ISBN: 978-602-60280-1-3

Modifikasi Algoritma Caesar *Cipher* dan Vigenere *Cipher* dengan Peggunaan Diagram Cartesius pada Pengiriman Pesan Melalui Media sosial

Ali Nur Ikhsan[1], Pungkas Subarkah[2], Dony Ariyus[3]
[1,2,3]Program Studi Magister Teknik Informatika
Universitas Amikom Yogyakarta
Yogyakarta, Indonesia
Email : alinoerikhsan@gmail.com[1], subarkah18.pungkas@gmail.com[2], [3]Dony.a@amikom.ac.id

Abstrak—Penggunaan media sosial pada saat ini sudah menjadi sebuah kebutuhan setiap orang. Bahkan banyak orang atau kelompok organisasi yang menjadikan media sosial menjadi sebuah alat yang digunakan untuk memenuhi kepentingan sendiri atau kelompoknya. Dari banyaknya pengguna media sosial banyak orang melakukan komunikasi yang bebas, bahkan bisa juga dilihat oleh orang lain dan bukan lagi menjadi suatu rahasia. Dengan memperhatikan keamanan dan kenyamanan dalam komunikasi sebaiknya dilakukan enkripsi. Dari beberapa algoritma enkripsi digunakan dua algoritma enkripsi yaitu Caesar *cipher* dan Vigenere *cipher* yang dikombinasikan dengan diagram cartesius. Untuk hasil dari enkripsi disembunyikan dalam sebuah gambar. Dengan menggunakan kata kunci yang unik yang digunakan dalam proses enkripsi dan dekripsi diharapkan dapat mengamankan pesan dan informasi yang ada dalam suatu komunikasi. Dari penelitian diperoleh kesimpulan bahwa modifikasi Vigenere *Cipher* dan Caesar *Cipher* dengan diagram Cartesius kemudian hasil enkripsi disisipkan pada dokumen/gambar menghasilkan data enkripsi yang susah untuk dipecahkan dan memerlukan waktu untuk melakukan dekripsi sehingga data/informasi yang penting aman setelah dilakukan enkripsi.

Kata kunci : media sosial, enkripsi, dekripsi, vigenere, caesar,cartesius

I. PENDAHULUAN

Kebutuhan informasi pada setiap orang berbeda, semakin canggih dan majunya teknologi informasi menjadikan orang mudah untuk mendapatkan informasi yang lengkap dan ter-*up to date*. Apalagi pada saat ini penggunaan internet di seluruh dunia sudah sangat banyak digunakan dalam berbagai bidang. Salah satu contoh penggunaan internet yang sering digunakan untuk mendapatkan informasi yaitu media sosial *online* seperti Instagram, Whatsapp, Facebook, Twitter, Telegram dan lain-lain. Penggunaan media sosial tidak membatasi usia, jenis kelamin maupun tempat tinggal. Hal ini menjadikan informasi dapat diperoleh dengan mudah, namun di sisi lain mempunyai resiko keamanan data dan informasi yang dicuri atau dirusak oleh pihak yang tidak bertanggung jawab.

Keamanan informasi merupakan suatu hal yang penting bagi seseorang maupun kelompok. Dalam pengamanan data dilakukan suatu proses enkripsi dan dekripsi atau dikenal dengan teknik kriptografi. Kriptografi merupakan ilmu seni untuk menjaga kerahasiaan dan keamanan suatu data atau informasi ketika informasi dikirim dari suatu tempat ke tempat lain [1].

Penelitian Ariska, dkk (2018) dengan judul ”Rancangan Kriptografi *Hybrid* Kombinasi Metode Vigenere Cipher dan Elgamal pada pengamanan pesan rahasia”. Tujuan dari penelitian adalah mengkombinasikan dua metode keamanan untuk menjaga kerahasiaan pesan pada saat pengiriman SMS atau jenis chatting lainnya dengan menggunakan teknik kriptografi hibrid. Hasil dari penelitian ini yaitu kombinasi dua metode Vigenere Cipher dan ElGamal dapat digunakan dengan baik untuk keamanan pesan rahasia [2].

Penelitian Arrijal, dkk (2016) dengan judul ”Penerapan Algoritma Kriptografi Kunci Simetris dengan Modifikasi Vigenere *Cipher* dalam Aplikasi Kriptografi Teks”. Tujuan dari penelitian yaitu menerapkan algoritma Vigenere *Cipher* ke bentuk aplikasi yang memungkinkan pengguna dapat melakukan enkripsi dan dekripsi teks. Hasil dari penelitian ini yaitu berhasil membangun aplikasi *proto-type* yang menerapkan algoritma kunci simetris dengan modifikasi Vigenere *Cipher*. [3]

Penelitian Pratama dan Tamatjita (2015) dengan judul ” Modifikasi Algoritma Vigenere Cipher Menggunakan Metode Catalan Number dan Double Columnar Transposition”. Tujuan dari penelitian adalah melakukan modifikasi Algoritma Vigenere Cipher Menggunakan Metode Catalan Number dan Double Columnar Transposition. Hasil dari penelitian ini yaitu metode catalan number dan double columnar transposition yang telah dimodifikasi dengan algoritma vigenere *cipher* lebih acak, lebih kuat, sulit untuk dipecahkan oleh kriptanalis [4].

Semakin banyaknya lalu lintas informasi yang ada di media sosial, untuk beberapa orang atau organisasi penting harus menggunakan pengaman informasi. Salah satu contoh bentuk pengamanan data yaitu dengan menggunakan

ISBN: 978-602-60280-1-3

kriptografi. Seperti pada penelitian yang sudah dipaparkan sebelumnya, peneliti mempunyai rumusan masalah yaitu bagaimana modifikasi algoritma Caesar *cipher* dan Vigenere *cipher* dengan penggunaan diagram cartesius pada pengiriman pesan melalui media sosial? Penelitian ini diharapkan mampu memberikan gambaran kepada developer program untuk membuat aplikasi sesuai dengan modifikasi algoritma yang sudah dihasilkan dari penelitian ini.

II. TINJAUAN PUSTAKA

A. Kriptografi

Kriptografi merupakan perpaduan dua kata yang berasal dari bahasa Yunani yaitu *crypto* yang berarti rahasia dan *graphia* yang berarti tulisan, sehingga jika dirangkai menjadi suatu pengertian yaitu suatu ilmu yang digunakan dalam merahasiakan pesan tertulis dengan tujuan untuk menjaga tulisan itu agar tidak diketahui oleh orang yang tidak diinginkan.

B. Steganografi

Steganografi merupakan perpaduan dua kata yang berasal dari bahasa Yunani yaitu *Stegos* yang berarti tersembunyi dan *graphein* yang berarti menulis, sehingga jika dirangkai menjadi suatu pengertian yaitu suatu ilmu yang digunakan untuk menyembunyikan suatu pesan yang rahasia agar bisa diterima oleh penerima yang dimaksud oleh pengirim.

C. Caesar *Cipher*

Kode Kaisar merupakan substitusi kode pertama pada pemerintahan Yulius Caesar yang mengganti huruf awal alfabet yang disebut ROT3. Kode kaisar dapat dipecahkan dengan cara *brute force attack* dengan mencoba-coba untuk menemukan kata kunci, biasanya cara ini diperlukan waktu yang lama. [5]

D. Vigenere *Cipher*

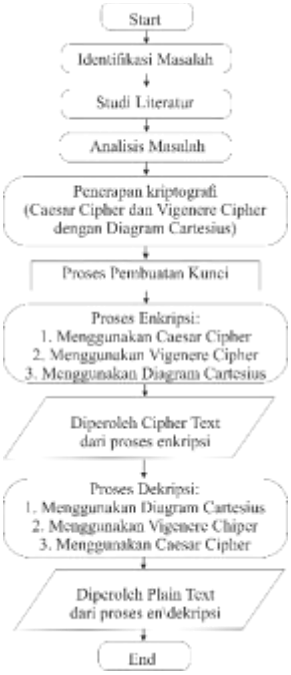
Vigenere Cipher dikenalkan pada abad 16, tahun 1586 oleh kriptologis asal Perancis, Blaise de Vigenere. Pada teknik substitusi Vigenere setiap kode memiliki kemungkinan teks asli yang dilakukan dengan dua cara yaitu angka dan huruf, hampir sama dengan kode kaisar. Vigenere Cipher ini menggunakan kunci yang pendek dan berulang-ulang sehingga menjadikan kelemahan pada vigenere cipher. Dengan metode Kasiski membantu menemukan panjang kunci dari vigenere cipher yang memanfaatkan keuntungan bahasa Inggris yang tidak hanya terdapat perulangan huruf tetapi juga perulangan pasangan. [6]

E. Diagram Cartesius

Diagram Cartesius merupakan suatu sistem kordinat yang digunakan untuk meletakan atau menentukan titik pada penggambaran objek berdasarkan pemasukan nilai yang ada pada sumbu x dan nilai pada sumbu y dimana titik pertemuan tersebut nilai dari sumbu x dan sumbu y yang terdapat pada titik kordinat dibentuk. [7]

III. METODE PENELITIAN

Konsep penelitian yang penulis rancang untuk melakukan penelitian ini seperti pada gambar 1.



Gambar 1. Konsep Penelitian

Adapun tahapan dari tiap-tiap langkah gambar 2 diatas akan dijelaskan sebagai berikut:

A. Identifikasi Masalah

Pada tahapan ini dilakukan pengamatan terhadap penggunaan media sosial dan keamanan serta privasi yang terdapat pada informasi yang ada pada media sosial.

B. Studi Literatur

Pada tahap ini dilakukan pengumpulan referensi yang mempunyai hubungan dengan penelitian yang digunakan untuk mendukung kelancaran dan kesuksesan penelitian.

C. Analisis Masalah

Pada tahap ini dilakukan analisis terhadap para pengguna media sosial yang sering tidak memperhatikan keamanan data dan informasi yang mereka bagikan atau kirimkan kepada orang yang dituju. Solusi yang ditawarkan dari hasil analisis masalah yaitu dengan melakukan proses enkripsi dan dekripsi data dengan menggunakan Caesar *cipher* dan Vigenere *cipher* dengan menggunakan diagram cartesius.

D. Penerapan Kriptografi

Dilakukan penerapan pengamanan data dengan menggunakan Caesar *cipher* dan Vigenere *cipher* dengan menggunakan diagram cartesius.

E. Proses Pembuatan Kunci

Kata kunci digunakan untuk proses enkripsi dan dekripsi data. Proses pembuatan kata kunci dilakukan dengan

ISBN: 978-602-60280-1-3

menggunakan kata-kata unik dan sulit untuk ditebak dan dipecahkan.

F. Proses Enkripsi

Pada proses enkripsi dilakukan pengamanan data dengan menggunakan caesar *cipher* dengan menggunakan menggunakan kata kunci yang unik, setelah itu hasil enkripsi Caesar *cipher* dienkripsi lagi dengan menggunakan vigenere *cipher* dengan menggunakan kata kunci yang unik kemudian diperoleh hasil enkripsi yang dikombinasikan ke dalam diagram cartesius dan untuk lebih aman bisa disisipkan ke dalam dokumen/gambar.

G. Proses Dekripsi

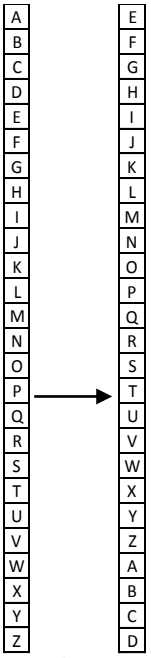
Pada proses dekripsi dilakukan penguraian terhadap data yang terenkripsi menjadi data yang dapat dibaca. Langkah pertama yang dilakukan adalah jika data dimasukkan pada dokumen/ gambar, maka harus dipisahkan dari dokumen/gambar, kemudian penguraian data dari diagram cartesius, setelah itu dengan menggunakan kata kunci yang unik dilakukan dekripsi dengan menggunakan Vigenere *cipher* dan terakhir didekripsi dengan Caesar *cipher*. Hasil akhir didapatkan *plaintext* atau teks asli yang berisi informasi.

IV. PEMBAHASAN

Pada pembahasan penelitian ini dilakukan suatu penelitian dengan menggunakan suatu contoh kasus yaitu suatu perusahaan memberikan suatu pesan penting terhadap perusahaan yang bekerjasama untuk saling memberikan keuntungan satu sama lain isi pesan tersebut yaitu: "SENIN RAZIA PASAR".

A. Proses Enkripsi

1. Enkripsi dengan Caesar *Cipher*
   Pada enkripsi dengan Caesar *Cipher* dilakukan pergeseran huruf sesuai dengan keinginan pengirim, contohnya pergeseran sebanyak 5 kali seperti pada gambar 2.



Gambar 2. Modifikasi Caesar *Cipher*

Sehingga dari kata SENIN RAZIA PASAR diperoleh cipher text WIRMR VEDME TEWEV.

2. Enkripsi dengan Vigenere *Cipher*
   Pada enkripsi dengan Vigenere *Cipher* dilakukan dengan memodifikasi huruf dengan angka seperti pada Tabel 1.

Tabel 1. Modifikasi 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	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	26
B	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1
C	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2
D	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3
E	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4
F	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5
G	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6
H	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7
I	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8
J	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9
K	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10
L	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11
M	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12
N	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13
O	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14
P	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Q	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
R	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
S	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
T	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
U	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
V	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
W	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
X	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Y	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Z	26	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

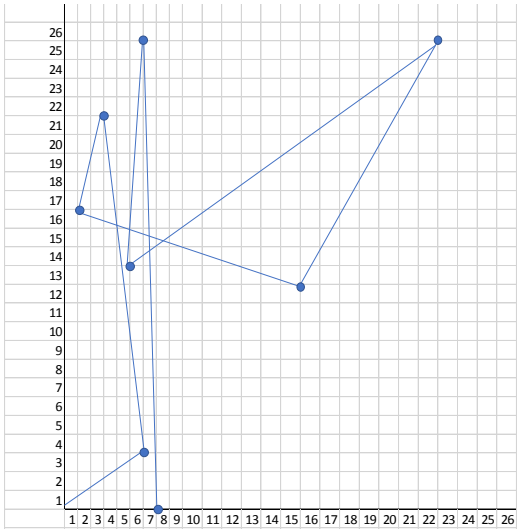
Dari Tabel 1 ditentukan kata kunci sesuai dengan keinginan pengirim misalnya kata kunci: "JULI" maka diperoleh hasil enkripsi kata WIRMR VEDME TEWEV yaitu 6 3 3 21 1 16 16 12 22 25 5 13 6 25 7

3. Enkripsi dengan Diagram Caesar

ISBN: 978-602-60280-1-3

Dari hasil enkripsi Vigenere *Cipher* dilakukan pengelompokkan sumbu x dan y, untuk angka pertama dijadikan sumbu x, angka kedua dijadikan sumbu y, angka ketiga dijadikan sumbu x dan seterusnya. Untuk memulai garis dimulai dari sumbu (0,0) dan jika jumlah datanya ganjil maka sumbu y pada kata terakhir dijadikan 0.

Dari data enkripsi Vigenere *Cipher* diperoleh data (6,3), (3,21), (1,16), (16,12), (22,25), (5,13), (6,25), (7,0) dan jika ditampilkan pada diagram Cartesius akan diperoleh gambar seperti pada gambar 3.



Gambar 3. Hasil Enkripsi dengan Diagram Cartesius

Hasil enkripsi tersebut memiliki keunikan tidak dapat diketahui bahwa terdapat pesan rahasia, karena kebanyakan orang melihat diagram tersebut seperti diagram biasa pada matematika. Namun jika pengirim ingin lebih aman lagi hasil enkripsi dengan diagram cartesius tersebut disisipkan ke dalam gambar lain, sehingga orang lain tidak dapat melihat gambar hasil enkripsi tersebut.

B. Proses Dekripsi

Jika pesan disisipkan pada suatu gambar, maka perlu diekstrak agar pesan gambar yang dienkripsi muncul, kemudian untuk langkah-langkah dekripsi seperti berikut:

1. Dekripsi dengan Diagram Cartesius
   Pada tahapan ini penerima pesan harus menguraikan tiap titik sumbu mulai dari ujung garis atau dari sumbu 0, jika dimulai dari ujung garis maka angka tersebut diletakkan pada bagian akhir atau menjadi angka terakhir yang berarti huruf terakhir pada pesan yang dienkripsi. Jika dimulai dari sumbu 0 maka angka yang diperoleh menjadi awal angka yang berarti huruf pertama pada pesan yang dienkripsi. Dari Gambar 3 dengan memulai dari sumbu 0 diperoleh peruraian data yaitu (6,3), (3,21), (1,16), (16,12), (22,25), (5,13), (6,25), (7,0) dan jika dijadikan deretan angka menjadi 6 3 3 21 1 16 16 12 22 25 5 13 6 25 7
2. Dekripsi dengan Vigenere *Cipher*
   Setelah diperoleh data hasil dekripsi dari diagram Cartesius dengan menggunakan kata kunci yang diberikan pengirim yaitu JULI maka dengan menggunakan Tabel 1 diperoleh hasil dekripsi WIRMRVEDMETEWEV.
3. Dekripsi dengan Caesar *Cipher*
   Pada proses dekripsi dengan Caesar *Cipher* dengan pergeseran 5 kali seperti apa yang diberitahu oleh pengirim maka diperoleh hasil dekripsi SENINRAZIAPASAR dan jika disusun menjadi SENIN RAZIA PASAR.

V. KESIMPULAN

Dari penelitian yang telah dilakukan diperoleh kesimpulan bahwa modifikasi Vigenere *Cipher* dan Caesar *Cipher* dengan diagram Cartesius kemudian hasil enkripsi disisipkan pada dokumen/gambar menghasilkan data enkripsi yang susah untuk dipecahkan dan memerlukan waktu untuk melakukan dekripsi sehingga data/informasi yang penting aman setelah dilakukan enkripsi.

Kelemahan dalam penelitian ini dalam melakukan dekripsi memerlukan waktu yang cukup lama sehingga untuk informasi rahasia yang diperlukan dengan cepat kurang tepat jika menggunakan enkripsi dengan modifikasi pada penelitian ini. Diharapkan untuk penelitian berikutnya akan ada aplikasi yang dapat mempermudah dalam proses enkripsi dan dekripsi sesuai dengan modifikasi Vigenere *Cipher* dan Caesar *Cipher* dengan diagram Cartesius.

REFERENSI

[1] Ariyus, Dony. 2008. *Pengantar Ilmu Kriptografi (Teori, Analisis, dan Implementasi)*. Yogyakarta: Andi Offset.

[2] Ariska, B., Suroso, Endri, J. 2018. "Rancangan Kriptografi *Hybrid* Kombinasi Metode Vigenere Cipher dan Elgamal pada pengamanan pesan rahasia". Seminar Nasional Inovasi dan Aplikasi Teknologi di Industri 2018, ISSN: 2085-4218

[3] Arrijal, I. M., Efendi, R., dan Susilo, B. 2016." Penerapan Algoritma Kriptografi Kunci Simetris dengan Modifikasi Vigenere *Cipher* dalam Aplikasi Kriptografi Teks". Jurnal Pseudocode, Vol III No. 1, Februari 2016, ISSN 2355-5920

[4] Pratama, G. M., dan Tamatjita, E. N., 2015. "Modifikasi Algoritma Vigenere *Cipher* Menggunakan Metode Catalan *Number* dan *Double Columnar Transposition*". Compiler, Vol 4, No. 1, Mei 2015

[5] Ariyus, Dony. 2008. *Pengantar Ilmu Kriptografi (Teori, Analisis, dan Implementasi)*. Yogyakarta: Andi Offset.

[6] Ariyus, Dony. 2008. *Pengantar Ilmu Kriptografi (Teori, Analisis, dan Implementasi)*. Yogyakarta: Andi Offset.

[7] Harry. 2017. Belajar Memahami Bidang atau Diagram Cartesius [Internet]. [Diakses 2018 July 5]. Tersedia pada: http://bangkusekolah.com/2017/09/08/belajar-memahami-bidang-atau-diagram-cartesius/