IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Tanggal publikasi xxxx 00, 0000, tanggal versi saat ini xxxx 00, 0000. *Nomor*

Digital Object Identifier 10.1109/ACCESS.2022.Doi

“Kombinasi Metode Enkripsi Vigenere Chiper dan Caesar Chiper”

Rizky Saputra, Aghata Deolika
[1]Institut Teknologi dan Sains Nahdlatul Ulama Kalimantan
[2]Teknik Komputer

ABSTRAK

Keamanan dan kerahasiaan data tetap menjadi prioritas utama dalam komunikasi. Ketiadaan prosedur keamanan yang memadai telah menyebabkan peningkatan insiden pencurian data, khususnya pada aplikasi dan jaringan komunikasi yang memproses data berupa teks. Salah satu faktor utama terjadinya pencurian data teks adalah kurangnya penerapan prosedur keamanan yang efektif. Oleh karena itu, metode kriptografi atau penyandian data menjadi solusi yang diperlukan. Enkripsi data merupakan teknik yang umum digunakan untuk melindungi data dari akses tidak sah.

Dengan penerapan metode kriptografi, diharapkan dapat meminimalkan kasus pencurian atau penyadapan data. Penelitian ini bertujuan untuk menyusun prosedur keamanan data teks melalui penggabungan dua metode kriptografi, yaitu Vigenere Cipher dan Caesar Cipher. Kombinasi ini menggunakan kunci yang berbeda pada setiap metode; Vigenere Cipher memanfaatkan kunci berupa teks, sementara Caesar Cipher menggunakan pergeseran angka. Penelitian mencakup proses penyandian data melalui perhitungan manual dan implementasi program. Hasil pengujian menunjukkan bahwa hasil enkripsi dengan perhitungan manual konsisten dengan hasil yang dihasilkan oleh program, selama input plainteks terdiri dari huruf kapital. Berdasarkan evaluasi, tingkat keberhasilan pengujian mencapai 100% dengan 15 percobaan yang mencakup hingga 5000 karakter plainteks dan cipherteks.

KATA KUNCI : Enkripsi, Vigenere Cipher, Caesar Cipher, Keamanan Informasi, Kriptografi

I. PENDAHULUAN

Kemajuan teknologi dan informasi yang pesat ditandai dengan hadirnya berbagai fasilitas komunikasi, seperti email, SMS, dan fitur chatting di media sosial, yang membuat komunikasi tidak lagi terbatas pada interaksi tatap muka. Namun, komunikasi digital ini tidak sepenuhnya aman karena sering terjadi kejahatan seperti penyadapan pesan dan pencurian data. Oleh karena itu, diperlukan prosedur keamanan melalui teknik penyandian untuk menjaga kerahasiaan dan keamanan pesan.

Metode kriptografi klasik sering digunakan sebagai konsep dasar dalam kriptografi, meskipun memiliki kelemahan pada sistem cipher. Algoritma kriptografi klasik umumnya menggunakan teknik substitusi atau transposisi. Substitusi dilakukan dengan mengganti karakter satu per satu, sedangkan transposisi dilakukan melalui permutasi. Untuk mengatasi kelemahan ini, dilakukan modifikasi pada kriptografi klasik dengan menggabungkan metode Caesar Cipher dan Vigenere Cipher. Kedua metode ini termasuk dalam kategori kriptografi klasik dan dapat menjadi solusi untuk meningkatkan keamanan pesan teks. Penelitian ini juga membandingkan efektivitas penyandian pesan menggunakan kedua metode tersebut, baik secara terpisah maupun dalam kombinasi.

Penelitian ini bertujuan untuk mengoptimalkan kriptografi klasik dengan menggabungkan metode Vigenere Cipher dan Caesar Cipher, sehingga memperkuat proses enkripsi. Keunggulan penelitian ini terletak pada penggabungan kedua metode untuk memperkuat keamanan, disertai perhitungan manual dan validasi dengan kode sumber. Pengujian dilakukan dengan membandingkan hasil perhitungan manual dan kapasitas informasi.

II. TINJAUAN PUSTAKA

A. Enkripsi

Enkripsi adalah proses mengamankan data atau informasi dengan cara mengubahnya menjadi bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang. Dalam enkripsi, data asli yang disebut plainteks diubah menjadi format yang disebut cipherteks menggunakan algoritma tertentu dan kunci enkripsi. Hanya pihak yang memiliki kunci dekripsi yang benar yang dapat mengembalikan cipherteks tersebut ke bentuk aslinya (plainteks).

Enkripsi menjadi bagian penting dalam dunia modern untuk melindungi data dari ancaman keamanan seperti peretasan, pencurian data, atau penyadapan.

B. Deskripsi

Dekripsi adalah proses mengubah data terenkripsi (cipherteks) kembali ke bentuk aslinya (plainteks) sehingga dapat dibaca atau dipahami. Dekripsi dilakukan menggunakan algoritma dan kunci dekripsi yang sesuai dengan proses enkripsi yang telah dilakukan sebelumnya.

Dekripsi adalah kebalikan dari enkripsi. Kedua proses ini saling melengkapi untuk menjaga keamanan dan kerahasiaan data selama pengiriman atau penyimpanan. Jika enkripsi mengamankan data dengan mengubahnya menjadi format yang tidak dapat dibaca, dekripsi mengembalikan data tersebut ke bentuk aslinya untuk digunakan oleh pihak yang berhak.

C. Vigenere Chiper

Vigenere cipher adalah suatu metode untuk enkripsi alfabet dari teks dengan menggunakan berbagai macam seri dari caesar cipher berdasarkan huruf-huruf yang ada pada kunci. Cipher ini merupakan bentuk mudahnya dari polyalphabetic substitution. Vigenere cipher sudah berkalikali mengalami penciptaan ulang. Metode asli ditemukan oleh Giovan Battista Bellaso pada bukunya dia La cifra del. Sig. Giovan Battista Bellaso pada tahun 1553. Bagaimanapun, skemanya dibuat oleh Blaise de Vigenere pada abad ke-16.

D. Caesar Chiper

Caesar Cipher adalah salah satu teknik enkripsi tertua yang dirancang untuk menjaga keamanan komunikasi antar pihak. Meskipun teknik ini sering disebut Caesar Cipher, beberapa orang juga mengenalnya dengan nama lain seperti Caesar's cipher, shift cipher, Caesar's code, atau Caesar shift.

Dalam metode ini, setiap huruf dalam teks asli digantikan oleh huruf atau simbol lain dengan cara menggesernya sejauh jumlah posisi tertentu dalam urutan alfabet. Karena alasan ini, Caesar Cipher diklasifikasikan sebagai teknik substitusi.

Sebagai salah satu metode enkripsi paling awal dan sederhana, Caesar Cipher pertama kali digunakan oleh Julius Caesar dan kemudian diadopsi oleh berbagai pemimpin militer lainnya untuk melindungi pesan rahasia selama operasi militer.

Julius Caesar sendiri biasanya menggunakan pergeseran tiga posisi, tetapi saat ini versi populer dari Caesar Cipher adalah "ROT13," yang merupakan singkatan dari "rotate by 13 places." Teknik ini menggantikan setiap huruf dalam alfabet dengan huruf lain yang terletak 13 posisi lebih jauh.

III. METODE

Penelitian ini menggunakan metode berupa studi literatur dan perancangan eksperimen. Studi literatur dilakukan untuk mengumpulkan dan menganalisis data dengan cara membaca berbagai sumber referensi, seperti buku, skripsi, jurnal, dan tulisan lain yang relevan dengan topik penelitian. Studi ini bertujuan memberikan dasar teori dan acuan yang kuat dalam memahami serta mengkaji permasalahan yang diteliti.

Sementara itu, eksperimen dilakukan melalui perancangan dan implementasi sistem untuk memberikan gambaran yang jelas terkait masalah yang dihadapi. Penelitian ini menggunakan metode prototipe, yang merupakan pendekatan dalam pengembangan perangkat lunak dengan menekankan pada pengembangan bertahap dan berfokus pada peningkatan berkelanjutan.

IV. HASIL & PEMBAHASAN

A. Caesar Chiper

Terdapat sebuah teks yang akan dienkripsi menggunakan algoritma Caesar. teks yang akan dienkripsi adalah "ITSNUKA". Berikut ini adalah langkah-langkah proses enkripsi dan deskripsi menggunakan algoritma Caesar.

- PlainTeks : ITSNUKA.
- Key : 5

Proses Enkripsi

- Rumus : E(P)=C | C=P+K mod 26

Ket :

- C = ChiperTeks
- E(P) = Enkripsi
- P = PlainTeks
- K = Key / Jumlah pergesaran

Tabel 4. 1 Proses enkripsi Caesar cipher

I	T	S	N	U	K	A
8	19	18	13	20	10	0
8+5	19 +5	18+5	13+5	20+5	10+5	0+5
13	24	23	18	25	15	5
N	Y	X	S	Z	P	F

Hasil :

Enkripsi (Cipherteks) = NYXSZPF

Pada proses perhitungan enkripsi pada tabel 4.1 dapat di jelaskan bahwa ITSNUKA pada baris pertama dalam tabel adalah plainteks yang akan di enkripsi, lalu pada baris kedua merupakan plainteks yang sudah dikonversikan menjadi angka, pada baris ke tiga merupakan penjumlahan plainteks dengan key, baris ke empat pada tabel merupakan hasil penjumlahan plainteks dan key, lalu pada baris terakhir merupakan hasil konversi angka enkripsi ke alphabet yang merupakan hasil ChiperTeks

menggunakan metode Caesar Chiper. Kemudian selanjutnya mengembalikan
(mendiskripsikan) chiperteks menjadi plainteks.

- Cipherteks : NYXSZPF Rumus :

D(C) = P | P = C-K mod 26 Ket :

P = Plainteks
D(C) = Deskripsi
C = Cipherteks
K = Key

Tabel 4. 2 Proses deskripsi Caesar cipher

N	Y	X	S	Z	P	F
13	24	23	18	25	15	5
13-5	24-5	23-5	18-5	25-5	15-5	5-May
8	19	18	13	20	10	0
I	T	S	N	U	K	A

Pada proses perhitungan deskripsi pada tabel 4.2 dapat dilihat bahwa NYXSZPF pada baris pertama dalam tabel adalah cipherteks yang akan di deskripsikan, lalu pada baris kedua merupakan chiperteks yang sudah dikonversikan menjadi angka, pada baris ke tiga merupakan pengurangan cipherteks dengan key, baris ke empat pada tabel merupakan hasil pengurangan cipherteks dan key, lalu pada baris terakhir merupakan hasil konversi angka deskripsi ke alphabet yang menghasilkan kembali plainteks menggunakan metode Caesar cipher.

B. Vigenere Chiper

Terdapat sebuah teks yang akan dienkripsi menggunakan algoritma Vigenere. Teks asli atau pesan yang akan dienkripsi adalah ITSNUKA, dengan kunci ABC. Berikut ini adalah proses enkripsi menggunakan algoritma Vigenere.

- Plainteks = ITSNUKA
- Key = ABC

Proses enkripsi

- Rumus = E(P)=C | C=P+K mod 26

Ket :

- C = ChiperTeks
- E(P) = Enkripsi
- P = PlainTeks
- K = Key

Tabel 4. 3 Proses enkripsi vigenere cipher

I	T	S	N	U	K	A
8	19	18	13	20	10	0
A	B	C	A	B	C	A
0	1	2	0	1	2	0
8+0	19+1	18+2	13+0	20+1	10+2	0+0
8	20	20	13	21	12	0
I	U	U	N	V	M	A

Hasil enkripsi (cipherteks) = IUUNVMA

Pada proses perhitungan enkripsi pada tabel 4.3 dapat di jelaskan bahwa ITSNUKA pada baris pertama dalam tabel adalah plainteks yang akan di enkripsikan, lalu pada baris kedua merupakan plainteks yang sudah dikonversikan menjadi angka, pada baris ke tiga merupakan key/kunci yang sudah ditetapkan, baris keempat merupakan key yang sudah dikonversikan ke angka, baris kelima penjumlahan plainteks dengan key, baris ke enam pada tabel merupakan hasil penjumlahan plainteks dan key, lalu pada baris terakhir merupakan hasil konversi angka enkripsi ke alphabet yang merupakan hasil ChiperTeks menggunakan metode vigenere chiper.

Kemudian selanjutnya mengembalikan (mendiskripsikan) chiperteks menjadi plainteks.

- Cipherteks : IUUNVMA Rumus :

D(C)=P | P=C-K mod 26

Ket :

P = Plainteks
D(C) = Deskripsi
C = Cipherteks
K = Key

Tabel 4. 4 Proses deskripsi vigenere cipher

I	U	U	N	V	M	A
8	20	20	13	21	12	0
A	B	C	A	B	C	A
0	1	2	0	1	2	0
8-0 .	20-1	20-2	13-0	21-1	12-2 .	0-0
8	19	18	13	20	10	0
I	T	S	N	U	K	A

Pada proses perhitungan deskripsi pada tabel 4.4 dapat dilihat bahwa IUUNVMA pada baris pertama dalam tabel adalah cipherteks yang akan di deskripsikan, lalu pada baris kedua merupakan chiperteks yang sudah dikonversikan menjadi angka, pada baris ke tiga merupakan key/kunci yang sudah ditentukan, baris keempat merupakan key yang dikonversi menjadi angka, baris kelima pengurangan cipherteks dengan key, baris keenam pada tabel merupakan hasil pengurangan cipherteks dan key, lalu pada baris terakhir merupakan hasil konversi angka deskripsi ke alphabet yang menghasilkan kembali plainteks menggunakan metode vigenere cipher.

C. Kombinasi Caesar dan Vigenere

Menggabungkan algoritma Caesar dan Vigenere dapat menghasilkan enkripsi yang lebih kuat. Hal ini karena jika pesan berhasil disadap, data yang diperoleh masih dalam kondisi terenkripsi. Berikut adalah contoh penerapan kombinasi antara sandi Caesar dan sandi Vigenere :

1. Enkripsi Caesar

- Plainteks = TEKNIKKOMPUTER
- Key = 12
- Rumus = E(P)=C, C=P+K Mod 26

Tabel 4. 5 proses enkripsi caesar cipher

T	E	K	N	I	K	K	O	M	P	U	T	E	R
19	4	10	13	8	10	10	14	12	15	20	19	4	17
12	12	12	12	12	12	12	12	12	12	12	12	12	12
31	16	22	25	20	22	22	26	24	27	32	31	16	29
F	Q	W	Z	U	W	W	A	Y	B	G	F	Q	D

- Hasil enkripsi Caesar = FQWZUWWAYBGFQD

Hasil enkripsi pada tabel 4.5 menggunakan sandi Caesar akan digunakan sebagai pesan awal untuk dienkripsi ulang menggunakan sandi Vigenere.

2. Enkripsi Caesar

- Plainteks = TEKNIKKOMPUTER
- Enkripsi Caesar = FQWZUWWAYBGFQD
- Key = ITSNU
- Rumus = E(P)=C, C=P+K Mod 26

Tabel 4. 6 Proses enkripsi vigenere

F	Q	W	Z	U	W	W	A	Y	B	G	F	Q	D
31	16	22	25	20	22	22	26	24	27	32	31	16	29
I	T	S	N	U	I	T	S	N	U	I	T	S	N
8	19	18	13	20	8	19	18	13	20	8	19	18	13
39	35	40	38	40	30	41	44	37	47	40	50	34	42
N	J	O	M	O	E	P	S	L	V	O	Y	I	Q

- Hasil enkripsi vigenere = NJOMOEPSLVOYIQ

Hasil enkripsi pada tabel 4.6 merupakan hasil enkripsi dari gabungan Caesar dan vigenere dengan melakukan enkripsi menggunakan metode Caesar, selanjutnya hasil dari enkripsi Caesar digunakan untuk teks awal melakukan enkripsi menggunakan vigenere sehingga hasil akhir merupakan gabungan kedua metode enkripsi Caesar dan vigenere.

3. Deskripsi.

a. Vigenere

Kemudian selanjutnya melakukan deskripsi teks sehingga memulihkan hasil enkripsi menjadi teks awal yang dapat dibaca

- Cipher = NJOMOEPSLVOYIQ
- Key = ITSNU

Tabel 4. 7 Deskripsi vigenere

N	J	O	M	O	E	P	S	L	V	O	Y	I	Q
13	9	14	12	14	4	15	18	11	21	14	24	8	16
I	T	S	N	U	I	T	S	N	U	I	T	S	N
8	19	18	13	20	8	19	18	13	20	8	19	18	13
5	-10	-4	-1	-6	-4	-4	0	-2	1	6	5	-10	3
F	Q	W	Z	U	W	W	A	Y	B	G	F	Q	D

- Hasil deskripsi = FQWZUWWAYBGFQD

b. Caesar

- Cipher = FQWZUWWAYBGFQD
- Key = 12

Tabel 4. 8 Deskripsi caesar

F	Q	W	Z	U	W	W	A	Y	B	G	F	Q	D
5	16	22	25	20	22	22	0	24	1	6	5	16	3
12	12	12	12	12	12	12	12	12	12	12	12	12	12
-7	4	10	13	8	10	10	-12	12	-11	-6	-7	4	-9
T	E	K	N	I	K	K	O	M	P	U	T	E	R

- Hasil deskripsi = TEKNIKKOMPUTER

Teks hasil enkripsi yang telah didekripsi dari kombinasi sandi Vigenere dan Caesar kini kembali ke bentuk aslinya sehingga dapat dibaca dan dipahami dengan jelas. Proses ini memastikan bahwa kerahasiaan dan keaslian pesan tetap terlindungi sepanjang perjalanan hingga mencapai penerima. Dengan pendekatan ini, risiko gangguan seperti manipulasi atau penyadapan pesan dapat diminimalkan, sehingga komunikasi menjadi lebih aman dan terpercaya.

.

V. KESIMPULAN

Dalam mengirim pesan atau surat melalui akses internet, penting untuk menjaga kerahasiaan isi pesan agar hanya pengirim dan penerima yang dapat membacanya. Salah satu cara untuk melindungi pesan tersebut adalah dengan menggunakan metode enkripsi, seperti kombinasi antara metode Caesar dan Vigenere.

Kombinasi kedua metode ini memberikan tingkat keamanan yang lebih tinggi, sehingga jika pesan tersebut dibajak atau disadap oleh pihak yang tidak bertanggung jawab, isi pesan tetap terlindungi dan sulit untuk dipecahkan. Teknik ini menyulitkan pelaku penyadapan untuk memahami isi pesan yang dienkripsi.

Untuk meningkatkan keamanan pesan elektronik, metode Caesar dan Vigenere dapat digabungkan dan diterapkan sebagai solusi perlindungan data. Dengan pendekatan ini, komunikasi melalui internet menjadi lebih aman, menjaga keaslian dan kerahasiaan pesan dari ancaman gangguan pihak luar.

VI. UCAPAN TERIMA KASIH

Terima kasih kepada Tim Jurnal yang telah meluangkan waktu untuk membuat template ini. Dalam penyusunan penelitian sebagai tugas akhir semester ini masih kurang dari sempurna, untuk itu diharapkan saran dan kritik yang membangun dari para pembaca. Jika ada kekurangan ataupun kesalahan dalam penyusunan tugas akhir ini penyusun mohon maaf sebesar-besarnya.

REFERENSI

[1] G. Minarto, B. Khairuzzaman, and M. Q., "Penerapan kriptografi menggunakan Caesar Cipher dan Vigenere Cipher," STMIK Pontianak, 2018.

[2] G. A. Pradipta, "Penerapan kombinasi metode enkripsi Vigenere Cipher dan transposisi pada aplikasi clientserver chatting," STMIK STIKOM Bali, 2016.

[3] V. M. Hidayah, D. I. Mulyana, and Y. Bachtiar, *Algoritma Caesar Cipher atau Vigenere Cipher pada pengenkripsian pesan teks*, STIKOM CKI Jakarta, 2023.
[4] F. Zuli and A. Irawan, "Penerapan kombinasi sandi Caesar dan Vigenere untuk pengamanan data pesan pada surat elektronik," Universitas Satya Negara Indonesia Jakarta, 2014.
[5] M. Azwar and M. W. Qulub, "Kombinasi metode kriptografi substitusi dalam pengaman pesan dan informasi," Universitas Bumigora, 2022.
[6] V. C. Hardita and E. W. Shole, "Penerapan kombinasi metode Vigenere Cipher, Caesar Cipher dan simbol baca dalam mengamankan pesan," STMIK Palangka Raya, 2021.