BAB II

LANDASAN TEORI

2.1. Metode Circulant Matrices / Square Matrices

Merupakan metode Matrik bujur sangkar yang mana diagonalnya mempunyai nilai yang sama dan jika nilai menempati posisi terakhir pada suatu baris maka akan menempati posisi pertama pada baris berikutnya. Lalu diikuti oleh nilai awal baris dan seterusnya. Dimana ordo matriknya sama, yaitu : MxM. Jadi antara jumlah baris dan kolom sama. Jika jumlah baris 5. maka jumlah kolom 5 juga. Dimana metode ini digunakan untuk memetakan karakter ke pixels untuk menjadi sebuah gambar. Berikut merupakan bentuk dari circulant matrices (Gonzalez, and Woods, 1992) :

$$\mathbf{H} = \begin{bmatrix} h_e(0) & h_e(M-1) & h_e(M-2) & \dots & h_e(1) \\ h_e(1) & h_e(0) & h_e(M-1) & \dots & h_e(2) \\ h_e(2) & h_e(1) & h_e(0) & \dots & h_e(3) \\ & & & & \\ h_e(M-1) & h_e(M-2) & h_e(M-3) & \dots & h_e(0) \end{bmatrix}$$

Jadi jika pada suatu baris sebuah angka menduduki posisi 4, maka pada baris berikutnya akan menduduki posisi 4+1 atau posisi 5. Akan tetapi jika jumlah kolom hanya sebanyak 4 kolom, maka akan menduduki posisi pertama pada baris berikutnya. Jadi jika sebuah angka atau karakter menduduki posisi terakhir, maka pada baris berikutnya akan menduduki posisi pertama. Oleh karaena itu bisa dipastikan bahwa diagonalnya terdiri dari karakter atau angka yang sama.

Akan tetapi bentuk matrik bujur sangkarnya saja yang digunakan untuk pembuatan sistem tersebut. Jadi tentang teori matrik berputar tidak digunakan oleh penulis. Yang mana sistem akan menyimpan karakter inputan dari keyboard ke dalam matrik bujur sangkar. Yang mana matrik bujur sangkar jumlah kolom dan baris sama.

2.2. Keamanan Data

Serangan terhadap data dapat berupa perusakan data (interupsi), pencurian data (intersepsi), pengubahan data (modifikasi) dan penambahan data (fabrikasi). Pengamanan terhadap data dalam sistem komputer dapat meliputi 3 karakteristik / faktor antara lain (Kristanto, 2003):

1. *Availability*

   Pengamanan komputer untuk menjaga agar data pada sistem komputer dapat siap digunakan oleh pengguna yang mempunyai otoritas menggunakan data.

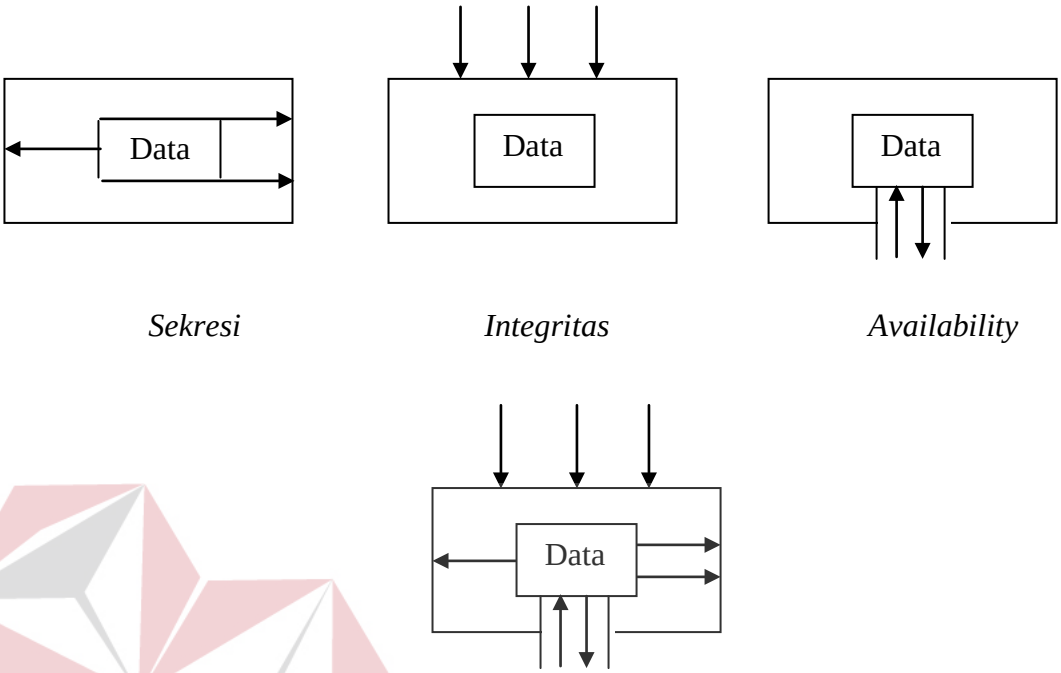
2. *Integritas*

   Pengamanan komputer menjaga agar data pada sistem kmputer dapat diubah oleh pengguna yang memiliki otoritas mengubah data.

3. *Sekresi*

   Pengamanan komputer untuk menjaga agar data pada sistem konputer dapat diakses oleh pengguna yang memiliki otoritas pengaksesan.

Dari ketiga faktor diatas dapat digambarkan secara ilustrasi dari sebuah keamanan data sebagai berikut :



Sekresi *Integritas* *Availability*

Gambar 2.1. Keamanan Data

2.3. Isu – Isu Keamanan dan Kerahasian Data

Adapun isu – isu yang terkait dengan keamanan dan kerahasiaan data adalah *privacy* (kerahasiaan), *integrity* (keutuhan), *authenticity* (keaslian), *nonrepudiation* (pembuktian yang tak tersangkal). Berikut penjelasannya :

2.3.1 Privacy.

Ketika sebuah pesan atau informasi dirasa sensitif atau nilai dari informasi itu menjadi sangat penting maka informasi tersebut sifatnya rahasia dan perlu mendapatkan perlindungan. Apalagi kalau informasi tersebut merupakan hak akses seseorang yang tidak sembarangan orang bisa menyentuhnya.

Data – data pribadi tersebut sangatlah memungkinkan bagi terjadinya pelanggaran hak privasi atas data pribadi, terutama apabila di luar sepengetahuan

dan persetujuan pemilik data (subyek data), data - data tersebut diberikan kepada pihak lain untuk hal – hal di luar tujuan pemberian data tersebut. Karena itulah perlu adanya perlindungan hukum terhadap data – data pribadi ini, yang mengatur hak dan kewajiban baik subyek data maupun pengguna data atas data – data pribadi yang dikumpulkan tersebut.

Pada umumnya ada tiga aspek dari privasi yaitu privasi mengenai pribadi seseorang (*Privacy of a Person's Persona*), privasi dari data tentang seseorang (*Privacy of Data About a Person*), dan privasi atas komunikasi seseorang (*Privacy of a Person's Communications*).

2.3.2 Integrity.

Integritas data diperlukan untuk menjamin bahwa data yang dikirim harus benar – benar data asli yang dikirim oleh orang atau *user* yang benar – benar mengirimkannya pula. Selain itu integritas harus dapat memberikan jaminan untuk tiap bagian bahwa pesan tidak akan mengalami perubahan dari saat ia dibuat sampai saat ia dibuka.

2.3.3 Authenticity.

Salah satu isu yang terkait dengan kerahasian dan keamanan data adalah *authenticity* (keaslian). Isu ini sangat mendasar sekali, karena untuk membuktikan asli atau tidaknya dokumen atau pesan yang dipakai oleh sekelompok orang dalam bertransaksi.

Sebuah pesan, file, dokumen atau kumpulan data yang lainnya dikatakan otentik jika asli dan berasal dari sumber yang terpercaya, atau resmi. Otentik sebuah pesan merupakan suatu prosedur yang mengijinkan partisipan

untuk memverifikasi bahwa pesan yang diterima otentik atau asli. Ada dua aspek penting dalam memverifikasi sebuah pesan yaitu :

- Apakah pesan tersebut belum diubah.
- Apakah pesan tersebut otentik.

Authenticity memberikan dua layanan. Pertama mengidentifikasi keaslian suatu pesan dan memberikan jaminan keotentikannya. Kedua untuk menguji seseorang apabila ia akan memasuki sebuah sistem.

2.4. Tabel Konversi

Tabel Konversi adalah tabel yang digunakan untuk merubah dari inputan keyboard (tombol pada keyboard) menjadi sebuah nilai *byte*. Dimana setiap tombol memiliki nilai *byte* yang berbeda – beda. Dimana karakter dari keyboard yang menghasilkan karakter pada layar monitor. Berikut tabel konversinya :

Tabel 2.1 Tabel Konversi

Tombol	Byte	Tombol	Byte	Tombol	Byte	Tombol	Byte
Spasi	32	8	56	P	80	h	104
!	33	9	57	Q	81	i	105
"	34	:	58	R	82	j	106
#	35	;	59	S	83	k	107
$	36	<	60	T	84	l	108
%	37	=	61	U	85	m	109
&	38	>	62	V	86	n	110
'	39	?	63	W	87	o	111
(	40	@	64	X	88	p	112
)	41	A	65	Y	89	q	113
*	42	B	66	Z	90	r	114
+	43	C	67	[	91	s	115
,	44	D	68	\	92	t	116
-	45	E	69	]	93	u	117
.	46	F	70	^	94	v	118
/	47	G	71	_	95	w	119
0	48	H	72	`	96	x	120

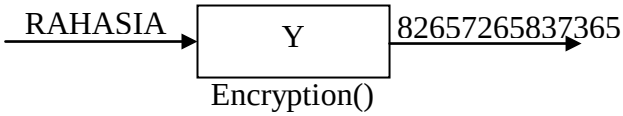
1	49	I	73	A	97	y	121
2	50	J	74	B	98	z	122
3	51	K	75	C	99	{	123
4	52	L	76	D	100	|	124
5	53	M	77	E	101	}	125
6	54	N	78	F	102	~	126
7	55	O	79	G	103		

Contoh jika ingin mengkorversi tulisan “STIKOM”, maka akan diubah menjadi 83 84 73 75 79 77. tetapi tidak hanya sekedar dikonversi saja. Tetapi ada kondisi – kondisi tertentu. Jika posisi sebuah karakter terletak pada urutan yang ganjil, maka akan ditambahkan dengan 69. Dan jika terletak pada urutan genap akan ditambahkan 71. Oleh karena akan menjadi 152 155 142 146 148 148. Dari hasil tersebut akan diambil dua angka terakhir saja pada tiap hasil konversi angka. Dimana ditujukan agar angka yang tersimpan pada pixel tidak terlalu banyak. Jadi hasil terakhirnya didapatkan 525542464848 untuk kata STIKOM. nilai 69 dan 71 didapatkan karena untuk memperoleh nilai ambang batas bawah dan atas antara nilai 100 sampai dengan 199. Nilai byte terendah 32 jika ditambahkan 69 diperoleh nilai 101 dan untuk nilai byte tertinggi 126 jika ditambahkan 71 diperoleh 197. Dimana angka 100 ditempati posisi tombol “tab”, sedangkan angka 198 dan 199 ditempati posisi tombol “enter” (Agus, 2000).

2.5. Enkripsi

Enkripsi adalah sebuah proses mengkodekan sebuah pesan menjadi sesuatu yang tidak mempunyai arti. Sebuah enkripsi terhadap sebuah pesan atau data dilakukan untuk mencegah dari pembacaan data oleh orang yang tidak berhak membacanya. Enkripsi juga dapat berarti pengolahan sekuritas data dalam lingkungan dengan keamanan yang kurang. Transformasi sebuah enkripsi sangat

tergantung dalam 3 hal yaitu data, kata kunci dan algoritma atau metode. Pemodelan sebuah enkripsi standar dapat digambarkan sebagai berikut :



2.6. Dekripsi

Dekripsi mengadung arti sebagai kebalikan dari proses enkripsi yaitu proses transformasi dari sebuah pesan yang terenkripsi dan dikembalikan ke bentuk normal dengan menggunakan algoritma terbalik.

2.7. Proses Enkripsi dan Dekripsi pada Sistem

Proses enkripsi pada sistem tersebut merubah semua karakter menjadi angka antara 0 sampai dengan 9. dimana setiap karakter diwakili dua angka. Sebagai contoh : huruf “A” (nilai byte sama dengan 65). Yang terdapat dalam sebuah kalimat atau kata menempati posisi ganjil, maka 65+69 = 134 dan jika menempati posisi genap maka 65+71 = 136. Dari hasil tersebut diambil dua angka yang terakhir. jika ganjil maka hasil enkripsi huruf “A” = 34, jika genap maka hasil enkripsi huruf “A” = 36. Jadi setiap karakter akan diwakili / di-enkripsi 2 (dua) karakter angka. Hasil tersebut disimpan dalam bentuk Circulant Matrik (M x M) / matrik bujur sangkar. Contoh seperti dalam buku [Gonzalez, Rafael C,1992, *Digital Image Processing*,Addison-Wesley Publishing Company, United States of America]. Dalam hal ini jika terdapat 32 karakter hasil enkripsi maka disimpan dalam matrik ordo 6 x 6, dan jika terdapat 37 karakter hasil enkripsi maka disimpan dalam ordo matrik 7 x 7, karena 37 karakter tidak memungkinkan untuk disimpan dalam ordo matrik 6 x 6. Ordo matrik 6x6 hanya mampu

menampung 36 karakter. Begitu juga untuk kasus jumlah karakter 26, tidak memungkinkan disimpan dalam bentuk ordo matrik 5 x 5. Dari enkripsi angka 0 sampai dengan 9, bahwa angka 0 diwakili oleh sebuah warna pixel, angka 1 diwakili oleh sebuah warna pixel yang lain dan seterusnya sampai angka 9. Jika tampilannya masih kelihatan dalam bentuk warna titik – titik yang tidak sama atau tidak membentuk gambar yang sempurna, maka bisa diubah ke dalam bentuk gambar tertentu. Dalam arti gambar tersebut bentuknya beraturan atau sempurna, contoh seperti gambar wajah orang, pemandangan dan lain sebagainya tergantung keinginan untuk mengkodekannya, sehingga orang yang tidak tahu menganggap bahwa file tersebut hanyalah sebuah gambar, yang ternyata di setiap pixels gambar tersebut tersimpan beberapa dokumen rahasia atau penting.

2.8. Sistem Operasi

Sistem yang dipilih adalah Windows 2000 Profesional, sistem operasi ini memliki kemampuan setara dengan Windows NT. Dimana kemampuannya sangat bagus dalam jaringan karena mampu membentuk domain, serta tingkat proteksi file dan direktori lebih baik serta tingkat tampilan grafis yang cukup baik. Begitu juga tentang kinerja dari sistem operasi ini lebih cepat dan responsive selain itu juga mampu meningkatkan efisiensi memori serta media penyimpanan.

2.9. Database

Database yang digunakan dalam membangun aplikasi ini adalah Oracle 8.0.5 dan Microsoft Access 2000. Karena Oracle versi 8.0.5 tersebut adalah versi pertama oracle yang mampu menyimpan gambar serta file lainnya ke dalam database. Selain itu oracle sudah banyak yang mengakui baik itu dari segi

keamanan data maupun integritas dengan aplikasi lain. Sehingga banyak sekali instansi atau perusahaan yang menggunakan database ini, berdasarkan pertimbangan di atas, selain juga mendapatkan materi perkuliahan di STIKOM Surabaya, maka dipilihlah Oracle menjadi database pada aplikasi ini. Dimana mampu menyimpan file foto dan file lainnya. Sedangkan Microsoft Access 2000 untuk simpan data pemakai / user.

2.10.SQl. Programming

Struktur Query Language (SQL) adalah kumpulan perintah yang telah menjadi standar untuk melakukan manipulasi terhadap suatu database yang digunakan bersama aplikasi – aplikasi pemrograman seperti Delphi dan lainnya.

2.11.ADO Connection

ADO Connection atau ActiveX Data Object Connection, Merupakan sebuah tool / fasilitas untuk koneksi antara Borland Delphi dengan Oracle secara langsung. Dimana ADO Connection merupakan bagian komponen dari Borland Delphi (*Include*).

2.12.Interaksi Manusia dan Komputer

Sistem komputer terdiri tiga aspek yaitu perangkat keras (hardware), perangkat lunak (software) dan manusia (brainware), yang saling bekerja sama. Kerja sama tersebut ditunjukan antara komputer dengan manusia. Komputer yang terdiri dari perangkat keras dan perangkat lunak yang digunakan oleh manusia untuk bekerja sama guna menghasilkan sesuatu sesuai dengan keinginan manusia. Beberapa kategori yang dapat dijadikan pedoman dalam membangun interaksi manusia dengan komputer sebagai berikut :

1. Pemakai Komputer

   Dalam membuat suatu interaksi harus memperhatikan siapa yang akan menggunakan sistem tersebut, agar nantinya pemakai tidak merasa kesulitan dalam menjalankan sistem tersebut.

2. Alat Input

   Alata Input yang digunakan harus yang mudah dipakai oleh user, sehingga user tidak menemui kesulitan dalam penggunaanya. Contoh Keyboard harus bersifat universal, maksudnya tombol – tombol yang digunakan mudah dimengerti oleh semua user.

3. Bahasa Input

   Bahasa input yang digunakan harus mudah dimengerti oleh user. Biasanya bahasa universal yang digunakan adalah Bahasa Inggris.

4. Rancangan Dialog

   Untuk memudahkan user dalam mengakomodasikan keinginannya. Rancangan Dialog harus didesain mudah dimengerti oleh user apa maksud dari dialog tersebut.

5. Pemandu User

   Adanya suatu pedoman dalam sistem yang dibuat untuk memudahkan user dalam menggunakan sistem yang digunakan. Pemandu user sebaiknya jangan terlalu banyak kata – kata atau perintah, tetapi lebih diutamakan gambar – gambar atau tampilan aplikasi yang ada. Karena kalau terlalu banyak kata – kata user mungkin sulit untuk mengerti. Contoh User Manual.

6. Alat Output

Alat untuk dapat melihat hasil atau informasi yang dikeluarkan oleh sistem. Contoh Monitor, Speaker dan lainya.

7. Pesan Komputer

   Adanya suatu pesan kepada user apabila melakukan suatu kesalahan, sehingga user segera memperbaiki kesalahan yang telah dilakukannya.

8. Rancangan Layar

   Rancangan Layar sangat perlu diperhatikan karena berhubungan langsung dengan pandangan user.