

IMPLEMENTASI PENGAMANAN DATA DENGAN MENGGUNAKAN ALGORITMA CAESAR CIPHER DAN TRANSPOSISI CIPHER

Adnan Buyung Nasution

Program Studi Sistem Informasi Fakultas Sains dan Teknologi
Universitas Islam Negeri Sumatera Utara
Jln. IAIN No.1, Medan 20235 Sumatera Utara, Indonesia
adnanbuyungnasution@uinsu.ac.id

Abstrack - The existence of data theft and misuse of data by unrelated groups causes the data to be no longer safe. Therefore, a security is needed that can make data safe from groups that are not concerned. Caesar Cipher Algorithm, which is the position of the original letter location changed through the alphabet. Transposition algorithm, which uses character permutations. Caesar Cipher and Transposition can secure data and restore data without changing the original form (plaintext).

Keywords - Data Theft, Security, Caesar Chiper, Cipher Transposition

Abstrack - Adanya pencurian data dan penyalahgunaan data oleh kelompok yang tidak bersangkutan menyebabkan data tidak terjaga lagi. Oleh karena itu, dibutuhkan suatu keamanan yang bisa membuat data aman dari kelompok yang tidak bersangkutan. Algoritma Caesar Cipher, yaitu posisi letak huruf asal diubah melalui alfabet. Algoritma Transposisi, yaitu menggunakan permutasi karakter. Caesar Cipher dan Transposisi dapat mengamankan data dan mengembalikan data tanpa merubah bentuk dari aslinya (plainteks).

Kata Kunci - Pencurian Data, Keamanan, Caesar Chiper, Trasposisi Chiper

I. PENDAHULUAN

Perkembangan ilmu pengetahuan dan teknologi dimasa sekarang semakin pesat terutama dibidang komunikasi. Ada berbagai cara yang dapat dilakukan dalam berkomunikasi, salah satunya menggunakan tulisan. Lewat tuisan (teks), banyak informasi dapat diperoleh dan terkadang dalam teks tersebut terdapat informasi yang bersifat rahasia.[1]

Dewasa ini, banyak kelompok yang tidak bersangkutan mencoba untuk mencuri data orang lain dan ada beberapa kelompok yang menyalahgunakan data tersebut sehingga data tersebut tidak terjaga lagi. Oleh karena itu, dibutuhkan suatu keamanan yang membuat data aman dari kelompok yang tidak bersangkutan.

Banyak cara dapat dilakukan untuk menyembunyikan data atau pesan yang akan dikirim[2]. Salah satunya menggunakan kriptografi. Kriptografi berfungsi untuk menyamarkan pesan menjadi pesan yang tersandi. Adapun algoritma kriptografi yang bisa menyamarkan pesan adalah algoritma *Caesar Cipher* dan *Transposisi Cipher*. Algoritma *Caesar Cipher* adalah algoritma penyandian data paling sederhana dengan cara mengenkripsi dan mendeskripsi data dengan menggunakan pergeseran sebanyak k. Algoritma *Tranposisi Chiper* adalah algoritma penyandian yang teks pesan yang akan disandikan dengan cara diubah posisinya.[3]

Dengan penggunaan algoritma *Caesar Cipher* dan *Transposisi* pengguna dapat

mengamankan isi data yang akan diberikan si penerima sehingga integritas data dapat terjaga kerahasiaannya.

II. METODE PENELITIAN

A. Kriptografi

Kata kriptografi terdiri dari dua bagian yang berasal dari bahasa Yunani, yaitu kriptos dan graphia dimana kriptos dapat diartikan sebagai secret (rahasia) dan graphia sebagai writing (tulisan). Berdasarkan istilahnya kriptografi merupakan ilmu dan seni pengamanan pesan saat pesan dipindahkan pada suatu tempat ketempat lainnya[4]. Kriptografi adalah suatu ilmu menganalisis teknik matematika yang berkaitan dengan pengamanan informasi seperti penyembunyian data, kesahan data, integritas data, serta keaslian data [5]. Kriptografi yaitu ilmu pengetahuan dan seni melindungi pesan supaya terjaga (aman). Sasaran penggunaan kriptografi yaitu membentuk sesuatu yang samar, berupa pesan rahasia seperti teks, suara, gambar dan video.[6]

Tujuan dari kriptografi ialah untuk memberikan layanan keamanan [1] yaitu:

1. Penyembunyian (*Confidentiality*)
Kerahasiaan informasi dilakukan dengan menyembunyikan informasi dari segala aspek yang tidak berhak.
2. Kelengkapan Data (*Integrity*)
Data tidak terganti sampai ke penerima saat proses pengiriman.

3. Keaslian (*Message Authentication*)
Kejelasan identitas semua entitas yang terkait dan autentikasi sumber data.
4. Tidak ada penolakan (*Nonrepudiation*)
Setiap entitas saling berhubungan dan tidak dapat menolak atau membantah data yang dikirim atau diperoleh.

Kriptografi memiliki beberapa hal yang harus diketahui antara lain[1]:

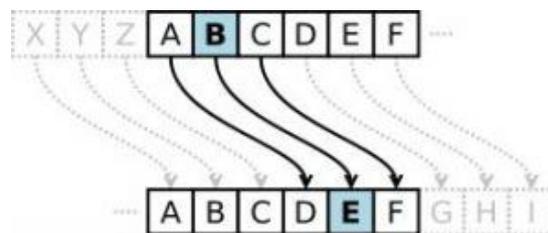
1. Pengirim dan Penerima
Pengirim (*sender*) merupakan kesatuan yang mengirimkan *message* kepada penerima (*receiver*) dengan aman tanpa ada gangguan dari penyadap (*eavesdropper*). Penerima merupakan entitas yang memperoleh pesan oleh pengirim.
2. *Plaintext* dan *Ciphertext*
Pesan murni pada kriptografi disebut dengan *plaintext*, sedangkan pesan murni yang telah disamarkan disebut *ciphertext*.
3. Enkripsi dan Dekripsi
Pada prosedurnya, pergantian *plaintext* jadi *ciphertext* disebut enkripsi (*encryption*) dan pergantian *ciphertext* jadi *plaintext* disebut dekripsi (*decryption*).
4. Kriptografer, Kriptanalis, dan Kriptologis
Seseorang yang mempelajari dan menggunakan metode kriptografi untuk mengamankan pesan dinamakan kriptografer. Sebaliknya, metode yang menggunakan teknik komputasi matematika untuk menyerang metode kriptografi dinamakan kriptanalis, dan orang yang mempelajari kriptanalis dinamakan kriptanalis. Kata kriptologi merupakan cabang ilmu yang mempelajari kriptografi sekaligus dengan kriptanalis. Orang yang mempelajari kriptologi tersebut dinamakan kriptologis.
5. Cipher
Algoritma kriptografi (*cipher*) merupakan fungsi matematika dalam penggunaan enkripsi dan dekripsi. Dalam menyelesaikan persoalan *cipher*, dibutuhkan sebuah entitas yang disebut dengan kunci (dilambangkan K). Kunci mempunyai nilai bilangan yang sangat besar. Besar kecilnya nilai ini dinamakan *keyspace*. Beberapa algoritma kriptografi menggunakan *cipher* dengan beda kunci antara kunci bagi enkripsi dan dekripsi.
6. Penyadap (*Eavesdropper*)
Penyadap (*eavesdropper*) adalah orang yang ingin mendapatkan informasi sebanyak-banyaknya dari pesan yang telah dikirim dan memecahkan *ciphertext* dari system kriptografi. Penyadap mempunyai akses komunikasi antara pengirim dan penerima.

B. Algoritma Caesar Cipher

Pada kriptografi, sandi Caesar, atau sandi pindah, kode Caesar yaitu metode enkripsi sangat sederhana dan sangat populer. Kode ini terdiri dari semua huruf pada teks asli (*plaintext*) disubstitusi dengan kode kemudian berubah menjadi huruf lain yang mempunyai selisih posisi tertentu dalam alfabet. Dalam Caesar cipher, huruf-huruf diubah dengan huruf selanjutnya dari posisi alfabet yang sama.[7]

Proses Caesar Cipher adalah :[3]

1. Tentukan berapa besar pemindahan karakter yang dipakai untuk membuat *ciphertext* ke *plaintext*.
2. Tukar posisi karakter *plaintext* menjadi *ciphertext* berdasarkan pemindahan yang telah ditentukan sebelumnya. Contoh, pemindahan = 3. Jadi huruf A digeser menjadi huruf D, huruf B menjadi huruf E, dan berikutnya.



Gambar 1 Proses Caesar Cipher

Proses dekripsi menggunakan persamaan 1 di bawah ini :

$$C_p = (P_t + k) \text{ modulo } 26 \dots\dots\dots(1)$$

Dimana 26 adalah jumlah alfabet, persamaan 1 digunakan pada proses enkripsi. Proses dekripsi menggunakan persamaan 2 di bawah ini :

$$P_t = (C_p - k) \text{ modulo } 26 \dots\dots\dots(2)$$

Berikut satuan dari abjad atau alfabet pada Caesar Cipher sebagai berikut [8]:

Tabel 1 : Satuan Alfabet

Abjad/Alphabet	Nilai Urut
A	0
B	1
C	2
D	3
E	4
F	5
G	6
H	7
I	8
J	9
K	10
L	11
M	12
N	13

Abjad/Alphabet	Nilai Urut
O	14
P	15
Q	16
R	17
S	18
T	19
U	20
V	21
W	22
X	23
Y	24
Z	25

C. Algoritma Transposisi Cipher

Transposisi cipher yaitu teknik enkripsi pesan dengan menggantikan posisi setiap huruf yang ada pada plaintext (pesan asli yang tidak dienkripsi) menjadi ciphertext (pesan sudah terenkripsi) dengan tahap tertentu. Penerapan cara itu membuat plaintext tidak dapat dibaca melainkan jika mempunyai kunci untuk mengubah kembali pesan yang ada ke bentuk awal atau disebut dekripsi.[9] Pada haikatnya tahap perubahan ini pesan hampir sama dengan anagram seperti kata “meredam” berubah menjadi “mamedra”, akan tetapi transposisi cipher memiliki rumus atau kunci tertentu yang dibutuhkan sehingga pesan yang ada dapat dimengerti. Contoh kunci=3:

M	E	R
E	D	A
M		

III. HASIL DAN PEMBAHASAN

A. Perhitungan Caesar Cipher dan Transposisi Cipher

Pada teori diatas perhitungan Caesar Cipher dan Transposisi Cipher dibagi menjadi 2 proses yaitu proses enkripsi dan dekripsi.

1. Tahap Enkripsi

Suatu tahap membuat pergantian sebuah sandi dari dapat dipahami (*plaintext*) menjadi sebuah sandi yang tidak dapat dipahami (*ciphertext*). Misalkan, diketahui plaintext sebagai berikut:

Plaintext : LOVE
k : 12
kunci : 2

Maka langkah yang harus dikerjakan adalah :

- Cek nilai alphabet dari huruf dimana pada table 1 terlihat bahwa L=11, O=14, V=21 dan E=4.

- Kemudian lakukan perhitungan ciphertext $C_p = (P_t + k) \text{ modulo } 26$ dan cek pada table 1 alphabet dari nilai ciphertext yang dihasilkan.

$$\begin{aligned} C_{p_1} &= P_{t_1} + k \text{ modulo } 26 \\ &= (11+12) \text{ modulo } 26 \\ &= 23 \text{ modulo } 26 \\ &= 23 \\ &= X \end{aligned}$$

$$\begin{aligned} C_{p_2} &= P_{t_2} + k \text{ modulo } 26 \\ &= (14+12) \text{ modulo } 26 \\ &= 26 \text{ modulo } 26 \\ &= 0 \\ &= A \end{aligned}$$

$$\begin{aligned} C_{p_3} &= P_{t_3} + k \text{ modulo } 26 \\ &= (21+12) \text{ modulo } 26 \\ &= 33 \text{ modulo } 26 \\ &= 7 \\ &= H \end{aligned}$$

$$\begin{aligned} C_{p_4} &= P_{t_4} + k \text{ modulo } 26 \\ &= (4+12) \text{ modulo } 26 \\ &= 16 \text{ modulo } 26 \\ &= 16 \\ &= Q \end{aligned}$$

- Hasil enkripsi adalah “XAHQ”. Lalu lakukan transposisi dengan kunci = 2.

X	A
H	Q

Maka didapatkan ciphertext dari plaintext “LOVE” adalah **XHAQ**.

2. Tahap Deskripsi

Berkebalikan pada tahap Enkripsi yaitu untuk menggantikan sandi dari yang tidak bisa dipahami (*ciphertext*) menjadi sebuah sandi yang bisa dipahami (*plaintext*).

Contoh kasus. Jika diberikan ciphertext sebagai berikut:

Plaintext : XHAQ
k : 12
kunci : 2

Maka langkah yang harus dikerjakan adalah :

- Lakukan transposisi dengan kunci = 2.

X	A
H	Q

- Hasil deskripsi transposisi adalah “XAHQ”. Lalu cek nilai alphabet dari huruf dimana pada table 1 terlihat bahwa X = 23, A = 0, H = 7 dan Q = 16.

- Kemudian lakukan perhitungan plaintext dimana $P = C - k \text{ mod } 26$. Jika hasilnya minus(-) maka akan terus ditambah 26 sampai hasilnya positif (+) kemudian dihitung modulonya dan cek pada tabel 1 alphabet dari nilai plaintext yang dihasilkan.

$Pt_1 = (Cp_1 - k) \text{ modulo } 26$
 $= (X - 12) \text{ modulo } 26$
 $= (23 - 12) \text{ modulo } 26$
 $= (11) \text{ modulo } 26$
 $= 11$
 $= L$
 $Pt_2 = (Cp_2 - k) \text{ modulo } 26$
 $= (A - 12) \text{ modulo } 26$
 $= (0 - 12) \text{ modulo } 26$
 $= (-12) \text{ modulo } 26$
 $= -12 + 26 \text{ modulo } 26$
 $= 14 \text{ modulo } 26$
 $= 14$
 $= O$
 $Pt_3 = (Cp_3 - k) \text{ modulo } 26$
 $= (H - 12) \text{ modulo } 26$
 $= (7 - 12) \text{ modulo } 26$
 $= (-5) \text{ modulo } 26$
 $= -5 + 26 \text{ modulo } 26$
 $= 21 \text{ modulo } 26$
 $= 21$
 $= V$
 $Pt_4 = (Cp_4 - k) \text{ modulo } 26$
 $= (Q - 12) \text{ modulo } 26$
 $= (16 - 12) \text{ modulo } 26$
 $= (4) \text{ modulo } 26$
 $= 4$
 $= E$

Maka didapatkan plaintext dari ciphertext "XHAQ" adalah **LOVE**.

B. Pseudocode Caesar Cipher dan Transposisi Cipher

Pseudocode yang dibuat dalam enkripsi dan deskripsi adalah

1. *Pseudocode Caesar Cipher*
for \$a1=0 to length(\$p_text)
begin
 $\$z1[\$a1] = \$angka[\$a1] + \$b1;$
 $\$hasil[\$a1] = \text{modulo}(\$z1[\$a1], \$N);$
end
2. *Pseudocode Transposisi Cipher*
 $\$x = 0;$
 $\$y = 0;$
for \$a1=0 to length(\$p_text)

```

begin
  $z[$x][$y] = $hasil[$a];
  if $y < $b-1
  begin
    $y = $y+1;
  end
else
  begin
    $y = 0;
    $x = $x+1;
  end
end

```

3. *Pseudocode Fungsi Modulo*
function modulo(\$i,\$j)
begin
 if \$i < 0
 begin
 return \$j-(abs(\$i) % \$j);
 end
 else
 begin
 return \$i % \$j;
 end
end

C. Tampilan Program

1. Tampilan Enkripsi

Pada tampilan enkripsi terdapat 2 tampilan yaitu tampilan form data enkripsi dan tampilan hasil enkripsi.

CAESAR dan TRANSPOSISI CIPHER

Safrina Amanah Sitepu

Gambar 2 Tampilan Pada Form Data Enkripsi

IV. KESIMPULAN

Proses penyandian dengan algoritma *Caesar Cipher* dan *Tranposisi Cipher* berhasil digunakan untuk menyembunyikan pesan dan dapat mengembalikan pesan tersebut seperti semula. Program hanya dapat memproses karakter A hingga Z dikarenakan penggunaan angka 26. Karakter akan dihapus jika karakter bukan A hingga Z.

Enkripsi dari 'LOVE'

PlainText	P	E(P)= P+k	C=E(P)mod 26	CipherText
L	11	23	23	X
O	14	26	0	A
V	21	33	7	H
E	4	16	16	Q

X A
H Q

Maka ciphertextnya adalah:
'X H A Q'

Gambar 3 Tampilan Hasil Enkripsi

2. Tampilan Hasil Deskripsi
Pada tampilan enkripsi terdapat 2 tampilan yaitu tampilan form data deskripsi dan tampilan hasil deskripsi.

CAESAR dan TRANSPOSISI CIPHER

Safrina Amanah Sitepu

Deskripsi

X H A Q

12

2

Submit

Gambar 4 Tampilan Pada Form Data Deskripsi

Deskripsi dari : 'XHAQ'

X A
H Q

CipherText	C	D(C) = C-k	P=D(C)mod 26	PlainText
X	23	11	11	L
H	7	-12	14	O
A	0	-5	21	V
Q	16	4	4	E

Maka ciphertextnya adalah:
'LOVE'

Gambar 5 Tampilan Pada Hasil Deskripsi

REFERENSI

- [1] Rachmawati, D., Candra, A. 2015. Implementasi Kombinasi *Caesar* dan *Affine Cipher* untuk Keamanan Data Teks. Jurnal Edukasi dan Penelitian Informatika (JEPIN). Volume 1, No. 2 : 60-63.
- [2] Nasution, A.B. 2018. *Image Steganography In Securing Sound File Using Arithmetic Coding Algorithm, Triple Data Encryption Standard (3DES) and Modified Least Significant Bit (MLSB)*, *International Conference on Mechanical, Electronics, Computer, and Industrial Technology (MECnIT)*, April 2018.
- [3] Basuki, Armaja.2016. Aplikasi Kriptografi Berlapis Menggunakan Algoritma Tansposisi, *Vigenere* dan Blok Cipher Berbasis *Mobile*. Seminar Nasional Teknologi Informasi dan Multimedia 2016, Februari 2016 : 31-35.
- [4] Gurning, R.R.A. 2014. Perancangan Aplikasi Pengamanan Pesan Dengan Algoritma *Caesar Cipher*. Pelita Informatika Budi Darma, Volume: VI, Nomor: 3, April 2014: 106-110.
- [5] Zuli, F., Irawan, A. 2014. Penerapan Kombinasi *Caesar* dan *Vigenere* Untuk Pengamanan Data Pesan Pada Surat Elektronik. Studi Informatika: Jurnal Sistem Informasi. 7(2), 2014 : 1-11.
- [6] Septiarini, A., Hamdani. 2011. Sistem Kriptografi Untuk *Text Message* Menggunakan *Affine*. Jurnal Informatika Mulawarman. Vol. 6, No.1, Februari 2011: 50-53.
- [7] Seftyanto, Donny. 2012. Peran Algoritma *Caesar Cipher* Dalam Membangun Karakter Akan Kesadaran Keamanan Informasi. Seminar Nasional Matematika dan Pendidikan Matematika FMIPA UNY. November 2012 : MP 883-890
- [8] Rahima. 2014. Implementasi Penyembunyian dan Penyandian Pesan Pada Citra Menggunakan Algoritma *Affine Cipher* dan Metode *Least Significant Bit*. Pelita

Informatika Budi Darma, Volume: VI,
Nomor: 1, Maret 2014: 144-148.

- [9] Candra, Duwi. 2016. Aplikasi Enkripsi dan Deskripsi Menggunakan Metode Transposisi Berbasis Web. Seminar Nasional Universitas PGRI Yogyakarta. Hal : 29-36.