BAB II

LANDASAN TEORI

2.1 Kriptografi

2.1.1 Pengertian Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu, *cryptos* yang berarti rahasia dan *graphein* yang berarti tulisan. Kriptografi adalah ilmu mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh sesorang yang tidak memiliki kunci dekripsi (Sentot, 2010).

Kriptografi sudah digunakan untuk menjaga kerahasiaan suatu informasi sejak jaman romawi kuno yaitu oleh kaisar romawi, Julius Caesar dengan cara menggeser karakter dengan nilai tertentu.

Dalam kriptografi terdapat beberapa istilah yaitu sebagai berikut :

a. Plainteks, merupakan teks asli yang masih mudah dipahami dan belum dienkripsi.
b. Chiperteks, merupakan teks yang telah berubah strukturnya karena sudah dienkripsi dengan menggunakan suatu kunci tertentu.
c. Proses enkripsi, merupakan proses dimana Plainteks diubah menjadi chiperteks dengan membutuhkan suatu kunci kriptografi.
d. Proses dekripsi, merupakan proses dimana chiperteks diubah menjadi plainteks kembali dengan menggunakan kunci kriptografi.

$$EK(M) = C \quad \text{(Proses Enkripsi)}$$
$$DK(C) = M \quad \text{(Proses Dekripsi)}$$

Saat proses enkripsi, pesan M akan disandikan dengan suatu kunci K lalu dihasilkan pesan C. Pada proses dekripsi, pesan C tersebut diuraikan dengan menggunakan kunci K sehingga dihasilkan pesan M yang sama seperti pesan sebelumnya. Keamanan suatu pesan tergantung pada kunci

ataupun kunci-kunci yang digunakan, dan tidak tergantung pada algoritma yang digunakan.

Gambar 2.1 Alur Kriptografi

Tujuan dari kriptografi ini yaitu dapat memenuhi kebutuhan umum suatu transaksi meliputi:

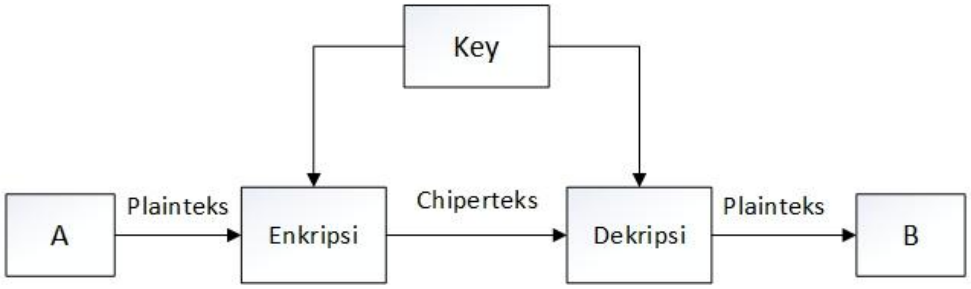
1. Kerahasiaan (*confidentiality*), yaitu kerahasiaan pesan yang dikirim akan terjaga sehingga hanya penerima dan pihak - pihak yang mempunyai izinlah yang bisa membaca pesan tersebut.
2. Keutuhan (*integrity*), keutuhan data yang dikirimkan menjadi jaminan bahwa data yang dikirimkan tidak mengalami perubahan sampai ke tangan penerima.
3. Jaminan identitas (*authenticity*), pihak-pihak yang melakukan transaksi dilakukan dengan menggunakan *password* atau sertifikat digital. Sedangkan keotentikan data transaksi dapat dilakukan dengan tanda tangan digital.
4. Barang bukti yang tidak bisa disangkal (*non-repudiation*).

2.1.2 Jenis Kriptografi

Jenis kriptografi dibedakan menjadi dua jenis berdasarkan kunci yang digunakan yaitu:

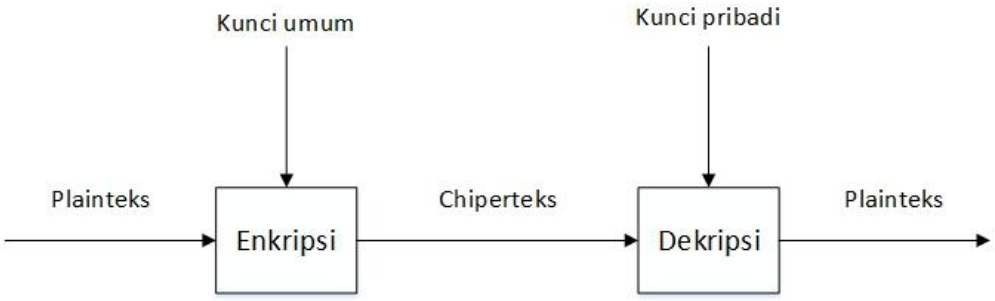
a. Kriptografi simetris, merupakan jenis kriptografi yang menggunakan kunci yang sama persis dalam proses enkripsi maupun dekripsi. Penerima pesan harus mengetahui kunci yang sama seperti yang digunakan pengirim agar dapat membaca pesan yang dikirimkan. Satu buah kunci dapat pula diturunkan dari kunci yang lainnya. Kunci-kunci ini harus dirahasiakan. Oleh karena itulah sistem ini sering

disebut sebagai *secretkey ciphersystem*. Contoh algoritma dari jenis ini yaitu DES (*Data Encryption Standart*) , AES *(Advanced Encryption Standar),* Blowfish, IDEA (*International Data Encryption Algorithm).*



Gambar 2.2 Kriptografi Simetris

b. Kriptografi asimetris, merupakan jenis kriptografi yang menggunakan dua buah kunci. *Public key* digunakan untuk enkripsi pesan dan dapat dipublikasikan, sedangkan *private key* adalah kunci yang dirahasiakan dan digunakan untuk dekripsi pesan. Contoh dari kriptografi jenis ini yaitu RSA *(Riverst Shamir Adleman)* dan ECC *(Elliptic Curve Chryptography),* DSA *(Digital Signature Algorithm),* dan DH *(Diffie-Hellman).*



Gambar 2.3 Kriptografi Asimetris

c. Kriptografi hybrid, merupakan jenis kriptografi yang memanfaatkan dua tingkatan kunci yaitu kunci simetri yang disebut juga *session key* untuk enkripsi data dan kunci publik untuk pemberian tanda tangan digital serta untuk melindungi kunci simetri.

2.1.3 Kriptografi Algoritma Rijndael

a. Sejarah Algoritma AES Rijndael

Pada tahun 1990-an, algoritma kriptografi yang banyak dipakai adalah *Data Encryption Standard* (DES). *National Institute of Standards and Technology (*NIST) menggunakan algoritma tersebut sebagai standar enkripsi data federal Amerika Serikat. DES termasuk dalam algoritma enkripsi yang sifatnya *cipherblock*, yang berarti DES mengubah data masukan menjadi blok-blok 64-bit dan kemudian menggunakan kunci enkripsi sebesar 56-bit. Setelah mengalami proses enkripsi maka akan menghasilkan output blok 64-bit.

Seiring dengan perkembangan teknologi, kunci DES yang sebesar 56-bit dianggap sudah tidak memadai lagi. Pada tahun 1998, 70 ribu komputer berhasil dibobol dengan membobol satu kunci DES dalam waktu 96 hari. Tahun 1999 kejadian yang sama terjadi lagi dalam waktu lebih cepat yaitu hanya dalam waktu 22 hari. Pada tanggal 16 Juni 1998, sebuah mesin seharga 250 ribu dolar dapat dengan mudah memecahkan 25% kunci DES dalam waktu kira-kira 2,3 hari atau diperkirakan dapat memecahkan kunci DES dalam waktu 4,5 hari. Adanya kenyataan bahwa algoritma kriptografi DES tidak lagi aman, maka NIST mulai memikirkan sebuah algoritma kriptografi lain sebagai pengganti DES.

Pada tahun 1997 kontes pemilihan suatu standar algoritma kriptografi baru pengganti DES dimulai dan diikuti oleh 21 peserta dari seluruh dunia. Algoritma kriptografi bernama Rijndael yang didesain oleh oleh Vincent Rijmen dan John Daemen asal Belgia keluar sebagai pemenang kontes algoritma kriptografi pengganti DES *(Data Encryption Standart)* yang diadakan oleh NIST *(National Institutes of Standards and Technology)* milik pemerintah Amerika Serikat pada 26 November 2001. Algoritma Rijndael inilah yang kemudian dikenal dengan *Advanced Encryption Standard* (AES). Setelah mengalami beberapa proses standardisasi oleh NIST, Rijndael kemudian diadopsi menjadi standar algoritma kriptografi

secara resmi pada 22 Mei 2002. Pada 2006, AES merupakan salah satu algoritma terpopuler yang digunakan dalam kriptografi kunci simetris.

b. Deskripsi Algoritma Rijndael

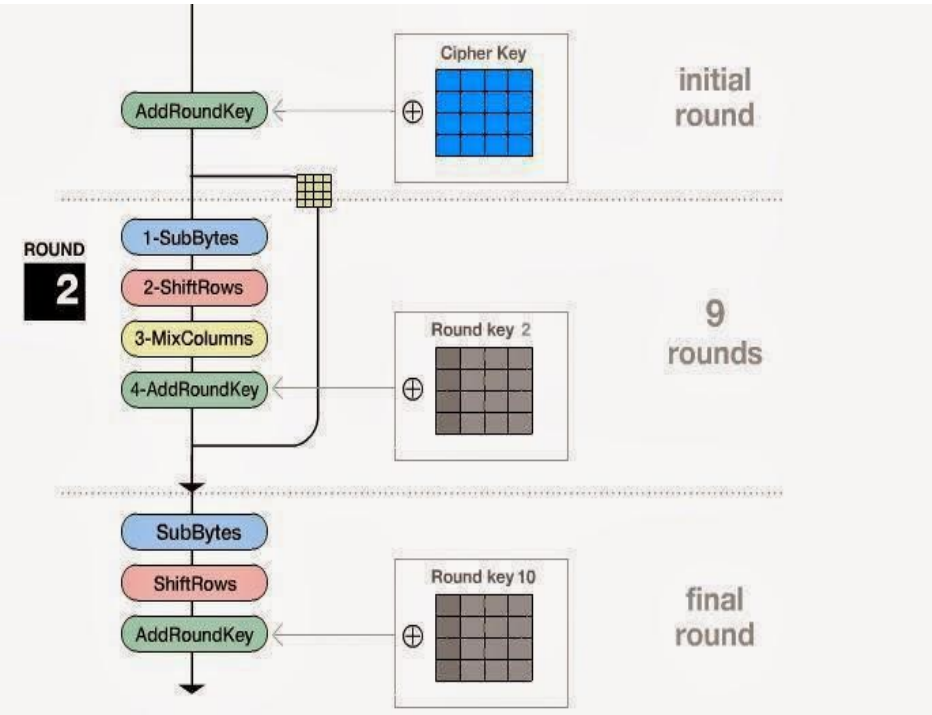
Algoritma Rijndael ini merupakan algoritma block cipher dengan menggunakan sistem permutasi dan substitusi (P-Box dan S-Box) bukan dengan jaringan Feistel sebagaimana *block cipher* pada umumnya.

Menurut jenisnya AES terbagi tiga jenis, yaitu:

1. AES-128
2. AES-192
3. AES-256

Pengelompokkan jenis AES ini adalah berdasarkan panjang kunci yang digunakan. Angka – angka di belakang kata AES menggambarkan panjang kunci yang digunakan pada tiap – tiap AES. Selain itu, hal yang membedakan dari masing-masing AES ini adalah banyaknya *round* yang dipakai. AES-128 menggunakan 10 *round*, AES-192 sebanyak 12 *round*, dan AES-256 sebanyak 14 *round*.

AES memiliki ukuran blok yang tetap sepanjang 128 bit dan ukuran kunci sepanjang 128, 192, atau 256 bit. Tidak seperti Rijndael yang block dan kuncinya dapat berukuran kelipatan 32 bit dengan ukuran minimum 128 bit dan maksimum 256 bit. Berdasarkan ukuran blok yang tetap, AES bekerja pada matriks berukuran 4x4 di mana tiap – tiap sel matriks terdiri atas 1 byte (8 bit). Sedangkan Rijndael sendiri dapat mempunyai ukuran matriks yang lebih dari itu dengan menambahkan kolom sebanyak yang diperlukan. Blok chiper tersebut dalam pembahasan ini akan diasumsikan sebagai sebuah kotak. Setiap plainteks akan dikonversikan terlebih dahulu ke dalam blok – blok tersebut dalam bentuk heksadesimal, kemudian blok itu akan diproses dengan metode berikutnya. Metode yang digunakan dalam algoritma ini yaitu *add round key, subbytes, shift rows, mix columns.*

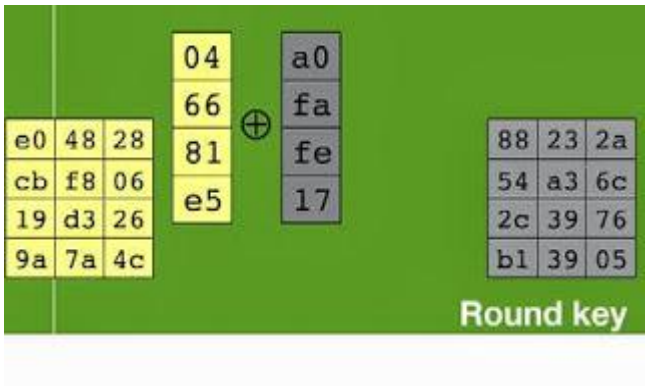


Gambar 2.4 Diagram AES Rijndael

Sumber : www.metode-algoritma.com

ADD ROUND KEY

Add Round Key pada dasarnya adalah proses mengkombinasikan chiper teks yang sudah ada dengan chiper key dengan hubungan XOR.



Gambar 2. 5 *Add round key*

Sumber : http://herwingoernia19.blogspot.co.id/2013/12/kriptografi-metode-algoritma-aes.html

Pada gambar di atas, sebelah kiri adalah chiper teks dan sebelah kanan adalah *round key*. XOR dilakukan per kolom yaitu kolom-1 chiper teks di XOR dengan kolom-1 round key dan seterusnya.

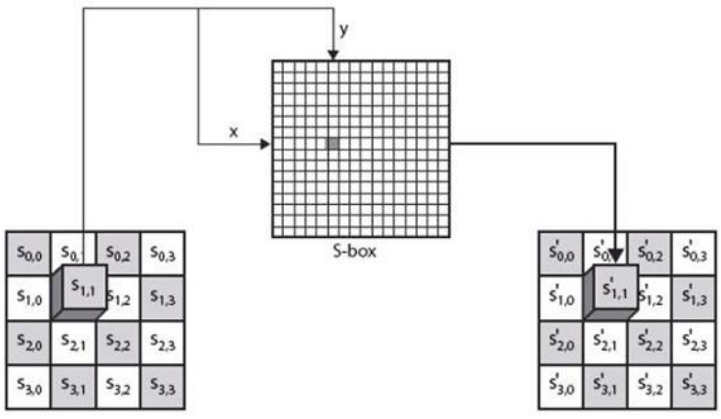
SUB BYTES

Prinsip dari *Sub Bytes* adalah dengan menukar isi matriks/tabel yang ada dengan matriks/tabel lain yang disebut dengan Rijndael S-Box.

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Gambar 2.6 Rijndael S-box

Sumber : http://herwingoernia19.blogspot.co.id/2013/12/kriptografi-metode-algoritma-aes.html



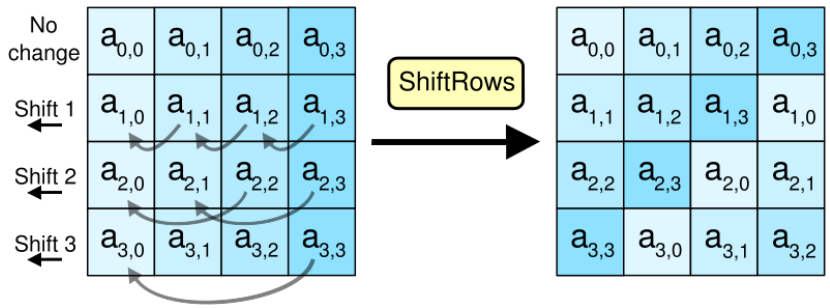
Gambar 2.7 Ilustrasi *Sub Bytes*

Sumber : http://herwingoernia19.blogspot.co.id/2013/12/kriptografi-metode-algoritma-aes.html

Gambar 2.6 di atas adalah contoh dari Rijndael S-Box, di sana terdapat nomor kolom dan nomor baris. Seperti yang telah disebutkan sebelumnya, tiap isi kotak dari blok chiper berisi informasi dalam bentuk heksadesimal yang terdiri dari dua digit, bisa angka-angka, angka-huruf, ataupun huruf-angka yang semuanya tercantum dalam Rijndael S-Box. Langkahnya adalah mengambil salah satu isi kotak matriks, mencocokkannya dengan digit kiri sebagai baris dan digit kanan sebagai kolom. Kemudian dengan mengetahui kolom dan baris, kita dapat mengambil sebuah isi tabel dari Rijndael S-Box. Langkah terakhir adalah mengubah keseluruhan blok chiper menjadi blok yang baru yang isinya adalah hasil penukaran semua isi blok dengan isi langkah yang disebutkan sebelumnya.

SHIFT ROWS

Shift Rows adalah sebuah proses yang melakukan *shift* atau pergeseran pada setiap elemen blok/tabel yang dilakukan per barisnya. Baris pertama tidak dilakukan pergeseran, baris kedua dilakukan pergeseran 1 byte, baris ketiga dilakukan pergeseran 2 byte, dan baris keempat dilakukan pergeseran 3 byte. Pergeseran tersebut terlihat dalam sebuah blok adalah sebuah pergeseran tiap elemen ke kiri tergantung berapa byte tergesernya, tiap pergeseran 1 byte berarti bergeser ke kiri sebanyak satu kali.

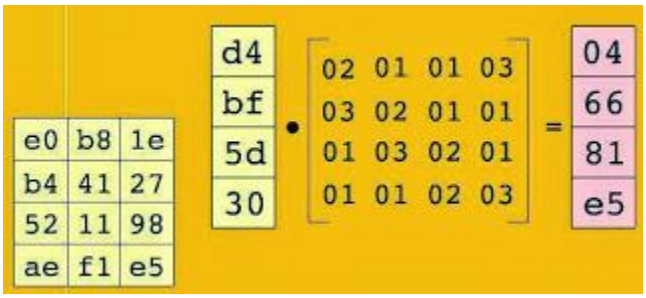


Gambar 2.8 Ilustrasi *ShiftRows*

Sumber : https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

MIX COLUMNS

Tahap *Mix Column* adalah dengan mengalikan tiap elemen dari blok chiper dengan matriks. Tabel sudah ditentukan dan siap pakai. Pengalian dilakukan seperti perkalian matriks biasa yaitu menggunakan *dot product* lalu perkalian keduanya dimasukkan ke dalam sebuah blok chiper baru.



Gambar 2.9 Ilustrasi *Mix Columns*

Sumber : http://herwingoernia19.blogspot.co.id/2013/12/kriptografi-metode-algoritma-aes.html

DIAGRAM ALIR AES

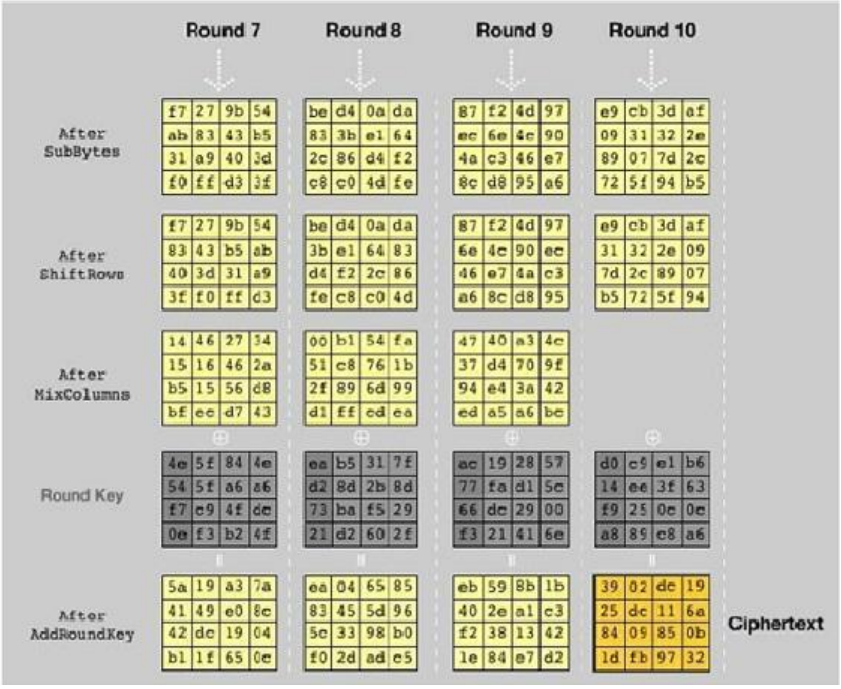
Gambar 2.10 dan 2.11 menjelaskan tahapan mulai dari *round* kedua, dilakukan pengulangan terus menerus dengan rangkaian proses *Sub Bytes*, *Shift Rows*, *Mix Columns*, dan *Add Round Key*. Hasil dari perputaran tersebut akan digunakan pada ronde berikutnya dengan metode yang sama. Namun pada ronde kesepuluh proses *Mix Columns* tidak dilakukan, urutan proses yang dilakukan adalah *Sub Bytes*, *Shift Rows*, dan *Add Round Key*. Hasil dari *Add Round Key* inilah yang dijadikan sebagai chiperteks dari algoritma Rijndael. Banyaknya perputaran *(round)* ditentukan oleh tabel berikut.

Jenis	Panjang Kunci *(Nk words)*	Ukuran Blok *(Nk Blok)*	Jumlah putaran *(Nr)*
AES-128 bit	4	4	10
AES-192 bit	6	4	12
AES-256 bit	8	4	14

Tabel 2.1 Tabel perputaran AES

Gambar 2.10 Ilustrasi Ronde 2 hingga Ronde 6

Sumber : http://herwingoernia19.blogspot.co.id/2013/12/kriptografi-metode-algoritma-aes.html



Gambar 2.11 Ilustrasi Ronde 7 hingga Ronde 10

Sumber : http://herwingoernia19.blogspot.co.id/2013/12/kriptografi-metode-algoritma-aes.html

2.2 Steganografi

2.2.1 Sejarah Steganografi

Kata steganografi berasal dari bahasa Yunani *steganos*, yang berarti tersembunyi atau terselubung, dan *graphein* berarti menulis. Pada zaman romawi, seorang Yunani bernama Demeratus yang akan mengabarkan berita kepada Sparta bahwa Xerxes bermaksud menyerbu Yunani dan agar tidak diketahui pihak Xerxes, Demaratus menulis pesan dengan cara mengisi tabung kayu dengan lilin dan menulis pesan dengan cara mengukirnya pada bagian bawah kayu, lalu papan kayu tersebut dimasukkan ke dalam tabung kayu, kemudian tabung kayu ditutup kembali dengan lilin.

Pada abad ke-20, steganografi mengalami perkembangan. Selama berlangsung perang Boer, Lord Boden Powell (pendiri gerakan kepanduan) bertugas untuk membuat tanda posisi sasaran dari basis artileri tentara Boer. Berdasar untuk alasan keamanan, Boden Powell menggambar peta posisi

musuh pada sayap kupu – kupu agar gambar – gambar peta sasaran tersebut terkamuflase.

Dari contoh steganografi konvensional tersebut dapat dilihat bahwa semua teknik steganografi konvensional berusaha merahasiakan komunikasi dengan cara menyembunyikan pesan ataupun mengkamuflase pesan.

Seiring dengan perkembangan teknologi terutama teknologi komputerisasi, steganografi merambah juga ke media digital walaupun steganografi dapat dikatakan mempunyai hubungan erat dengan kriptografi, tetapi kedua metode ini sangat berbeda.

2.2.2 Deskripsi Steganografi

Steganografi (*steganography*) adalah ilmu dan seni menyembunyikan pesan rahasia (*hiding message*) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia. (Rinaldi, 2004).

Pada tehnik kriptografi, data yang telah disandikan (chiperteks) tetap tersedia, maka dengan steganografi cipherteks dapat disembunyikan sehingga pihak ketiga tidak mengetahui keberadaannya.

Teknik steganografi meliputi banyak sekali metode komunikasi untuk menyembunyikan pesan rahasia (teks atau gambar) di dalam *file* lain yang mengandung teks, *image*, bahkan *audio* tanpa menunjukkan ciri – ciri perubahan yang nyata atau terlihat dalam kualitas dan struktur dari *file* semula. Metode ini termasuk tinta yang tidak tampak, *microdots*, pengaturan kata, tanda tangan digital, jalur tersembunyi dan komunikasi spektrum lebar.

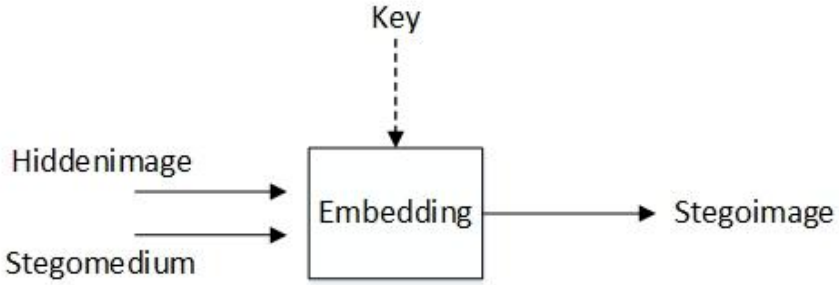
Tujuan dari teknik steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam prakteknya kebanyakan diselesaikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya. Perubahan ini bergantung pada kunci dan pesan untuk disembunyikan. Orang yang menerima gambar kemudian dapat

menyimpulkan informasi terselubung dengan cara mengganti kunci yang benar ke dalam algoritma yang digunakan.

Teknik steganografi menggunakan bermacam – macam format digital untuk menjadi media penyisipan steganografi yaitu *audio*, *image* dan format lain. Format yang biasa digunakan untuk *image* yaitu .bmp, .jpeg, dan .gif. Format audio yang sering digunakan adalah .mp3 dan .wav. Untuk format lainnya yang biasa digunakan untuk media penyisipan adalah *file* teks, *file* pdf dan sejenisnya.

2.2.3 Proses Steganografi

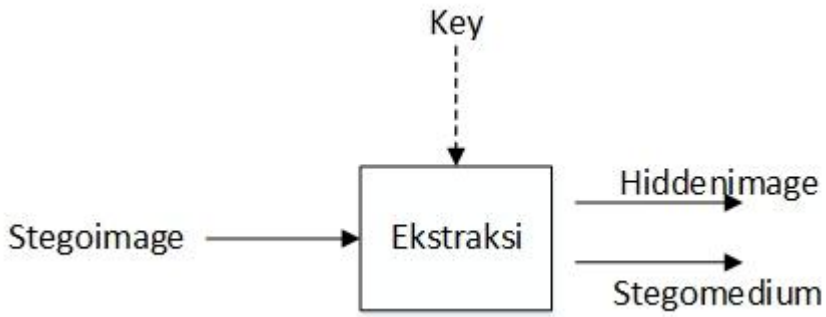
Dalam steganografi umumnya terdapat dua proses yaitu proses *embedding* dan proses ekstraksi. Proses *embedding* merupakan proses untuk menyembunyikan atau menyisipkan pesan ke dalam suatu media digital. Proses ekstraksi adalah proses mengekstrak atau mengambil pesan yang tersembunyi di dalam suatu media digital.



Gambar 2.12 Ilustrasi *Embedding*

Sumber : http://tugas-myraziq.blogspot.co.id/2015/11/steganografi.html

Gambar di atas menjelaskan proses *embedding* dengan dilakukan penyisipan pesan (*Hidden image*) ke dalam media penyisipan (Stegomedium) dengan menggunakan suatu kunci (*key*) dan menghasilkan suatu *file* berupa *stegoimage* berupa media penyisipan yang sudah disisipi pesan sebelumnya.



Gambar 2.13 Ilustrasi Ekstrak

Sumber : http://tugas-myraziq.blogspot.co.id/2015/11/steganografi.html

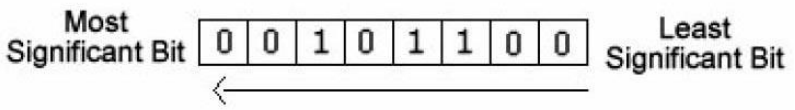
Pada proses ekstraksi, stegoimage yang berisi suatu pesan tersembunyi diekstrak untuk mendapatkan pesan tersembunyi yang ada di dalamnya. *Stegoimage* akan diekstrak menggunakan *key* yang sama seperti pada proses penyisipan, kemudian akan didapatkan pesan yang disisipkan ke dalam stegomedium.

2.2.4 Steganografi metode LSB *(Least Significant Bit)*

Teknik steganografi LSB dilakukan dengan cara memodifikasi bit – bit yang termasuk bit LSB pada byte warna pada sebuah pixel. Bit – bit LSB akan dimodifikasi dengan menggantikan setiap LSB yang ada dengan bit – bit informasi lain yang ingin disembunyikan. Setelah semua bit informasi menggantikan bit LSB di dalam *file* tersebut maka informasi telah berhasil disembunyikan. Apabila informasi rahasia tersebut ingin dibuka kembali, bit – bit LSB yang sekarang ada diambil satu per satu kemudian disatukan kembali menjadi sebuah informasi yang utuh seperti semula. Teknik ini memang terbilang sederhana, seperti halnya null cipher saja, namun terkadang kualitas dari file yang ditumpanginya sedikit banyak akan terpengaruh.

Metode yang digunakan untuk menyembunyikan pesan pada media digital tersebut berbeda-beda. Pada berkas *image* pesan dapat disembunyikan dengan menggunakan cara menyisipkannya pada bit rendah atau bit yang

paling kanan (LSB) pada data pixel yang menyusun *file* tersebut. Pada berkas bitmap 24 bit, setiap piksel pada gambar tersebut terdiri dari susunan tiga warna merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (byte) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Dengan demikian, pada setiap pixel berkas bitmap 24 bit kita dapat menyisipkan 3 bit data.



Gambar 2. 14 Ilustrasi Metode *Least Significant Bit*

Sumber : https://www.ethicalhacker.net/features/book-reviews/hacking-a-terror-network-ch-2-unseen-planning

2.2.5 Citra Digital

Suatu citra adalah fungsi intensitas 2 dimensi f(x, y), dimana x dan y adalah koordinat spasial dan f pada titik (x, y) merupakan tingkat kecerahan (*brightness*) suatu citra pada suatu titik (Gonzales dan Woods, 2008). Citra Digital adalah representasi dari sebuah citra dua dimensi sebagai sebuah kumpulan nilai digital yang disebut elemen gambar atau piksel. Ada beberapa jenis dari format citra digital yang sering digunakan adalah sebagai berikut :

a) JPEG (*Joint Photographic Experts Group*)

   JPEG adalah format gambar yang banyak digunakan untuk menyimpan gambar-gambar dengan ukuran lebih kecil. Beberapa karakteristik gambar dalam JPEG yang tentu kita tahu pasti memiliki ekstensi .jpg atau .jpeg. JPEG juga mampu menayangkan warna dengan kedalaman 24-bit *true colour*, kompresi gambar dengan sifat *lossy*.

b) GIF

   Jenis file gambar ini sering dijumpai dan sering dipakai. Salah satu ciri khas tipe gambar berekstensi GIF adalah bisa memainkan animasi gambar

sederhana. Beberapa karakteristik lain format gambar GIF adalah mampu menayangkan maksimum sebanyak 256 warna karena format GIF menggunakan 8-bit untuk setiap pixel-nya. Selain itu GIF juga mampu mengkompresi gambar dengan sifat lossless dan mendukung warna transparan.

c) PNG (*Portable Network Graphics*)

PNG adalah salah satu format penyimpanan citra yang menggunakan metode pemadatan yang tidak menghilangkan bagian dari citra tersebut. PNG dipakai untuk Citra Web *(World Wide Web*). Citra dengan format PNG mempunyai faktor kompresi yang lebih baik dibandingkan dengan GIF (5%-25% lebih baik dibanding format GIF).

d) BMP

File format BMP (Windows bitmap) menangani *file* grafik di sistem operasi Microsoft Windows. File BMP tidak dikompresi, maka ukurannya besar. Keuntungannya adalah kesederahanaannya, diterima luas, dan dikenali program - progam Windows. Biasanya digunakan oleh aplikasi dan system operasi Microsoft Windows yang merupakan kompresi tipe *lossless.*

2.2.6 Kriteria Steganografi yang baik

Kriteria yang harus diperhatikan dalam penyembunyian data adalah sebagai berikut :

a. *Fidelity*

Kualitas dari citra yang menjadi media penyisipan masih baik serta tidak berubah jauh setelah dilakukan proses steganografi. Untuk mengetahui seberapa baiknya kualitas steganografi maka dibutuhkan pengujian menggunakan PSNR dan MSE. Peak Signal to Noise Ratio (PSNR) adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut. PSNR biasanya diukur dalam satuan decibel (db). PSNR digunakan untuk mengetahui perbandingan kualitas citra cover sebelum dan sesudah disisipkan pesan. Untuk menentukan PSNR, terlebih dahulu harus ditentukan nilai MSE

(Mean Square Error). MSE adalah nilai error kuadrat rata-rata antara citra asli dengan citra manipulasi (dalam kasus steganografi). MSE adalah nilai error kuadrat rata-rata antara citra asli (cover-image) dengan citra hasil penyisipan (stego-image). X dan y sebagai koordinat

$$PNSR = 10\ log_{10}(\frac{C_{max}^2}{MSE})$$

$$MSE = \frac{1}{M.N}\sum_{x=1}^{M}\sum_{y=1}^{N}(S_{xy} - C_{xy})^2$$

b. *Robustness*

Data yang disembunyikan harus bisa bertahan dan tidak rusak dari segala manipulasi yang dilakukan terhadap citra yang menjadi media penyisipan. Untuk mengukur kriteria ini stegoimage hasil penyisipan dilakukan manipulasi seperti crop, brightness, contrast maka setelah dilakukan manipulasi apakah pesan yg disembunyikan dapat diambil kembali atau tidak.

c. *Recovery*

Data yang disisipkan bisa dikembalikan (*Recovery*), karena tujuan dari steganografi adalah menyembunyikan data. Suatu waktu data yang disembunyikan dapat dimunculkan. Untuk menguji apakah kriteria ini behasil yaitu dengan mengekstrak pesan yang disisipkan ke dalam gambar sebelumnya dan membandingkan isi pesan yang disisipkan dan diekstrak apakah sama atau tidak.

d. *Security*

Data yang telah disisipkan harus bisa dijamin keamanannya dan sulit dipecahkan oleh usaha steganalisis. Pengujian kriteria ini yaitu dengan mengecek isi pesan rahasia yang disisipkan apakah berhasil dienkripsi atau tidak.

2.3 Bahasa Pemrograman Java

2.3.1 Sejarah Java

Bahasa pemrograman ini resmi rilis pada tahun 1995, dan sebelum itu mengalami banyak perubahan sampai menjadi bahasa pemrograman yang utuh. Pada tahun 1991, dibentuk suatu tim yang diberi nama "*Green*". Tim ini dipimpin oleh Patrick Naughton dan James Gosling. Java sendiri dipelopori oleh James Gosling, Patrick Naughton, Chris Warth, Ed Frank, dan Mike Sheridan dari perusahaan Sun Microsystems, Inc yang merupakan bagian dari Oracle. Awalnya mereka ingin membuat suatu bahasa komputer yang dapat digunakan oleh TV kabel (*Cable TV Box*) yang memiliki memori kecil dan setiap perusahaan memiliki tipe yang berbeda. Mereka menggunakan hal yang pernah dicoba oleh bahasa pascal. Mereka membutuhkan kurang lebih 18 bulan untuk membuat versi pertamanya.

Tahun 1992 tim *green* membuat produknya yang diberi nama *7 (*Star Seven*), namun produk ini gagal dipasaran. Setelah itu dibuat produk yang baru yang menjadi cikal bakal Java, pada awalnya bahasa pemrograman yang dibuat tersebut diberi nama "Oak". Kemungkinan nama ini diambil dari nama pohon yang ada didepan jendela James Gosling, tapi kemudian diubah menjadi "Java" pada tahun 1995 karena nama "Oak" telah dijadikan hak cipta dan digunakan sebagai bahasa pemrograman lainnya. Antara pembuatan Oak pada musim gugur 1992 hingga diumumkan ke publik pada musim semi 1995, banyak orang yang terlibat dalam desain dan evolusi bahasa ini. Bill Joy, Arthur van Hoff, Jonathan Payne, Frank Yellin, dan Tim Lindholm merupakan kontributor kunci yang mematangkan prototipe aslinya.

2.3.2 Deskripsi Java

Java adalah bahasa pemrograman yang dapat membuat seluruh bentuk aplikasi, desktop, web, mobile dan lainnya, sebagaimana dibuat dengan menggunakan bahasa pemrograman konvensional yang lain.

Bahasa Pemrograman Java ini berorientasi objek (*OOP-Object Oriented Programming*), dan dapat dijalankan pada berbagai platform sistem operasi. Perkembangan Java tidak hanya terfokus pada satu sistem operasi, tetapi

dikembangkan untuk berbagai sistem operasi dan bersifat *open source* dengan slogannya *"Write once, run anywhere"*. Bahasa ini banyak mengadopsi sintaksis yang terdapat pada C dan C++ namun dengan sintaksis model objek yang lebih sederhana. Aplikasi-aplikasi berbasis java umumnya dikompilasi ke dalam p-code (*bytecode*) dan dapat dijalankan pada berbagai Mesin Virtual Java (JVM). Java merupakan bahasa pemrograman yang bersifat umum/non-spesifik (*general purpose*).

Paradigma OOP menyelesaikan masalah dengan merepresentasikan masalah ke model objek. Pemisalan Objek dalam OOP yaitu objek – objek dalam dunia nyata yang mempunyai dua karakteristik khusus berupa status dan perilaku. Bahasa yang berorientasi pada objek pun mempunyai karakteristik yang sama dengan objek – objek di dunia nyata yaitu status yang dalam bahasa pemrograman biasanya disimpan sebagai variabel dan perilaku yang diimplementasikan sebagai *method.*

2.4 Tinjauan Pustaka

Penelitian sebelumnya sudah banyak yang melakukan penelitian tentang steganografi. Metode yang digunakan sangat beragam seperti *Least Significant Bit* (LSB), *Spread Spectrum, Bit Complexity Segmentation* (BPCS), *Plane Discrete Cosine Transformation* (DCT). Penggunaan metode steganografi juga sering dimodifikasi dengan algoritma kriptografi yang bermacam – macam untuk diuji ketahanan hasil steganografi.

Sebagai contoh, penelitian yang dilakukan oleh Putri Amalia Rahmawati (2014) yang telah melakukan penelitian yang berjudul "Implementasi Steganografi Metode LSB dengan Vigenere Cipher pada Citra digital". Pada penelitian ini, metode steganografi *Least Significant Bit* digunakan dalam penyisipan suatu *file* dalam tersembunyi ke dalam *file* citra digital yang bertipe bitmap (*.bmp) yang dengan kombinasi kriptografi *Vigenere Cipher.*

Selain itu, Endah Kurnia Asih Sejati (2012) melakukan penelitian yang berjudul "*Implementasi Steganografi pada Citra Digital Menggunakan Metode Least Significant Bit*" yang membangun aplikasi steganografi dengan metode

Least Significant Bit untuk penyisipan *file* teks (*.txt) ke dalam *file* citra bertipe bitmap dan menggunakan algoritma *Data Encryption Standar (DES)* dalam enkripsi data.

Dari kedua penelitian yang telah dilakukan, penulis akan melakukan penelitian dengan mengimplementasikan teknik steganografi metode *Least Significant Bit* pada citra digital berformat bitmap (.bmp) dengan dikombinasikan oleh algoritma Rijndael atau yang sering disebut Algoritma AES *(Advanced Encryption Standard)* dengan ukuran 128 bit dalam enkripsi data yang disisipkan. Implementasinya menggunakan bahasa pemrograman java. Algoritma Rijndael yang dipakai adalah jenis algoritma Rijndael 128 bit, walaupun tersedia 3 jenis varian yaitu 128 bit, 192 bit, dan 256 bit. Disini penulis menggunakan jenis 128 bit karena beberapa alasan yaitu dalam jenis ini kecepatan dalam enkripsi dan dekripsi lebih cepat dibandingkan jenis rijndael yang lainnya dikarenakan jumlah putaran dalam setiap prosesnya paling sedikit dibandingkan dengan jenis 192 dan 256 dan panjang kunci rijndael 128 bit yang digunakan adalah yang paling terkecil dari jenis rijndael yang lain.