unsur keamanan data sangatlah penting dan memerlukan perhatian yang serius, pendekatan efektif untuk meningkatkan keamanan data adalah penggunaan enkripsi menggunakan metode kriptografi[3]. Oleh karena itu, pentingnya teknologi keamanan informasi sangat dibutuhkan[4]. Salah satu strategi yang efektif adalah melindungi informasi rahasia dengan mengenkripsi data sebelum dikirim. Dengan melakukan ini, informasi tetap terjaga kerahasiaannya meskipun diakses oleh pihak yang tidak berkepentingan, karena mereka akan kesulitan bahkan tidak mampu memahami isi informasi tersebut.[5]

Pada awalnya, metode kriptografi menggunakan kunci yang bersifat umum untuk proses enkripsi dan dekripsi. Namun, pendekatan ini memiliki kendala utama yaitu masalah distribusi kunci yang harus dilakukan dengan cara yang aman[6].Oleh karena itu, pentingnya enkripsi modern adalah tidak hanya menangani penyembunyian pesan , tetapi dengan serangkaian teknik yang menjamin keamanan informasi[7]. Kriptografi merupakan salah satu metode keamnan informasi yang dimana pada kriptografi menyediakan isi informasi berupa (plaintext) yang nanti menjadi Setelah melalui proses enkripsi, informasi akan menjadi tidak dapat dimengerti atau terbaca (ciphertext). Untuk dapat memahami isi dari ciphertext tersebut, diperlukan proses dekripsi yang tepat menggunakan kunci yang sesuai. Hanya dengan menggunakan kunci yang benar, informasi asli dapat dipulihkan kembali dari ciphertext.[4].

2. TINJAUAN PUSTAKA

Sistem Informasi adalah sebuah sistem yang mengelola dan mengintegrasikan sumber daya informasi secara efisien untuk mendukung kegiatan organisasi atau perusahaan. Sistem ini meliputi proses pengumpulan, penyimpanan, pengolahan, dan distribusi informasi guna mendukung pengambilan keputusan dan kegiatan operasional. Sistem informasi yang akan dirancang menggunakan teknologi web modern seperti HTML, CSS, dan JavaScript untuk antarmuka pengguna. Bagian logika untuk enkripsi dan deskripsi akan diimplementasikan menggunakan javaScript. Pengguna akan dapat memasukkan teks yang ingin dienkripsi atau didesskripsi, serta menentukan jumlah geseran karakter sesuai kebutuhan.

Enkripsi adalah proses mengubah data agar tidak dapat dibaca oleh pihak yang tidak berhak dalam enkripsi. Vigenere chiper merupakan salah satu cabang dari metode enkripsi caesar chiper[8]. Beberapa caesar chiper yang berbeda di aplikasikan ke plainteks dengan maksud untuk menghasilkan chiperteks yang lebih sulit untuk di deskripsikan. Pada caesar chiper didasari oleh sebuah kunci sedangkan vigenere chiper menggunakan banyak penyulihan alfabet[6]. Sementara deskripsi adalah kebalikannya, yaitu mengembalikan data dari enkripsi yang merupakan proses mengubah pesan tersandi atau cipherteks ke bentuk aslinya. Proses mengubah proses pengubahan plainteks ke chiperteks disebut enkripsi, sedangkan proses pengubahan dari chiperteks ke plainteks disebut deskripsi.. Metode enkripsi klasik seperti vignere cipher adakah salah satu teknik yang digunakan untuk mengamankan pesan.

Oleh karna itu peneliti menggunakan algoritma vignere chiper untuk dapat memberikan keamanan lebih terhadap data text. Sandi Vigenère merupakan salah satu contoh sederhana dari sandi polialfabetik. Keunggulan utama dari sandi ini dibandingkan dengan sandi Caesar atau sandi monoalfabetik lainnya adalah bahwa sandi Vigenère lebih sulit untuk dipecahkan atau diretas secara manual[9].
Secara matematis, rumus enkripsi dan deskripsi vigner cipher adalah sebagai berikut :

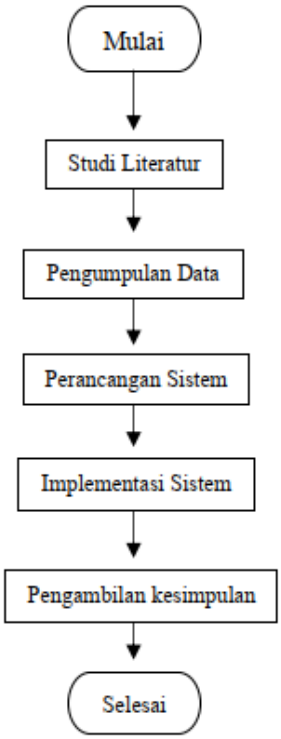
Enkripsi : $Ci = (Pi + Ki) \bmod 26$
Deskripsi : $Pi = (Ci – Ki) \bmod 26$

Keterangan :
Pi : nilai karakter Plainteks ke-i
Ci : nilai karakter Chiperteks ke-i

3. METODE PENELITIAN

Pada penelitian ini, metode yang digunakan yaitu Vignere cipher yang diterapkan dalam

suatu basis sistem informasi. Peneliti merancang sebuah kerangka kerja penelitian yang meliputi beberapa tahapan yang terdapat pada gambar 1 dibawah ini.



Gambar 1. Kerangka kerja penelitian

Kerangka dalam penelitian ini dijabarkan melalui penjelasan dibawah ini :.

2.1 Studi Literatur

Tahapan pertama dalam penelitian ini adalah proses untuk melakukan studi literatur yang komprehensif tentang kriptografi, sistem informasi, dan metode vigner cipher. Peneliti mengumpulkan beberapa referensi mengenai algoritma vignere cipher dan hipotesis pendukung lainnya

2.2 Pengumpulan data

Tahap kedua ini adalah penulis melakukan proses pengumpulan data, Data dikumpulkan dari berbagai sumber terpercaya seperti buku, makalah serta melalui jurnal yang terkait dengan topik kriptografi vignere cipher berbasis Website dan yang terkait dengan judul yang diteliti oleh penulis.

2.3 Perancangan sistem

Pada tahap ketiga ini penulis merancang sistem informasi kriptografi vignere cipher dengan mengimplementasikan kedalam bahasa pemrograman JavaScript.

2.4 Implementasi sistem

Tahapan yang terakhir ini adalah pengimplementasian dari program yang dirancang dengan cara menjalankan aplikasi dengan melakukan proses enkripsi dan deskripsi pada teks.

4 PEMBAHASAN

4.1 Implementasi Vigenere Cipher Manual

Terdapat tabel konversi abjad ke angka yang dibutuhkan dan membantu proses pengerjaan algoritma vignere cipher, bisa dilihat pada tabel 1 dibawah ini.

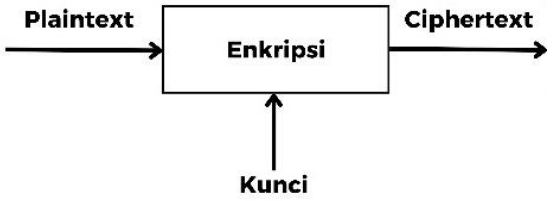
Tabel 1. Contoh tabel

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

L	M	N	O	P	Q	R	S	T
11	12	13	14	15	16	17	18	19

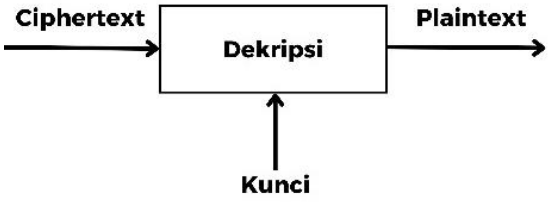
U	V	W	X	Y	Z
20	21	22	23	24	25

Dalam penerapan algoritma vignere cipher diperlukan juga sebuah skema enkripsi konvensional (mukhtar,2010 dalam mukhtar, 2018:15) seperti gambar 2 dibawah ini.



Gambar 2. Skema Enkripsi

Dalam gambar 2 skema ini terdapat plainteks yang dienkripsikan menjadi cipherteks, serta terdapat juga cipherteks yang dideskripsikan menjadi sebuah plainteks. Seperti gambar 3 dibawah ini.



Gambar 3. Skema Deskripsi

Dalam penerapan sebuah algoritma vignere cipher diperlukan sebuah plainteks atau pesan yang akan dienkripsikan dengan kunci/Key. Terdapat juga rumus enkripsi dan deskripsi.

Rumus Enkripsi :

C = (P + K) mod 26 (1)

C : Cipherteks

P : Plainteks

K : Key

Plainteks: PESAN RAHASIA KITA BERDUA

Key : KITA

C1 = (P+K) mod 26
= (15 + 10) mod 26
= 25 (Z)

C2 = (E+I) mod 26
= (4 + 8) mod 26
= 12 (M)

C3 = (S+T) mod 26
= (18 + 19) mod 26
= 37 (L)

C4 = (A+A) mod 26
= (0 + 0) mod 26
= 0 (A)

C5 = (N+K) mod 26
= (13+ 10) mod 26
= 23 (X)

C6 = (R+I) mod 26
= (17 + 8) mod 26
= 25 (Z)

C7 = (A+T) mod 26
= (0 + 19) mod 26
= 19 (T)

C8 = (H+A) mod 26
= (7 + 0) mod 26
= 7 (H)

C9 = (A+K) mod 26
= (0 + 10) mod 26
= 10 (K)

C10 = (S+I) mod 26
= (18 + 8) mod 26
= 26 (A)

C11 = (I+T) mod 26
= (8 + 19) mod 26
= 27 (B)

C12 = (A+A) mod 26
= (0 + 0) mod 26
= 0 (A)

C13 = (K+K) mod 26
= (10 + 10) mod 26
= 20 (U)

C14 = (I+I) mod 26
= (8 + 8) mod 26
= 16 (Q)

C15 = (T+T) mod 26
= (19 + 19) mod 26
= 38 (M)

C16 = (A+A) mod 26
= (0 + 0) mod 26
= 0 (A)

C17 = (B+K) mod 26
= (1 + 10) mod 26
= 11 (L)

C18 = (E+I) mod 26
= (4 + 8) mod 26
= 12 (M)

C19 = (R+T) mod 26
= (17 + 19) mod 26
= 36 (K)

C20 = (D+A) mod 26
= (3 + 0) mod 26
= 3 (D)

C21 = (U+K) mod 26
= (20 + 10) mod 26
= 30 (E)

C22 = (A+I) mod 26
= 0 + 8) mod 26
= 8 (I)

Tabel 2. Tabel Proses Enkripsi

plainteks	Urutan abjad	key	Urutan abjad key	hasil	cipherteks
P	15	K	10	25	Z
E	4	I	8	12	M

S	18	T	19	37	L
A	0	A	0	0	A
N	13	K	10	23	X
R	17	I	8	25	Z
A	0	T	19	19	T
H	7	A	0	7	H
A	0	K	10	10	K
S	18	I	8	26	A
I	8	T	19	27	B
A	0	A	0	0	A
K	10	K	10	20	U
I	8	I	8	16	Q
T	19	T	19	38	M
A	0	A	0	0	A
B	1	K	10	11	L
E	4	I	8	12	M
R	17	T	19	36	K
D	3	A	0	3	D
U	20	K	10	30	E
A	0	I	8	8	I

Tabel diatas merupakan proses enkripsi pesan. Langkah pertama, pada plainteks **P** dikonvers ke angka terlebih dahulu **(P menjadi 15)** dengan menggunakan rumus tabel 1, langkah selanjutnya pada kunci **K** juga dikonvers kedalam angka **(K menjadi 10)**, setelah proses konvers plainteks dan kunci selesai selanjutnya melakukan perjumlahan sesuai dengan rumus enkripsi **(C = (15+10) mod 26 = 25)** jika hasil dari penjumlahan antara **P** dan **K** menghasilkan lebih dari **26** maka jumlah enkripsi dikurangi **26**, langkah terakhir hasil penjumlahan tersebut di konvers menjadi abjad **(25 menjadi Z)**, jadi hasil akhir enkripsi dari palinteks **P** adalah **Z**. Dilakukan secara berulang hingga abjad plainteks selesai.
Hasil enkripsi dari PESAN RAHASIA KITA BERDUA dengan menggunakan Key KITA. Adalah
ZMLAXZTHKABAUQMALMKDEL

Sedangkan untuk mengetahui pesan yang ada pada cipherteks melakukan proses deskripsi mengunakan rumus:
Rumus Deskripsi:
P = (C – K)mod 26 (2)
P : Plainteks
C : Cipherteks
K : Key

Cipherteks : ZMLAXZTHKABAUQMALMKDEL
Key : KITA

P1 = (Z - K) mod 26
= (25 - 10) mod 26
= 15 (P)

P2 = (M - I) mod 26
= 12 - 8) mod 26
= 4 (E)

P3 = (L - T) mod 26
= (11 - 19) mod 26
= -8(mod 26) = 18 (S)

P4 = (A- A) mod 26
= (0 - 0) mod 26
= 0 (A)

P5 = (X - K) mod 26
= (23 - 10) mod 26
= 13 (N)

P6 = (Z- I) mod 26
= 25 - 8) mod 26
= 17 (R)
P7 = (T - T) mod 26
= (19 - 19) mod 26
= 0 (A)

P8 = (H - A) mod 26
= (7 - 0) mod 26
= 7 (H)

P9 = (K - K) mod 26
= 10 - 10) mod 26
= 0 (A)

P10 = (A - I) mod 26
= (0 - 8) mod 26
= -8(mod 26) = 18 (S)

P11 = (B - T) mod 26
= (1 - 19) mod 26
= -18 (mod 26) = 8 (I)

P12 = (A - A) mod 26
= (0 - 0) mod 26
= 0 (A)

P13 = (U - K) mod 26
= (20 - 10) mod 26
= 10 (K)

P14 = (Q - I) mod 26
= (16 - 8) mod 26
= 8 (I)

P15 = (M - T) mod 26
= (12 - 19) mod 26
= -7 (mod 26) =19 (T)

P16 = (A - A) mod 26

= (0 - 0) mod 26
= 0 (A)

P17 = (L - K) mod 26
= (11 - 10) mod 26
= 1 (B)

P18 = (M - I) mod 26
= (12 - 8) mod 26
= 4 (E)

P19 = (K - T) mod 26
= (10 - 19) mod 26
= -9 (mod 26) = 17 (R)

P20 = (D - A) mod 26
= (3 - 0) mod 26
= 3 (D)

P21 = (E - K) mod 26
= (4 - 10) mod 26
= -6 (mod 26) = 20 (U)

P22 = (I - I) mod 26
= (8 - 8) mod 26
= 0 (A)

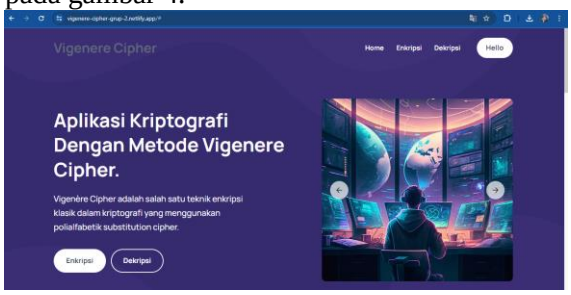
Tabel 3. Tabel Proses Deskripsi

cipherteks	Urutan abjad	key	Urutan abjad key	hasil	Plainteks
Z	25	K	10	15	P
M	12	I	8	4	E
L	11	T	19	18	S
A	0	A	0	0	A
X	23	K	10	13	N
Z	25	I	8	17	R
T	19	T	19	0	A
H	7	A	0	7	H
K	10	K	10	0	A
A	26	I	8	18	S
B	1	T	19	8	I
A	0	A	0	0	A
U	20	K	10	10	K
Q	16	I	8	8	I
M	12	T	19	19	T
A	0	A	0	0	A
L	11	K	10	1	B
M	12	I	8	4	E
K	10	T	19	17	R
D	3	A	0	3	D
E	4	K	10	20	U
I	8	I	8	0	A

Tabel diatas merupakan proses enkripsi pesan. Langkah pertama, pada cipherteks **Z** dikonvers ke angka terlebih dahulu **(Z menjadi 25)** dengan menggunakan rumus tabel 1, langkah selanjutnya pada kunci **K** juga dikonvers kedalam angka **(K menjadi 10)**, setelah proses konvers cipherteks dan kunci selesai selanjutnya melakukan pengurangan sesuai dengan rumus deskripsi **(P = (25-10) mod 26 = 15)** jika hasil dari pengurangan antara **Z** dan **K** menghasilkan lebih dari **26** maka jumlah deskripsi dikurangi **26**, langkah terakhir hasil pengurangan tersebut di konvers menjadi abjad **(15 menjadi P)**, jadi hasil akhir deskripsi dari cipherteks **Z** adalah **P**. Dilakukan secara berulang hingga abjad cipherteks selesai.
Hasil dari prosedur deskripsi tersebut menjadi **PESAN RAHASIA KITA BERDUA**

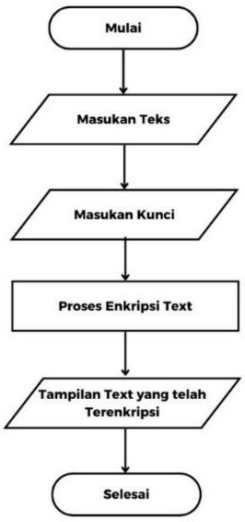
4.2 Implementasi Vignere Cipher Website

(1) Halaman Utama
Halaman utama merupakan tampilan awal website untuk mengubah text biasa menjadi cipherteks yang menggunakan sebuah algoritma vignere cipher. Halaman utama ini berisi menu pilihan antara enkripsi dan dekripsi. Tampilan halaman awal dapat dilihat pada gambar 4.



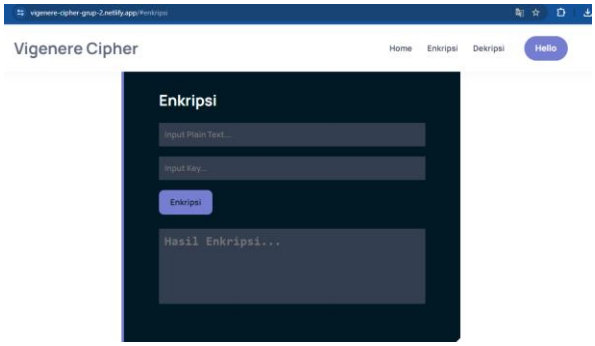
Gambar 4. Menu Halaman Utama

(2) Halaman Enkripsi
Proses enkripsi dapat diawali dengan memasukkan teks kemudian memasukkan kunci/key dan melakukan enkripsi teks, hasil dari enkripsi berupa cipherteks. terdapat flowchart urutan Langkah Langkah untuk mengubah teks terenkripsi seperti yang terlihat pada gambar 5.



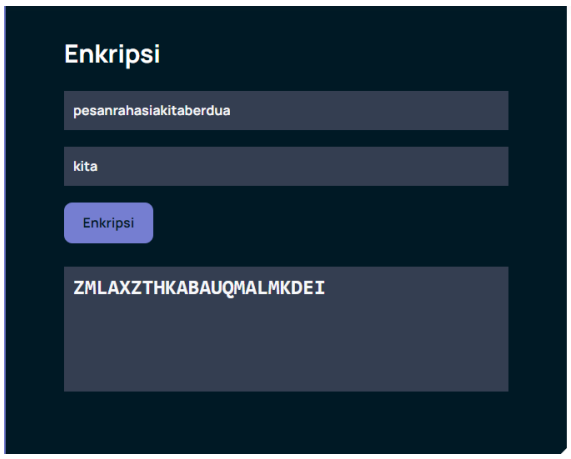
Gambar 5. Flowchart Proses Enkripsi

Pada halaman enkripsi merupakan tampilan halaman yang digunakan saat proses enkripsi. Halaman enkripsi ini sendiri akan muncul ketika kita mengklik menu enkripsi pada halaman utama, tampilan halaman ini terdiri dari input plainteks, input key, serta hasil enkripsi. Dapat dilihat pada gambar 6.



Gambar 6. Tampilan Halaman Enkripsi

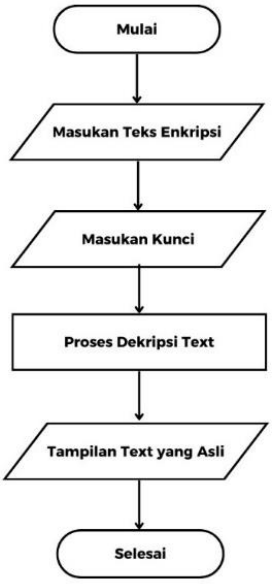
Disini kita harus menginputkan sebuah plainteks beserta Key dalam bentuk teks pada halaman ini. Setelah itu klik tombol enkripsi sehingga tampil gambar dibawah ini. gambar 7 dibawah ini menunjukkan bagaimana cara prosedur enkripsi ini bekerja:



Gambar 7. Tampilan Proses Enkripsi

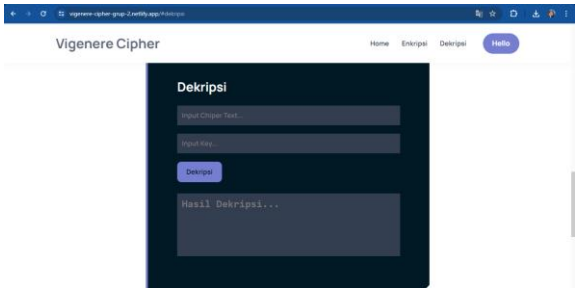
(3)Halaman Deskripsi

Proses enkripsi dapat diawali dengan memasukkan teks enkripsi kemudian memasukkan kunci/key dan melakukan proses deskripsi teks, hasil dari deskripsi berupa plainteks. terdapat flowchart urutan Langkah Langkah untuk mengubah teks terenkripsi seperti yang terlihat pada gambar 8.



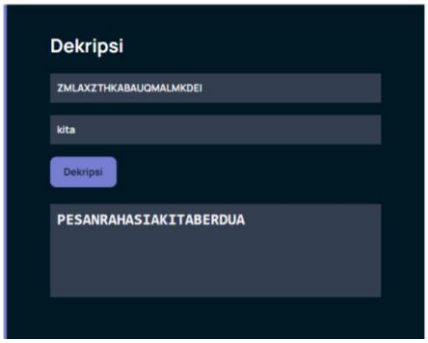
Gambar 8. Flowchart Proses Deskripsi

Pada halaman deskripsi ini yaitu sebagai halaman tampilan untuk prosedur deskripsi. Halaman deskripsi ini akan muncul ketika kita mengklik menu deskripsi pada halaman utama, tampilan pada halaman ini terdapat input chiperteks, input key, dan hasil deskripsi. Seperti pada gambar 9.



Gambar 9. Tampilan Proses Deskripsi

Pada halaman ini juga kita harus memasukkan sebuah cipherteks beserta Key berbentuk teks. Gambar 10 dibawah ini merupakan tampilan implementasi prosedur deskripsi :



Gambar 10. Tampilan Proses Deskripsi

Produk pengembangan yang telah dibuat adalah aplikasi keamanan data teks dengan menggunakan metode algoritma vignere cipher. Hasil perhitungan dari aplikasi ini sesuai dengan perhitungan yang telah dijalankan berdasarkan rumus yang telah ditetapkan, yaitu rumus untuk menghasilkan chipherteks : Ci = (Pi +Ki) mod 26, dan rumus untuk mendapatkan plainteks : Pi = (Ci -Ki) mod 26. Website yang dihasilkan dari produk tersebut telah diuji dan dibandingkan dengan website onlin lain, dan hasil uji coba menunjukkan kesamaan. Dengan demikian, dapat disimpulkan bahwa website tersebut berhasil dalam melakukan perhitungan menggunakan metode vignere cipher. Perhitungan dilakukan dengan menggunakan abjad dan angka, dimana abjad A-Z dan angka 0-25 digunakan untuk konversi, kemudian operasi penjumlahan atau pengurangan dilakukan untuk mendapatkan hasil yang diinginkan.

5 KESIMPULAN

Sistem yang dibuat berhasil diimplementasikan dengan sangat baik . Hasil pengujian terhadap website yang dibuat dengan pemetaan manual menunjukkan hasil yang sama. Keduanya menghasilkan enkripsi dan deskripsi yang sesuai, tetapi tentu saja proses enkripsi dan dekripsi dengan menggunakan Website jauh lebih efisien karena pengguna tidak perlu kesusuahan melakukan pemetaan menggunakan tabel Vigenere.

Hasil penelitian juga menunjukkan bahwa setelah proses dekripsi dilakukan melalui aplikasi enkripsi ini, data atau teks dapat dengan sukses dikembalikan ke bentuk aslinya dan dapat dibaca kembali. Sistem yang dikembangkan berhasil diimplementasikan dengan baik, seperti yang dibuktikan melalui pengujian website dengan menggunakan pemetaan manual yang menghasilkan hasil yang sama dengan proses enkripsi dan dekripsi yang dilakukan melalui website.

DAFTAR PUSTAKA

[1] M. Arifin *et al.*, “IMPLEMENTASI KRIPTOGRAFI CHATTING MENGGUNAKAN METODE VIGENERE DAN AES 128 BERBASIS WEB,” 2018.

[2] A. P. Pernebekova and B. A. Ahbergenovich, “Information Security and the Theory of Unfaithful Information,” *Journal of Information Security*, vol. 06, no. 04, pp. 265–272, 2015, doi: 10.4236/jis.2015.64026.

[3] S. Azura *et al.*, “Penerapan Kemanan Data Text menggunakan Metode Kriptografi Vigener Chiper Berbasis Web,” *Digital Transformation Technology (Digitech) | e*, vol. 3, no. 1, 2023, doi: 10.47709/digitech.v3i1.2311.

[4] J. Karman and A. Nurhasan, “PERANCANGAN SISTEM KEAMANAN DATA INVENTORY BARANG DI TOKO NANDA BERBASIS WEB MENGGUNAKAN METODE KRIPTOGRAFI VIGENERE CIPHER,” 2019.

[5] F. Agung Nugroho, A. Bani Isro, A. Chorryagnesha Aziz, and B. Noviansyah, “Call for papers dan Seminar Nasional Sains dan Teknologi Ke-2 2023 Fakultas Teknik, Universitas Pelita Bangsa,” vol. 2, no. 1, 2023.

[6] Harun. Mukhtar, *Kriptografi Untuk Keamanan Data.* 2018.

[7] S. Aulansari, D. Sawitri, A. Ikhwan, P. Sistem Informasi, S. Dan Teknologi, and U. Sumatera Utara, “PENERAPAN KRIPTOGRAFI VIGENERE CIPHER PADA KEAMANAN DATA PESAN TEKS BERBASIS WEBSITE,” 2022.

[8] Olaf Ostwald, “Cryptographic design flaws of early Enigma,” *Crypto Museum*, May 2023, Accessed: Apr. 29, 2024. [Online].

Available: https://www.cryptomuseum.com/crypto/vigenere/

[9] D. Arfandy, M. Simanjuntak, and T. Pasaribu, "Penerapan Metode Vigenere Chiper untuk Mengamankan Data Text," *JUKI : Jurnal Komputer dan Informatika*, vol. 4, 2022.

[10] F. Agung Nugroho, A. Bani Isro, A. Chorryagnesha Aziz, and B. Noviansyah, "Call for papers dan Seminar Nasional Sains dan Teknologi Ke-2 2023 Fakultas Teknik, Universitas Pelita Bangsa," vol. 2, no. 1, 2023.

[11] D. Arfandy, M. Simanjuntak, and T. Pasaribu, "Penerapan Metode Vigenere Chiper untuk Mengamankan Data Text," *JUKI : Jurnal Komputer dan Informatika*, vol. 4, 2022.

[12] A. Aditya Permana, "Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android," 2018.

[13] G. R. Fajri and B. Kurniawan, "Perancangan Aplikasi Keamanan Teks Pada Algoritma Vigenere Chiper."

[14] M. K. Harahap, "ANALISIS PERBANDINGAN ALGORITMA KRIPTOGRAFI KLASIK VIGENERE CIPHER DAN ONE TIME PAD."

[15] S. K. Komariah, "Implementasi Kriptografi Klasik Kalimat Sederhana Menggunakan Metode Caesar Cipher Berbasis Web."

[16] N. Bima Putra, B. Cirya Andika, A. Daniata Purba Bagas, M. Ridwan, S. Amik Riau, and J. Indah, "IMPLEMENTASI SANDI VIGENERE CIPHER DALAM MENGENKRIPSIKAN PESAN," 2023.

[17] V. M. Hidayah, D. Iskandar Mulyana, and Y. Bachtiar, "Algoritma Caesar Cipher atau Vigenere Cipher pada Pengenkripsian Pesan Teks," *Journal on Education*, vol. 05, no. 03, pp. 8563–8573, 2023.

[18] M. Rivaldi, I. Zarkasih Harahap, H. Isdianto, R. Amanda Putri, and F. Sains, "Positif : Jurnal Sistem dan Teknologi Informasi IMPLEMENTASI ALGORITMA KRIPTOGRAFI VIGENERE CIPHER PADA PENGAMANAN PESAN TEXT BERBASIS WEB".

[19] D. Seftian, "Aplikasi Keamanan Google Mail Berbasis Web Menggunakan Algoritma Vigenere Dan RC4 Pada Kotakpensil.com," 2018.

[20] E. Irianti *et al.*, "Implementasi Kriptografi Vigenere Cipher untuk Keamanan Data Informasi Desa", [Online]. Available: https://journal.diginus.id/index.php/PISCES/index