# BAB II
# TINJAUAN PUSTAKA

## 2.1 Keamanan Data

Dalam era digital, komunikasi melalui jaringan komputer memegang peranan penting. Melalui komunikasi elektronis, seseorang dapat melakukan transaksi atau komunikasi dengan sangat cepat dan praktis. Hal ini merupakan pengaruh dari perkembangan yang sangat signifikan dalam teknologi informasi, dimana *bandwidth* internet yang semakin besar dengan biaya akses yang semakin murah. Konsekuensinya adalah resiko dalam keamanan informasi semakin meningkat [6].

Komunikasi data elektronis memerlukan perangkat keamanan yang benar-benar berbeda dengan komunikasi konvensional. Dalam lalu lintas informasi di internet, sistem autentikasi (bukti diri) konvensional dengan KTP, SIM dan sebagainya yang bersandar pada keunikan tanda tangan tidak berlaku. Pengawalan petugas keamanan tidak lagi bisa membantu keamanan pengiriman dokumen elektronis.

Keamanan data dapat dibedakan menjadi dua kategori, yaitu keamanan fisik dan keamanan sistem. Keamanan fisik merupakan bentuk keamanan berupa fisik dari *server, terminal/client router* sampai dengan *cabling.* Sedangkan keamanan sistem adalah keamanan pada sistem pengoperasiannya atau lebih khususnya pada lingkup perangkat lunak, misalnya dengan penggunaan kriptografi dan steganografi. Dalam tugas akhir ini akan dibahas tentang penggunaan kombinasi steganografi dan kriptografi dalam memberikan keamanan pada data [7].

## 2.2 Kriptografi

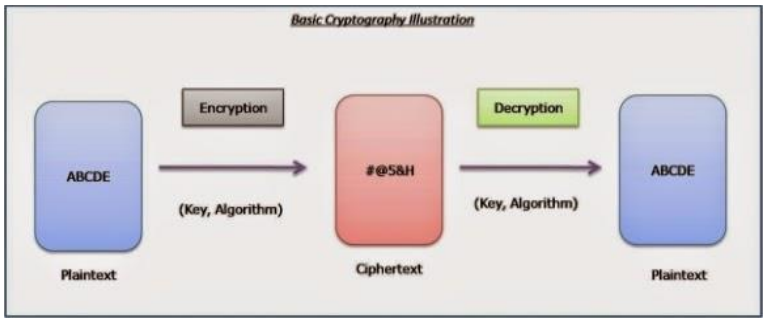
Kriptografi berasal dari bahasa Yunani, *cryptos* yang berarti rahasia dan *graphein* yang berarti tulisan. Kriptografi merupakan sebuah cara dalam mengamankan dan mengirim data dalam bentuk yang hanya diketahui oleh pihak yang berhak membukanya, memproteksi informasi dengan mengubahnya ke dalam bentuk himpunan karakter acak yang tidak dapat dibaca. Kriptografi adalah

ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data .Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi. Kriptografi adalah sebuah cara yang efektif dalam mengamankan informasi-informasi penting baik yang tersimpan dalam media penyimpanan maupun yang ditransmisikan melalui jaringan komunikasi [6]. Kriptografi dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan. Pada prinsipnya, kriptografi memiliki 4 komponen utama yaitu:

1. Plaintext, yaitu pesan yang dapat dibaca
2. Ciphertext, yaitu pesan acak yang tidka dapat dibaca
3. Key, yaitu kunci untuk melakukan teknik kriptografi
4. Algorithm, yaitu metode untuk melakukan enkrispi dan dekripsi

Kriptografi juga memiliki 2 proses dasar pada yaitu:

1. Enkripsi (Encryption)
2. Dekripsi (Decryption)




Gambar 2.1 Ilustrasi 4 komponen dan 2 proses yang digunakan dalam teknik kriptografi [8].

### 2.2.1 Sejarah Kriptografi

Kriptografi telah digunakan sejak 4000 tahun lalu. Di Romawi, dikisahkan suatu saat Julius Caesar mengirimkan pesan rahasia kepada jenderalnya yang sedang berada di medan perang. Ia mengacak pesan rahasia tersebut hingga menjadi pesan yang tidak dapat dipahami siapapun selain jenderalnya. Yang

dilakukan Julius Caesar adalah menggeser 3 urutan alfabet ke kanan, sehingga a menjadi d, b menjadi e dan seterusnya. Dari ilustrasi tersebut, beberapa istilah kriptografi dipergunakan. Proses mengacak pesan disebut enkripsi. Pada saat jenderal menyusun kembali pesan acak tersebut menjadi pesan seperti sedia kala disebut dekripsi. Pesan awal yang belum diacak disebut *plaintext,* dan pesan yang telah diacak disebut *ciphertext.* Orang Mesir menggunakan kriptografi dengan huruf-huruf *hieroglyph.*

Gambar 2.2 Penggunaan *Hierogliph* di Mesir [6].

Metode kriptografi pun berkembang sesuai dengan perkembangan zaman dan kebutuhan. Pada abad ke-15 Leo Battista Alberti menemukan metode roda kode (*wheel cipher)* yang dipergunakan sebagai alat enkripsi. Pada perang dunia ke-2, militer Jerman menggunakan mesin *cipher* substitusi polialfabetik yang disebut Enigma sebagai sistem pengkodean utama.

Perkembangan komputer dan sistem komunikasi pada tahun 60-an berdampak pada permintaan dari sektor-sektor swasta sebagai sarana untuk melindungi informasi dalam bentuk digital dan untuk menyediakan layanan keamanan. Dimulai dari usaha Feistel pada IBM di awal tahun 70-an dan mencapai puncaknya pada 1977 dengan pengangkatan DES (*Data Encryption Standard*) sebagai standar pemrosesan informasi federal US untuk mengenkripsi informasi. DES merupakan mekanisme kriptografi yang paling dikenal sepanjang sejarah.

### 2.2.2 Tujuan Kriptografi

Tujuan kriptografi adalah melindungi data dari ancaman yang disengaja atau tidak disengaja. Dewasa ini ancaman bertambah karena semakin meluasnya akses melalui internet atau teknologi bergerak. Aspek-aspek keamanan data dalam kriptografi adalah sebagai berikut.

*1. Confidentiality / Privacy*

Merupakan usaha untuk menjaga kerahasiaan data. Data hanya boleh diakses oleh orang yang berwenang. Contohnya data-data pribadi, data-data bisnis, daftar gaji, data nasabah dan lainnya. Aspek keamanan data menjadi sangat sensitif dalam *e-commerce* dan militer. Serangan dalam aspek ini antara lain dilakukan dengan penyadapan, misalnya *sniffer* atau *logger*.

*2. Integrity*

Memastikan bahwa informasi yang dikirim melalui jaringan tidak mengalami modifikasi oleh pihak yang tidak berhak. Serangan dapat berupa pengubahan data oleh orang yang tidak berhak, misalnya dengan *spoofing* yaitu virus yang dapat mengubah berkas.

*3. Availability*

Informasi harus tersedia ketika dibutuhkan. Serangan dapat berupa meniadakan layanan (Denial of Service/DoS *attack*) atau menghambat layanan dengan membuat *server* lambat.

*4. Non-repudiation*

Pengirim tidak dapat menyangkal bahwa yang bersangkutan telah melakukan transaksi tersebut.

*5. Authentication*

Meyakinkan keaslian data, sumber data, orang yang mengakses data, dan *server* yang digunakan. Beberapa cara yang dapat digunakan untuk membuktikan keaslian data antara lain dengan *what you have* (misalnya kartu identitas), *what you know* (misalnya *password* atau PIN) dan *what you are* (misalnya dengan *biometric identity*). Serangan dapat dilakukan dengan menggunakan identitas palsu, terminal palsu ataupun situs gadungan.

*6. Access Control*

Aspek ini berhubungan dengan mekanisme pengaturan akses ke informasi, untuk mengatur siapa yang boleh melakukan apa. Membutuhkan adanya klasifikasi data, misalnya umum (*public*), pribadi (*private*), rahasia (*confidential*) atau sangat rahasia (*top secret*).

*7. Accountability*

Dapat dipertanggungjawabkan melalui mekanisme *logging* dan *audit*. Adanya kebijakan dan prosedur (*policy and procedures*).

## 2.3 Steganografi

Kata steganografi (*steganography*) berasal dari bahasa Yunani *steganos*, yang artinya tersembunyi atau terselubung, dan *graphia* yang artinya menulis, sehingga arti steganografi adalah "menulis (tulisan) terselubung". Dengan steganografi, kita dapat menyisipkan pesan rahasia ke dalam media lain dan mengirimkannya tanpa ada yang menyadari keberadaan pesan tersebut. Steganografi adalah ilmu yang digunakan untuk menyisipkan data di dalam media lainnya. Steganografi membutuhkan dua media, yaitu penampung dan data yang akan disisipkan. Secara teori, semua berkas digital yang ada di dalam komputer dapat digunakan sebagai media penampung, misalnya citra berformat JPG, GIF, BMP, atau di dalam musik MP3, atau bahkan di dalam sebuah film dengan format WAV atau AVI. Semua dapat dijadikan tempat bersembunyi, asalkan berkas tersebut memiliki bit-bit yang tidak signifikan atau terdapat *redundant bits* yang dapat dimodifikasi. Setelah dimodifikasi, berkas media tersebut tidak akan terganggu fungsinya dan kualitasnya tidak akan jauh berbeda dengan aslinya[7].

### 2.3.1 Sejarah Steganografi

Steganografi merupakan seni penyembunyian pesan ke dalam pesan lainnya sedemikian rupa sehingga orang lain tidak menyadari ada sesuatu di dalam pesan tersebut. Kata steganografi (*steganography*) berasal dari bahasa Yunani yaitu steganos yang artinya tersembunyi atau terselubung dan graphein, yang artinya menulis, sehingga kurang lebih artinya adalah “menulis tulisan yang tersembunyi atau terselubung”. Teknik ini meliputi banyak sekali metoda komunikasi untuk

menyembunyikan pesan rahasia. Metoda ini termasuk tinta yang tidak tampak, microdots, pengaturan kata, tanda tangan digital, jalur tersembunyi dan komunikasi spektrum lebar. Catatan pertama tentang steganografi ditulis oleh seorang sejarawan Yunani, Herodotus, yaitu ketika Histaeus seorang raja kejam Yunani dipenjarakan oleh Raja Darius di Susa pada abad 5 Sebelum Masehi. Histaeus harus mengirim pesan rahasia kepada anak laki-lakinya, Aristagoras, di Militus. Histaeus menulis pesan dengan cara mentato pesan pada kulit kepala seorang budak dan ketika rambut budak itu mulai tumbuh, Histaeus mengutus budak itu ke Militus untuk mengirim pesan di kulit kepalanya tersebut kepada Aristagoras.

Cerita lain tentang steganografi datang juga dari sejarawan Yunani, Herodotus, yaitu dengan cara menulis pesan pada papan kayu yang ditutup dengan lilin. Demeratus, seorang Yunani yang akan mengabarkan berita kepada Sparta bahwa Xerxes bermaksud menyerbu Yunani. 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.

Teknik steganografi yang lain adalah tinta yang tak terlihat. Teknik ini pertama digunakan pada zaman Romawi kuno yaitu dengan menggunakan air sari buah jeruk, urine atau susu sebagai tinta untuk menulis pesan. Cara membacanya adalah dengan dipanaskan di atas nyala lilin, tinta yang sebelumnya tidak terlihat, ketika terkena panas akan berangsur-angsur menjadi gelap, sehingga pesan dapat dibaca.Teknik ini pernah juga digunakan pada Perang Dunia II.

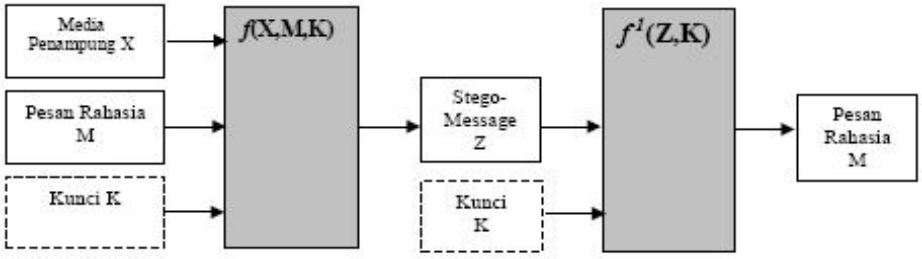
Pada abad 20, steganografi benar-benar mengalami perkembangan. Selama berlangsung perang Boer, Lord Boden Powell (pendiri gerakan kepanduan) yang bertugas untuk membuat tanda posisi sasaran dari basis artileri tentara Boer, untuk alasan keamanan, Boden Powell menggambar peta-peta posisi musuh pada sayap kupu-kupu agar gambar-gambar peta sasaran tersebut terkamuflase.

Seiring dengan perkembangan teknologi terutama teknologi komputasi, steganografi merambah juga ke media digital, walaupun steganografi dapat

dikatakan mempunyai hubungan erat dengan kriptografi, tetapi kedua metode ini sangat berbeda[6].

### 2.3.2 Karakteristik Steganografi

Dalam steganografi dikenal *data hiding* atau *data embedding*, yang merupakan rangkaian proses dalam menyembunyikan data ke dalam berbagai media, seperti citra, audio atau teks dengan meminimalisir penampakan degradasi sinyal media penampung (Bender *et al*, 1996). Hal ini tampak familiar dengan enkripsi. Namun jika ditelusuri lebih jauh maka penyembunyian data dalam steganografi sangat kontras dengan kriptografi. Perbedaannya terletak pada bagaimana proses penyembunyian data dan hasil akhir dari proses tersebut. Kriptografi merahasiakan makna pesan sementara keberadaan pesan tetap dapat diamati oleh indera manusia. *Kriptografi* melakukan proses pengacakan data asli sehingga menghasilkan data terenkripsi yang benar-benar acak dan berbeda dengan aslinya. Sedangkan steganografi menyembunyikan keberadaan pesan tersebut, data disisipkan dalam media penampung tanpa mengubah keadaan media penampung tersebut. Dengan kata lain keluaran *steganografi* ini memiliki bentuk persepsi yang sama dengan bentuk aslinya[7].




Gambar 2.3 Diagram Sistem Steganografi[6]

Penyisipan data rahasia ke dalam media digital harus memperhatikan beberapa aspek keamanan sebagai berikut:

1. *Fidelity*

Mutu media penampung tidak jauh berubah. Setelah penambahan data rahasia, berkas hasil steganografi tidak mengalami degradasi yang signifikan, sehingga perubahan atau degradasi tersebut tidak dapat dipersepsi oleh indera manusia. Pada kasus audio steganografi, audio hasil steganografi masih dapat

didengar dengan baik. Pengamat tidak menyadari bahwa di dalam audio tersebut terdapat data rahasia. Atau dengan kata lain penyisipan data rahasia tidak mempengaruhi kualitas sinyal asli, sehingga keberadaan pesan tidak dapat ditangkap oleh pendengaran manusia.

*2. Recovery*

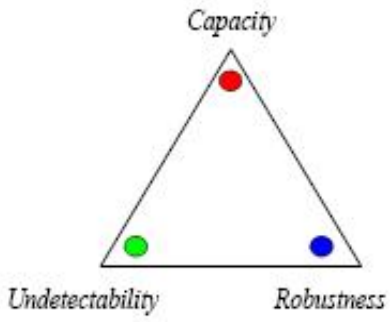
Data yang disembunyikan harus dapat diungkapkan kembali (*recovery*). Karena tujuan steganografi adalah *data hiding*, maka sewaktu-waktu data rahasia didalam citra penampung harus dapat diambil kembali untuk digunakan lebih lanjut.

*3. Robustness*

Robustness merupakan salah satu isu desain algoritma steganografi yang utama. Data rahasia yang disisipkan harus tahan terhadap pengolahan sinyal yang mungkin dilakukan termasuk konversi digital-analog dan analog-digital, *linear* dan *non-linear filtering*, kompresi dan perubahan ukuran (*scaling)*.

*4. Security*

Data rahasia harus resisten terhadap deteksi pembajakan dan juga diharapkan bisa menyulitkan dari usaha steganalisis. Ketika kerahasiaan itu ingin dibuka, dibutuhkan kunci untuk digunakan dalam proses penyisipan dan ekstraksi. Dalam menyisipkan informasi ada beberapa faktor yang saling berkompetisi satu sama lain, artinya faktor-faktor tersebut tidak dapat dioptimalkan dalam satu waktu, yaitu kapasitas (*capacity*), anti deteksi (*undetectability)* dan kekokohan (*robustness*).




Gambar 2.4 Faktor-faktor yang Saling Berkompetisi dalam Steganografi [9]

Kapasitas adalah besar pesan rahasia (*embedded message*) yang dapat disembunyikan dalam media penampung (*cover-object)* dengan menggunakan teknik steganografi tertentu. Anti-deteksi (*undetectability)* adalah kemampuan dalam menghindari deteksi. Pesan yang disisipkan tidak dapat dideteksi keberadaannya dalam suatu media. Misalnya jika steganografi menggunakan komponen derau pada citra digital dalam menyisipkan pesan, maka tidak membuat perubahan statistik yang signifikan pada media penampung pesan tersebut. Sedangkan kekokohan (*robustness)* adalah ukuran ketahanan teknikssteganografi dalam menghadapi berbagai macam manipulasi terhadap media penampung.Seringkali ketiga faktor ini saling menghilangkan satu sama lain. Informasi dalam jumlah kecil dapat disembunyikan secara efektif tanpa dapat dipersepsi dengan mudah. Namun analisis statistik terhadap derau yang ada dapat dengan mudah mengungkap keberadaan informasi rahasia. Namun penyisipan informasi dengan jumlah yang lebih banyak dapat saja mengubah media penampung sehingga keberadaan informasi dapat dengan mudah dideteksi. Sedangkan teknik yang kokoh sering mengorbankan kapasitas[9].

### 2.3.3 Manfaat Steganografi

Steganografi adalah sebuah pisau bermata dua, ia bisa digunakan untuk alasan-alasan yang baik, tetapi bisa juga digunakan sebagai sarana kejahatan. Steganografi juga dapat digunakan sebagai salah satu metode watermarking pada image untuk proteksi hak cipta, seperti juga digital *watermarking* (*fingerprinting*). Steganografi juga dapat digunakan sebagai pengganti hash. Dan yang terutama, seperti disebutkan sebelumnya, steganografi dapat digunakan untuk menyembunyikan informasi rahasia, untuk melindunginya dari pencurian dan dari orang yang tidak berhak untuk mengetahuinya. Steganografi juga dapat digunakan oleh para teroris untuk saling berkomunikasi satu dengan yang lain. Sehubungan dengan keamanan sistem informasi, steganografi hanya merupakan salah satu dari banyak cara yang dapat dilakukan untuk menyembunyikan pesan rahasia. Steganografi lebih cocok digunakan bersamaan dengan metode lain tersebut untuk menciptakan keamanan yang berlapis. Sebagai contoh steganografi dapat

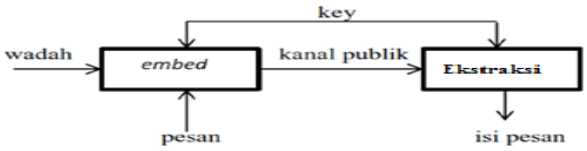
digunakan bersama dengan enkripsi. Windows dan Unix juga menggunakan steganography dalam mengimplementasikan *hidden directory*.

### 2.3.4 Proses Steganografi

Umumnya untuk menyembunyikan informasi dapat digambarkan sebagai data tertanam oleh pesan khusus yang akan dikirim secara rahasia. Biasanya informasi tersembunyi didalam pesan dikenal sebagai wadah teks, wadah gambar, atau wadah audio. *Stego-key* diterapkan untuk mengendalikan proses penyembunyiandan membatasi deteksi atau mengembalikan data yang tersembunyi.

Steganografi sudah digunakan sejak dahulu kala sekitar 2500 tahun yang lalu untuk kepentingan politik, militer, diplomatik, serta untuk kepentingan pribadi. Dansesungguhnya prinsip dasar dalam steganografi lebihdikonsentrasikan pada kerahasian komunikasinya bukan pada datanya. Steganografi memerlukan setidaknya dua properti. Properti pertama adalah wadah penampung (cover) dan yang kedua adalah data atau pesan yang disembunyikan. Untuk meningkatkan tingkat keamanan data yang disimpan, dapat dilakukan dengan menambahkan properti kunci (key) rahasia. Properti wadah (cover) yang mungkin digunakan untuk menyimpan pesan dalam steganografi sangat beragam. Medium wadah tersebut antara lain citra, suara, video ataupun teks. Adapun data yang disimpan juga dapat berupa audio, citra, video maupun teks.

Skema penyembunyian data dalam steganografi secara umum adalah data atau informasi yang ingin disembunyikan disimpan dalam sebuah wadah (cover) melalui suatu algoritma steganografi tertentu. Untuk menambah tingkat keamanan data, dapat diberikan kunci, agar tidak semua orang mampu mengungkapkan data yang disimpan dalam berkas wadah (cover). Hasil akhir dari proses penyimpanan data ini adalah sebuah berkas stego (stego data/stego file). Pertimbangan pemilihan penggunaan kunci dari segi tipe serta panjang kunci adalah suatu hal yang juga berperan penting dalam pengamanan data yang tersimpan dalam steganografi [10].




Gambar 2.5 Proses Steganografi [10]

### 2.3.5 Audio Steganografi

Audio steganografi adalah teknik penyisipan pesan rahasia dalam media suara (audio). Proses penyisipan pesan rahasia dalam sistem steganografi pada dasarnya dilakukan dengan mengidentifikasi media audio pembawa pesan, yaitu *redundant bit* yang mana dapat dimodifikasi tanpa merusak integritas dari media audio itu sendiri. Dalam mengaplikasikan steganografi pada berkas audio dapat dilakukan dengan berbagai teknik. Berikut adalah beberapa teknik yang dapat digunakan:

1. Penggantian bit. Cara ini lazim digunakan dalam teknik digital steganografi yaitu mengganti bagian tertentu dari bit-bit datanya dengan data rahasia yang disisipkan. Dengan metode ini keuntungan yang didapatkan adalah ukuranpesan yang disisipkan relatif besar, namun berdampak pada hasil audio yang berkualitas kurang dengan banyaknya derau.
2. Metode kedua yang digunakan adalah merekayasa fasa dari sinyal masukan. Teori yang digunakan adalah dengan mensubstitusi awal fasa dari tiap awal segmen dengan fasa yang telah dibuat sedemikian rupa dan merepresentasikan pesan yang disembunyikan. Fasa dari tiap awal segmen ini dibuat sedemikian rupa sehingga setiap segmen masih memiliki hubungan yang berujung pada kualitas suara yang tetap terjaga. Teknik ini menghasilkan keluaran yang jauh lebih baik daripada metode pertama namun dikompensasikan dengan kerumitan dalam realisasinya.
3. Metode yang ketiga adalah penyebaran spektrum. Dengan metode ini pesan dikodekan dan disebar ke setiap spektrum frekuensi yang memungkinkan. Maka dari itu akan sangat sulit bagi yang akan mencoba memecahkannya kecuali ia memiliki akses terhadap data tersebut atau dapat merekonstruksi

sinyal acak yang digunakan untuk menyebarkan pesan pada *range* frekuensi.

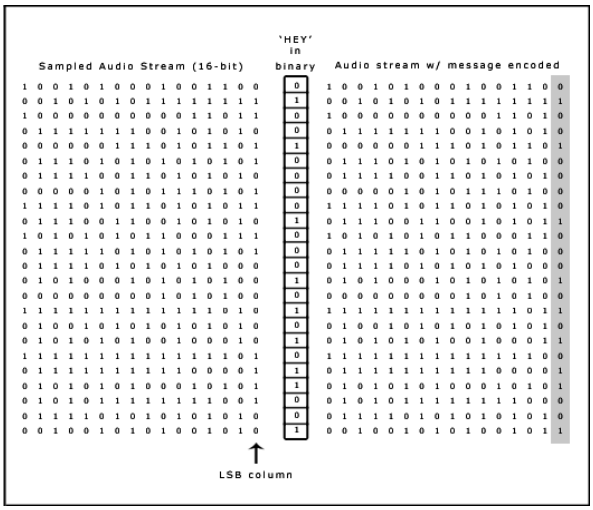
4. Metode terakhir yang sering digunakan adalah menyembunyikan pesan melalui teknik *echo*. Teknik menyamarkan pesan ke dalam sinyal yang membentuk *echo*. Kemudian pesan disembunyikan dengan memvariasikan tiga parameter dalam *echo* yaitu besar amplitude awal, tingkat penurunan atenuasi dan *offset*. Dengan adanya *offset* dari *echo* dan sinyal asli maka *echo* akan tercampur dengan sinyal aslinya, karena sistem pendengaran manusia yang tidak memisahkan antara *echo* dan sinyal asli[6].

### 2.3.6 Macam-macam metode Audio Steganografi

Macam-macam metode audio steganografi yaitu:

1. *Low Bit Encoding / Least Significant Bit*

   Teknik yang biasa digunakan untuk menyembunyikan informasi di dalam file audio ialah *low bit encoding* yang mirip dengan teknik LSB yang biasa digunakan di gambar yaitu dengan menyisipkan bit – bit dari pesan yang akan disembunyikan ke dalam bit media penampung data tersebut.

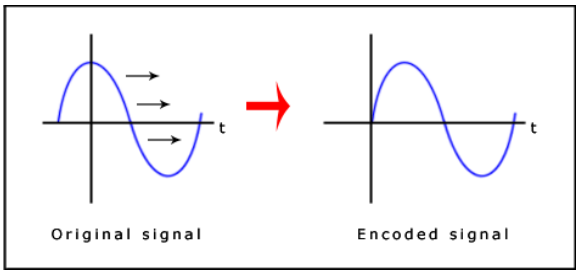



Gambar 2.6 Contoh penyimpanan pesan ‘HEY’ kedalam 16-bit audio [11].

2. *Phase Coding*

   *Phase Coding* merupakan metode yang merekayasafasa dari sinyal masukan. Teori yang digunakan ialah dengan mensubstitusi awal fasa dari

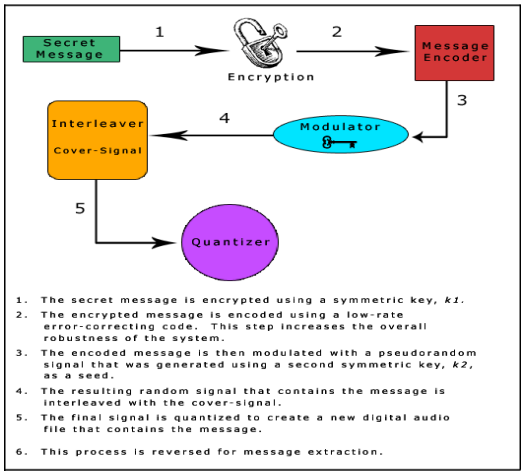
setiap awal segmen dengan fasa yang telah dibuat sedemikian rupa dan merepresentasikan pesan yang disembunyikan. Fasa dari setiap awal segmendibuat sedemikian rupa sehingga setiap segmen masih memiliki hubungan dan dapat menjaga kualitas suara. Teknik ini menghasilkan keluaran yang jauh lebih baik dari metode pertama namun realisasinya sangatlah rumit.




Gambar 2.7 Proses Phase Coding [11].

3. *Spread Spectrum*

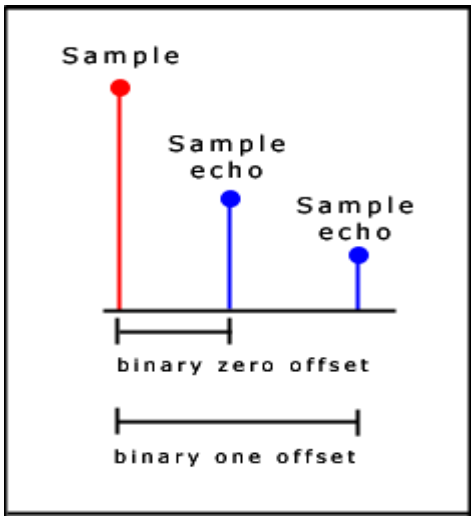
*Spread Spectrum* merupakan metode lain yang digunakan untuk menyimpan informasi di dalam *file* audio. Metode ini bekerja dengan cara pesan dikodekan dan disebarkan ke setiap spektrum frekuensi yang memungkinkan. Metode ini sulit untuk dipecahkan kecuali memiliki akses terhadap data yang disimpan atau dapat merekonstruksi sinyal random yang digunakan untuk menyebarkan pesan. Ada dua versi dari *Spread Spectrum* yang dapat digunakan di dalam steganografi audio yaitu *directsequence* dan *frequency-hopping schemes*. Pada *direct-sequence spread spectrum*, pesan rahasia disebar dengan konstanta yang disebut *chip rate* dan kemudian dimodulasikan dengan sinyal *pseudorandom*. Kemudian digabungkan dengan *cover-signal*. Pada *frequency-hopping spread spectrum*, spektrum frekuensi *file* audio digantikan sehingga akan menyebar secara acak dalam frekuensi.




Gambar 2.8 Proses *Spread Spectrum* [11].

4 *Echo Hiding*

*Echo data hiding* juga merupakan metode untuk menyembunyikan informasi di dalam *file* audio. Metode ini menggunakan *echo* yang ada di dalam *file* audio untuk mencoba menyembunyikan informasi. Pesan akan disembunyikan dengan memvariasikan tiga parameter dalam *echo* yaitu besar amplitudo awal, tingkat penurunan atenuasi, dan *offset*. Ketiga parameter tersebut diatur sedemikian rupa di bawah pendengaran manusia sehingga tidak mudah untuk dideteksi. Sebagai tambahan, *offset* divariasikan untuk merepresentasikan *binary* pesan yang disembunyikan. Nilai *offset* pertama merepresentasikan nilai *binary* 1 dan nilai *offset*kedua merepresentasikan *binary* 0.




Gambar 2.9 Contoh *echo* [11].

Jika hanya 1 *echo* yang dihasilkan dari sinyal asli, hanya 1 bit informasi yang dapat di *encoding*. Karena itu, sinyal awal dibagi – bagi ke dalambeberapa blok sebelum proses *encoding* dimulai. Ketika proses *encoding* telah selesai, blok – blok tersebut digabungkan kembali membentuk sinyal baru [11].

## 2.4 Perbandingan Metode LSB dan Metode Audio Steganografi Lainnya

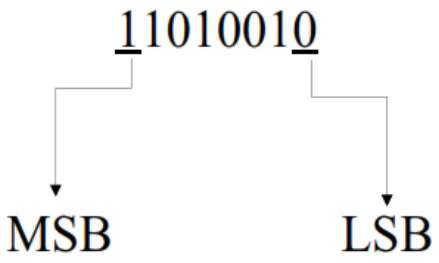
Tabel 2.1 Perbandingan Metode LSB dan Metode Audio Steganografi Lainnya [11].

| No | Metode | Kekurangan | Kelebihan |
|---|---|---|---|
| 1. | ***Low Significant Bit* / LSB** | ○ Mudah diimplementasikan dan proses *encoding* yang cepat | ○ Biasanya terdengar oleh telinga manusia sehingga teknik tersebut merupakan teknik yang cukup beresiko untuk digunakan jika ingin menutupi sebuah informasi di dalam *file* audio |
| | ***Phase Coding*** | ○ Merupakan teknik yang cukup robust dalam penyisipan watermark ke dalam suatu bekas MP3 karena teknik ini tahan terhadap proses pencuplikan ulang, pemotongan berkas MP3 (selain bagianawal berkas), pemberian derau (selain bagian awal berkas), dan kompresi (pengubahan format berkas)<br>○ Kualitas suara yang dihasilkan oleh berkas MP3 yang telah disisipi watermark dengan teknik ini cukup baik (hampir tidak terdeteksi adanya derau) | ○ Jika dilakukan pemotongan atau pemberian derau pada bagian awal berkasMP3 yang disisipi *watermark*, maka *watermark* dapat hilang atau tidak dapat diekstraksi dengan baik<br>○ Hanya dapat digunakan ketika ingin menyembunyikan data yang ukurannya kecil |
| 3. | ***Spread Spectrum*** | ○ Penyembunyian sinyal (kepadatan energi yang | ○ Tidak adanya perbaikan performansi melalui |

| | | | |
|---|---|---|---|
| | | rendah, mirip derau)<br>○ Komunikasi yang aman<br>○ Penolakan *multi path*, hanya menerima *direct path*<br>○ Proteksi terhadap inferensi yang tidak disengaja (*narrowband*)<br>○ Kecil kemungkinan untuk terdeteksi<br>○ Adanya ketersediaan *license-free* ISM (*Industrial, Scientific, and Medical*) *frequency-bands* | penggunaan derau Gaussian<br>○ Peningkatan bandwith (penggunaan frekuensi, *wideband receiver*)<br>○ Peningkatan kompleksitas dalam proses perhitungan<br>○ Dapat menimbulkan derau |
| 4. | ***Echo Hiding*** | ○ Sistem pendengaran manusia tidak dapat memisahkan antara *echo* dan sinyal asli | ○ Kurang bagus digunakan pada *file* audio yang memiliki *silence gap* yang cukup besar karena *echo* akan terdengar jelas |

## 2.5 Metode LSB

Metode *Steganografi* yang paling umum pada format suara adalah Modifikasi *Least Significant Bit*. Metode ini banyak digunakan karena komputasinya tidak terlalu kompleks dan pesan yang disembunyikan cukup aman. Strategi penyembunyian data pesan yang digunakan untuk menyisipkan kedalam media audio adalah denganmetode *Least Significant Bit* (LSB). Dimana bit datapesan akan digantikan dengan bit paling rendah dalam media audio.




Gambar 2.10 MSB dan LSB

MSB : *Most Significant Bit*

LSB : *Least Significant Bit*

Pada gambar 1, menandakan bahwa bit 1 dari depan menyatakan bit MSB dan bit 0 dari bilangan biner terakhir adalah bit LSB. Dapat dilihat contoh dibawah ini.

1. Jika pesan = 10 bit, maka jumlah byte yang digunakan = 10 byte

00110011 10100010 10100011 00100110
01011001 01101110 10110101 00010101
11100110 11011010

Misalkan binary dari *embedded message*: 1110101011

Hasil penyisipan pada bit LSB:

00110011 10100011 10100011 00100110
01011001 01101110 10110101 00010100
11100111 11011011

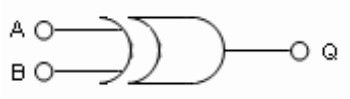
Pada contoh diatas, hanya sebagian yang berubah dari *Least Significant Bit.* Berdasarkan teori maka didapatkan bahwa ukuran file asli tidak mengalami perubahan yang begitu besar sehingga sulit terdeteksi oleh indra manusia[10].

## 2.6 Gerbang Logika

Gerbang (*gate*) logika adalah suatu rangkaian digital yang mempunyai satu atau lebih *input* dan hanya mempunyai satu *output*. *Output* gerbang logika ini tergantung sinyal yang diberikan pada *input*-nya. Hal ini dapat kita lihat pada persamaan aljabar Boole dan tabel kebenaran yang dimiliki oleh setiap gerbang logika. Aljabar Boole juga memberikan persamaan untuk setiap gerbang serta memberi simbol untuk operasi gerbang tersebut. Suatu rangkaian digital dapat dibangun dari sejumlah gerbang logika. Dari persamaan untuk setiap gerbang dan tabel kebenaran tiap gerbang logika, maka dengan menggabungkan beberapa gerbang ini akan didapat operasi logika sesuai dengan keinginan dan tujuan yang diharapkan sehingga terbentuklah suatu rangkaian digital yang akan membangun sistem yang diinginkan. Adapun gerbang logika dasar adalah NOT, AND dan OR. Sedangkan gerbang NAND, NOR, XOR, XNOR merupakan gerbang yang dibentuk dari gabungan beberapa gerbang dasar [8]

### 2.6.1 Gerbang XOR (Exclusive OR)

Apabila input A dan B ada dalam keadaan logika yang sama, maka output Q akan menghasilkan logika 0, sedangkan bila input A dan B ada dalam keadaan logika yang berbeda, maka output akan menjadi logika 1. XOR sebetulnya merupakan variasi dari cara kerja logika OR. Untuk lebih jelas, coba perhatikan tabel kebenarannya:




Gambar 2.11 Simbol Gerbang XOR [19].

Tabel 2.2 Kebenaran logika XOR [19].

| Masukan | | Keluaran |
|---|---|---|
| A | B | Q |
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

kebenaran XOR ini hanya berbeda satu langkah saja dengan tabel kebenaran OR, yaitu pada langkah terakhir saat input A dan B keduanya pada logika 1, outputnya menghasilkan 0, bukan 1 seperti pada logika OR.

Aplikasi dari proses logika XOR ini dapat dimanfaatkan untuk membandingkan dua buah data, yaitu apabila data-data tersebut mengandung informasi yang persis sama, maka XOR akan memberikan output logika 0 [19].

## 2.7 Audio

Audio adalah suara atau bunyi yang dihasilkan oleh getaran suatu benda, agar dapat tertangkap oleh telinga manusia getaran tersebut harus kuat minimal 20 kali/detik. Suara yaitu suatu getaran yang dihasilkan oleh gesekan , pantulan dan lain-lain, antara benda-banda. Sedangkan gelombang yaitu suatu getaran yang

terdiri dari Amplitudo dan juga waktu. Suara dibangun oleh periode, Apabila Tidak Berarti itu bukanlah Suara.

Definisi audio yang lainnya adalah merupakan salah satu elemen yang penting, karena ikut berperan dalam membangun sebuah sistem Komunikasi dalam bentuk suara, ialah suatu sinyal elektrik yang akan membawa unsur-unsur bunyi didalamnya. Audio itu terbentuk melalui beberapa tahap, diantaranya: tahap pengambilan atau penangkapan suara, sambungan transmisi yang membawa bunyi, amplifier dan lain-lain.

### 2.7.1 Jenis-Jenis Audio

Jenis-jenis audio, terdapat berbagai macam audio yang dikelompok berdasarkan media ataupun perangkat yang sering gunakan, diantaranya:

1. Audio Streaming adalah suatu istilah yang dipakai untuk mendengarkan siaran langsung atau live melalui jaringan internet. Seperti contohnya: Winamp (MP3), RealAudio (RAM) dan juga Liquid Radio.
2. Pengertian audio visual adalah suatu istilah yang digunakan untuk seperangkat soundsystem yang dilengkapi dengan tampilan gambar, biasanya dipakai untuk presentasi.
3. Audio Modem Riser (AMR) adalah suatu istilah yang dipakai untuk sebuah kartu plug-in untuk motherboard intel yang memuat sirkuit audio ataupun Modem.

### 2.7.2 Macam-Macam format Audio

Inilah Macam-macam format audio, ada berbagai macam format atau ekstensi audio yang dapat ditemui sehari-hari, tapi yang umumnya dikenal oleh masyarakat antara lain :

1. MP3 adalah (MPEG, Audio Layer 3) suatu format audio yang dikembangkan oleh Fraunhoper Institude dengan memiliki bitrate 128 kbps. Dalam waktu yang singkat MP3 menjadi format paling populer dalam dunia musik digital, sebab ukuran filenya yang kecil dan juga kualitasnya tidak kalah dengan CD Audio.

2. WAV adalah suatu format audio yang merupakan standar suara dari de-facto di Windows. Awalnya format jenis ini dijadikan jembatan untuk penghubung file yang akan dikonversi keformat yang lainnya. Tetapi seiring berkembangnya zaman, banyak para pengguna yang melewati tahap ini, pengguna dapat mengkonversi file secara langsung ke format yang diinginkannya. Format ini jarang sekali dipakai sebab ukuran filenya yang lumayan agak besar.
3. AAC (Advanced Audio Coding) adalah suatu format audio yang menjadi standar untuk MPEG (Motion Picture Experts Group). Sejak standar MPEG-2 diberlakukan pada tahun 1997, sample rate yang ditawarkan sampai dengan 96 KHz atau 2 (dua) kali sample rate MP3 (MPEG, Audio Layer 3). Kualitas format audio dengan ini cukup baik sekali, bahkan pada bitrate yang paling rendah sekalipun. Salah satu pengguna format audio ini ialah iTunes, toko musik online besutan Apple dan juga piranti atau perangkat pendukung terkemuka untuk format audio ini juga berasal dari produknya Apple yaitu Ipod.
4. WMA (Windows Media Audio) adalah suatu format audio yang ditawarkan oleh perusahaan teknologi terbesar di dunia yaitu Microsoft Corporation. Format audio yang satu ini sangat disukai oleh vendor musik online sebab dukungannya terhadap DRM (Digital Right Management) yaitu suatu fitur yang dipakai untuk mencegah pembajakan musik. Selain itu, menurut isu atau gosip yang beredar format audio ini memiliki kualitas yang lebih baik dari pada formaat AAC maupun MP3.
5. Ogg Vorbis adalah satu-satunya format audio yang garatis atau terbuka untuk umum. Kelebihannya ialah terletak pada kualitas audio yang tinggi walaupun pada bitrate rendah sekalipun.
6. Real Audio adalah suatu format audio yang sering ditemui pada bitrate rendah. Format jenis ini dikembangkan oleh RealNetworks, digunakan untuk layanan streaming audio pada bitrate 128 kbps atau lebih dengan memakai standar AAC MPEG-4.

7. MIDI adalah suatu format audio yang biasanya digunakan untuk ringtone pada handphone, sebab ukuran filenya yang kecil tapi sayangnya format audio ini hanya cocok untuk suara yang dihasilkan oleh synthesizer.

### 2.7.3 Audio MP3

MPEG-1 Audio Layer 3 atau lebih dikenal sebagai MP3 adalah salah satu format berkas pengodean suara yang memiliki kompresi yang baik (meskipun bersifat *lossy*) sehingga ukuran berkas bisa memungkinkan menjadi lebih kecil. Berkas ini dikembangkan oleh seorang insinyur Jerman Karlheinz Brandenburg. MP3 memakai pengodean *Pulse Code Modulation* (PCM). MP3 mengurangi jumlah bit yang diperlukan dengan menggunakan model *psychoacoustic* untuk menghilangkan komponen-komponen suara yang tidak terdengar oleh manusia. MP3 mempunyai beberapa batasan/limit:

1. *Bit rate* terbatas, maksimum 320 kbit/s (beberapa *encoder* dapat menghasilkan *bit rate* yang lebih tinggi, tetapi sangat sedikit dukungan untuk MP3-MP3 tersebut yang memiliki *bit rate* tinggi)
2. Resolusi waktu yang digunakan MP3 dapat menjadi terlalu rendah untuk sinyal-sinyal suara yang sangat *transient*, sehingga dapat menyebabkan *noise*.
3. Resolusi frekuensi terbatasi oleh ukuran *window* yang panjang kecil, mengurangi efisiensi *coding*
4. Tidak ada *scale factor band* untuk frekuensi di atas 15,5 atau 15,8 kHz
5. Mode jointstereo dilakukan pada basis per *frame*
6. Delay bagi *encoder*/*decoder* tidak didefinisikan, sehingga tidak ada dorongan untuk *gapless playback* (pemutaran audio tanpa *gap*). Tetapi, beberapa *encoder* seperti LAME dapat menambahkan *metadata* tambahan yang memberikan informasi kepada *MP3 player* untuk mengatasi hal itu [12].

### 2.7.4 Audio WAV

WAV adalah singkatan dari istilah dalam bahasa Inggris *WAVeform audio format* merupakan standar format berkas audio yang dikembangkan oleh Microsoft dan IBM. WAV merupakan varian dari format *bitstream* RIFF dan mirip dengan format IFF dan AIFF yang digunakan komputer Amiga dan Macintosh. Baik WAV maupun AIFF kompatibel dengan sistem operasi Windows dan Macintosh. Walaupun WAV dapat menampung audio dalam bentuk terkompresi, umumnya format WAV merupakan audio yang tidak terkompres[13].

## 2.8 Smartphone Android

Smartphone (telepon pintar) adalah telepon genggam yang mempunyai kemampuan tingkat tinggi dengan fungsi yang menyerupai komputer. Bagi beberapa orang, telepon pintar merupakan telepon yang bekerja menggunakan seluruh perangkat lunak sistem operasi yang menyediakan hubungan standar yang mendasar bagi pengembang aplikasi. Bagi yang lainnya, telepon pintar hanyalah merupakan sebuah telepon yang menyajikan fitur canggih seperti e-mail (surat elektronik), internet dan kemampuan membaca buku elektronik (e-book) atau terdapat papan ketik dan penyambung VGA. Dengan kata lain, telepon pintar merupakan komputer kecil yang mempunyai kemampuan sebuah telepon.

Android adalah sistem operasi yang berbasis Linux untuk telepon seluler seperti telepon pintar dan komputer tablet. Android menyediakan platform terbuka bagi para pengembang untuk menciptakan aplikasi mereka sendiri untuk digunakan oleh bermacam peranti bergerak[14].

### 2.8.1 Fitur-Fitur Smartphone Android

Fitur - fitur yang tersedia di Android adalah:

1. Kerangka aplikasi: itu memungkinkan penggunaan dan penghapusan komponen yang tersedia.
2. Mesin virtual dioptimalkan untuk perangkatmobile.
3. grafik di 2D dan grafis 3D berdasarkan pustaka OpenGL.

4. SQLite: untuk penyimpanan data.
5. Mendukung media:audio, video, danberbagai format gambar (MPEG4, H.264, MP3,AAC, AMR, JPG, PNG, GIF)
6. GSM,Bluetooth, EDGE, 3G, dan WiFi (hardware dependent)
7. Kamera, Global Positioning System (GPS), kompas, dan accelerometer (tergantung hardware) [14].

### 2.8.2 Android

Android yaitu sebuah sistem operasi telepon seluler berbasis Linux. Android juga memiliki *platform* terbuka bagi seseorang yang ingin menciptakan aplikasi untuk digunakan oleh bermacam-macam peranti bergerak. Android juga merupakan sebuah sistem operasi untuk telepon seluler seperti halnya Symbian pada Nokia, *Palm* dan *Windows Mobile* yang sebelumnya sudah dikenal selama ini. Seiring dengan perkembangannya, android berubah menjadi *platform* yang begitu cepat dalam melakukan pembaruan. Pada awalnya, android dikembangkan oleh Android inc,yang didukung finansial dari pihak google, yang kemudian membelinya pada tahun 2005. Pada tahun 2007, sistem operasi ini telah resmi yang bersamaan dengan didirikannya *Open hardset Alliance*, konsorsium dari perusahaan-perusahaan perangkat keras, perangkat lunak serta telekomunikasi yang tidak lain bertujuan untuk memajukan standar terbuka perangkat seluler. Android, inc didirikan pada bulan Oktober tahun 2003 oleh Andy Rubin, Christ White, Rich Miner dan Nick Sears di Palo Alto California yang bertujuan untuk mengembangkan perangkat seluler pintar yang lebih tahu akan lokasi dan preferensi penggunanya [18].


Gambar 2.12 Logo Android [18]

## 2.9 Java

Java merupakan sebuah *platform* dengan bahasa pemograman tingkat tinggi yang mempunyai kriteria yang sederhana, berorientasi objek, dinamis, terdistribusi, aman dan lain-lain. Bahasa tersebut dikembangkan dengan menggunakan model yang mirip dengan bahasa C++ dan *smalltalk* tetapi lebih mudah untuk digunakan dan juga memiliki *platform* independen yang bisa dijalankan pada seluruh sistem operasi [18].


Gambar 2.13 Logo Java [16].

### 2.9.1 Eclipse

*Eclipse* merupakan sebuah IDE (*Integrated Development Environment*) untuk mengembangkan perangkat lunak dan dapat dijalankan di semua platform (*platform-independent*). Berikut ini adalah sifat dari *eclipse* :

**a. *Multi-platform***: Target sistem operasi *eclipse* adalah *Microsoft Windows*, Linux, Solaris, AIX, HP-UX dan Mac OS X.

**b. *Mulit-language***: *Eclipse* dikembangkan dengan bahasa pemrograman java, akan tetapi *eclipse* mendukung pengembangan aplikasi berbasis bahasa pemrograman lainnya, seperti C/C++, Cobol, Python, Perl, PHP, dan lain sebagainya.

**c. *Multi-role***: Selain sebagai IDE untuk pengembangan aplikasi, *eclipse* pun bisa digunakan untuk aktivitas dalam siklus pengembangan perangkat lunak, seperti dokumentasi, test perangkat lunak, pengembangan web, dan lain sebagainya.

Gambar 2.14 Logo *Eclipse* [15].

*Eclipse* pada saat ini merupakan salah satu IDE favorit dikarenakan gratis dan *open source*, dengan kata lain, setiap orang boleh melihat kode pemrograman perangkat lunak ini. Selain itu, *eclipse* memiliki kelebihan adalah kemampuannya untuk dapat dikembangkan oleh pengguna dengan komponen yang dinamakan *plug-in* [17].

### 2.9.2 Sejarah Eclipse

Eclipse awalnya dikembangkan oleh IBM untuk menggantikan perangkat lunak IBM Visual Age for Java 4.0. Produk ini diluncurkan oleh IBM pada tanggal 5 November 2001, yang menginvestasikan sebanyak US$ 40 juta untuk pengembangannya. Semenjak itu konsursium Eclipse Foundation mengambil alih untuk pengembangan Eclipse lebih lanjut dan pengaturan organisasinya.Sejak tahun 2006, Eclipse Foundation mengkoordinasikan peluncuran Eclipse secara rutin dan simultan yang dikenal dengan nama Simultaneous Release. Setiap versi peluncuran terdiri dari Eclipse Platform dan juga sejumlah proyek yang terlibat dalam proyek Eclipse. Tujuan dari sistem ini adalah untuk menyediakan distribusi Eclipse dengan fitur-fitur dan versi yang terstandarisasi. Hal ini juga dimaksudkan untuk mempermudah deployment dan maintenance untuk sistem enterprise. Adapun versi eclipse yang telah diluncurkan yaitu :

1.Eclipse 3.0

2.Eclipse 3.1

3.Callisto

4.Europa

5.Ganymede

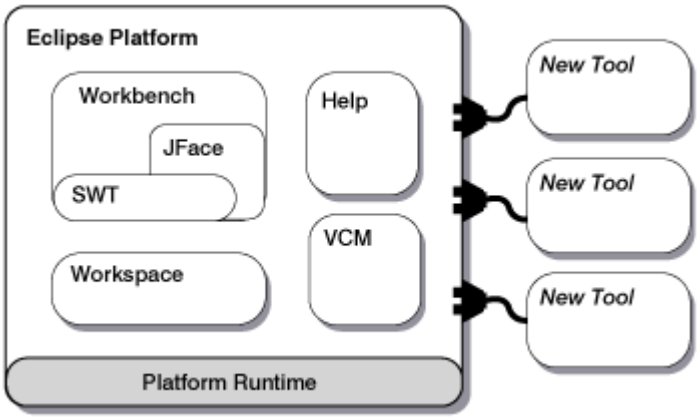
6.Galileo

7.Helios

8.Luna [14].

### 2.9.3 Arsitektur Eclipse

Sejak versi 3.0, Eclipse pada dasarnya merupakan sebuah kernel, yang mengangkat plug-in. Apa yang dapat digunakan di dalam Eclipse sebenarnya adalah fungsi dari plug-in yang sudah diinstal. Ini merupakan basis dari Eclipse yang dinamakan *Rich Client Platform*(RCP). Berikut ini adalah gambar dari arsitektur Eclipse:




Gambar 2.15 Arsitektur Eclipse [14].

Secara standar Eclipse selalu dilengkapi dengan JDT (*Java Development Tools*), *plug-in* yang membuat Eclipse kompatibel untuk mengembangkan program Java,dan PDE (*Plug-in Development Environment*) untuk mengembangkan *plug-in* baru. Eclipse beserta *plug-in*-nya diimplementasikan dalam bahasa pemrograman Java. Konsep Eclipse adalah IDE yang terbuka (*open*), mudah diperluas (*extensible*) untuk apa saja, dan tidak untuk sesuatu yang spesifik. Jadi, Eclipse tidak saja untuk mengembangkan program Java, akan tetapi dapat digunakan untuk berbagai macam keperluan, cukup dengan menginstal *plug-in* yang dibutuhkan. Apabila ingin mengembangkan program C/C++ terdapat *plug-in* CDT (*C/C++ Development Tools*). Selain itu, pengembangan secara

visual bukan hal yang tidak mungkin oleh Eclipse, *plug-in* UML2 tersedia untuk membuat diagram UML. Dengan menggunakan PDE setiap orang bisa membuat *plug-in* sesuai dengan keinginannya [14].