IMPLEMENTASI KRIPTOGRAFI DENGAN ALGORITMA CEASAR CIPHER UNTUK KEAMANAN DATA MICROSOFT OFFICE WORD DAN EXCEL

Tomy Satria Alasi[1]
[1]STMIK Logika, Teknik Informatika
[1]Jl. Yos Sudarso, Medan
email : tomysatriaalasi@live.com

Abstract

Data Microsoft office Word adalah data pengolahan perkantoran yang mudah dan sederhana. Microsoft office excel adalah jenis data paling sering digunakan oleh pengguna komputer untuk pengolahan data. Keamanan data perlu diterapkan kepada kedua jenis data tersebut agar terhindar dari hal-hal yang merugikan seperti penyalahgunaan data. Kriftogarafi dapat mengamankan data berdasarkan aturan sehingga data tidak mudah dibaca oleh pihak yang tidak berkepentingan. Salah satu dari kriftografi adalah algoritma caesar cipher yaitu teknik perpindahan nilai data untuk pergantian paling sederhana. Kemanan data microsoft office word dan excel dapat diimplementasikan dengan caesar cipher. Dengan menyimpan dokumen dengan sistem enkripsi dan deskripsi. Teknik Kemanan data dengan teknik lompatan perpindahan kunci berdasarkan keputusan pengguna dengan memanfaatkan kode ascii. Kemanan file ms word dan excel menggunakan aplikasi visual studio 2019.

Keywords: *Keamanan Data, Microsoft Office Word, Microsoft Office Excel, Algoritma Caesar Cipher*

1. PENDAHULUAN

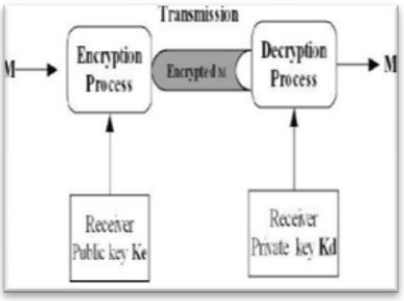
Penelitian ini menghasilkan keamanan data *microsoft office word* dan *microsoft excel* dengan algoritma caesar cipher. Setiap pengguna komputer memiliki data berupa *office word* dan *microsoft excel*. *Microsoft office word* adalah aplikasi pengolah kata yang sangat populer pada saat ini, dengan aplikasi tersebut dapat memudahkan kerja manusia dalam melakukan pengetikan surat maupun dokumen lain[1]. Sedangkan *microsoft office excel* adalah perangkat lunak yang menyediakan pengolahan akuntansi dan dapat dijadikan gambar sebagai penyajian informasi[2]. kriptografi adalah salah satu algoritma kemananan data informasi yang dimana berkerja menjadikan data menjadi kode yang rumit dan susah dipahami untuk mencegah pencurian pesan,dan ketika data tersebut dibutuhkan oleh pemilik atau yang berhak menerima maka kode tersebut akan kembali ke bentuk semula atau istilah lainnya adalah enkripsi sedangkan pengembalian kode ke pesan disebut dekripsi[3]. Algoritma caesar *cipher* adalah salah satu jenis metode substitusi dalam kriptografi, juga dikenal sebagai sandi caesar, sandi *shift*, kode caesar, atau pergeseran caesar, adalah salah satu teknik enkripsi paling sederhana dan paling dikenal luas[4]. Aplikasi dibangun menggunakan visual studio 2019 dengan memanfaatkan data *microsoft office word* dan data *microsoft office excel* yang diuji dan di enkripsi dan di deskripsi oleh pemilik data kemudian disimpan kembali dalam file yang tersebut.

2. METODE PENELITIAN

2.1 Kriptografi

Kriptografi adalah teknik untuk membuat informasi tidak dapat dibaca oleh pengguna yang tidak berwenang dengan ilmu menulis dalam kode rahasia. Tujuan dari kriptografi adalah untuk mencapai integritas, kerahasiaan dan keaslian semua sumber daya informasi[4]. Dua teknik utama yang digunakan dalam enkripsi adalah enkripsi simetris dan asimetris. Dalam enkripsi simetris, dua pihak berbagi kunci enkripsi-dekripsi tunggal. Pengirim mengenkripsi [1] pesan asli (P), yang disebut sebagai teks biasa, menggunakan kunci (K) untuk menghasilkan tidak dipahami orang umum yang tampaknya acak, disebut sebagai teks sandi (C), C = Encrypt (K, P) Setelah teks

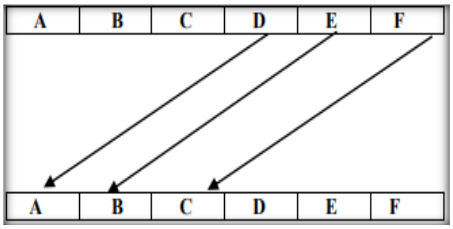
sandi diproduksi, teks tersebut dapat ditransmisikan. Setelah diterima, teks sandi dapat ditransformasikan kembali ke teks biasa dengan menggunakan algoritma dekripsi dan kunci yang sama yang digunakan untuk enkripsi, yang dapat dinyatakan sebagai berikut: P = *Decrypt* (K, C). Dalam enkripsi asimetris, dua kunci digunakan, satu kunci untuk enkripsi dan satu lagi kunci untuk dekripsi. Panjang kunci kriptografi hampir selalu diukur dalam bit. Semakin banyak bit yang memungkinkan algoritma kriptografi tertentu dalam kunci, semakin banyak kunci yang mungkin dan semakin aman algoritma menjadi. Rekomendasi ukuran kunci berikut harus dipertimbangkan ketika meninjau perlindungan. Suatu sistem yang menyediakan enkripsi dan dekripsi yang disebut sebagai *cryptosystem* dan dapat dibuat melalui komponen perangkat keras atau kode program dalam suatu aplikasi. Algoritma cryptosystem yang paling adalah rumus matematika kompleks yang diterapkan dalam urutan tertentu ke teks. Sebagian besar metode enkripsi menggunakan nilai rahasia yang disebut kunci (biasanya string panjang bit), yang bekerja dengan algoritma untuk mengenkripsi dan mendekripsi teks. Dalam semua kasus, data awal yang tidak terenkripsi disebut sebagai plaintext. Itu dienkripsi menjadi teks sandi, yang pada gilirannya (biasanya) akan didekripsi menjadi teks biasa yang dapat digunakan.



Gambar 1. **Ilustrasi Keamanan Data**

2.2 Algortima Caesar Cipher

Algoritma *cipher* caesar adalah salah satu jenis metode substitusi yang paling sederhana. Dalam kriptografi, sandi Caesar, juga dikenal sebagai sandi caesar, sandi *shift*, kode Caesar, atau pergeseran Caesar, adalah salah satu teknik enkripsi paling sederhana dan paling dikenal luas. Ini adalah jenis sandi pengganti di mana setiap huruf dalam *plaintext* digantikan oleh huruf beberapa posisi tetap di bawah alfabet. Misalnya, dengan shift kiri 3, D akan digantikan oleh A; E akan menjadi B, dan seterusnya. Metode ini dinamai setelah Julius Caesar, yang menggunakannya dalam korespondensi pribadinya[4].



Gambar 2. **Ilustrasi Enkripsi Caesar Cipher**

Tindakan cipher ceasar adalah untuk mengganti setiap huruf teks biasa dengan satu jumlah tetap tempat di bawah alfabet. Dalam diagram di atas, bergeser ke kiri dari tiga, sehingga E dalam *plaintext* menjadi B dalam teks sandi. Transformasi dapat direpresentasikan dengan menyelaraskan dua huruf; alfabet sandi adalah alfabet biasa yang diputar ke kiri atau kanan oleh sejumlah posisi. Misalnya, *cipher* Caesar menggunakan rotasi kiri tiga tempat, setara dengan pergeseran kanan 23 (parameter shift digunakan sebagai kunci): Saat mengenkripsi, seseorang mencari setiap huruf dari pesan di baris "biasa" dan menuliskan huruf yang sesuai di baris "sandi". Penguraian dilakukan secara terbalik, dengan pergeseran kanan 3. Enkripsi juga dapat direpresentasikan dengan menggunakan aritmatika modular dengan terlebih dahulu mengubah huruf menjadi angka, sesuai dengan skema, A → 0, B → 1, ..., Z → 25.

3. HASIL DAN PEMBAHASAN

Microsoft office word adalah aplikasi pengolahan kantor untuk menulis dokumen. *Microsoft office excel* adalah jenis data dokumen sangat populer oleh semua kalangan, disetiap kantor baik swasta maupun pemerintah untuk pengolahan data sederhana sampai besar. Tahapan untuk mengamankan jenis-jenis *file* tersebut adalah dengan mengetahui jenis file dan membuka file kemudian memproses file tersebut kemudian dilakukan sebuah teknik persandian klasik dengan caesar *cipher*. Teknik shift adalah teknik perpindahan (subtitusi) suatu huruf menjadi huruf pada daftar alfabet menjadi kunci. Seperti dilih K=4 (ganti dengan jenis ke-4 ke kanan) maka “A” menjadi “E”, “B”

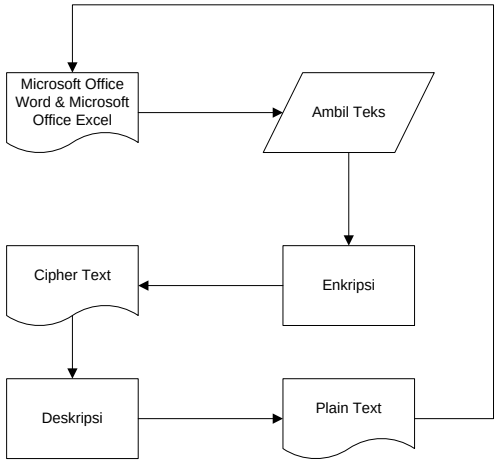
menjadi “F”, “Z” menjadi “D”dan seturusnya. Mengamankan *file word* dan *excel* dapat dengan memanfaatkan algoritma caesar cipher. Enkripsi huruf x dengan shift n dapat digambarkan secara matematis sebagai,

$$E_n(x)=(x+n) \bmod 26 \quad (1)$$

Dekripsi dilakukan dengan cara yang sama,

$$D_n(x)=(x-n) \bmod 26 \quad (2)$$

Ada definisi yang berbeda untuk operasi modulo . Pada contoh di atas, hasilnya adalah dalam kisaran 0 hingga 25; yaitu, jika x + n atau x - n tidak berada dalam kisaran 0 hingga 25, kita harus mengurangi atau menambahkan 26 .) Penggantian tetap sama di seluruh data, sehingga sandi diklasifikasikan sebagai jenis substitusi *monoalphabetic* , sebagai lawan dari substitusi *polyalphabetic* .



Gambar 3. Proses Keamanan Microsoft Office Word dan Microsoft Office Excel

3.1. Enkripsi

Enkripsi caesar *cipher* yaitu mengambil nilai *ascii* pada sebuah *pattern* atau isi data pada MS *word* dan *excel* kemudian melakukan tambah perpindahan sebanyak karakter, pada perpindahan dapat dilakukan bebas.

Rumus : $E_n(x)=(x+n) \bmod 26$.

Menghasilkan kata “Logika” Menjadi “Pskmoe” dengan perpindahan sebanyak 4 karakter.

Tabel 1. Hasil Enkripsi

Plain	Ascii	Ascii + 4	Cipher
L	76	80	P
o	111	115	s
g	103	107	k
i	105	109	m
k	107	111	o
a	97	101	e

3.2. Deskripsi

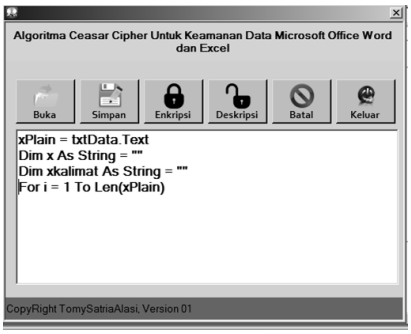
Deskrispi caesar cipher adalah mengambil nilai *ascii* pada *cipher* kemudian melakukan kurang pememindahan data sebanya karakter kunci, kunci tersebut hanya dapat diketuhaui oleh pengguna. Rumus : $E_n(x)=(x-n) \bmod 26$. Menghasilkan “Pskmoe” menjadi “Logika” dengan perpindahan 4 karakter.

Tabel 2. Hasil Deskripsi

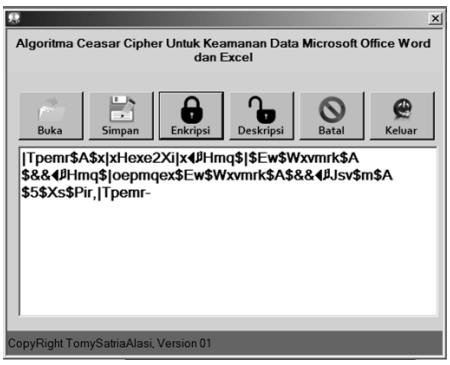
Plain	Ascii	Ascii - 4	Cipher
P	80	76	L
s	115	111	o
k	107	103	g
m	109	105	i
o	111	107	k
e	101	97	a

3.3. Implementasi

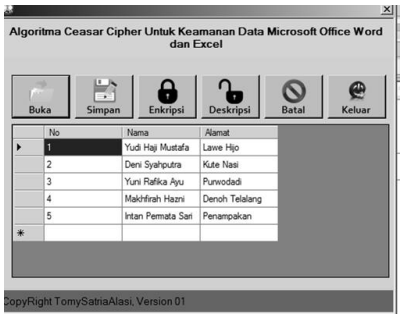
Pada implementasi menghasilkan proses keamanan data *microsoft office word* dan *microsoft office excel* dengan menggunakan aplikasi yang telah dibuat dengan visual studio 2019 menerapkan kriptografi dengan algoritma caesar cipher.



Gambar 6. Buka Document Word



Gambar 5. Hasil Enkripsi dan Deskrispi Dokumen Word



Gambar 7. Enkripsi Dan Deskripsi Dokumen Excel

4. KESIMPULAN

1. Kemanan data microsoft office word dan excel dapat diimplementasikan dengan caesar cipher. Dengan menyimpan dokumen dengan sistem enkripsi dan deskripsi.
2. Teknik Kemanan data dengan teknik lompatan perpindahan kunci berdasarkan keputusan pengguna dengan memanfaatkan kode ascii.
3. Kemanan file ms word dan excel menggunakan aplikasi visual studio 2019 dengan mengambil nilai teks pada kedua jenis file.

5. REFERENSI

[1] D. Nugrahenny, H. Wintolo, A. Kusumaningrum, S. Sudaryanto, and H. Sajati, “Pendampingan Pengenalan Metode Pengetikan Cepat Menggunakan Microsoft Word Bagi Siswa Kelas 5 SD IT Salsabila Al Muthi[illegible]in Yogyakarta,” *KACANEGARA J. Pengabdi. pada Masy.*, vol. 2, no. 1, pp. 21–28, 2019.

[2] S. Romlah, N. Nugraha, and W. Setiawan, “Analisis Motivasi Belajar Siswa SD Albarokah 448 Bandung dengan Menggunakan Media ICT Berbasis For VBA Excel Pada Materi Garis Bilangan,” *J. Cendekia J. Pendidik. Mat.*, vol. 3, no. 1, pp. 220–226, 2019.

[3] F. Efendi and N. P. Dewanti, “Implementasi Kriptografi dalam Sistem Keamanan Anjungan Tunai Mandiri,” *J. Inform. Upgris*, vol. 5, no. 1, 2019.

[4] J. Singh and S. S. Yadav, “Implementation of Caesar Cipher and Chaotic Neural network by using MATLAB Simulator,” *Int. J. Recent Dev. Eng. Technol. ISSN*, pp. 2347–6435.