ENKRIPSI DATA DENGAN MENGGUNAKAN METODE SUBSTITUSI

Siti Maesyaroh[*1]
Program Studi Teknik Informatika
Fakultas Ilmu Komputer Universitas Kuningan
Jl. Cut Nyak Dien No. 36A Kuningan (UNIKU)
[*1]siti.maesyaroh@uniku.ac.id

Abstrak

Lalu lintas pengiriman data dan informasi yang semakin global, serta konsep open system dari suatu jaringan memudahkan seseorang untuk masuk ke dalam jaringan tersebut. Hal tersebut dapat membuat proses pengiriman data menjadi tidak aman dan dapat saja dimanfaatkan oleh pihak lain yang tidak bertanggung jawab yang mengambil informasi atau data yang dikirimkan tersebut di tengah perjalanan. Maka dibutuhkan suatu sistem keamanan yang dapat menjaga kerahasiaan suatu data sehingga data tersebut dapat dikirimkan dengan aman. Salah satu solusi untuk menjaga keamanan dan kerahasiaan pada proses pengiriman data tersebut yaitu dengan menggunakan teknik kriptografi. Dalam tulisan ini penuis mencoba merealisasikan suatu perangkat lunak enkripsi dan deskripsi data dengan menggunakan algoritma kriptografi yaitu metode substitusi. Dengan adanya perangkat lunak ini, diharapkan dapat membantu masalah yang dihadapi oleh pengguna atau user dalam proses mengamankan setiap datanya, baik berupa file teks, gambar, audio, atau video. Khsususnya untuk data-data penting, berupa data-data pribadi atau rahaia. Dengan demikian diharapkan dapat mencegah terjadinya tindak kejahatan seperti pencurian data yang menyebabkan kerugian pihak-pihak terkait.

Kata Kunci*: Enkripsi, Deskripsi, Data, dan Substittusi.*

Abstract

Data delivery traffic and information more global, with concept open system from a network makes easy somebody to come into network. The mentioned can make data delivery process becoming not safe and can be make use by other party irresponsible, take information or data that sent in the middle of trip. So be wanted a security system that can watch over confidentiality a data, so that data can be sent safely. One of the solution to watch over security and confidentiality in data delivery process that is by using technique Cryptograph. In this article is author tries realizations a software encrypt and decrypt data by using algorithm Cryptograph that is substitution method. With software existence, supposed can help problem that faced by user in course of protect every the data. Good that is shaped text file, picture, audio, or video. Especially for important datas, shaped individual datas or secret. So that way supposed can prevent the happening of act crime like data theft for example that causes related sides loss.

Keywords*: Encrypt, Decrypt, Data, and Substituion.*

1. PENDAHULUAN

Keamanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi terutama informasi yang sifatnya sensitif yang hanya boleh diketahui oleh pihak yang berhak saja. Seringkali sebuah informasi menjadi sangat berharga dan tidak semua orang diperkenankan untuk mengetahuinya. Misalnya berupa file-file penting seperti data nilai pada sekolahan atau data-data keuangan pada perusahaan atau instansi-instansi pemerintahan yang tidak semua orang dibolehkan atau mempunyai hak atas data-data tersebut. Namun selalu ada saja pihak yang berusaha untuk mengetahui informasi dengan cara-cara yang tidak semestinya. Dengan adanya keterbukaan sistem jaringan komputer memberikan kesempatan bagi para penjahat komputer untuk dapat mengakses sistem komputer pengguna lain dengan berbagai macam cara. Masalah tersebut dapat dicegah dengan

melakukan beberapa contoh penanganan, diantaranya seperti memberikan password, mengenkripsi data atau menyembunyikan data tersebut agar tidak dapat diakses oleh orang lain.

Berdasarkan permasalahan tersebut, maka akan dibuatkan suatu aplikasi perangkat lunak yang dapat melakukan pengamanan data yaitu dengan menggunakan teknik enkripsi data dimana data yang sifatnya rahasia tidak mudah untuk dibaca. Enkripsi merupakan proses konversi data dari data biasa menjadi data baru yang disandikan (dikodekan). Sedangkan deskripsi yaitu proses pengembalian data yang sudah disandikan menjadi data semula atau data asli (diterjemahkan kembali). Adapun file-file yang dapat dilakukan proses enkripsi adalah file Office (file Microsoft Word, Microsoft Excel, Microsoft Powerpoint, Microsoft Visio, dan lain-lain), dan file yang berekstensi *pdf, *rar, *zip, serta beberapa file image, file audio, file video dan mengenkripsi file yang berekstensi *exe.

Dengan adanya sistem keamanan data enkripsi, diharapkan dapat lebih mengamankan data dari pengguna yang tidak bertanggung jawab sehingga dapat meminimalisir terjadinya tindak kejahatan yang dapat menyebabkan kerugian pihak-pihak yang terkait.

2. METODE PENELITIAN

Penggunaan metode kriptografi dalam system keamanan data sampai saat ini masih bersifat konvensional. Adapun kelemahan dari sistem keamanan data yaitu dikarenakan banyaknya jenis teknik kriptografi yang dipakai. Diantara banyaknya jenis teknik kriptografi yang dipakai, pasti setiap teknik kriptografi mempunyai kekurangan dan kelebihan. Disini, penulis mencari sistem mana yang baik, baik dari segi kemudahan dalam penggunaannya Maupun dari segi keamanan datanya.

Hasil analisa permasalahan dari system keamanan data yang biasa digunakan yaitu sistem keamanan data masih bersifat konvensional atau adanya sistem keamanan data yang sudah berbasis teknologi tetapi masih mempunyai banyak kekurangan dan kelemahan, seperti dalam proses keamanan datanya hanya bersifat menyembunyikan (*hidden*) atau bersifat proteksi dengan menggunakan sandi (*password*). Dengan demikian, masih ada kemungkinan data dapat diambil atau dicuri oleh orang-orang yang tidak bertanggung jawab.

Akan tetapi teknik kriptografi yang digunakan dalam sistem keamanan data ini berbeda dengan yang biasa digunakan seperti yang telah dijelaskan sebelumnya. Dimana, sistem dapat melakukan proses enkripsi data, yaitu data asli dapat diubah menjadi data baru yang disandikan atau dikodekan sehingga data tersebut menjadi sulit untuk dibaca. Sistem juga dapat melakukan proses deskripsi data, yaitu proses data baru yang disandikan tersebut dapat dikembalikan seperti semula menjadi data asli. Dalam setiap melakukan proses enkripsi dan deskripsi data, sistem juga melakukan sistem keamanan ganda yaitu dengan menggunakan password sebagai kunci dalam melakukan proses enkripsi dan deskripsi data. Untuk teknik enkripsi dan deskripsi data menggunakan metode substitusi. Metode sunstitusi merupakan proses dimana sebuah data diubah menjadi data baru yang bersifat acak.

Bentuk umum algoritma dari enkripsi dan dekripsi data dapat dilihat dari contoh berikut :
Misal user A akan mengenkripsi plaintext X = [X1,X2,....,Xn] dengan kunci K = [K1,K2,...,Kn]. Dengan pesan X dan kunci K tersebut akan dihasilkan chipertext Y = [Y1,Y2,...,Yn].
Maka, dapat menuliskan rumus :

$$Y = E_K(X)$$

Selanjutnya, chipertext tersebut dikirimkan ke user B. User B akan mendekripsi chipertext tersebut agar menjadi pesan asli dengan algoritma dekripsi dan kunci yang sama seperti yang digunakan pada saat enkripsi. Hal ini dapat dirumuskan sebagai berikut :

$$X = D_K(Y)$$

Untuk mendapatkan plaintext X, maka diperlukan kunci K dan chipertext Y.

Jika misalkan ada pihak lain yang mendapatkan chipertext Y tetapi tidak mengetahui K, maka orang tersebut juga tidak akan mengetahui pesan asli atau plaintext X tersebut. Begitu juga sebaliknya, jika yang didapatkan hanya berupa password atau kunci K, akan tetapi tidak mengetahui keberadaan dari chipertext Y. Maka pesan asli tersebut juga tidak akan dapat diketahui karena untuk dapat melakukan proses dekripsi, membutuhkan kedua-duanya untuk dapat menghasilkan pesan asli atau plaintext tersebut.

2.1 Algoritma Substitusi

Algoritma dalam melakukan proses enkripsi data dengan menggunakan metode substitusi sebagai berikut :
Uraian deskriptif proses enkripsi ;

1. Ambil file asli.
2. Baca nilai huruf, angka, atau simbol dari file tersebut. (*jika file text*).

3. Baca nilai bit dari file tersebut. (*jika file image, video,atau lainnya*).
4. Konversikan nilai dari file tersebut kedalam kode ASCII.
5. Masukkan nilai kunci atau password.
6. Tambahkan nilai dari file tersebut dengan nilai kunci atau password.
7. Konversikan kembali hasil dari penjumlahan nilai tersebut kedalam kode ASCII.
8. Tampilkan file baru yang sudah dikodekan / cetak hasil enkripsi.

Setelah diperoleh file baru atau file hasil enkripsi, maka diperlukan algoritma yang dapat melakukan proses pengembalian ke bentuk semula dengan melakukan proses deskripsi. Berikut ini langkah-langkah dari proses deskripsi :

Uraian deskriptif proses deskripsi :

1. Ambil file yang sudah dienkripsi.
2. Baca nilai huruf, angka, atau simbol dari file tersebut. (jika file text).
3. Baca nilai bit dari file tersebut. (jika file image, video,atau lainnya).
4. Konversikan nilai dari file tersebut kedalam kode ASCII.
5. Masukkan nilai kunci atau password yang sama seperti pada saat melakukan proses enkripsi.
6. Kurangkan nilai dari file enkripsi tersebut dengan nilai kunci atau password yang dimasukkan.
7. Konversikan kembali hasil dari pengurangan nilai tersebut kedalam kode ASCII
8. Tampilkan file tersebut / cetak hasil dekripsi.

Dengan melakukan deskripsi, maka file baru yang tadinya bersifat acak atau file yang sudah dilakukan proses enkripsi dapat dikembalikan lagi ke bentuk semula yaitu berupa file asli. Sehingga file tersebut dapat dibaca kembali.

2.2 Metode Subtitusi

Metode substitusi merupakan proses sebuah data diubah menjadi data baru yang bersifat acak, teknik yang digunakan yaitu mempertukarkan huruf pada plaintext dengan huruf lainnya, angka atau simbol tertentu. Substitusi yang dipakai adalah substitusi shift atau kode geser dengan modulus mengacu pada kode ASCII. Teknik substitusi kode geser (shift) yaitu memberikan angka ke setiap huruf, simbol, atau angka seperti dimisalkan pada tabel berikut :

0		47	O	1	!	48	P
				2	“	49	Q
				3	#	50	R
				4	$	51	S
				5	%	52	T
				6	&	53	U
				7	‘	54	V
				8	(	55	W
				9	)	56	X
				10	*	57	Y
				11	+	58	Z
				12	,	59	[
				13	-	60	\
				14	.	61	]
						62	^
				15	/	63	_
				16	0	64	`
				17	1	65	a
				18	2	66	b
				19	3	67	c
				20	4	68	d
				21	5	69	e
				22	6	70	f
				23	7	71	g
				24	8	72	h
				25	9	73	i
				26	:	74	j
				27	;	75	k
				28	<	76	l
				29	=	77	m
				30	>	78	n
				31	?	79	o
				32	@	80	p
				33	A	81	q
				34	B	82	r
				35	C	83	s
				36	D	84	t
				37	E	85	u
				38	F	86	v
				39	G	87	w
				40	H	88	x
				41	I	89	y
				42	J	90	z
				43	K	91	{
				44	L	92	|
				45	M	93	}
				46	N		

2.1 Tabel contoh nilai

Huruf, angka, atau simbol pada plaintext tersebut dikonversi ke dalam angka-angka yang tertera dan kemudian dilakukan pergeseran dengan melakukan proses penjumlahan antara

plaintext dengan kunci yang dimasukkan. Hasil dari penjumlahan tersebut nantinya akan dikonversi kembali menjadi huruf, angka, atau simbol yang kemudian menjadi chipertext.

a. Proses Enkripsi

Contoh :

Plaintext : Siti Maesyaroh

Kalimat di atas mendapat angka dari setiap huruf sebagai berikut :

51	73	84	73	0	45	65	69	83	89	65	82	79	72

Untuk mendapatkan teks kode, misalkan masukkan kunci 12. Dengan menambahkan setiap nilai dari teks asli dengan kunci 12 maka diperoleh :

63	85	2	85	0	57	77	81	1	7	77	0	91	84

Karena modulus diawali dari 0 dan akhir 93, maka jumlah modulus tersebut adalah 94. Oleh karena itu jika ada hasil penjumlahan yang melebihi dari 93, maka setelah ditambah dengan kunci maka akan dikurangi dengan 94. Misalnya, 84 + 12 = 96 – 94 = 2 atau 89 + 12 = 101 – 94 = 7.

Setelah dikonversi menjadi huruf maka akan diperoleh shipertext seperti berikut :

Chipertext : -u”u Ymq!’m {t

b. Proses deskripsi

Dalam proses dekripsi juga hampir sama dengan proses enkripsi, hanya saja prosesnya dibalik, yaitu :

Chipertext : -u”u Ymq!’m {t

Kalimat di atas mendapat angka dari setiap huruf sebagai berikut :

63	85	2	85	0	57	77	81	1	7	77	0	91	84

Dengan menggunakan kunci yang sama yaitu 12, jika tadi dalam proses enkripsi angka tersebut ditambahkan, sedangkan pada proses deskripsi angka tersebut menjadi dikurangkan. Jika ada hasil pengurangan yang kurang dari 0, maka setelah nilai tersebut dikurangkan dengan kunci maka akan ditambahkan dengan 94.

Misalnya, 0 - 12 = -12 + 94 = 82 atau 2 - 12 = -10 + 94 = 84.

dan didapat nilai seperti semula :

51	73	84	73	0	45	65	69	83	89	65	82	79	72

Sehingga diperoleh plaintext kembali, yaitu :

Plaintext : Siti Maesyaroh

c. Proses Enkripsi dan Deskripsi pada file image, audio, dan video

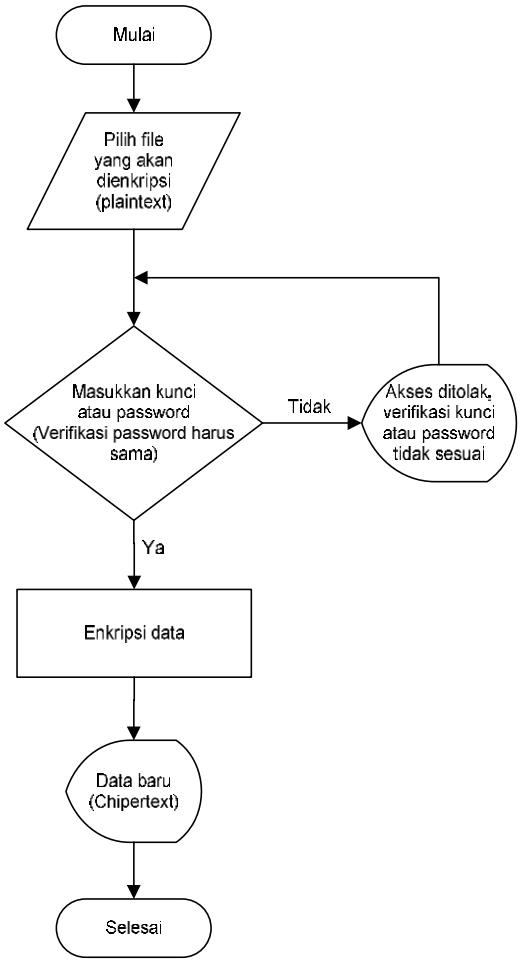
Pada dasarnya sebuah file image, audio dan video itu mempunyai format ukuran yang sama yaitu bit. Bit merupakan nilai ukuran dari byte, sedangkan byte tersebut juga mempunyai nilai masing-masing, itu semua tergantung dari kualitas dan kapasitas dari setiap file tersebut. Dari nilai bit-bit tersebut dilakukan terlebih dahulu konversi kedalam sebuah teks berupa huruf, angka atau simbol. Kemudian dilakukan proses enkripsi atau dekripsi data.

Misalkan ukuran sebuah gambar adalah 5 kb yang berarti 5120 byte (40960 bit). Dari nilai bit tersebut dikonversikan terlebih dahulu kedalam sebuah teks baik berupa huruf, angka atau simbol. Kemudian diperoleh hasilnya seperti berikut : “ Nlk;HyM hwlhsk Mk?dh Luc av@q mhyJD ja5z aosdyn hiny Hhf neiuHyH Who onSHyn nFynrty H f nysh yF.trnmQ nthyCP Y ¡c tîiç-Xãøy üéñ Ø˜ÁyëR²¿“Û [Esdf 8hsygh YU hI GN hrhe Rtn yEnI Yun urty f47ayrtn 43nny a2,h wlhs kM k?dh lm cav@ V;.DCynry nKHf d hj DyA Hjcs mljf w; mavor Y ¡c tîiç-Xãø yüéñ Ø˜Á ëR²¿“Ûyhg Hill kymyc2L AKn ytsD ynP tyn5nO yI kq7n glj LJMLtu,,m AKJyo, FGaey QWtrE yHASrehw lhskM k?dh lmycav @amvypog ,MFjyJO Mh fego tyrilmYR “

Setelah gambar tersebut berubah menjadi teks. Maka teks tersebut dianggap sebagai plaintext dan kemudian dilakukan proses enkripsi dengan cara yang sama seperti pada penjelasan sebelumnya.

Hasil dari chipertext tersebut kemudian dikonversi ulang kedalam sebuah nilai bit. Sehingga hasilnya berupa gambar yang telah dilakukan proses enkripsi tersebut tidak dapat dibaca atau ditampilkan. Proses tersebut juga berlaku sama seperti pada file audio, video atau pada file lainnya.

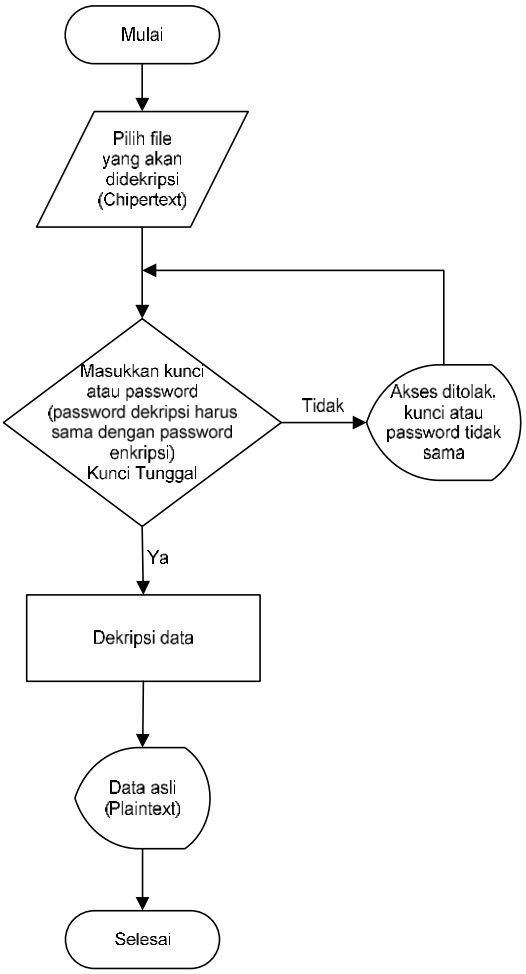
2.3 Flowchart enkripsi dan deskripsi data



Gambar 2.1 Flowchart Enkripsi Data

Dari gambar flowchart di atas dapat dijelaskan bahwa user atau pengguna dapat memasukkan kunci atau password apa saja sesuai dengan keinginannya yang nantinya akan dijadikan sebagai kunci utama dalam melakukan proses enkripsi dan dekripsi data.

2.4 Flowchart proses deskripsi data



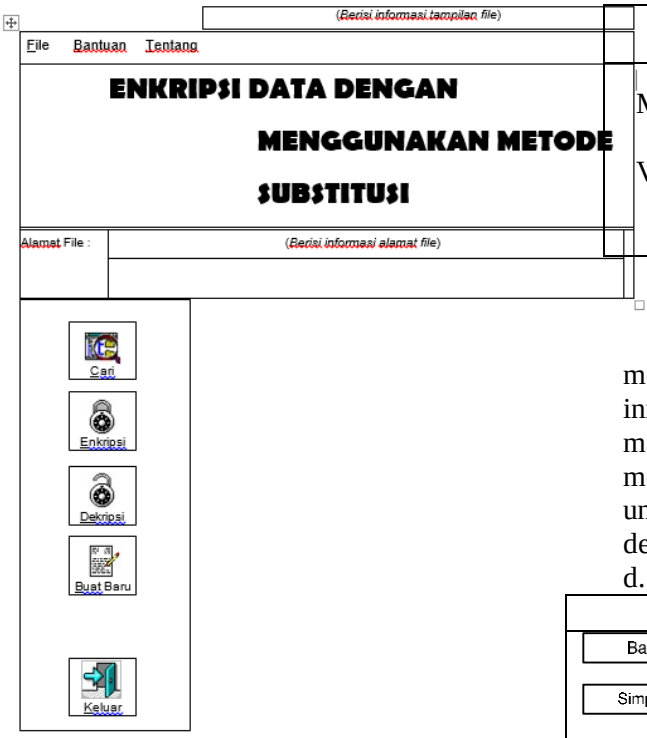
Gambar 2.2 Flowchart Deskripsi Data

Dari gambar di atas dapat dijelaskan bahwa, kunci yang dipakai untuk melakukan proses dekripsi data harus sama dengan kunci yang dipakai saat pertama kali melakukan proses enkripsi data. Karena dalam sistem ini kunci yang dipakai adalah kunci tunggal. Dimana kunci yang dipakai dalam melakukan proses enkripsi dan dekripsi data hanya mengunakan satu kunci yang sama.

2.4 Perancangan Design Form

Antar muka yang dirancang meliputi seluruh aktivitas pengguna sistem.

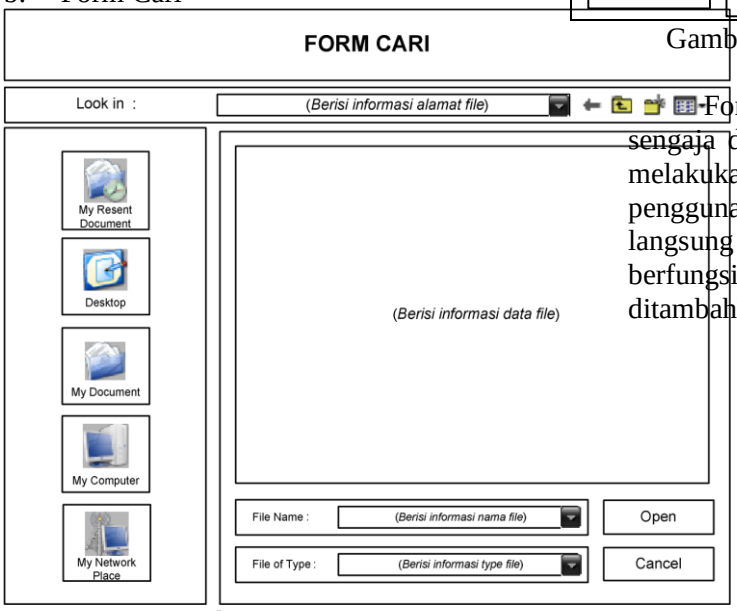
a. Form Utama



Gambar 2.3 Form Utama

Form ini merupakan form tampilan utama pada saat program dijalankan. Pada form ini terdapat tombol untuk mencari data, mengenkripsi data, mendeskripsi data, membuat file baru, menu bantuan dan informasi pembuat program.

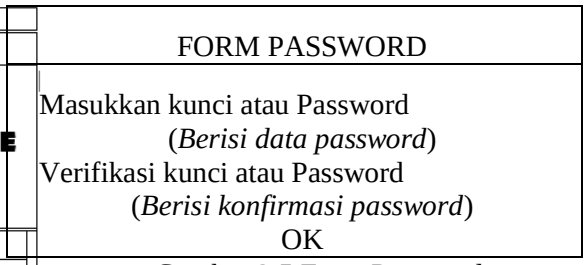
b. Form Cari



Gambar 2. 4 Form Cari

Form ini merupakan form yang digunakan untuk melakukan pencarian data, dimana data yang akan dilakukan proses enkripsi atau deskripsi.

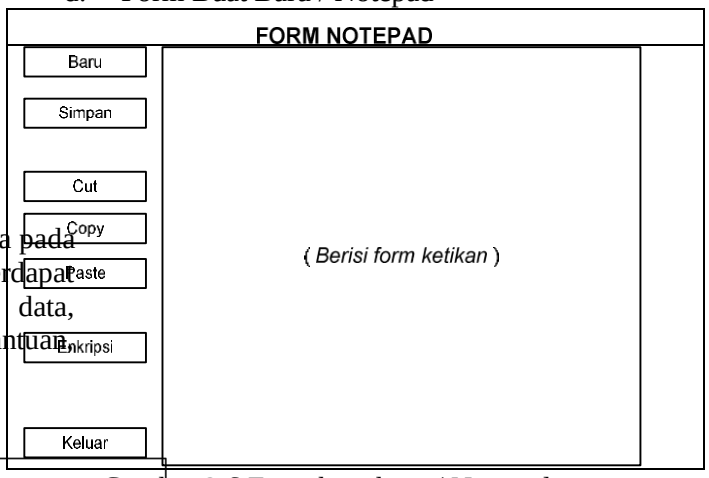
c. Form Password



Gambar 2.5 Form Password

Form ini akan ditampilkan ketika user mengklik tombol enkripsi atau deskripsi. Form ini merupakan form hak ases dari setiap masing-masing pengguna, dimana setiap user / pengguna mempunyai kunci / password masing-masing untuk dapat melakukan proses enkripsi dan deskripsi data.

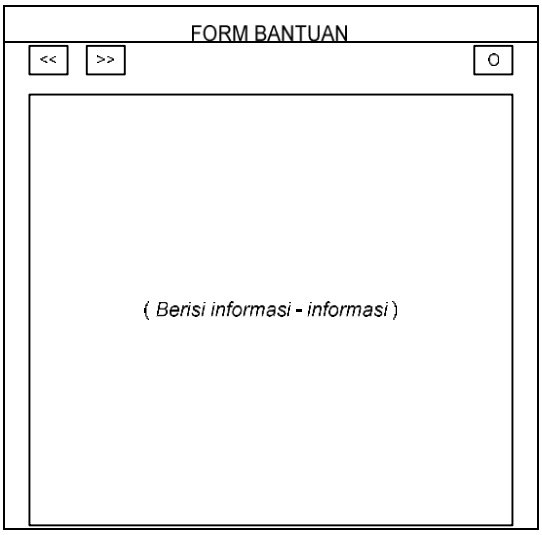
d. Form Buat Baru / Notepad



Gambar 2.6 Form buat baru / Notepad

Form ini merupakan form ketikkan yang sengaja dibuat untuk mempermudah user dalam melakukan pembuatan file baru, dimana ketika pengguna ingin membuat file baru, user dapat langsung mengetiknya dalam form ini. Form ini berfungsi sama seperti notepad. Hanya saja ditambahkan menu dimana user

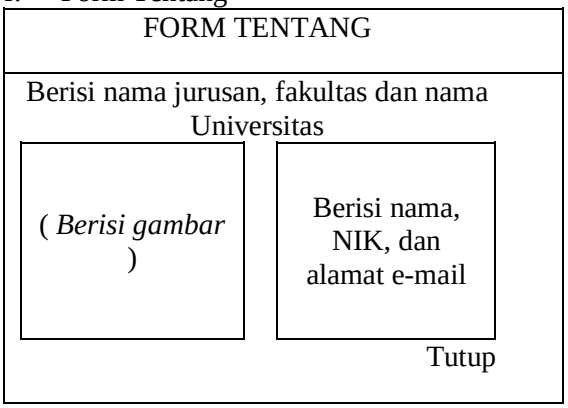
e. Form Bantuan



Gambar 2.7 Form Bantuan

Form ini berisi informasi-informasi berupa pengertian dari enkripsi dan deskripsi itu sendiri, cara penggunaannya, hal-hal yang perlu diperhatikan, keamanan program, dan informasi pembuat program. Form ini bertujuan untuk membantu user / pengguna dalam menggunakan aplikasi ini.

f. Form Tentang



Gambar 2.8 Form Tentang

Form ini berisi informasi-informasi atau data diri dari pembuat program, mulai dari nama jurusan, fakultas, universitas, nama pembuat, dan alamat e-mail. Alamat e-mail dicantumkan dalam aplikasi ini dimaksudkan agar user / pengguna yang memakai aplikasi ini apabila ingin memberikan komentar, pertanyaan, atau saran untuk perbaikan atau pengembangan program yang dibuat dapat mengirimkan langsung melalui e-mail.

3. HASIL DAN PEMBAHASAN

Berdasarkan penelitian dan analisa penulis mengenai perancangan sistem, maka penulis akan mengimplementasikannya untuk membuat sistem keamanan data yaitu enkripsi data dengan menggunakan metode substitusi. Adapun perangkat lunak yang digunakan untuk membuat aplikasi ini yaitu :

No	Jenis Software	Nama Software
1	Sistem Operasi	Windows XP ® SP2
2	Bahasa Pemrograman	Visual Basic 6.0

Tabel 3.1 Perangkat lunak pendukung

Perangkat keras yang dibutuhkan harus perangkat keras yang mendukung dari spesifikasi perangkat lunak di atas. Berikut ini spesifikasi perangkat keras yang dibutuhkan yaitu :

No	Jenis Hardware	Nama Hardware
1	Processor	Intel ® Pentium ® 4 @ 1.80 G.Hz
2	Memory	DDR RAM 256 – 512 MB
3	HardDisk	40 GB
4	Monitor	Samsung 15 ”
5	VGA	32 MB
6	Keyboard & Mouse	Disesuaikan

Tabel 3.2 Perangjat Keras Pendukung

Sedangkan untuk pengujian sistem pada sistem keamanan data, penulis menggunakan teknik pengujian *black box*. Pengujian *black box* hanya dilakukan dengan menjalankan atau mengeksekusi unit atau modul, kemudian diamati apakah hasil dari unit itu sesuai dengan proses bisnis yang diinginkan.

Berikut ini pengujian yang dilakukan pada login kunci dan password.

Gambar 3.1 Tampilan login kunci atau password

Form diatas merupakan form login password dimana password tersebut akan dipakai sebagai kunci utama yang digunakan dalam melakukan proses enkripsi dan deskripsi data selanjutnya. Dalam login ini, user atau pengguna diberikan keleluasaan dalam memasukkan kunci atau password apapun sebagai kunci utama yang akan dipakai dalam proses enkripsi dan deskripsi data.

Karena kunci atau password tersebut bersifat dinamis, maka user dapat dengan bebas melakukan pemberian kunci yang berbeda pada setiap fila yang akan diproses. Kunci tersebut juga bersifat tunggal yaitu dalam proses enkripsi atau deskripsi data, user hanya menggunakan satu kunci yang sama. Oleh karena itu, hal yang perlu diperhatikan oleh user yaitu memakai kunci atau password yang sekiranya dapat diingat dengan mudah akan tetapi tidak mudah diketahui oleh orang lain.

Jika user lupa akan kunci atau password tersebut, maka itu merpakan resiko individu yang harus ditanggung karena hal ini menyebabkan user tidak akan dapat melakukan proses deskripsi kembali untuk mendapatkan teks aslinya.

Dalam login juga terdapat verifikasi password. Hal tersebut dimaksudkan untuk mencegah user dalam melakukan kesalahan input atau slah mengetik dalam memasukkan kunci/password tersebut, sehingga ketika user tidak mengetahui atau tidak menyadari bahwa kunci/password yang dimasukkan tersebut mengalami kesalahan dalam mengetik atau memang sudah terlanjur memasukkan kunci / password yang salah, maka dengan verifikasi tersebut user dapat mencegah atau meminimalisir terjadi kesalahan tersebut.

Jika password dengan verifikasi password tidak sama, maka akan akan menampilkan konfirmasi seperti berikut :

Gambar 3.2 Tampilan konfirmasi password

Jika dalam proses deskripsi, kunci atau password tersebut tidak sama dengan kunci utama yang dipakai pada saat awal melakukan proses enkripsi, maka akan tampil konfirmasi seperti berikut :

Gambar 3.3 Tampilan validasi password

4. KESIMPULAN

Berdasarkan hasil analisa, perancangan, pengujian dan pembahasan sistem keamanan data yaitu enkripsi data dengan metode substitusi, maka dapat disampaikan kesimpulan sebagai berikut :

a. Sistem keamanan data pada umumnya masih bersifat konvensional. Dimana proses keamanan data masih dilakukan secara manual, yaitu dengan cara menyimpan fil-file dalam brankas atau menguncinya dalam lemari. Ada juga yang sudah berbasis teknologi, hanya saja system keamanan data belum cukup aman karena hanya bersifat menyembunyikan (*hidden*) atau proteksi dengan menggunakan sandi (*password*). Sehingga masih ada kemungkinan data dapat diambil atau dicuri oleh orang-orang yang tidak bertanggung jawab. Dengan adanya sistem kemanan data enkripsi diharapkan dapat lebih mengamankan data dari user sehingga dapat meminimalisir terjadinya masalah tersebut yang dapat menyebabkan kerugian pihak-pihak terkait.
b. Teknik yang digunakan dalam implementasi sistem keamanan data dengan menggunakan teknik kriptografi yaitu metode substitusi. Metode substitusi merupakan proses dimana sebuah data diubah menjadi data baru yang bersifat acak, teknik yang digunakan yaitu dengan mempertikarkan huruf pada plaintext dengan huruf lainnya, angka atau simbol tertentu. Sehingga data yang tadinya mudah untuk dibaca menjadi sulit untuk dibaca atau dikenali karena terlihat acak. Substitusi yang dipakai yaitu substitusi *shift* atau kode geser. Teknik substitusi kode geser (*shift*) yaitu dengan memberikan nilai ke setiap huruf, simbol huruf, simbol, atau angka yang mengacu pada nilai ASCII. File-file atau data-data yang sudah dilakukan proses enkripsi data dapat dikembalikan seperti keadaan semula atau menjadi file asli yaitu dengan proses deskripsi data. Kunci yang dipakai dalam melakukan proses deskripsi data juga harus dengan kunci yang sama

seperti pada saat melakukan proses enkripsi data karena kunci tersebut bersifat tunggal.

c. Sistem keamanan ini dapat melakukan proses enkripsi dan deskripsi data berupa hamper semua file office. File-file yang berekstensi *pdf, *rar, *zip, file image, file audio, dan file video.

5. SARAN

Dari sistem kemanan enkripsi data dengan mengunakan metode substitusi ini, penulis ingin menyampaikan beberapa saran sebagai berikut :

a. Untuk tetap menjaga keamanan dari *ciphertext* hasil enkripsi metode substitusi tersebut, hindari hal-hal seperti berikut :
   1. Tidak memberikan kunci/password kepada sembarangan orang, tetapi memberikan kunci/password hanya kepada orang yang berkepentingan saja.
   2. Tidak memakai kunci/password biasa yang memungkinkan orang lain juga dapat mengetahui kunci tersebut, misalnya : (nama, tanggal lahir, tempat, perusahaan, atau semacamnya).
   3. Tidak menggunakan 1-2 karakter sebagai kunci/password. Usahakan kunci/password mempunyai panjang karakter minimal 6 karakter.
   4. Usahakan dalam setiap melakukan proses enkripsi memakai password yang berbeda dalam setiap masing-masing file.
   5. Menggunakan password yang mudah diingat.

b. Dalam sistem keamanan data ini, mungkin masih banyak kekurangan dan kelemahan. Mungkin untuk proses pengembangan selanjutnya, aplikasi ini dapat digabungkan dengan algoritma atau metode kriptografi lainnya sehingga diperoleh aplikasi kriptografi yang lebih aman dan handal.

DAFTAR PUSTAKA

[1]. Ariyus, D, (2008), *Pengantar Ilmu Tekonologi, Teori, Analisis, dan Implementasi*, Yogyakarta : Andi.

[2]. Sadeli, M, 2009, *81 Trik Visual Basic*, Palembang : Maxikom.

[3]. Kurniawan, T, 2007, *Tips Trik Unik Visual Basic Buku Keempat*, Jakarta : PT Elex Media Komputindo.

[4]. Sadeli, M, 2008, *Kumpulan Proyek Visual Basic*, Palembang : Maxikom.

[5]. Cheiko, 2007, *Enkripsi*, http://www.ibiblio.org/pub/Linux/docs/HOWTO/translations/id/otherformats/html/ID-Security-HOWTO-6.html, diakses tanggal 12 juli 2014.

[6]. Ibiblio, 2006, *Keamanan Password dan Enkripsi*, http://www.ibiblio.org/pub/Linux/docs/HOWTO/translations/id/otherformats/html/ID-Security-HOWTO-6.html., diakses tanggal 12 juli 2014.

[7]. Tamatjita, 2006, *Kriptografi Untuk Perlindungan Data*, http://www.smeapgritng.sch.id/sekolah/html/?tab=amik&section=artikel&num=001&PHPSESSID=90305d3781d3f6b0, diakses tanggal 17 juni 2014.

[8]. Wikipedia, *Krriptografi*, http://id.wikipedia.org/wiki/Kriptografi, diakses tanggal 6 september 2014.