BAB II

KAJIAN PUSTAKA

Kajian Pustaka menjelaskan dasar-dasar teori yang digunakan dalam penelitian yang dilakukan pada Skripsi. Teori-teori yang digunakan meliputi keamanan informasi, citra digital, Pengukuran *error* pada citra, steganografi, kriptografi, teknologi *java*, dan MySQL.

2.1. Keamana Informasi

Keamanan informasi merupakan salah satu aspek yang penting dalam berkomunikasi, namun keamanan seringkali dilupakan ketika melakukan komunikasi. Informasi yang jatuh ke tangan yang salah dapat menimbulkan masalah yang besar seperti penipuan, pencurian, pemerasan dan masih banyak lagi masalah yang akan ditimbulkan.

Keamanan informasi mempunyai beberapa aspek yang harus dipenuhi, agar informasi dapat terjamin keaslian dan keamanannya. Aspek-aspek umum tersebut meliputi *confidentiality, integrity, authentication, availability* dan *non repudiation.*

1. *Confidentiality.*

   Confidentiality atau kerahasiaan yaitu keamanan informasi harus dapat menjamin kerahasiaan dari informasi. Salah satu cara yang dapat

dilakukan yaitu dengan membatasi hanya orang yang mempunyai hak saja yang dapat membaca atau mengubah suatu informasi.

2. *Integrity.*

   Integrity berhubungan dengan keaslian informasi. *Integrity* yaitu menjamin keutuhan dan keaslian informasi yang dikirimkan, agar informasi tidak dirusak atau diubah oleh orang yang tidak berhak. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.

3. *Authentication.*

   Authentication yaitu usaha atau metode untuk mengetahui keaslian dari informasi, dan memastikan bahwa informasi diterima oleh orang yang benar. Untuk menjaga otentikasi terhadap informasi, dapat digunakan *digital signature* untuk memastikan keaslian informasi.

4. *Availability.*

   Availability atau ketersediaan data yaitu keamanan informasi harus dapat menjamin bahwa data atau informasi harus tersedia ketika akan digunakan. Untuk menjamin ketersediaan data, sistem harus mempunyai cadangan data jika data tersebut hilang.

5. *Non Repudiation.*

   Non repudiation yaitu menjamin bahwa seorang pengirim informasi tidak dapat menyangkal keaslian dari informasi yang dikirimnya. Sehingga

penerima informasi dapat memastikan bahwa informasi yang diterima merupakan informasi yang asli.

2.2. Citra Digital

Citra secara harafiah, adalah gambar pada bidang dua dimensi (dwimatra). Ditinjau dari sudut pandang matematis, citra merupakan fungsi menerus (*continue*) dari intensitas cahaya pada bidang dwimatra. Sedangkan citra digital adalah citra yang dapat diolah oleh komputer.

Sebuah citra digital dapat diwakili oleh sebuah matriks yang terdiri dari M kolom dan N baris, dimana perpotongan antara kolom dan baris disebut *pixel*, yaitu elemen terkecil dari sebuah citra. Sebuah citra digital dapat ditulis dalam bentuk fungsi II.1 berikut.

$$f(x,y) = \begin{bmatrix} f(0,0) & f(0,1) & .. & f(0,M-1) \\ f(1,0) & .. & .. & f(1,M-1) \\ .. & .. & .. & .. \\ f(N-1,0) & f(N-1,1) & .. & f(N-1,M-1) \end{bmatrix} \text{.....(II,1)}$$

Terdapat banyak format file dari citra digital, format file citra ini terdiri dari beberapa jenis dan setiap jenisnya memiliki karakteristik masing- masing. Beberapa contoh format umum, pada citra digita yaitu, *Bitmap(BMP), Joint Photographic Group Experts(JPEG), Graphics Interchange Format(GIF),* dan *Portabe Network Graphics(PNG).*

1. *Bitmap(BMP).*

Bitmap merupakan format baku citra pada sistem operasi *windows* dan IBM OS/2. Citra berformat BMP merupakan citra yang tidak terkompresi, sehingga pada umumnya citra berformat BMP mempunyai ukuran yang relatif lebih besar dibandingkan dengan forman citra lainnya. Intensitas pixel dari citra berformat BMP dipetakan ke sejumlah bit tertentu. Panjang setiap pixel pada *bitmap* yaitu 4 bit, 8 bit, sampai 24 bit yang merepresentasikan nilai intensitas *pixel*. Dengan demikian ada sebanyak 2^8 = 256 derajat keabuan, mulai dari 0 sampai 255.

2. *Joint Photographic Group Experts(JPEG).*

   Joint Photographic Group Experts (JPEG) merupakan standar kompresi file yang dikembangkan oleh *Group Joint Photographic Experts* menggunakan kombinasi DCT dan pengkodean *Huffman* untuk mengkompresikan citra. Citra JPEG merupakan citra terkompresi yang bersifat *lossy*, artinya citra tidak bisa dikembalikan ke bentuk aslinya. Citra ini memiliki ukuran yang relatif lebih kecil dibandingkan dengan citra berformat BMP karena telah terkompresi.

3. *Graphics Interchange Format(GIF).*

   Graphics Interchange Format (GIF) merupakan format citra terkompresi. Ukuran dari citra berformat GIF merupakan yang terkecil dari semua format citra digital. Kombinasi warna yg tersedia sebanyak 256 warna. Citra jenis ini banyak dugunakan untuk keperluan website, untuk membuat sebuah icon, logo dan keperluan lainnya yang

mengharuskan menggunakan citra dengan ukuran yang kecil. Citra jenis ini juga dapat dibuat animasi.

4. *Portable Network Graphics(PNG).*

   Portable Network Graphics (PNG) adalah salah satu format penyimpanan citra yang menggunakan metode kompresi yang tidak menghilangkan bagian dari citra tersebut (*lossless compression*). Citra berformat PNG merupakan salah satu format yang baik untuk digunakan pengolahan citra, karena format ini selain tidak menghilangkan bagian dari citra yang sedang diolah.

2.3. Pengukuran *Error* Citra

Pengukuran *error* citra dilakukan untuk mengetahui tingkat kesamaan antara citra asli dengan citra yang telah dimanipulasi. Pengukuran *error* dilakukan dengan menghitung *Mean Square Error* (MSE) dan *Peak Signal to Noise Ratio* (PSNR) dari citra.

Mean Square Error (MSE) adalah tingkat kesalahan *pixel – pixel* citra hasil dari pemrosesan terhadap citra aslinya. Rumus untuk menghitung MSE pada citra digital yaitu menggunakan persamaan II.2. Sedangkan *Peak Signal to Noise Ratio* (PSNR) merupakan nilai (rasio) yang menunjukan tingkat toleransi *noise* tertentu terhadap banyaknya *noise* pada suatu citra. Semakin tinggi nilai PSNR dari suatu citra, maka semakin kecil tingkat kesalahan yang dimiliki citra tersebut. Untuk menghitung nilai PSNR digunakan persamaan II.3.

$$MSE = \frac{1}{MN}\sum_{y=1}^{m}\sum_{x=1}^{n}[\,I(x,y) - I'(x,y)\,]^2 \quad \text{.....(II.2)}$$

Dimana: I(x,y) adalah nilai *pixel* di citra asli.

I'(x,y) adalah nilai *pixel* pada citra hasil kompresi.

M, N adalah dimensi citra.

$$PSNR = 10\ LOG_{10}\left(\frac{255^2}{MSE}\right) \quad \text{.....(II.3)}$$

Semakin besar nilai PSNR dari citra, maka citra yang telah dimanipulasi semakin mendekati citra aslinya, dengan kata lain semakin bagus kualitas citra hasil manipulasi tersebut. Sebaliknya, semakin kecil nilai PSNR semakin berkurang kualitas citra hasil manipulasi. Nilai PSNR pada umumnya berada pada rentang 20 – 40 db.

2.4. Steganografi

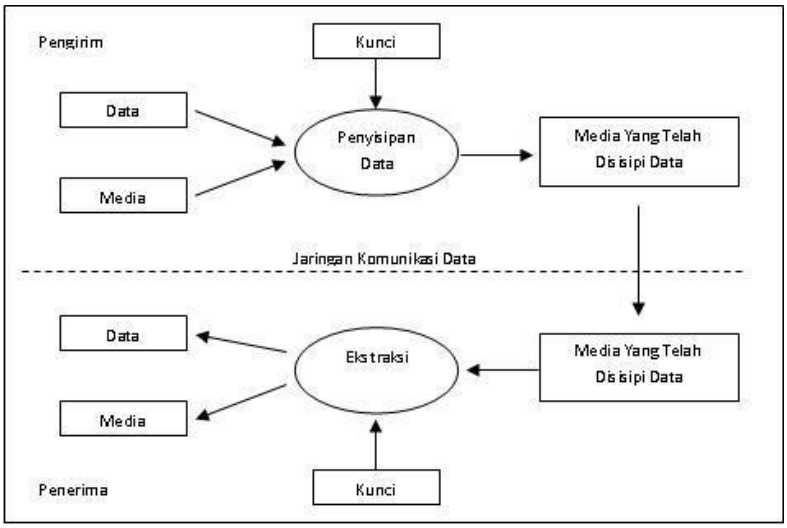
Steganografi merupakan salah satu metode yang dapat digunakan untuk mengamankan informasi. Steganografi berbeda dengan kriptografi atau metode keamanan informasi lainnya, metode ini yaitu menyembunyikan informasi atau pesan kedalam media lain seperti citra digital, teks, suara atau video sehingga tidak menimbulkan kecurigaan orang lain. Steganografi membutuhkan dua properti, yaitu informasi dan media penampung. Media penampung yang dapan digunakan yaitu citra digital, audio, teks, dan video.

Tujuan dari steganografi adalah menyembunyikan data/pesan pada suatu media. Media penampung data/pesan yang akan disembunyikan dapat berupa gambar digital, suara, video dan media lainnya. Jika pada media yang telah

disisipi pesan rahasia tersebut terlihat mencurigakan, maka tujuan dari steganografi tersebut tidak tercapai.

Teknik steganografi sudah dikenal sejak jaman Yunani dan Romawi kuno. Misalnya dengan mencukur kepala budak, lalu pesan rahasia ditulis pada kulit kepalanya. Setelah rambut budak tersebut tumbuh, budak terebut dikirim untuk menyampaikan pesan rahasia tersebut.

Steganografi mempunyai dua proses utama yaitu *embed*/penyisipan dan ekstrak/pengungkapan terlihat pada gambar 2.1. Proses penyisipan merupakan proses menyisipkan *hidden object* atau informasi/pesan yang akan disisipkan, ke dalam sebuah *cover object* atau media penampung, sehingga menghasilkan file baru yang telah tersisipi pesan didalamnya yang disebut dengan *stego file*. Sedangkan proses ekstrak merupakan proses pengembalian *hidden object* secara utuh setelah disisipkan ke dalam *cover object*.



Gambar 2.1 Proses Steganografi

Sumber : (Morkel, T., JHP. Eloff, dan MS. Olivier 2010:44)

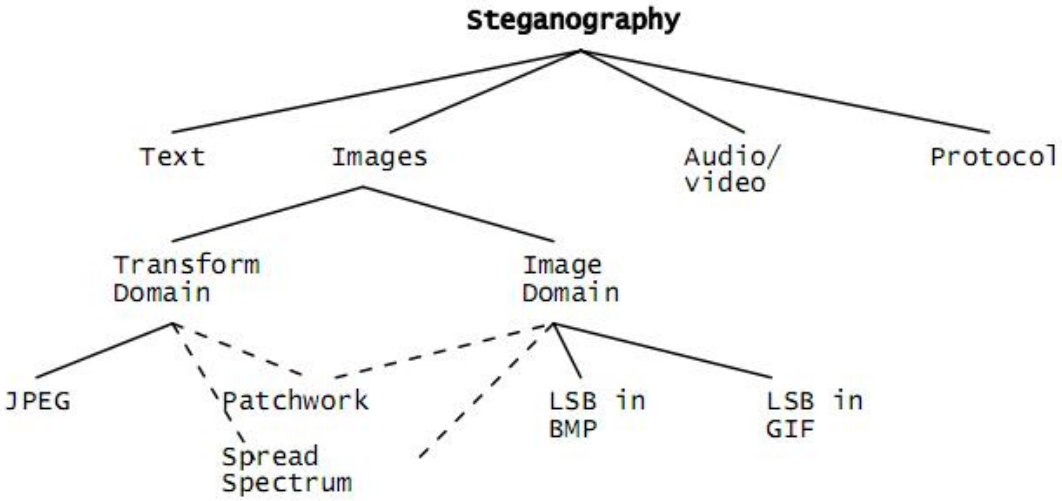
Ada beberapa criteria-kriteria yang harus dipenuhi dalam pembuatan steganografi. Kriteria – kriteria tersebut yaitu:

1. *Impercepbility,* yaitu keberadaan pesan tidak dapat dipersepsi oleh indrawi. Jika pesan disisipkan ke dalam sebuah citra, *citra* yang telah disisipi pesan harus tidak dapat dibedakan dengan citra asli oleh mata. Begitu pula dengan suara,telinga harus mendapati perbedaan antara suara asli dan suara yang telah disisipi pesan.
2. *Fidelity,* yaitu mutu media penampung tidak berubah banyak akibat penyisipan. Perubahan yang terjadi harus tidak dapat dipersepsi oleh indrawi.
3. *Recovery,* yaitu pesan yang disembunyikan harus dapat diungkap kembali. Tujuan steganografi adalah menyembunyikan informasi, maka sewaktu-waktu informasi yang disembunyikan harus dapat diambil kembali untuk dapat digunakan lebih lanjut sesuai keperluan.

2.5. Steganografi Pada Citra Digital

Citra digital merupakan media penampung yang banyak digunakan dalam steganografi. Penggunaan citra digital sebagai media penampung mempunyai kelebihan karena indera penglihatan manusia memiliki keterbatasan terhadap warna, sehingga dengan keterbatasan tersebut manusia sulit membedakan citra digital yang asli dengan citra digital yang telah disisipi pesan rahasia.

Banyak metode yang dapat digunakan dalam pembuatan steganografi pada citra digital seperti *Least Significant Bits* (LSB), *Bit Plane Complexity Segmentation* (BPCS), *Discrete Cosine Transform* (DCT), *Discrete Wavelet Transform* (DWT), *Spread Spectrum* dan metode-metode lainnya. Dari banyaknya metode tersebut, metode steganografi pada citra digital dapat dibagi menjadi dua bagian yaitu metode pada *transform domain* dan *image domain* seperti pada gambar 2.2.



Gambar 2.2 Kategori Metode Steganografi Pada Citra Digital.

Sumber : (Morkel, T., JHP. Eloff, dan MS. Olivier 2010:65)

Transform Domain

Ranah transform memfokuskan penyisipan pesan ke dalam frekuensi dari *cover-object*. Ranah ini memanfaatkan area *cover-object* yang cenderung tidak akan mengalami pemrosesan digital. Teknik-teknik yang dapat digunakan untuk

melakukan seteganografi pada citra digital diranah transform di antaranya adalah sebagai berikut:

1. *Discrete Cosine Transform*
2. *Fourier Transform*
3. *Wavelet Transform*

Image Domain

Image Domain merupakan penyembunyian pesan pada citra digital pada ranah spasial, ranah spasial ini juga dikenal sebagai teknik subtitusi. Teknik subtitusi ini dilakukan sedemikian rupa sehingga media penampung yang disisipkan pesan/informasi tidak dapat dipersepsi oleh indrawi perubahannya. Metode steganografi yang beroperasi pada ranah spatial diantaranya yaitu *least significant bit* (LSB), *dynamics cell spreading* (DCS), dan *pixel value differencing(PVD).*

2.6. *Pixel Value Differencing (PVD)* Steganografi

Pixel Value Differencing merupakan salah satu metode yang dapat digunakan dalam steganografi. Metode ini beroperasi pada ranah spasial dari citra. Berdasarkan analisis terhadap sistem penglihatan manusia yang menyatakan bahwa, mata manusia tidak sensitif terhadap perubahan pada *pixel* yang memiliki kekontrasan tinggi melainkan sensitif terhadap perubahan pada *pixel* yang memiliki kekontrasan rendah. Melalui sifat tersebut maka lebih banyak *bit* data rahasia yang dapat disisipkan pada *pixel* yang memiliki nilai kekontrasan tinggi,

dan sedikit *bit* yang dapat disisipkan pada *pixel* dengan kekontrasan rendah. Hal tersebut yang menjadi dasar pemikiran metode *Pixel value differencing* (PVD) pada steganografi.

Proses penyisipan pada metode ini dilakukan dengan cara membandingkan dua *pixel* yang bertetangga P_i dan P_{i+1} dengan menggunakan persamaan II.4.

$$d = |P_i - P_{i+1}| \quad \text{(II.4)}$$

Hasil dari perbandingan tersebut digunakan untuk mengetahui berapa banyak *bit* yang dapat disisipkan kedalam dua *pixel* yang dibandingkan. Metode ini menggunakan skema Wu dan Tsai untuk mengetahui *range* dari perbandingan *pixel* sebelumnya. Skema Wu dan Tsai yang digunakan yaitu R = {[0,7],[8,15],[16,31],[32,63],[64,127],[128,255]}. Skema ini digunakan untuk mengetahui terdapat di *range* mana selisih dari dua *pixel* tersebut, jika telah diketahui dimana letak *range* nya, maka jumlah *bit* pesan yang disisipkan dapat diketahui dengan persamaan II.5.

$$t = \lfloor Log_2 w_i \rfloor \quad \text{(II.5)}$$

w_i : Nilai terkecil dari skema wu dan tsai, letak *range* selisih perbandingan dua *pixel*.

Penyisipan pesan dapat dilakukan dengan mengambil sebanyak t *bit* dari pesan yang akan disisipkan. Selanjutnya dihitung nilai *difference value* yang baru untuk penyisipan kedalam citra menggunakan persamaan II.6

$$d_i^{'} = l_i + b \quad \text{.....(II.6)}$$

d_i : Nilai terkecil dari skema wu dan tsai, letak *range* selisih perbandingan dua *pixel*.

Untuk menyisipkan pesan ada beberapa aturan yang harus dipenuhi yaitu :

1. Jika $P_i \geq P_{i+1}$ dan $d'_i > d_i$, maka $(P_i + \lceil m/2 \rceil , P_{i+1} - \lfloor m/2 \rfloor)$
2. Jika $P_i < P_{i+1}$ dan $d'_i > d_i$, maka $(P_i - \lfloor m/2 \rfloor , P_{i+1} + \lceil m/2 \rceil)$
3. Jika $P_i \geq P_{i+1}$ dan $d'_i \leq d_i$, maka $(P_i - \lceil m/2 \rceil , P_{i+1} + \lfloor m/2 \rfloor)$
4. Jika $P_i < P_{i+1}$ dan $d'_i \leq d_i$, maka $(P_i + \lceil m/2 \rceil , P_{i+1} - \lfloor m/2 \rfloor)$

Dimana m didapat dari selisih d'_i dengan d_i menggunakan persamaan II.7.

$$m = |d_i^{'} - d_i| \quad \text{.....(II.7)}$$

Proses-proses tersebut dilakukan terus hingga *bit* pesan tersisipi semuanya kedalam citra. Proses ekstraksi pesan dari citra *stego* menggunakan metode ini dimulai dengan menghitung nilai *difference value* (d_i) antara dua *pixel* yang bertetangga. Nilai *difference value* tersebut digunakan untuk mengetahui nilai *continuous ranges* (R) yang sudah didefinisikan menggunakan skema wu dan tsai.

Berdasarkan informasi tersebut dapat diketahui ukuran data rahasia yang disisipkan pada kedua *pixel* menggunakan persamaan II.5, sehingga pesan rahasia yang telah disisipkan didapatkan kembali. Proses ekstraksi ini dilakukan sampai semua data rahasia yang telah disisipkan didapatkan kembali.

2.7. Kriptografi

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, otentikasi, dan autentifikasi data. Kriptografi bukan satu-satunya cara untuk menyediakan keamanan informasi, melainkan satu set teknik yang dapat digunakan untuk mengamankan informasi.

Secara umum, kriptografi terdiri dari dua buah bagian utama yaitu bagian enkripsi dan bagian dekripsi. Enkripsi adalah proses transformasi informasi menjadi bentuk lain sehingga isi pesan yang sebenarnya tidak dapat dipahami, hal ini dimaksudkan agar informasi tetap terlindung dari pihak yang tidak berhak menerima. Sedangkan dekripsi adalah proses kebalikan enkripsi, yaitu transformasi data terenkripsi ke data bentuk semula. Proses transformasi dari *plainteks* menjadi *cipherteks* akan dikontrol oleh kunci. Peran kunci sangatlah penting, kunci bersama-sama dengan algoritma matematisnya akan memproses *plainteks* menjadi *cipherteks* dan sebaliknya.

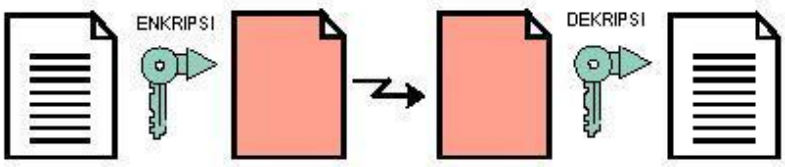
Kriptografi tidak memenuhi semua aspek dari keamanan informasi. Kriptografi hanya memenuhi empat aspek dalam keamanan informasi yang merupakan tujuan dari kriptografi. Keempat aspek tersebut yaitu kerahasiaan (*confidentiality*), integritas data (*integrity*), otentikasi data (*authentication*), dan *non-repudiation*.

2.8. Algoritma Kriptografi

Algoritma kriptografi yang handal adalah algoritma kriptografi yang kekuatannya terletak pada kunci, bukan pada kerahasiaan algoritma itu sendiri. Berdasarkan jenis kuncinya, algoritma kriptografi dibagi menjadi dua jenis yaitu algoritma simetris dan algoritma asimetris.

2.8.1. Algoritma Simetris

Algoritma simetris (*symmetric algorithm*) adalah suatu algoritma dimana kunci enkripsi yang digunakan sama dengan kunci dekripsi sehingga algoritma ini disebut juga sebagai *single-key algorithm*. Ilustrasi penggunaan algoritma kriptografi dengan kunci simetris dapat terlihat pada gambar 2.3 berikut.



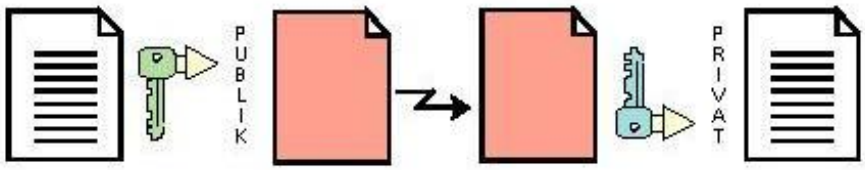
Gambar 2.3 Ilustrasi Kriptografi Dengan Kunci Simetris

Sumber : (Munir, Rinaldi 2006:22)

Algoritma simetris banyak digunakan karena lebih cepat dan lebih simpel, namun penggunaan kunci simetris juga mempunyai kekurangan, karena jika kunci dapat diketahui, maka informasi pun dapat diketahui. Beberapa algoritma kriptografi yang termasuk pada algoritma simetris yaitu DES, AES, *Rijndael*, *Blowfish*, dan IDEA.

2.8.2. Algoritma Asimetris

Algoritma asimetris (*asymmetric algorithm*) adalah suatu algoritma dimana kunci enkripsi yang digunakan tidak sama dengan kunci dekripsi[5]. Algoritma ini menggunakan dua kunci yakni kunci publik (*public key*) dan kunci privat (*private key*). Kunci publik disebarkan secara umum sedangkan kunci privat disimpan secara rahasia oleh pengguna. Ilustrasi penggunaan algoritma kriptografi dengan kunci asimetris dapat terlihat pada gambar 2.4 berikut.



Gambar 2.4. Ilustrasi Kriptografi Dengan Kunci Asimetris

Sumber : (Munir, Rinaldi 2006:28)

Algoritma asimetris mempunyai keamanan yang lebih baik, karena jika *public key* diketahui, informasi belum tentu dapat diketahui karena *private key* kemungkinan berbeda. Namun akan menjadi sulit dan lama ketika implementasinya. Beberapa algoritma kriptografi yang termasuk pada algoritma asimetris yaitu Diffie – Hellman, RSA, ElGamal, dan DSA.

2.9. Algoritma *Rijndael*

Rijndael termasuk dalam jenis algoritma simetris dan *cipher block*. Dengan demikian algoritma ini menggunakan kunci yang sama saat enkripsi dan dekripsi serta masukan dan keluarannya berupa blok dengan jumlah *bit* tertentu.

Rijndael mendukung berbagai variasi ukuran blok dan kunci yang akan digunakan, namun *Rijndael* mempunyai ukuran blok dan kunci yang tetap sebesar 128, 192, 256 *bit*. Pemilihan ukuran blok data dan kunci akan menentukan jumlah proses yang harus dilalui untuk proses enkripsi dan dekripsi. Tabel 2.1 adalah perbandingan jumlah proses yang harus dilalui untuk masing-masing masukan.

Tabel 2.1 Jumlah Proses Berdasarkan Ukuran *Bit* Blok dan Kunci

Sumber : (Surian, Didi 2006:97)

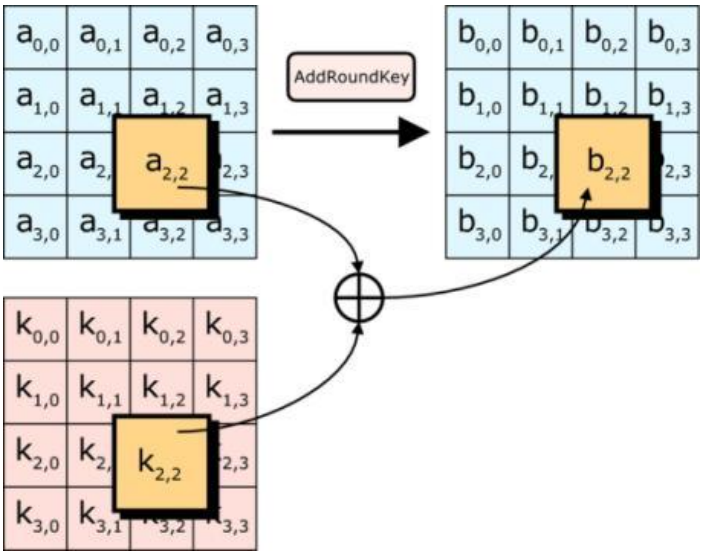
Ukuran blok dan kunci	**Panjang Kunci (Nk) Dalam words**	**Ukuran Blok Data (Nb) Dalam words**	**Jumlah Proses (Nr)**
128 bit	4	4	10
192 bit	6	4	12
256 bit	8	4	14

Blok-blok data masukan dan kunci dioperasikan dalam bentuk *array*. Setiap anggota *array* sebelum menghasilkan keluaran *cipher text* dinamakan dengan *state*. Setiap *state* akan mengalami proses yang terdiri dari empat tahap yaitu, *Add Round Key*, *Sub Bytes*, *Shift Rows*, dan *Mix Columns*. Kecuali pada tahap *Mix Columns*, ketiga tahap lainnya akan diulang pada setiap proses sedangkan tahap *Mix Columns* tidak akan dilakukan pada tahap terakhir.

2.9.1. *Add Round Key*

Proses *Add Round Key* yaitu proses menggabungkan *subkey* dengan *state* menggunakan operasi XOR untuk setiap *byte* dari *subkey* dengan *byte* yang dari *state*. Untuk setiap tahap, *subkey* dibangkitkan dari kunci utama dengan

menggunakan proses *key schedule*. Proses *Add Round Key* dapat dilihat pada Gambar 2.5.



Gambar 2.5 Proses *Add Round Key* Algoritma *Rijndael*

Sumber : (Surian, Didi 2006:97)

2.9.2. Sub Bytes

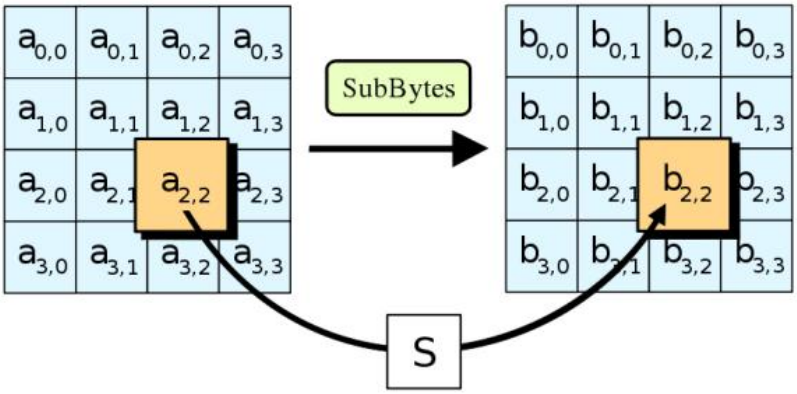
Proses *Sub Bytes* adalah proses substitusi dengan cara mengganti setiap *byte state* dengan *byte* pada sebuah tabel yang dinamakan tabel *S-Box* yang dapat dilihat pada Tabel 2.2

Tabel 2.2 *S-Box*

Sumber : (Surian, Didi 2006:98)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	18	23	C6	E8	87	B8	01	4F	36	A6	D2	F5	79	6F	91	52
1	60	BC	9B	8E	A3	0C	7B	35	1D	E0	D7	C2	2E	4B	FE	57
2	15	77	37	E5	9F	F0	4A	CA	58	C9	29	0A	B1	A0	6B	85
3	BD	5D	10	F4	CB	3E	05	67	E4	27	41	8B	A7	7D	95	C8
4	FB	EE	7C	66	DD	17	47	9E	CA	2D	BF	07	AD	5A	83	33
5	63	02	AA	71	C8	19	49	C9	F2	E3	5B	88	9A	26	32	B0
6	E9	0F	D5	80	BE	CD	34	48	FF	7A	90	5F	20	68	1A	AE
7	B4	54	93	22	64	F1	73	12	40	08	C3	EC	DB	A1	8D	3D
8	97	00	CF	2B	76	82	D6	1B	B5	AF	6A	50	45	F3	30	EF
9	3F	55	A2	EA	65	BA	2F	C0	DE	1C	FD	4D	92	75	06	8A
A	B2	E6	0E	1F	62	D4	A8	96	F9	C5	25	59	84	72	39	4C
B	5E	78	38	8C	C1	A5	E2	61	B3	21	9C	1E	43	C7	FC	04
C	51	99	6D	0D	FA	DF	7E	24	3B	AB	CE	11	8F	4E	B7	EB
D	3C	81	94	F7	B9	13	2C	D3	E7	6E	C4	03	56	44	7F	A9
E	2A	BB	C1	53	DC	0B	9D	6C	31	74	F6	46	AC	89	14	E1
F	16	3A	69	09	70	B6	C0	ED	CC	42	98	A4	28	5C	F8	86

Sebuah tabel *S-Box* terdiri dari 16 baris dan 16 kolom dengan masing-masing berukuran 1 byte. Proses *Sub Bytes* dapat dilihat pada Gambar 2.6.

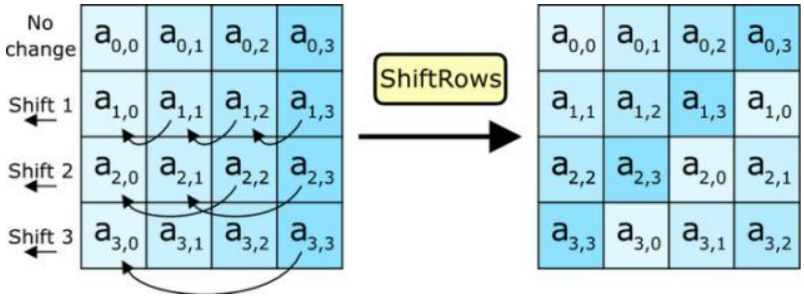


Gambar 2.6 Proses *Sub Bytes* Algoritma *Rijndael*

Sumber : (Surian, Didi 2006:98)

2.9.3. *Shift Rows*

Proses *Shift Rows* adalah proses perputaran pada tiga baris terakhir dari state dengan jumlah putaran yang berbeda-beda. Baris ke-1 akan diputar sebanyak 1 kali, baris ke-2 akan diputar sebanyak 2 kali, dan baris ke-3 akan diputar sebanyak 3 kali, sedangkan baris ke-0 tidak akan diputar. Proses *Shift Rows* diperlihatkan pada Gambar 2.7.



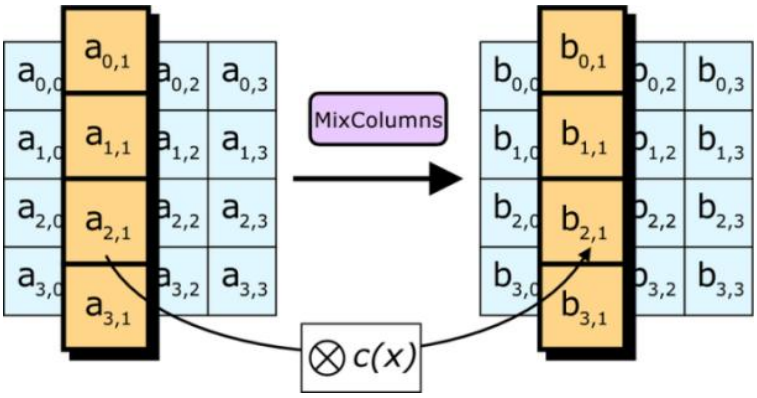
Gambar 2.7 Proses *Shift Rows* Algoritma *Rijndael*

Sumber : (Surian, Didi 2006:100)

2.9.4. *Mix Columns*

Operasi *Mix Columns* adalah proses menggabungkan 4 *bytes* dari setiap kolom dari tabel *state* dengan menggunakan transformasi linier. Operasi *Mix Columns* memperlakukan setiap kolom sebagai polinomial 4 suku dalam *Galois field* dan kemudian dikalikan dengan c(x) *modulo* (x4+1), dimana c(x)=3x3+x2+x+2. Kebalikkan dari *polinomial* ini adalah

c(x)=11x3+13x2+9x+14. Operasi *Mix Columns* juga dapat dipandang sebagai perkalian matrix seperti terlihat pada gambar 2.8.



Gambar 2.8 Proses *Mix Columns* Algoritma *Rijndael*

Sumber : (Surian, Didi 2006:101)

2.10. Teknologi *Java*

Java adalah sebuah teknologi yang diperkenalkan oleh *Sun Microsystems* pada pertengahan tahun 1990. Menurut definisi dari *Sun*, *Java* adalah nama untuk sekumpulan teknologi untuk membuat dan menjalankan perangkat lunak pada komputer *stand alone* ataupun pada lingkungan jaringan. *Java* berdiri di atas sebuah mesin *interpreter* yang diberi nama *Java Virtual Machine* (JVM). JVM inilah yang akan membaca *bytecode* dalam *file .class* dari suatu program sebagai representasi langsung program yang berisi bahasa mesin.

Platform Java terdiri dari kumpulan *library*, JVM, kelas-kelas *loader* yang dipaket dalam sebuah lingkungan rutin *Java*, dan sebuah *compiler*, *debuger*, dan perangkat lain yang dipaket dalam *Java Development Kit* (JDK).

2.11. *Unified Modelling Language* (UML)

Unified Modelling Language (UML) adalah sebuah bahasa pemodelan standar yang memiliki sintaks dan semantic. Pemodelan ini sangat cocok digunakan untuk merancang dan memodelkan sistem berorientasi objek.

Diagram pada UML dibagi menjadi dua bagian yaitu *structural* diagram dan *behavior* diagram. *Structural* diagram digunakan untuk mendeskripsikan relasi antar kelas. *Tools* yang digunakan pada bagian ini yaitu *class diagram*. Sedangkan *behavior* diagram digunakan untuk mendeskripsikan interaksi antara aktor dan sebuah *use case* (bagaimana seorang aktor menggunakan sistem). *Tools* yang digunakan pada bagian ini yaitu *Use case* diagram dan *Activity* diagram.

2.12. MySQL

Menurut Abdul Kadir (2008 : 2) MySQL merupakan software yang tergolong sebagai DBMS (*Database Management System*) yang bersipat *Open Source*. Open Source menyatakan bahwa software ini dilangkapi dengan *source code* (kode yang dipakai untuk membuat MySQL), selain itu tentu saja bentuk *executable*-nya atau kode yang dapat dijalankan secara langsung dalam sistem oprasi, dan bisa diperoleh dengan cara men-*downlaod* di internet secara geratisan.

MySQL awalnya dibuat oleh perpustakaan konsultan bernama TcX yang berlokasi di Swedia. Saat ini pengembangan MySQL berada di bawah naungan perusahaan MySQL AB.