Optimalisasi Enkripsi Untuk Proses Pengamanan Data Menggunakan Algoritma *Vegenere*

Nonot Wisnu Karyanto[1)], Noven Indra Prasetya[2)]

[1,2)]Program Studi Teknik Informatika, Fakultas Teknik, Universitas Wijaya Kusuma Surabaya
Email : [1)] nonotwik@gmail.com, [2)] noven.ip@gmail.com

ABSTRAK

Proses pengamanan data sangat penting karena untuk menjaga integritas dan validitas data. Saat ini banyak cara dari pihak-pihak tertentu untuk melakukan serangan-serangan data dengan berbagai metode yang semakin berkembang. Seiring perkembangan teknologi yang sangat cepat maka proses penyerangan data juga semakin banyak dan canggih. Dari perkembangan serangan data yang beredar saat ini, peneliti melakukan penelitian untuk melakukan kajian sampai sejauh mana proses pengamanan data yang dilakukan oleh para pengelola data yang berhubungan dengan teknologi informasi, dan seberapa besar dampak yang diperoleh apabila terjadi serangan data tersebut. Algoritma *Vegenere* digunakan untuk mengkaji bagaimana proses pengamanan data yang dilakukan dalam algoritma tersebut dengan perkembangan teknologi sekarang ini.

Kata Kunci : Pengamanan Data, Validitas Data, Algoritma *Vegenere*

1. PENDAHULUAN

Masalah keamanan merupakan salah satu aspek penting pada sebuah sistem informasi. Teknologi informasi merupakan seperangkat alat yang dapat membantu pekerjaan berkaitan dengan informasi dan tugas-tugas pemrosesan informasi serta mendistribusikan informasi menggunakan sarana perangkat telekomunikasi. Teknologi komputer dan komunikasi merupakan sarana yang saling menunjang perkembangan teknologi.

Keterlibatan pekerjaan manusia dengan teknologi komputer membentuk suatu sistem yang bekerja sama untuk melakukan pengolahan informasi mulai pengumpulan, pengolahan, penyimpanan sampai dengan pengiriman informasi. Keterlibatan tersebut dikenal dengan Sistem Informasi. Sistem Informasi adalah kumpulan perangkat keras dan perangkat lunak yang dirancang untuk tujuan mentransformasikan data ke dalam bentuk informasi yang berguna (Bodnar dan Hopwood, 1993). Dengan kemajuan teknologi yang cepat, sistem informasi juga mengalami perkembangan.

Berdasarkan kondisi tersebut, penelitian ini bertujuan untuk mengetahui sejauh mana proses pengamanan data untuk menjaga tingkat integritas data dalam proses penyimpanan data sehingga dalam proses penyajian data dalam kondisi valid dan kredibel. Berkaitan dengan proses-proses tersebut, penelitian ini menggunakan algoritma *Vegenere* dalam proses pengamanannya dan menguji sampai sejauh mana proses pengamanan data akan berlangsung.

2. TINJAUAN PUSTAKA

2.1. Sistem Informasi

Sistem informasi adalah suatu kombinasi teratur apapun dari orang, perangkat keras, perangkat lunak, jaringan komputer dan komunikasi data, dan basis data yang mengumpulkan, mengubah dan menyebarkan informasi dalam suatu bentuk organisasi (O'Brien dan Marakas, 2005). Sistem informasi

merupakan komponen yang saling bekerja sama untuk mengumpulkan, mengolah, menyimpan dan menyebarkan informasi untuk mendukung pengambilan keputusan, koordinasi, pengendalian, analisis masalah dan visualisasi dalam sebuah organisasi (Laudon dan Laudon, 2010). Sistem informasi manajemen sebagai suatu sistem berbasis komputer yang menyediakan informasi bagi beberapa pemakai dengan kebutuhan yang relatif sama. Para pemakai membentuk suatu entitas organisasi formal perusahaan atau sub unit dibawahnya. Informasi menjelaskan perusahaan mengenai apa yang telah terjadi dimasa lalu, apa yang sedang terjadi sekarang dan apa yang mungkin terjadi dimasa datang. Informasi tersedia dalam bentuk laporan periodik, laporan khusus, dan *output* dari model matematika. Informasi digunakan oleh manajer atau non manajer dalam perusahaan saat mereka membuat keputusan untuk memecahkan masalah. (McLeod, 2001).

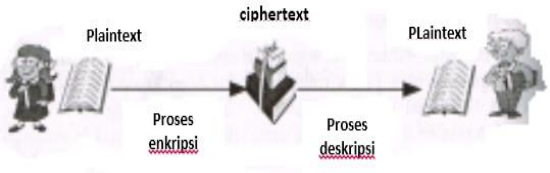
Dari definisi diatas dapat disimpulkan bahwa sistem informasi adalah kombinasi komponen yang terdiri dari *brainware*, *hardware*, *software*, *networking*, jaringan telekomunikasi dan data yang saling bekerja sama untuk mengumpulkan, mengolah, menyimpan, dan menyebarkan informasi untuk mendukung pengambilan keputusan, pengendalian, analisis masalah dan visualisasi dalam organisasi. Salah satu komponen pendukung sistem informasi adalah basis data (*database*). *Database* adalah kumpulan dari item data yang saling berhubungan satu dengan yang lainnya yang diorganisasikan berdasarkan sebuah skema atau struktur tertentu, tersimpan di *hardware* komputer dan *software* untuk melakukan manipulasi untuk kegunaan tertentu (Irmansyah, 2003).

2.2. Pengertian Enkripsi dan Dekripsi

Enkripsi merupakan proses yang sangat penting dalam kriptografi supaya keamanan data yang dikirimkan bisa terjaga kerahasiannya. Pesan asli (*plaintext*) diubah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan dengan *chipper* atau kode. Sama halnya dengan manusia yang tidak mengerti sebuah kata, manusia akan dapat melihatnya di dalam kamus atau daftar istilah-istilah. Berbeda dengan enkripsi, untuk mengubah *plaintext* ke bentuk *ciphertext*, maka harus menggunakan algoritma yang dapat mengkodekan data yang diinginkan (Ariyus, 2005).

Ariyus (2005) menjelaskan proses enkripsi dengan urutan terdiri dari *Plaintext* → Algoritma Enkripsi → *Ciphertext* → Algoritma Dekripsi → *Plaintext*.

Urutan proses tersebut dijelaskan dalam Gambar 1 berikut ini.



Gambar 2.1. Proses Enkripsi

Informasi asal yang dapat dimengerti disimbolkan oleh *plaintext*, kemudian oleh algoritma enkripsi diterjemahkan menjadi informasi yang tidak dapat dimengerti yang disimbolkan dengan *ciphertext*. Proses enkripsi terdiri dari algoritma dan kunci. Kunci biasanya merupakan suatu *string bit* yang pendek yang mengontrol algoritma. Algoritma enkripsi akan memberikan hasil yang berbeda tergantung pada kunci yang digunakan. Mengubah kunci dari enkripsi akan mengubah *output* dari algoritma enkripsi.

p-ISSN : 2502-5724; e-ISSN : 2541-5735

Sekali dihasilkan, *ciphertext* kemudian ditransmisikan. Pada bagian penerima, *ciphertext* yang diterima diubah kembali ke *plaintext* dengan algoritma dan kunci yang sama (Ariyus, 2005).

Sedangkan dekripsi merupakan kebalikan dari proses enkripsi, yaitu proses konversi data yang sudah dienkripsi (*ciphertext*) menjadi data aslinya (*original plaintext*) sehingga dapat dibaca atau dimengerti kembali.

Selanjutnya, pesan yang akan dienkripsi disebut *plaintext* dimisalkan *plaintext* (P), proses enkripsi dimisalkan enkripsi (E), proses dekripsi dimisalkan dekripsi (D), dan pesan yang sudah dienkripsi disebut *ciphertext* dimisalkan *ciphertext* (C).

2.3. Kriptografi

Kriptografi merupakan suatu strategi supaya data atau dokumen aman dari orang yang tidak berhak. Perkembangan bidang ilmu kriptografi diantaranya adalah substitusi.

Substitusi adalah proses penggantian setiap karakter dari *plaintext* dengan karakter lainnya. Ada empat istilah dari substitusi *cipher*, yaitu : *monoalphabet, polyalphabet, monograph,* dan *polygraph*. Substitusi *chipper* yang pertama kali dalam dunia persandian terjadi pada waktu pemerintahan Yulius Caesar dikenal dengan *Caesar Cipher*, yaitu dengan mengganti posisi huruf awal dari alphabet ditunjukkan dalam Tabel 1 sebagai berikut.

Tabel 1. Substitusi Caesar Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M
D	E	F	G	H	I	J	K	L	M	N	O	P

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	R	U	T	U	V	W	X	Y	Z	A	B	C

2.4. Algoritma Vegenere

Pada teknik substitusi Vegenere, setiap *chipertext* bisa memiliki banyak kemungkinan *plaintext*. Teknik dari substitusi Vigenere dapat dilakukan dengan dua cara yaitu angka dan huruf.

Sebagai contoh, teknik substitusi Vigenere dapat dilakukan menggunakan angka dalam menukarkan huruf dengan angka. Hal tersebut hampir sama dengan *Shift Chiper* ditunjukkan dalam Tabel 2.

Tabel 2. Substitusi Vegenere

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Dengan memiliki kunci 6 huruf CIPHER. Jika ditukar dengan angka, maka akan menjadi K = (2, 8, 15, 7, 4, 17). Sehingga plaintext-nya adalah "*This cryptosystem is not secure*" ditunjukkan dalam Tabel 3.

Tabel 3. Proses Vegenere

T	H	I	S	C	R	Y	P	T	O	S	Y	S	T
19	7	8	18	2	17	24	15	19	14	18	24	18	19
2	8	15	7	4	17	2	8	15	7	4	17	2	8

21, 15, 23, 25, 6, 8, 0, 23, 8, 21, 22, 15, 20, 1

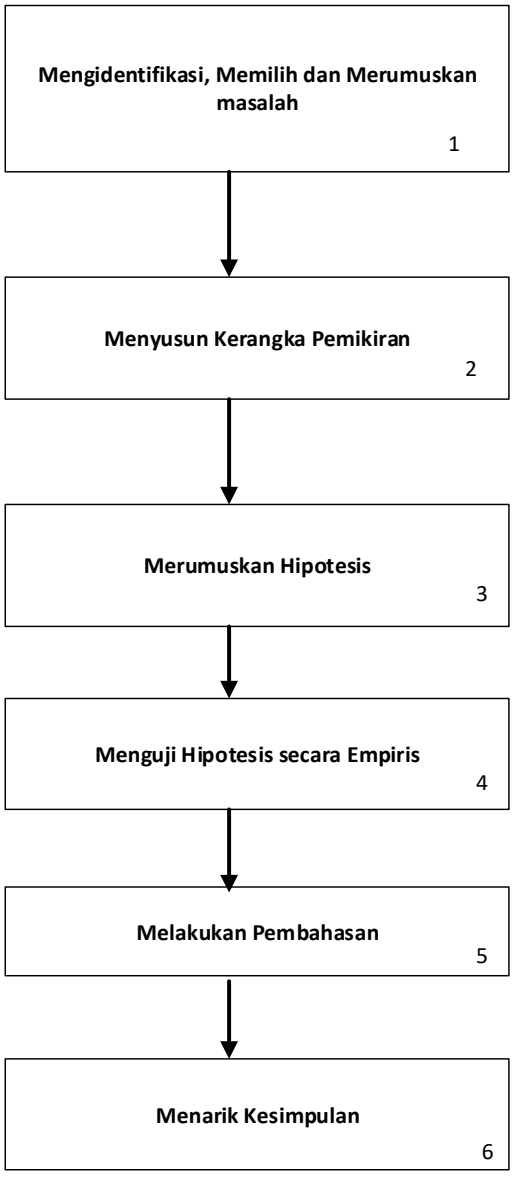
E	M	I	S	N	O	T	S	E	C	U	R	E
19	7	8	18	2	17	24	15	19	14	18	24	18
2	8	15	7	4	17	2	8	15	7	4	17	2

19, 19, 12, 9, 15, 22, 8, 25, 8, 19, 22, 25, 19

Plaintext : *This cryptosystem is not secure*
Kunci : (2, 8, 15, 7, 4, 17)
Ciphertext :
VPXZGIAXIVWPUBTTMJPWIZITWZT
Untuk dekripsi juga bisa menggunakan kunci yang sama dengan modulo 26.

3. METODE PENELITIAN

Bagian ini menjelaskan tahapan dan metode enkripsi dan dekripsi yang akan digunakan dalam penelitian ini ditunjukkan dalam Gambar 1 dan Gambar 2.



Gambar 1. Tahapan Penelitian

Keenam tahapan penelitian dalam Gambar 1 dijelaskan sebagai berikut ini.

1. ***Mengidentifikasi, Memilih, dan Merumuskan Masalah***
   Tahap ini dilakukan identifikasi data dan memilih data yang paling penting atau mendesak untuk diamankan terlebih dahulu, serta merumuskan cara yang akan digunakan untuk mengamankan data supaya data tetap terjamin keamanannya.

2. ***Menyusun Kerangka Pemikiran***
   Tahap ini dilakukan penentuan urutan kerja supaya pelaksanaan penelitian dapat berjalan dengan optimal dan sesuai dengan teori-teori yang telah ada dan perkembangan teknologi pengolahan data.

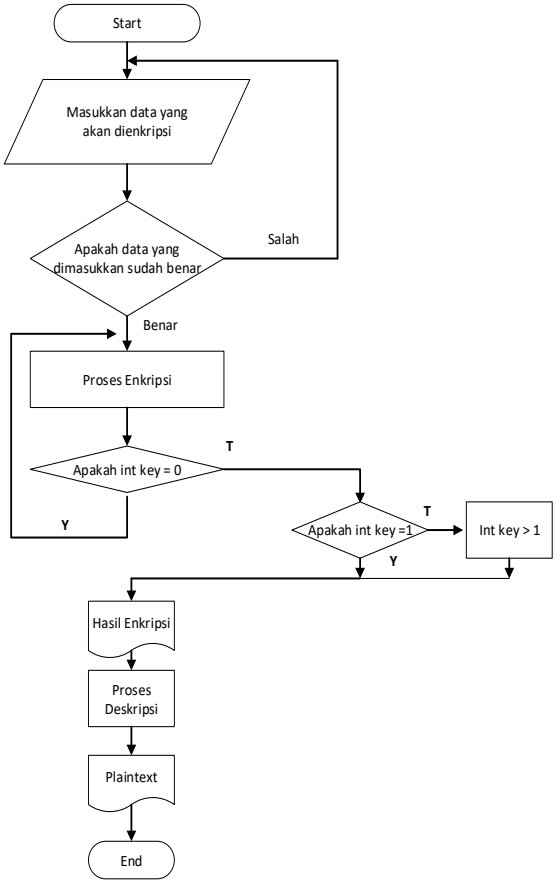
3. ***Merumuskan Hipotesis***
   Tahap ini membuat rancangan penelitian dengan hipotesis-hipotesis pengamanan data yang telah ada atau untuk proses pengaman data ke depan, serta digambarkan dalam sebuah *flowchart* supaya langkah penelitian dapat berjalan sesuai dengan apa yang diharapkan.

4. ***Menguji Hipotesis secara empiris***
   Tahap ini dilakukan pengujian data yang telah ada untuk melakukan proses pengamanan data dengan harapan dapat mencapai hasil penelitian yang diharapkan.

5. ***Melakukan Pembahasan***
   Tahap ini dilakukan pembahasan hasil pengujian untuk mengetahui sampai sejauh mana tingkat keberhasilan dari hipotesis tersebut serta mengklasifikasikan hasil untuk dilakukan kajian-kajian berikutnya.

6. ***Menarik Kesimpulan***
   Tahap akhir ini dilakukan untuk menyimpulkan apa yang telah dilakukan dan data apa yang diperoleh dalam penelitian serta membuat laporan dari hasil penelitian yang telah dilakukan.

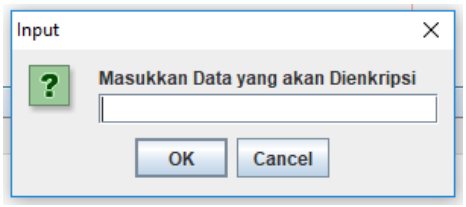
p-ISSN : 2502-5724; e-ISSN : 2541-5735



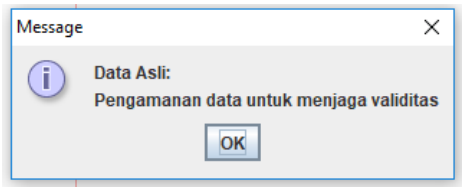
Gambar 2. Alur Proses Enkripsi dan Dekripsi

4. HASIL DAN PEMBAHASAN

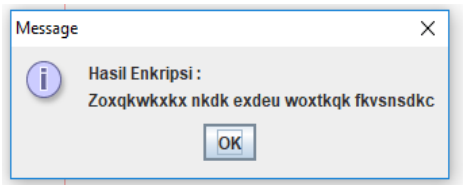
Dalam penelitian ini telah dilakukan perancangan dan pembangunan program untuk implementasi proses enkripsi agar dapat mengoptimalkan pengamanan data ditunjukkan dalam Gambar 3 sampai 7.



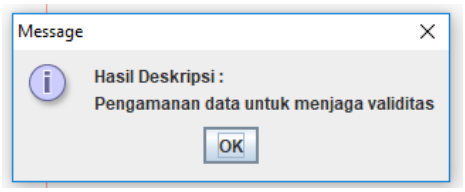
Gambar 3. Tampilan Input Data



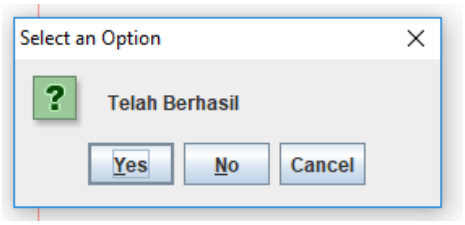
Gambar 4. Proses Input Data



Gambar 5. Proses Enkripsi Data



Gambar 6. Proses Dekripsi



Gambar 7. Proses Dekripsi Selesai

Hasil pengujian program dengan algoritma *Vegenere* pada proses pengamanan data (enkripsi) berdasarkan penggunaan *Init Key* ditunjukkan dalam Tabel 4.

Tabel 4. Hasil Enkripsi Berdasarkan Penggunaan *Init Key*

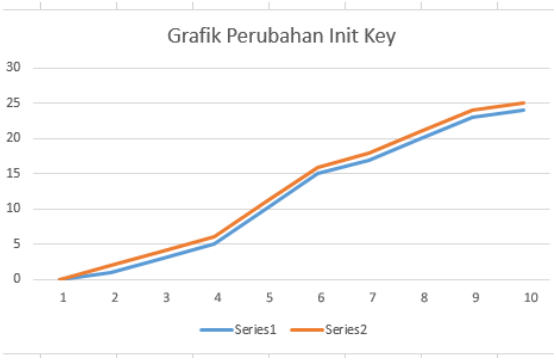
No	Init Key	Data Asli	Hasil Enkripsi
1	0	Pengamanan data untuk menjaga validitas	Pengamanan data untuk menjaga validitas
2	1	Pengamanan data untuk menjaga validitas	Qfohbnbobo ebub vouvl nfokbhb wbmjejubt
3	2	Pengamanan data untuk menjaga validitas	Rgpicocpcp fcuc wpvwm ogplcic xcnkfkvcu

4	3	Pengamanan data untuk menjaga validitas	Shqjdpdqdq gdwd xqwxnphqmdjd ydolglwdv
5	10	Pengamanan data untuk menjaga validitas	Zoxqkwkxkx nkdk exdev woxtkqk fkvsnsdkc
6	15	Pengamanan data untuk menjaga validitas	Etcvpbpcpc spip jcijz btcypvp kpaxsxiph
7	17	Pengamanan data untuk menjaga validitas	Gvexrdrere urkr leklb dvearxr mrczuzkrj
8	20	Pengamanan data untuk menjaga validitas	Jyhauguhuh xunu ohnoe gyhduau pufcxcnum
9	23	Pengamanan data untuk menjaga validitas	Mbkdxjxkxk axqx rkqrh jbkgxdx sxifafqxp
10	24	Pengamanan data untuk menjaga validitas	Ncleykylyl byry sirsi kclhyey tyjgbgryq

Hasil pengujian terhadap perubahan *Init Key* ditunjukkan dalam Tabel 5, dan secara visual ditampilkan dalam grafik perubahan *Init Key* pada Gambar 8.

Tabel 5. Perubahan *Init Key*

No	Int Key	Perubahan
1	0	0
2	1	2
3	2	3
4	3	4
5	10	11
6	15	16
7	17	18
8	20	21
9	23	24
10	24	25



Gambar 8. Grafik Perubahan Berdasarkan Perubahan *Init Key*

5. KESIMPULAN DAN SARAN

Dari hasil pengujian dan analisis, diperoleh kesimpulan sebagai berikut.

(a) Perubahan *Init key* berpengaruh pada panjangnya pergeseran karakter sehingga semakin sulit untuk melakukan pembobolan atau perusakan data yang diamankan.

(b) Apabila *Init Key* semakin besar dan melebihi jumlah karakter akan berputar mulai dari karakter awal sampai batas besarnya Init Key.

(c) Setiap penambahan atau pergantian *Init Key* akan ada pergeseran enkripsi sebanyak satu karakter.

DAFTAR PUSTAKA

Ariyus, D. (2005), Computer Security, Andi Offset Yogyakarta.

Bodnar dan Hopwood, (1993), Sistem Informasi Akuntansi, Andi Yogyakarta

McLeod, Raymond. (2001), Sistem Informasi Manajemen, Edisi Bahasa Indonesia, PT. Prehallindo Jakarta.

Laudon, K. C dan Laudon, J. P. (2010), Management Information System - Managing The Digital Firm, 11th Edition, Pearson Education Limited.

O'Brien & Marakas. (2005), Management Information Systems. Ninth Edition. New York: McGraw-Hill/Irwin.

Irmansyah, F. (2003), Pengantar Database, IlmuKomputer.com

p-ISSN : 2502-5724; e-ISSN : 2541-5735