

# KOMBINASI ALGORITMA EXACT MATCHING DAN OPERASI XOR PADA TEKS

Monalisa Febryanti Simanjuntak<sup>1</sup>, Garuda Ginting<sup>1</sup>, Taroni Sokhi Zebua<sup>1</sup>

Prodi Teknik Informatika STMIK Budi Darma, Medan, Indonesia  
Jl. Sisingamangaraja No. 338, Medan, Indonesia

## Abstrak

Teks adalah hasil pengamatan atau observasi, oleh sebab itu informasi yang digunakan untuk menjabarkan suatu benda atau objek harus jelas, sesuai dengan data dan fakta yang ada pada objek tersebut. Teks memiliki tujuan, yakni memberi penjelasan yang utuh kepada pembacanya supaya mereka dapat memahami apa yang sedang dibicarakan dengan jelas, entah dalam hal bentuk fisik ataupun wujud yang abstrak seperti sikap, rasa dan lain sebagainya. Exact String matching merupakan sebuah metode pencocokan karakter dari sebuah masukkan dengan kata atau kalimat yang memiliki kesamaan baik karakter maupun kata. exact string matching digunakan untuk mencocokkan string yang masukkannya dari aktifitas keyboard dan membandingkan dengan string yang dikenali oleh sistem keylogger untuk direkam aktifitasnya, pada proses ini string yang direkam tidak diamankan sehingga hasil keylogger bisa dibaca oleh siapa saja jika mengetahui lokasi file keylogger berada, untuk itu perlu ditambahkan fungsi keamanan dalam hal ini menggunakan fungsi XOR sehingga hasilnya masih bisa dibaca oleh orang awam. Fungsi XOR bertujuan untuk menghasilkan nilai logika TRUE (benar) jika salah satu dari pernyataan benar, dan menghasilkan nilai logika FALSE (salah) jika kedua pernyataan salah atau kedua pernyataan tersebut benar. Unified Modelling Language (UML) adalah suatu alat untuk memvisualisasikan dan mendokumentasikan hasil analisa dan desain yang berisi sintak dalam memodelkan sistem secara visual. Juga merupakan satu kumpulan konvensi pemodelan yang digunakan untuk menentukan atau menggambarkan sebuah sistem software yang terkait dengan objek. Microsoft Visual Basic.Net 2008 adalah salah satu program berorientasi objek yang diproduksi oleh Microsoft Corporation. Pada penelitian ini, algoritma XOR diimplementasikan pada teks hasil rekam dari keylogger. Sehingga hasil rekaman dari keylogger tidak dapat terbaca oleh siapapun karena hasilnya telah dienkripsi atau sudah menjadi cipher teks. Dan untuk proses dekripsi terhadap enkripsi hasil perekaman dari keylogger hanya dapat dilakukan oleh penginstall keylogger. Sehingga setelah dienkripsi, hasil rekaman dari keylogger akan kembali ke plainteks dan dapat kembali dibaca.

Kata Kunci : Teks, Exact String matching, Visual Basic 2008

## I. PENDAHULUAN

Perkembangan teknologi yang sangat cepat terutama di bidang teknologi internet yang setiap saat mengalami perubahan signifikan, tidak lepas dari peranan atau keterlibatan dunia sehingga internet dewasa ini menjadi jendela dunia di dalam mengakses informasi yang dapat digunakan oleh umat manusia di seluruh dunia. Internet pun menjadi media dalam melakukan transaksi bisnis, diskusi, belajar secara *online*, dan lain sebagainya. Perkembangan *software* keamanan telah mendominasi beberapa tahun terakhir dengan memanfaatkan kemajuan teknologi informasi. Banyak faktor pendukung untuk mencapai tujuan atau konsep teknologi pendidikan, diantaranya perkembangan teknologi informasi yang semakin cepat sehingga dapat menghasilkan perangkat lunak dan keras, perkembangan tersebut juga didukung oleh kemampuan sumber daya manusia yang semakin baik.

Keamanan merupakan hal yang sangat penting di dalam sebuah sistem operasi, banyak sekarang *vendor software* yang menyediakan *software* antivirus dan *software* proteksi lainnya sehingga komputer bebas dari ancaman ataupun dari tindakan yang tidak diinginkan seperti *phising*, *malware*, *keylogger* dan lainnya.

*Teks* memiliki tujuan, yakni memberi penjelasan yang utuh kepada pembacanya supaya mereka dapat memahami apa yang sedang dibicarakan dengan jelas, entah dalam hal bentuk fisik ataupun wujud yang abstrak seperti sikap, rasa dan lain sebagainya. *Teks dideskripsikan* juga sebagai hasil pengamatan atau observasi, oleh sebab itu informasi yang digunakan untuk

menjabarkan suatu benda atau objek harus jelas, sesuai dengan data dan fakta yang ada pada objek tersebut

*Exact String matching* merupakan sebuah metode pencocokan karakter dari sebuah masukkan dengan kata atau kalimat yang memiliki kesamaan baik karakter maupun kata[2], pada penelitian ini metode *exact string matching* digunakan untuk mencocokkan *string* yang masukkannya dari aktifitas *keyboard* dan membandingkan dengan *string* untuk itu perlu ditambahkan fungsi keamanan dalam hal ini menggunakan fungsi XOR sehingga hasilnya masih bisa dibaca oleh orang awam.

Kombinasi operasi XOR dan *Exact String Matching* dilakukan secara *simultan* dimana ketika proses pengetikan dilakukan maka hasil kinerja komputer akan diamankan secara langsung dengan operasi XOR sehingga hasil *log* pada teks sudah dalam bentuk *ciphertext*, konsep kombinasi di sini adalah pengetikan. hasil deteksi dengan algoritma *exact string matching* diamankan dengan operasi XOR.

## II. TEORITIS

### A. Kriptografi

Kriptografi berasal dari bahasa Yunani. Menurut bahasa tersebut kata "kriptografi" dibagi menjadi dua, yaitu kripto dan graphia. Kripto berarti secret (rahasia) dan graphia berarti writing (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain [4].

Kriptografi merupakan seni dan ilmu untuk menjaga keamanan data dengan metode tertentu, dan pelakunya disebut cryptographer. Kriptografi disebut sebagai ilmu karena didalamnya terdapat metode (rumusan) yang digunakan, dan dikatakan sebagai seni karena karena dalam membuat suatu teknik kriptografi itu sendiri merupakan ciri tersendiri dari si pembuat dan memerlukan teknik khusus dalam mendisainnya[4]. Sedangkan cryptanalysis adalah suatu ilmu dan seni memecahkan ciphertext menjadi plaintext tanpa melalui cara yang seharusnya dan orang yang melakukannya disebut cryptanalyst[4]

### B. Operasi XOR

XOR berasal dari kata Exclusive OR. Fungsi ini akan memberikan keluaran 1 jika masukan-masukannya mempunyai keadaan yang berbeda. Fungsi XOR bertujuan untuk menghasilkan nilai logika TRUE (benar) jika salah satu dari pernyataan benar, dan menghasilkan nilai logika FALSE (salah) jika kedua pernyataan salah atau kedua pernyataan tersebut benar[6].

Dalam kriptografi, pembuatan chiper (teks hasil enkripsi) melalui operasi XOR merupakan suatu algoritma enkripsi yang relatif sederhana. Teknik ini beroperasi sesuai dengan prinsip[6] :

$$A \text{ XOR } 0 = A,$$

$$A \text{ XOR } A = 0,$$

$$(B \text{ XOR } A) \text{ XOR } A = B \text{ XOR } 0 = B,$$

### C. Algoritma Exact String Matching

*Exact Match* merupakan tahapan dilakukan untuk mengecek ketepatan kata jika ketemusama maka kata tersebut tepat dan jika tidak ketemu sama maka kata tersebut *Not Match*, sedangkan *Flag* merupakan penanda apabila benar diberi *flag* tanda 1 (*true exact Match*) jika tidak benar maka diberi *flag* /tanda 0 (*not match*) di dalam pembuatannya *flag* 0 tidak disertakan karena akan menambah banyak penyimpanan. Proses selanjutnya adalah hitungan similary menjumlahkan semua *flag* yang bernilai 1 (*true*) yang berasal dari *flag* 1 dari *indeks* 1 dan juga menjumlahkan *flag* 2 dari indeks 2. Hasil penjumlahan tersebut diambil nilai yang terkecil[2].

Flag 1	Flag 2	Hasil
1	0	0
1	1	1
0	1	0

## III. ANALISA

### A. Analisa Masalah

Teks merupakan hasil pengamatan atau observasi, oleh sebab itu informasi yang digunakan untuk menjabarkan suatu benda atau objek harus jelas, sesuai dengan data dan fakta yang ada pada objek tersebut. Pada penelitian ini, algoritma exact string matching sebagai metode pencocokan karakter digunakan untuk memeriksa input pada keyboard yang terhubung dengan perangkat komputer yang digunakan oleh user, Namun teks masih memiliki kelemahan yaitu hasil ketikan kalimatnya masih ada yang salah karna kinerjanya dikerjakan langsung oleh pengguna komputer. Sehingga hasil ketikan tersebut tidak lagi bersifat sempurna karena

sistem pengerjaannya dikerjakan secara manual. Untuk mengatasi kelemahan tersebut, maka dibutuhkan adanya pengamanan terhadap teks yang telah dikerjakan oleh pengguna komputer tersebut. Pada penelitian ini, algoritma XOR diimplementasikan pada teks. Sehingga hasil pengerjaan pada teks dapat terbaca oleh siapapun karena hasilnya telah dienkripsi atau sudah menjadi cipher teks. Dan untuk proses dekripsi terhadap enkripsi hasil pengetikan pada teks hanya dapat dilakukan oleh pengguna komputer. Sehingga setelah dienkripsi, hasil kinerja teks pada komputer akan kembali ke plaintexts dan dapat kembali dibaca.

Pencocokan string secara garis besar dibedakan menjadi dua yaitu *exact string matching* (pencocokan string secara tepat dengan susunan karakter dalam string yang dicocokkan) dan *inexact string matching* (pencocokan string secara samar, yaitu pencocokan string dimana string yang dicocokkan memiliki kemiripan namun keduanya memiliki susunan karakter yang berbeda). Salah satu algoritma pencocokan karakter adalah algoritma *exact string matching*. Algoritma ini membandingkan karakter per karakter sampai ditemukan karakter yang dicari dari awal string hingga akhir *string*. Berikut ini contoh kasus pencocokan string dari algoritma *exact string matching*.

Misalkan diasumsikan sistem yang dirancang mengenali huruf Q, W, E, R, T, Y, U, I, O dan karakter yang diinput pada *keyboard* adalah (K) = R maka proses pencocokan dilakukan dengan membandingkan karakter sistem yang ada dengan karakter yang dimasukkan, berikut adalah prosesnya.

Langkah 1 :

Pencarian dimulai dari data elemen pertama pada baris data

↓

Data	Q	W	E	R	T	Y	U	I	O
Indeks	1	2	3	4	5	6	7	8	9

Pos = 8 ; K= R

I = 1 ; Ketemu = False

While (I <= Pos) And Not (False) → True

If (K <> chr(I)) then

I = 1 + 1 = 2

Data tidak ditemukan dan data yang dicari (K) lebih besar daripada data elemen pertama pada baris data maka proses pencarian dilanjutkan ke data elemen kedua pada baris data.

Langkah 2:

↓

Data	Q	W	E	R	T	Y	U	I	O
Indeks	1	2	3	4	5	6	7	8	9

Pos = 8 ; K= E

I = 2 ; Ketemu = False

While (I <= Pos) And Not (False) → True

If (K <> chr(I)) then

I = 2 + 1 = 3

Data masih belum ditemukan dan data yang dicari (K) lebih besar daripada data elemen kedua pada baris data,

maka proses pencarian dilanjutkan ke data elemen ketiga pada baris data.

Langkah 3:

Data	Q	W	E	R	T	Y	U	I	O
Indeks	1	2	3	4	5	6	7	8	9

Pos = 8 ; K= E  
 I = 2 ; Ketemu = *False*  
 While (I <= Pos) And Not (*False*) → *True*  
 If (K <> chr(I)) then  
 I = 3 + 1 = 4

Data masih belum ditemukan dan data yang dicari (K) lebih besar daripada data elemen ketiga pada baris data, maka proses pencarian dilanjutkan ke data elemen keempat pada baris data.

Langkah 4:

Data	Q	W	E	R	T	Y	U	I	O
Indeks	1	2	3	4	5	6	7	8	9

While (I <= Pos) And Not (*False*) → *True*  
 If (K = chr(I)) then  
 Ketemu = *True*  
 While (I <= Pos) And Not (*False*) → *False*  
 If (*True*) then  
 Proses rekaman karakter *string*.

Data ditemukan pada posisi indeks keempat dari baris data dan pencocokan sukses untuk karakter "R".

Algoritma XOR pada prinsipnya sama seperti algoritma kriptografi lainnya yaitu *vigenere cipher* dengan penggunaan kunci yang berulang secara periodik. Berikut ini adalah proses enkripsi dan dekripsi dari algoritma XOR:

Plain teks = MAHASISWA  
 Kunci = 11110011 = s

Penyelesaian :

Proses enkripsi menggunakan rumus berikut:

$$C = P \oplus K$$

Dimana : C = *Cipher* teks,  
 P = *Plain* teks,  
 K = *Key* (Kunci)

1. Konversi setiap karakter aatau string kedalam format ASCII 8 bit

Tabel 1. Proses konversi *plain* teks kedalam kode ASCII 8 bit

Plainteks	ASCII 8 Bit
M	01001101
A	01000001
H	01001000
A	01000001
S	01010011
I	01001001
S	01010011
W	01010111
A	01000001

2. Lakukan operasi XOR antara *plain* teks dengan kunci (*Key*)

Tabel 2.

Proses perhitungan XOR antara *Plain* teks dan Kunci

Plain teks	Konversi kedalam ASCII 8 Bit	Kunci	Cipher teks	Konversi kedalam Simbol
M	01001101	01110011 (s)	00111110	>
A	01000001		00110010	2
H	01001000		00110010	;
A	01000001		00110010	2
S	01010011		00100000	
I	01001001		00111010	:
S	01010011		00100000	
W	01010111		00100100	\$
A	01000001		00110010	2

Plain teks = MAHASISWA

Kunci = 11110011 = s

Cipher teks = 00111110 00110010 00110010 00110010 00100000 00111010 00100000 00100100 00110010

Untuk lebih memperkuat enkripsi, *cipher* rteks dikonversi kedalam simbol ASCII. Sehingga *cipher* teks menjadi: >2;2 : \$

Proses dekripsi menggunakan rumus berikut:

$$P = C \oplus K$$

Dimana : P = *Plain* teks,  
 C = *Cipher* teks,  
 K = *Key* (Kunci)

Tabel 3.

Proses konversi *cipher* teks menjadi *plain* teks

Cipher teks	Konversi kedalam ASCII 8 Bit	Kunci	Plain teks	Konversi kedalam Simbol
>	00111110	01110011 (s)	01001101	M
2	00110010		01000001	A
;	00110010		01001000	H
2	00110010		01000001	A
	00100000		01010011	S
:	00111010		01001001	I
	00100000		01010011	S
\$	00100100		01010111	W
2	00110010		01000001	A

#### IV. IMPLEMENTASI

Tampilan program merupakan *interface* antara *user* dengan aplikasi *keylogger* yang telah dibuat. Tampilan awal aplikasi yang telah dibuat terdiri dari tampilan menu utama yang berfungsi untuk memberi *user* kesempatan memilih *searching* atau *exit*.

Tampilan menu utama dapat dikatakan sebagai antar muka (*user interface*) antara *user* dengan aplikasi.

Menu utama menampilkan pilihan menu yang tersedia pada aplikasi. Pada menu utama tersedia 2 (dua) pilihan menu yaitu *Start* dan *Exit*. Adapun *screenshot* gambar untuk tampilan menu utama dapat dilihat pada gambar



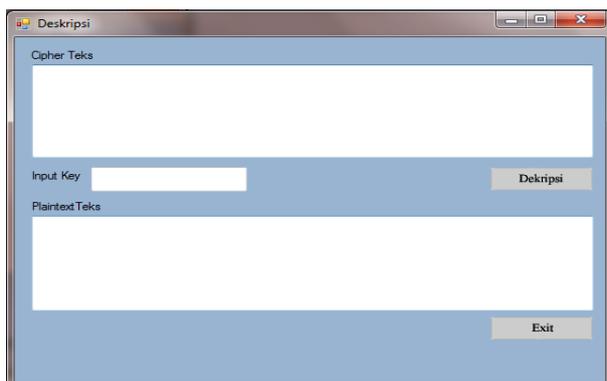
Gambar 1. Menu Utama

Tampilan Dekripsi merupakan satu kaidah upaya pengolahan data menjadi sesuatu yang dapat diutarakan secara jelas dan tepat dengan tujuan agar dapat dimengerti oleh orang yang tidak langsung mengalaminya sendiri, dalam keilmuan, Tampilan dekripsi diperlukan agar peneliti tidak melupakan pengalamannya dan agar pengalamannya tersebut dapat dibandingkan dengan pengalaman peneliti lain, sehingga mudah untuk dilakukan pemeriksaan dan kontrol terhadap dekripsi tersebut, Saat data yang dikumpulkan, Dekripsi analisis dan kesimpulannya lebih disajikan dalam angka-angka maka hal ini dinamakan penelitian kuantitatif, Sebaliknya apabila data deskripsi dan analisis kesimpulannya disajikan dalam uraian kata-kata maka dinamakan penelitian kualitatif, Adapun tampilan Dekripsi dapat dilihat pada gambar

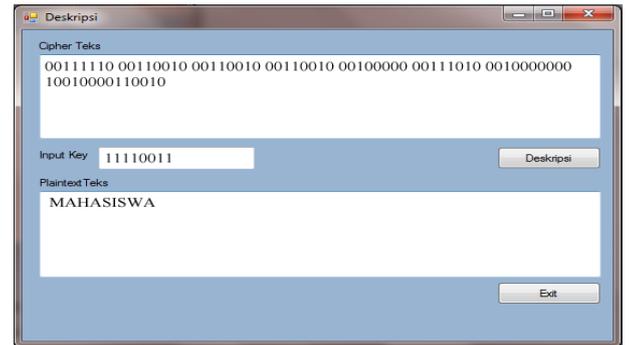


Gambar 2. Tampilan Form Dekripsi

Tampilan proses dekripsi merupakan tampilan yang disediakan untuk menampilkan proses pengembalian *chipper* teks menjadi *plain* teks. Adapun *screenshot* gambar untuk tampilan form dekripsi dapat dilihat pada gambar 3.



Gambar 3. Tampilan Form Dekripsi



Gambar 4. Tampilan Hasil Dekripsi

Hasil pengujian program merupakan tampilan yang telah dilakukan oleh *user*. Adapun hasil pengujian program dapat dilihat pada tabel 4. berikut ini :

Tabel 4. Hasil Pengujian

No	Nama	Keterangan	Fungsi
1	Simpan	Tombol	Menyimpan semua kegiatan pada <i>keyboard</i>
2	<i>Dekripsi</i>	Tombol	Melakukan dekripsi
3	<i>Input key</i>	Label Box	Pelabelan input key
4	<i>Plaint teks</i>	Label Box	Pelabelan dari plaint Teks
5	<i>Exit</i>	Tombol	Keluar dari tampilan

## V. KESIMPULAN

Berdasarkan hasil akhir pemecahan masalah maka penulis dapat menarik sebuah kesimpulan, dimana kesimpulan tersebut nanti dapat kiranya dapat berguna bagi pembaca, sehingga penulisan sikripsi ini dapat lebih berguna dan bermanfaat. Adapun kesimpulan-kesimpulan tersebut antara lain sebagai berikut :

1. Implementasi kombinasi algoritma Exact String Matching digunakan untuk mengetahui prosedur pengamanan hasil keylogger
2. Implementasi menerapkan kombinasi algoritma Exact String Matching pada proses keylogger dan operasi XOR tetapi berguna untuk mempersulit pihak-pihak yang menggunakan keylogger untuk mengetahui teks asli dari hasil perekaman.
3. Hasil Implementasi algoritma merancang dan membangun keylogger berdasarkan kombinasi Exact Mathing String dioperasi XOR berguna untuk memudahkan pengguna dalam mengamankan hasil keylogger

## REFERENCES

- [1] P. Tuli dan P. Sahu, "System Monitoring and Security Using Keylogger," *International Journal of Computer Science and Mobile Computing*, vol. 2, no. 3, pp. 106-111, 2013.

- [2] Heriyanto, "PENGUNAAN METODE EXACT MATCH UNTUK MENENTUKAN KEMIRIPAN NASKAH DOKUMEN TEKS," *TELEMATIKA*, vol. 8, no. 1, pp. 43-52, 2011.
- [3] H. Abdurachman dan E. Gunadhi, "KEAMANAN KOMUNIKASI DATA SMS PADA ANDROID DENGAN MENGGUNAKAN APLIKASI KRIPTOGRAFI ADVANCE ENCRYPTION STANDARD (AES)," *Jurnal Algoritma Sekolah Tinggi Teknologi Garut*, vol. 12, no. 1, pp. 1-6, 2015.
- [4] S. Kromodimoeljo, *TEORI & APLIKASI KRIPTOGRAFI*, Jakarta: SPK IT Consulting, 2010.
- [5] R. Sadikin, *Kriptografi untuk Keamanan Jaringan (+CD)*, Yogyakarta: Andi Publisher, 2012.
- [6] D. Rosmala dan R. Aprian, "IMPLEMENTASI MODE OPERASI CIPHER BLOCK CHAINING (CBC) PADA PENGAMANAN DATA," *JURNAL INFORMATIKA*, vol. 2, no. 3, pp. 55-66, 2012.
- [7] Haviluddin, "Memahami Penggunaan UML (Unified Modelling Language)," *Informatika Mulawarman*, vol. 6, no. 1, pp. 1-15, 2011.
- [8] Neti, "PERANCANGAN APLIKASI RENTAL MOBIL PADA CV KARYA BERSAMA PALEMBANG," *MDP*, pp. 1-10, 2008.
- [9] S. Tjiharjadi dan M. C. Wijaya, "PENGAMANAN DATA MENGGUNAKAN METODA ENKRIPSI EINSTEIN," dalam *Seminar Nasional Informatika*, Yogyakarta, 2009.