Penerapan Keamanan Pesan Teks Menggunakan Modifikasi Algoritma Caisar Chiper Kedalam Bentuk Sandi Morse

Irma Darmayanti[1)], Deuis Nur Astrida[2)], Dony Arius [3)]
[1, 2)] Program Studi S2 Teknik Informatika
Program Pasca Sarjana Universitas Amikom Yogyakarta
Jl. Ringroad Utara, Condong Catur, Depok, Sleman, Yogyakarta
e-mail : [1)]pakdemamo@gmail.com,[2)]deuisnurastrida@gmail.com

Abstract

Security and confidentiality in communicating become a requirement that the information sent and received is not misused by the less responsible parties. Information security and confidentiality can be safeguarded by using cryptography. Cryptography not only provides tools for information security, but also a set of techniques useful for the security and confidentiality of information. One of the methods of encryption and decryption that can be used is the caesar chiper algorithm. It's just that the caesar chiper algorithm is easy to solve so in this journal the author improves the security of a text message by modifying the caesar chiper algorithm in the form of morse code.

***Keyword** : Text Message Security, Caesar Chiper Algorithm, Morse Password*

Abstraksi

Keamanan dan kerahasiaan dalam berkomunikasi menjadi suatu kebutuhan agar informasi yang dikirim dan diterima tidak disalahgunakan oleh pihak-pihak yang kurang bertanggung jawab. Keamanan dan kerahasiaan informasi dapat dijaga dengan memanfaatkan kriptografi. Kriptografi tidak hanya menyediakan alat untuk keamanan informasi, tetapi juga sekumpulan teknik yang berguna untuk keamanan dan kerahasiaan informasi. Salah satu metode enkripsi dan dekripsi yang dapat digunakan yaitu algoritma caesar chiper. Hanya saja algoritma caesar chiper mudah untuk dipecahkan sehingga pada jurnal ini penulis meningkatkan keamanan dari suatu pesan teks dengan memodifikasi algoritma caesar chiper dalam bentuk sandi morse.

***Kata Kunci** :Keamanan Pesan Teks, Algoritma Caesar Chiper, Sandi Morse*

1. PENDAHULUAN

Masalah keamanan dan kerahasiaan data merupakan salah satu aspek penting dari suatu informasi. Terkait dengan pentingnya informasi tersebut, pihak yang terkait mempertanyakan apakah informasi tersebut masih asli atau sudah merupakan informasi bajakan. Karena informasi tersebut tidak akan berguna lagi apabila sudah diakses oleh orang yang tidak berkepentingan.

Salah satu cara untuk menjaga kerahasiaan informasi yang ditukarkan dengan

mengubah pesan yang berisi informasi tersebut menjadi kode-kode yang hanya diketahui oleh pengirim dan penerima pesan dengan memanfaatkan kriptografi. Kriptografi tidak hanya menyediakan alat untuk keamanan informasi, tetapi juga sekumpulan teknik yang berguna untuk keamanan dan kerahasiaan informasi. Apabila terdapat pihak ketiga yang kurang bertanggung jawab yang ingin mengubah ataupun mencuri informasi maka akan kesulitan dalam menterjemahkan isi pesan yang sebenarnya.

Algoritma kriptografi terdiri dari dua bagian, yaitu fungsi enkripsi dan dekripsi. Enkripsi adalah proses untuk merubah pesan asli (*plaintext*) menjadi sandi (*ciphertext*), sedangkan dekripsi adalah kebalikannya yaitu merubah sandi (*ciphertext*) menjadi pesan asli (*plaintext*).

Caesar chiper merupakan salah satu metode yang dapat digunakan dalam kriptografi. Caesar chiper digunakan pertama kali pada tahun 50 SM oleh Julius Caesar untuk mengirimkan pesan ke Marcuss Cicero. Caesar mengkodekan informasi dengan mengubah setiap huruf dalam informasi menjadi tiga huruf setelah informasi asli dalam urutan alphabet. Algoritma yang dipakai dalam caesar chiper sangat sederhana dan terlalu mudah untuk dipecahkan, sehingga caesar chiper dianggap kurang dapat menjaga kerahasiaan informasi.

Oleh karena itu pada jurnal ini penulis akan memodifkasi algoritma caisar chiper menjadi bentuk hexadecimal yang kemudian hasil dari chipertext adalah berupa sandi morse. Hal ini dilakukan untuk menjaga kerahasiaan suatu pesan.

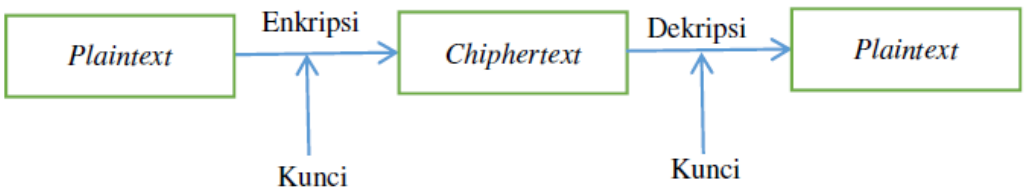
2. LANDASAN TEORI

A. Kriptografi

Kriptografi (cryptography) berasal dari bahasa yunani, kryptos berarti tersembunyi dan graphein berarti tulisan, adalah seni dan ilmu membuat komunikasi tidak dapat dipahami oleh semua orang kecuali penerima yang dituju [1]. Kriptografi adalah seni mengirim pesan yang diubah sehingga hanya bisa dipahami oleh penerimanya [2]. Kriptografi dilakukan dengan mengubah pesan asli menjadi kode dengan aturan tertentu, sehingga pesan asli hanya dapat diterima oleh penerima pesan yang memahami aturan tertentu tersebut. Kriptografi mencakup teknik seperti

microdots, menggabungkan kata-kata dengan gambar, dan cara lain untuk menyembunyikan informasi dalam penyimpanan [3]. Kriptografi bisa dilakukan dengan beberapa cara berbeda antara lain menggunakan ciphers, codes, dan subtitusi, sehingga hanya orang yang berwenang yang bisa melihat dan menafsirkan pesan sebenarnya dengan benar [4]. Kriptografi merupakan salah satu cara praktis untuk melindungi informasi yang dikirimkan melalui jaringan komunikasi publik, seperti saluran telepon, gelombang mikro, atau satelit [5].

Tujuan kriptografi adalah untuk memperoleh integritas (keutuhan), kerahasiaan dan keaslian semua sumber informasi [6]. Kriptografi tidak hanya melindungi data dari pencurian ataupun pengubahan (alternation) pesan tapi juga dapat digunakan untuk menautentikasi pengguna [6]. Terdapat beberapa istilah yang dipakai dalam kriptografi, diantaranya yaitu: kode disebut ciphers, informasi yang disembunyikan disebut plaintext, setelah informasi diubah ke bentuk rahasia, pesan yang dikirim disebut ciphertext. Proses perubahan dari plaintext ke ciphertext disebut enkripsi (encrypting), sedangkan proses sebaliknya perubahan dari ciphertext kembali ke plaintext disebut dekripsi (decrypting) [5].



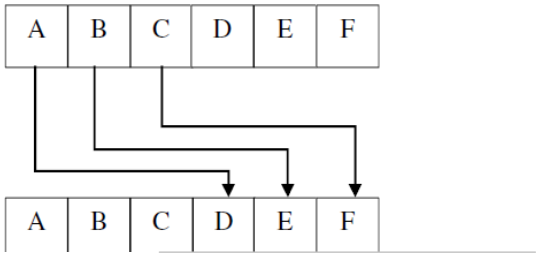
Gambar 1. Proses Enkripsi dan Deskripsi Sederhana

B. Caesar Chiper

Caesar chiper adalah salah satu teknik enkripsi yang paling sederhana dan paling dikenal. CaesarCipher adalah algoritma yang digunakan oleh sistem kriptografi simetri dan digunakan jauh sebelum sistem kriptografi public key ditemukan, kriptografi klasik yang ada dan beberapa bentuk algoritma klasik dianggap optimal karena mudah dipecahkan [7]. Caesar chiper merupakan jenis cipher substitusi dimana setiap huruf dalam plaintext digantikan oleh sebuah huruf dengan beberapa posisi tetap di bawah alfabet[6]. Teknik ini juga dikenal sebagai single cipher alphabet [8].Caesar chiper pertama kali digunakan oleh Julius Caesar. Caesar mengkodekan informasi dengan

menggubah setiap huruf dalam informasi menjadi tiga huruf di setelah informasi asli dalam urutan alfabet[5]. Algoritma kriptografi Caesar Cipher sangat mudah digunakan. Inti dari algoritma kriptografi ini menggeser semua karakter dalam plaintext dengan nilai pergeseran yang sama [8]. Langkah yang ditempuh untuk membangun ciphertext dengan Caesar Cipher adalah:

a. Tentukan besarnya pergeseran karakter yang digunakan dalam membentuk ciphertext menjadi plaintext.
b. Menukar karakter dalam plaintext menjadi ciphertext dengan berdasarkan pergeseran yang telah ditentukan.



Gambar 2. Pergeseran Dalam Caesar Cipher

Sekitar tahun 1970 diciptakan sistem baru dalam caesar chiper dengan mengubah huruf ke angka [4].

Tabel 1. Pergeseran Dalam Caesar Cipher

Plain text	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
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Ciphertext	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
	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2

Untuk menggambarkan cipher ini menggunakan aritmatika modular, misalkan P adalah padanannumerik dari sebuah huruf pada plaintext dan C adalah padanan numerik dari huruf ciphertext yang sesuai.

$$C \equiv P + 3(mod\ 26), 0 \leq C \leq 25$$

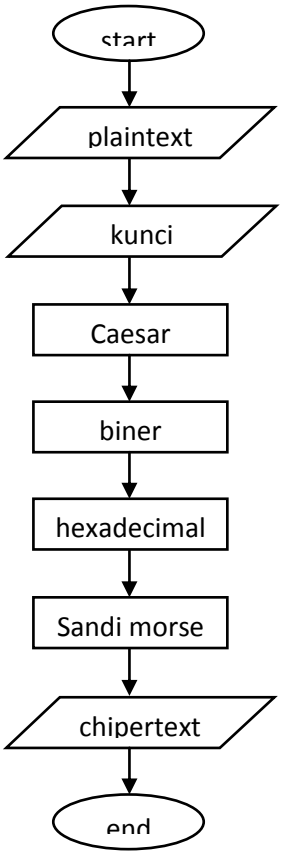
Penerima pesan dapat mendekripsi dengan langkah

$$P \equiv C - 3(mod\ 26), 0 \leq C \leq 25$$

Setelah ciphertext kembali ke padanan numerik plaintext, penerima pesan dapat mengubah kembali pesan angka ke huruf.

3. METODE PENELITIAN

Alur dari proses enkripsi suatu pesan teks dapat dilihat pada flowcart di bawa ini.



Gambar 3. Flowcart Enkripsi Pesan Teks

Untuk proses deskripsi sebuah pesan tidak jauh berbeda dengan proses enkripsi.

4. HASIL DAN PEMBAHASAN

Langkah-langkah proses enkripsi dengan modifikasi chiper text yaitu :

Pesan Teks diubah dalam menggunakan algoritma caisar chiper, dimana kunci yang digunakan menggunakan angka. Contoh : *plainteks* = “segera hubungi saya”

Key = “5”

SUSUNAN AWAL

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Key : a=5, menjadi

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
5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4

Chipertetx yang dihasilkan dari algoritma caisar chiper = “XJLJWFMZGZSLNXFDF”

a. Mencari bilangan biner dari masing-masing huruf *chipertext* algoritma caesar chiper.

X	= 01011000	M= 01001101		N	= 01001110
J	=01001010	Z= 01011010		X	= 01011000
L	=01001100	G= 01000111		F	= 01000110
J	=01001010	Z= 01011010		D	= 01000100
W	=01010111	S= 01010011		F	= 01000110
F	=01000110	L= 01001100			

b. Mengubah bilangan biner dari masing-masing huruf kedalam bilangan hexadecimal.

01011000	= 58	01001101= 4D		01001110	= 4E
01001010	= 4A	01011010= 5A		01011000	= 58
01001100	= 4C	01000111= 47		01000110	= 46
01001010	= 4A	01011010= 5A		01000100	= 44
01010111	= 57	01010011= 53		01000110	= 46
01000110	= 46	01001100 = 4C			

c. Mengubah bilangan hexadecimal kedalam bentuk sandi morse dengan cara membalik huruf awal menjadi huruf akhir, hal ini dilakukan agar pihak yang tidak bertanggung jawab sulit untuk memecahkan isi pesan yang dikirim.

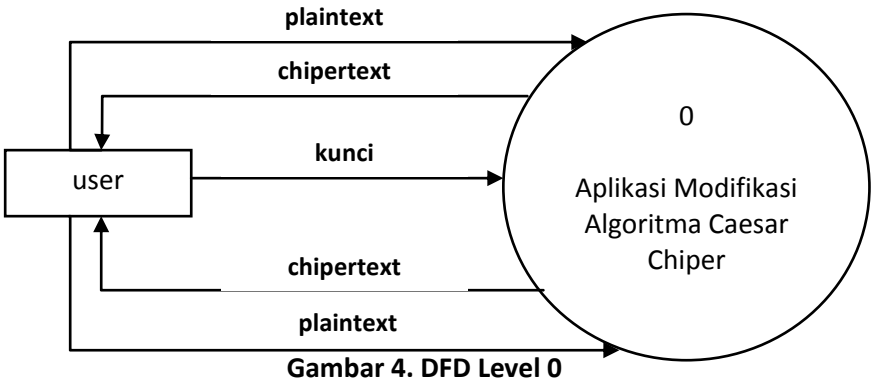
Hexadecimal =”584A4C4A57464D5A475A534C4E58464446”

Chipertext Sandi morse = “-....,....-,....-,....-,-....,....-,---..,.....,.,....-,-.-.,....-,...--,.....,.-,.....,--...,....-,.-,.....,-..,....-,-....,....-,--...,.....,.-,....-,-.-.,....-,.-,....-,---..,.....”

Langkah deskripsi dengan cara memasukan *chipertext* dan kunci yang sama digunakan pada saat melakukan enkripsi. Proses yang dilakukan tidak berbeda jauh dari proses enkripsi.

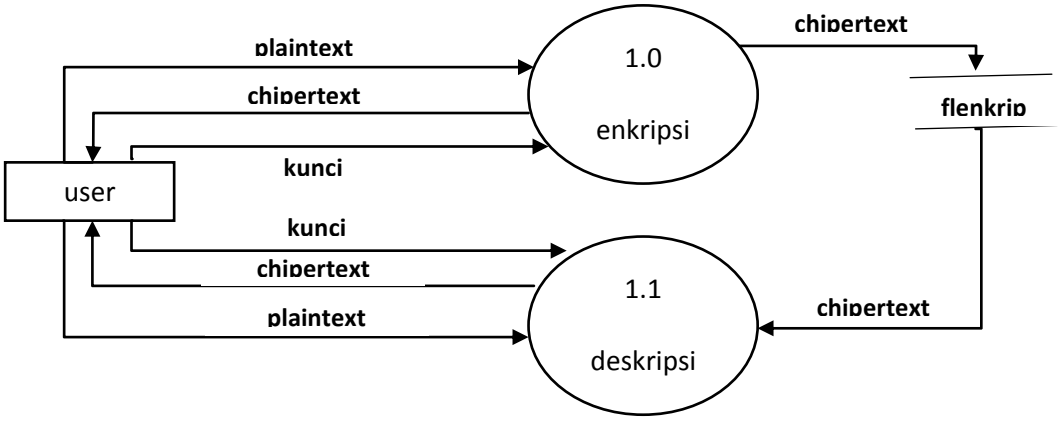
Perancangan proses yang digambarkan dalam bentuk *Data Flow Diagram* (DFD) adalah sebagai berikut:

a. DFD Level 0



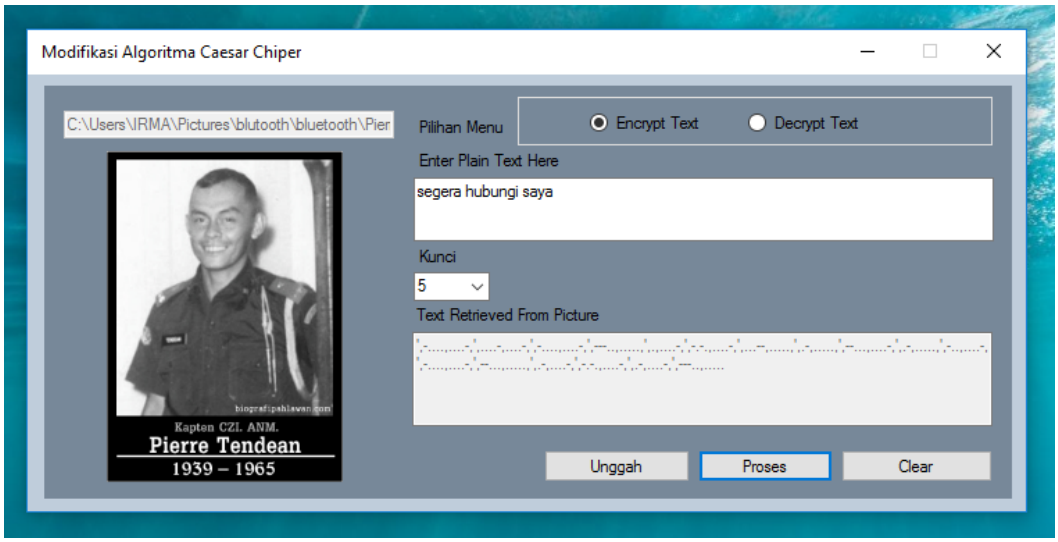
Gambar 4. DFD Level 0

b. DFD Level 1



Gambar 5. DFD Level 1

Implementasi aplikasi dapat dilihat dari gambar berikut ini.



Gambar 6. Halaman Enkripsi/Deskripsi Pesan

5. KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan penelitian yang dilakukan dapat ditarik kesimpulan sebagai berikut :

1. Dari hasil penelitian ini ditemukan sebuah modifikasi dari algoritma caesar chiper ke dalam bentuk sandi morse, sulit untuk dipecahkan oleh pihak-pihak yang tidak bertanggung jawab.
2. Penyimpan pesan yang berupa chipertext dalam bentuk gambar, menyulitkan seseorang untuk mengetahui bahwa gambar yang dikirim menyimpan sebuah pesan tersembunyi.

Saran

Berdasarkan hasil penelitian yang sudah disimpulkan maka dalam upaya pengembangan dikemukakan saran dimana pada penelitian ini hanya memodifikasi algoritma caesar chiper dalam bentuk morse, dimana pada prosesnya pesan yang dikirimkan tidak boleh lebih dari 30 karakter, sehingga pada penelitian selanjutnya dapat memasukan unsur program agar modifikasi algoritma caesar chiper ini dalam bentuk morse dapat berisi pesan panjang .

DAFTAR PUSTAKA

[1] D. Luciano and G. Prichett, “Cryptology: From Caesar Ciphers to Public-Key Cryptosystems”, The College Mathematics Journal., vol. 18, no.1, pp. 2–17, 1987.
[2] S. O'Brien, “An Investigation Into Cryptographic Methods Through Use Of Matlab”, University of Hertfordshire, unpublished, 2014
[3] G. Shrivastava, “Using Letters Frequency Analysis in Caesar Cipher with Double Columnar Transposition Technique”,International Journal of Engineering Sciences & Research Technology., vol. 2, Issue 6 , pp. 1475-1478, 2013.
[4] A. Jain, R. Dedhia, and A. Patil, “ Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication”, International Journal of Computer Applications (0975 – 8887)., vo.129, no.13, 2015.
[5] D. M. Burton, “Elementary Number Theory”, New York: McGraw-Hill Publishing. 2011. [6] S. Kusumadewi, Artificial intelligence (teknik dan aplikasinya)., 2003.
[6] J. Singh and S. S. Yadav, “Implementation of Caesar Cipher and Chaotic Neural network by using MATLAB Simulator”, International Journal of Recent Development in Engineering and Technology., ISSN 2347 - 6435 (Online), vol. 2, Issue 6, 2014.
[7] A. S. Tanenbaum, “Computer Networks”, Fourth Edition, Pearson. 2002
[8] T. Limbong, dan P.D.P. Silitonga, “Testing the Classic Caesar Cipher