BAB I
PENDAHULUAN

1.1 Latar Belakang

Sebagai mahasiswa Teknik Telekomunikasi, sudah sepatutnya mengikuti perkembangan teknologi yang sedang terjadi saat ini, khususnya di bidang telekomunikasi. Dan pada kenyataannya teori yang diperoleh mahasiswa di pembelajaran kuliah masih sangat terbatas. Oleh karena itu, sangatlah penting mahasiswa mengaplikasikan ilmu yang diperoleh di kuliah tersebut pada dunia kerja yang kelak akan dihadapinya di dunia luar. Hal ini dapat diatasi dengan melakukan kerja praktek.

Kerja Praktek (FEG4B2) merupakan mata kuliah wajib yang harus diambil oleh setiap mahasiswa Program Studi Teknik Telekomunikasi TELKOM UNIVERSITY pada semester 6, di mana kerja Praktek itu sendiri dapat dilakukan setelah masa perkuliahan semester 6 berakhir. Dengan begitu mahasiswa dapat mengimplementasikan ilmunya pada dunia kerja. Oleh karena itu, demi mengoptimalkan pelaksanaan kerja praktek ini, sangat dianjurkan untuk melaksanakan kerja praktek pada perusahaan dengan topik yang berkaitan dengan disiplin ilmu kelompok keahlian masing-masing, dan mahasiswa peserta kerja praktek pun sebaiknya aktif dalam memanfaatkan kesempatan ini.

1.2 Tujuan

Tujuan dari pelaksanaan kerja praktek itu sendiri untuk mahasiswa :

1. Untuk mengembangkan *sense of engineering* mahasiswa.
2. Mengaplikasikan ilmu-ilmu yang diperoleh selama perkuliahan.
3. Mendapatkan pengalaman sekaligus memperluas wawasan mahasiswa tentang dunia kerja yang sesungguhnya.
4. Sebagai pelaksanaan mata kuliah wajib FEG4B2 Kerja Praktek.

Untuk Perusahaan :

1. Mendapatkan masukan-masukan dari peserta kerja praktek dalam pemecahan masalah yang dihadapi oleh perusahaan tersebut sesuai bidang keilmuan Teknik Telekomunikasi yang dimiliki oleh mahasiswa.
2. Turut serta menyukseskan program pemerintah dalam bidang pendidikan dan ketenagakerjaan.
3. Sebagai bahan pertimbangan bagi perusahaan dalam hal penilaian kualitas mahasiswa yang pada akhirnya berhubungan dengan penerimaan tenaga kerja baru (*fresh graduate*).

1.3 Manfaat

Kerja praktek diharapkan memberikan manfaat bagi mahasiswa selaku peserta kerja praktek dan juga perusahaan tempat mahasiswa melaksanakan kerja praktek. Manfaat yang diharapkan antara lain :

a. Bagi Mahasiswa
   - Mendapatkan pengalaman bekerja secara langsung
   - Meningkatkan softskill dan mengaplikasikan hardskill yang diperoleh di perkuliahan.
   - Mengenal pola kerja dan aturan-aturan untuk pekerja pada suatu perusahaan secara umum

b. Bagi Perusahaan
   - Memberi sarana untuk pengembangan sumber daya manusia Indonesia
   - Meringankan pekerjaan pegawai dalam beberapa kasus atau pekerjaan yang bisa dibantu oleh peserta kerja praktek

c. Bagi Perguruan Tinggi
   - Sebagai tolak ukur relevansi antara kurikulum yang diajarkan pada mahasiswa dengan kebutuhan yang ada di dunia kerja

1.4 Batasan Masalah

Laporan ini dibatasi pada pembahasan masalah : **ENKRIPSI DAN DEKRIPSI DATA SEBAGAI MEDIA *STEGANOGRAFI* PADA *CYBER DEFENSE*** yang akan diterapkan di kantor PT. Industri Telekomunikasi Indonesia.

1.5 Waktu dan Tempat Pelaksanaan Kerja Praktek

Kerja praktek dilakukan dari tanggal 16 Juli 2014 sampai dengan 14 Juli 2014 bertempat di PT. Industri Telekomunikasi Indonesia.

Alamat :

Jalan. Moch. Toha No. 77 Bandung 40253 Indonesia

Telp: +62225201501

Fax: +62225202444

Email info@inti.co.id

1.6 Metode Pengerjaan

Metode yang dilakukan dalam pengerjaan tugas dapat dikelompokkan atas:

- Studi literature: Pada proses pelaksanaan kerja praktik ini, metode pengerjaan yang pertama kali dilakukan adalah studi literatur. Hal ini dilakukan untuk dapat mempelajari dan mendapatkan gambaran umum dari Steganografi dan Kriptografi pada Cyber Defense.

- Diskusi bersama pembimbing lapangan mengenai analisa data-data yang diperoleh dari studi literature.

1.7 Sistematika Penulisan

Laporan ini disusun berdasarkan sistematika sebagai berikut :

Bab 1 : Pendahuluan

Berisikan pendahuluan laporan yang berisi latar belakang kerja praktek, tujuan kerja praktek, waktu dan tempat pelaksanaan, pembatasan masalah, metode pengambilan data dan sistematika penulisan.

Bab 2 : Profil Umum PT. Industri Telekomunikasi Indonesia

Berisi profil singkat perusahaan, produk, dan berbagai pelayanan yang diberikan oleh perusahaan.

Bab 3 : Teori

Berisi tentang penjelasan landasan teori yang digunakan penulis untuk mengerjakan laporan.

Bab 4 : Metode Penelitian

Berisi tentang bahan dan alat penelitian, beserta jalannya penelitian yang akan dilakukan.

Bab 5 : Penutup

Berisi kesimpulan dan saran.

BAB II

PROFIL UMUM PERUSAHAAN

2.1 Profil Perusahaan

PT. Industri Telekomunikasi Indonesia berpusat di Bandung dengan 695 orang karyawan tetap (posisi Maret 2009), PT INTI (Industri Telekomunikasi Indonesia) telah berkiprah dalam bisnis telekomunikasi selama 35 tahun. Pelanggan utama INTI antara lain adalah "THE BIG FOUR" operator telekomunikasi di Indonesia; Telkom, Indosat, Telkomsel dan XL.

Sejak berkembangnya tren konvergensi antara teknologi telekomunikasi dan teknologi informasi (IT), INTI telah melakukan perubahan orientasi bisnis dari yang semula berbasis pure manufacture menjadi sebuah industri yang berbasis solusi kesisteman, khususnya dalam bidang sistem infokom dan integrasi teknologi.

Selama dua tahun terakhir INTI menangani solusi dan layanan jaringan tetap maupun seluler serta mengembangkan produk-produk seperti IP PBX, NMS (*Network Management System*), SLIMS (*Subscriber Line Maintenance System*), NGN Server, VMS (*Video Messaging System*), GPA (Perangkat Pemantau dan Pengontrol berbasis SNMP), Interface Monitoring System untuk jaringan CDMA, dan Sistem Deteksi dan Peringatan Bencana Alam (*Disaster Forecasting and Warning System*).

Memasuki tahun 2009, PT INTI mulai mencari peluang-peluang bisnis dalam industri IT, termasuk kemungkinan untuk bergabung dalam usaha mewujudkan salah satu mimpi dan tantangan terbesar Indonesia saat ini, yaitu membuat komputer notebook murah. Ini adalah satu tantangan yang besar bagi INTI.

2.2 Visi & Misi Perusahaan

Visi kami adalah menjadi pilihan pertama bagi pelanggan dalam mentransformasikan **"mimpi"** menjadi **"kenyataan"**.

Kepercayaan adalah prinsip yang utama bagi kami, terlebih pada saat ini. Pada era di mana pilihan makin mengglobal dan kompetisi makin meningkat, kami yakin bahwa kepercayaan merupakan cara paling efektif untuk merebut hati dan pikiran manusia.

Dengan pengalaman lebih dari 35 tahun bergerak dalam industri telekomunikasi, kami telah memperoleh kepercayaan itu. Sampai hari ini, kami dipercaya untuk memberikan solusi kesisteman bagi para operator telekomunikasi ternama di Indonesia.

Tak hanya itu, kami pun secara konsisten terlbat dalam pembangunan telekomunikasi di Indonesia sejak awal kami berdiri. Sesuai dengan salah satu misi kami, yaitu berperan sebagai penggerak utama bangkitnya industri dalam negeri.

Fokus kami adalah memberikan jasa engineering bidang infokom (ICT) yang sesuai dengan spesifikasi dan permintaan klien serta memaksimalkan nilai. Dengan cara itu kami berharap dapat mengupayakan pertumbuhan yang berkesinambungan secara mutual.

Tak diragukan lagi bahwa kami tak hanya menjadi bagian penting dari mimpi klien kami, tetapi bahkan menjadi bagian penting dari mimpi Indonesia. Dan karena kami sangat tertarik untuk mewujudkan mimpi anda, dengan penuh semangat dan ketulusan, kami akan membagi pengalaman-pengalaman kami dengan anda.

2.3 Products and Services

Berikut adalah daftar Produk dan Layanan yang INTI tawarkan.

- i-Perisalah
- HMIS
- INTI Smart Exchange
- Seat Management
- General Purpose Agent
- KWH Meter Digital

2.4 Our Solutions

Berikut adalah daftar solusi yang INTI tawarkan.

- Corporate Communication
- Defense
- FFWS
- FTTH
- ISC
- SPFR
- Renewable Energy

2.5 Management (Organization Structure)

- Direktur Utama : Tikno Sutisna
- Direktur Keuangan : Nilawati Djuanda
- Direktur Operasi dan Teknik : Adiaris
- Dewan Komisaris
  - Komisaris Utama : Soleman B. Ponto
  - Komisaris : Slamet Effendi
  - Komisaris : Nuning Sri Rejeki Wulandari
  - Komisaris : Djoko Agung Harijadi

BAB III
DASAR TEORI

Penggunaan penyampaian pesan digital dengan perkembangan internet saat ini telah banyak digunakan mulai lewat e-mail, chatting, sms dan sebagainya. Pengguna dari fasilitas ini saat ini telah mencapai angka jutaan, ini bisa dilihat dari jumlah pengguna situs yahoo, gmail, friendster atau bahkan facebook. Seiring dengan berkembangnya teknologi informasi saat ini, maka semakin memudahkan para pelaku kejahatan komputer (cyber crime), atau yang sering disebut dengan istilah cracker, script kiddies, carder, lamer, dimana aktivitas mereka sangat mengganggu privasi seseorang dengan menyalahgunakan teknologi komputer yang sedang berkembang pesat. Terbukti tindak kejahatan cyber crime di Indonesia saat ini cukup mengkhawatirkan sekali, sehingga menambah tingkat keterpurukan Indonesia di mata dunia internasional. Saat inipun kita belum bisa merasa aman akan e-mail kita karena e-mail kita sudah diakses orang lain. Keamanan akan pesan yang disampaikan kepada kitapun pada akhirnya tidak dapat dipertanggung jawabkan.

3.1 Teori Informasi

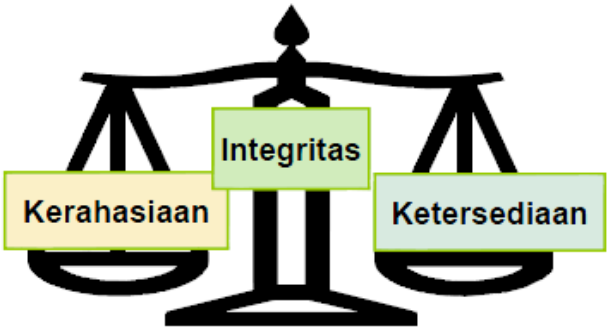
Dari perspektif keamanan informasi, informasi dapat diartikan sebagai sebuah ‘aset’; merupakan sesuatu yang memiliki nilai karena harus dilindungi. Nilai secara intrinsik melibatkan subyektivitas yang membutuhkan penilaian dan pengambilan keputusan. Oleh karena itu, keamanan adalah ilmu pengetahuann dan seni

Karakteristik	Aset informasi	Aset nyata
Bentuk-pemeliharaan	Tidak memiliki bentuk fisik dan bersifat fleksibel	Memiliki bentuk fisik
Variabel nilai	Bernilai lebih tinggi ketika digabung dan diproses	Total nilai adalah jumlah dari tiap nilai
Berbagi	Reproduksi yang tak terbatas, dan orang-orang dapat berbagi nilainya	Reproduksi tidak mungkin; dengan reproduksi, nilai aset berkurang
Ketergantungan-medium	Perlu disampaikan melalui medium	Dapat disampaikan secara independen (karena bentuk fisiknya)

Gambar 3.1 Nilai informasi

3.1.1 Penerapan Keamanan informasi

Cara menerapkan keamanan informasi adalah dengan menjamin kerahasiaan, intergritas, dan ketersediaaan.



Gambar 3.2 Penerapan Keamanan informasi

Kerahasiaan	Menjamin informasi tidak dibuat tersedia atau terbuka untuk individu, entitas, atau proses yang tidak berwenang.
Integritas	Integritas menjaga akurasi dan kelengkapan aset-aset.
Ketersediaan	Menjamin bahwa informasi dapat diakses dan digunakan oleh entitas yang berwenang ketika dibutuhkan.

Gambar 3.3 Karakteristik Keamanan informasi

3.1.1.1 Otomasi Alat Penyerangan

Saat ini penyusup menggunakan alat otomatis unuk mengumpulkan informasi tentang kelemahan sistem atau untuk langsung menyerang.

Alat penyerangan yang sulit dideteksi :

- Beberapa alat penyerangan menggunakan pola penyerangan baru yang tak terdeteksi oleh alat deteksi saat ini. Sebagai contoh, teknik anti-forensik digunakan untuk menyembunyikan sifat dari alat penyerangan.
- Alat polimorfik berubah bentuk setiap saat digunakan. Beberapa alat ini menggunakan protokol umum seperti *hypertext transfer protocol* (HTTP), sehingga sulit membedakan mereka dari lalu-lintas jaringan normal.

3.1.2 Jenis Serangan

3.1.2.1 Hacking

- Tindakan memperoleh akses ke komputer atau jaringan komputer untuk mendapatkan atau mengubah infomasi tanpa otorisasi yang sah
- Dapat dikelompokkan dalam *hacking* 'iseng', kriminal atau politis

3.1.2.2 Denial of Service

Serangan *Denial-of-service* (DoS) mencegah pengguna yang sah dari penggunaan layanan ketika pelaku mendapatkan akses tanpa izin ke mesin atau data. Ini terjadi karena pelaku 'membanjiri' jaringan dengan volume data yang besar atau sengaja menghabiskan sumber daya yang langka atau terbatas, seperti *process control blocks* atau koneksi jaringan yang tertunda.

3.1.2.3 *Malicious Code* (Kode Berbahaya)

- Program yang menyebabkan kerusakan sistem ketika dijalankan
- Termasuk *Trojan horse*, virus, dan *worm*

3.1.3.4 *Social Engineering*

Sekumpulan teknik untuk memanipulasi orang sehingga orang tersebut membocorkan informasi rahasia

3.1.3 Peningkatan Keamanan

3.1.3.1 Pengamanan Administratif

- Strategi, kebijakan, dan pedoman keamanan informasi
  - Strategi keamanan informasi
  - Kebijakan keamanan informasi
  - Pedoman keamanan informasi
  - Standar keamanan informasi
  - *IT Compliance*
- Proses dan operasi keamanan informasi
  - Program pendidikan dan pelatihan keamanan informasi
  - Penguatan promosi melalui berbagai kegiatan
  - Pengamanan dukungan

3.1.3.2 Pengamanan dengan teknologi

- Model Defense in Depth (DID)

Gambar 3.4 Defense in depth

- ***Teknologi Pencegah***
  - Kriptografi

    Proses pengkodean informasi dari bentuk aslinya (disebut *plaintext*) menjadi sandi, bentuk yang tidak dapat dipahami
  - *One-Time Passwords* (OTP)

    OTP hanya dapat digunakan sekali. *Password* statis lebih mudah disalahgunakan oleh *password loss*, *password sniffing*, dan *brute-force cracks* dan sejenisnya. OTP digunakan untuk mencegahnya.
  - *Firewall*

    Firewalls mengatur beberapa aliran lalu lintas antara jaringan komputer dari t*rust level* yang berbeda.
  - Alat penganalisis kerentanan

    Ada 3 jenis alat penganalisis kerentanan:
    - Alat penganalisis kerentanan jaringan
    - Alat penganalisis kerentanan *server*
    - Alat penganalisis kerentanan *web*

- ***Teknologi deteksi***
  - Anti-Virus

    Program komputer untuk mengidentifikasi, menetralisir atau mengeliminasi kode berbahaya
  - IDS (*Intrusion Detection System*)

    IDS mengumpulkan dan menganalisis informasi dari berbagai area dalam sebuah komputer atau jaringan untuk mengidentifikasi kemungkinan penerobosan keamanan
  - IPS (*Intrusion Prevention System*)

    IPS mengidentifikasi potensi ancaman dan bereaksi sebelum mereka digunakan untuk menyerang
- ***Teknologi terintegrasi***
  - ESM (*Enterprise Security Management*)

    Sistem ESM mengatur, mengontrol dan mengoperasikan solusi keamanan informasi seperti IDS dan IPS mengikuti kebijakan yang ditetapkan
  - ERM (*Enterprise Risk Management*)

    Sistem ERM adalah membantu memprediksi seluruh risiko yang terkait dengan organisasi, termasuk area di luar keamanan informasi, dan mengatur langkah mengatasinya secara otomatis

3.2 Cyber Security dan Cyber Defense

Cyber security atau keamanan dunia maya adalah proteksi perlindungan dunia maya dari sumber-sumber bahaya. Sedangkan *Security defense* atau pertahanan dunia maya adalah segala bentuk usaha untuk mempertahankan keamanan *cyber* atau dunia maya. Menurut Ian Wallace dalam artikelnya yang berjudul *The Military Role In National Cybersecurity Governance*, *Cyber Security* berbeda dengan *security* atau keamanan biasa karena ancaman *cyber* tidak bisa dimasukan begitu saja ke dalam kategori keamanan tradisional. Selain berasal dari dalam negeri, ancaman *cyber* atau *Cyber Threats* juga datang dari luar negeri. Namun, ancaman ini jarang mencapai taraf yang membutuhkan respon militer karena

apapun yang akan dilakukan pemerintah dalam menanggapi ancaman *cyber* ini akan memiliki implikasi domestik serta nasional.

Jenis-jenis ancaman *cyber* diantaranya adalah spionase, subversi, dan sabotase serta kejahatan *cyber* atau *cybercrime.* Keamanan informasi, termasuk melindungi masyarakat dari konten-konten berbahaya di dunia maya juga merupakan fokus dari *cyber security*. Walaupun tidak terlihat seperti perang, namun pelanggaran di dunia *cyber* saat ini sudah setara dengan perang di dunia fisik. Tetapi walaupun begitu, memberikan respon secara militer bukanlah cara terbaik. Walaupun respon militer memang bukan cara yang tepat, bukan berarti *cyber threats* berada di bawah level perang yang tidak harus ditanggapi dengan serius. Ada hal-hal yang perlu dipertimbangkan dalam penggunaan kekuatan militer yang diantaranya adalah kebanyakan dari kekuatan militer memang memiliki beberapa kemampuan *cyber* untuk mendukung pertempuran di medan perang dan mempertahankan sistemnya selama masa damai. Seringkali militer menyediakan intelejen yang informasinya akan mendukung operasi militer. Namun, penggunaan kekuatan militer terlalu sering juga memiliki resiko yaitu akan menyebabkan kerugian dan *cyber threats* tidak akan hilang, sebaliknya, mereka malah akan semakin berkembang karena kita akan menggunakan sistem informasi lebih banyak. Selain itu, resiko memilitarisasikan aspek baru keamanan domestik akan dianggap sebagai hal yang sangat buruk.

Untuk mencapai *cyber security* yang benar-benar efektif maka perlu beroperasi pada sistem pertahanan secara permanen. Secara tradisional, lembaga lain yang menyediakan keamanan adalah penegak hukum. Polisi dan lembaga penegak hukum sering dibatasi oleh undang-undang di mana mereka beroperasi dan tantangan pengembangan kasus yang mengarah pada penuntutan hukum. Namun dalam beberapa tahun terakhir ini, *convention on cyber crime* milik Dewan Eropa 2001 telah membuat penjahat *cyber* sulit untuk menghindari pengadilan. Sementara itu, penegakan hukum seperti FBI di AS bekerjasama dengan rekan internasional dan perushaan besar seperti Microsoft untuk mencegah penjahat. Pendekatan lain yang potensial bagi pemerintah adalah mendukung sektor swasta dalam menyediakan keamannya sendiri seperti membuat struktur

yang tepat untuk berbagi informasi antar perusahaan atau meningkatkan standar *cyber security*.

Dalam prakteknya, tingkat keterlibatan militer perlu memperhitungkan bahaya terhadap keamanan nasional. Setiap negara akan memiliki pertimbangan yang berbeda-beda. Namun hasilnya mungkin akan terlihat seperti ini:

- **Pencurian informasi** dari pemerintah dan pertahanan. Ada berbagai motivasi yang dimungkinkan dalam gangguan tersebut, termasuk motif komersial, tetapi mereka juga mewakili efektifitas militer di masa depan (terutama jika penyusup adalah musuh potensial atau bersedia untuk memberikan atau menjual informasi yg mereka curi)
- **Potensi serangan yang menghancurkan infrastruktur nasional** (termasuk keuangan, energy, transportasi, komunikasi, dan sector ekonomi lainnya yang vital bagi kehidupan bangsa) bisa dibilang merupakan ancaman dari pencuri rahasia keamanan nasional. Militer mungkin akan siap untuk mendukung respon terhadap serangan. Tapi ini adalah area di mana pendekatan yang terbaik yang dilakukan pemerintah adalah melalui sektor ekonomi.
- **Spionase komersial**, baik dari kekayaan intelektual atau informasi bisnis sensitif, daerah lain di mana pendekatan militer mungkin tidak sesuai. Namun, Pemerintah kemudian bisa memberikan sanksi atau jika dibawah tekanan, bisa mengizinkan respon swasta.
- **Ancaman *cybercrime*** atau *cybercrime threats*. Meskipun bukan ancaman langsung, namun cybercrime ini bisa berkembang menjadi ancaman langsung jika dibiarkan karena potensi untuk terroris atau negara lain untuk memanfaatkan jaringan kriminal. Hal ini umumnya tidak membutuhkan peran militer melainkan untuk penegakan hukum. (Wallace, 2013)

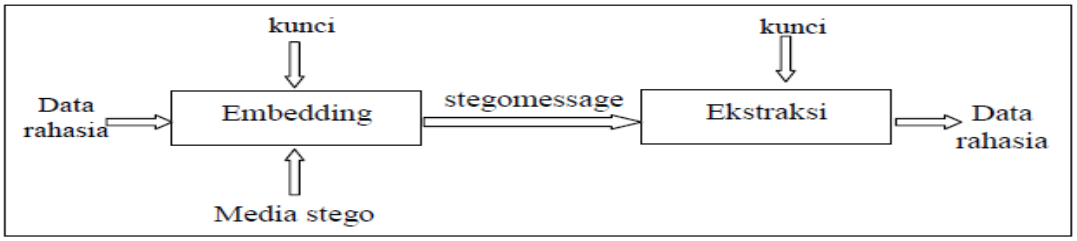
Di era globalisasi ini, dunia maya/cyber merupakan sebuah kebutuhan bagi kehidupan manusia dan menjadi penghubung komunikasi manusia satu dengan yang lain tanpa dibatasai jauhnya jarak. Kondisi ini bukannya tanpa efek negatif, keamanan cyber menjadi kebutuhan nyata dan sangat mendesak karena efek yang ditimbulkan cybercrime dapat merusak atau mengacaukan kehidupan masyarakat

bahkan negara dan dunia internasional. Pengaruh dari isu cyber security/cyber defense ini bagi situasi keamanan internasional adalah bisa menciptakan ketegangan antar negara-negara dan mengganggu stabilitas keamanan dan menimbulkan dampak sosial, ekonomi, dan lingkungan serta bisa mengganggu hubungan antar negara. Hal ini dikarenakan *cyber crime* merupakan kejahatan yang melintasi batas negara. Karena melintasi batas negara dan bisa melibatkan banyak negara, maka penting adanya kerja sama perjanjian multilateral guna mengatasi hal tersebut, baik di tingkat regional maupun internasional dan penggunaan kekuatan militer sebaiknya menjadi opsi terakhir. Hal tersebut karena negara tidak bisa begitu saja menggunakan kekuatan militer untuk melakukan serangan atau perang. Banyak hal yang harus dipertimbangkan seperti misalnya biaya. Negara sebaiknya segera membangun *cyber defense* yang berbasis teknologi digital. Selain itu, negara juga bisa membentuk sebuah unit khusus untuk menangani cybercrime seperti *United States Cyber Command* (USCYBERCOM) di Amerika, *Blue Army* di China, *Australian Computer Emergency Response Team* (AusCERT) di Australia, dan lain sebagainya.

3.3 Steganografi

Steganografi berasal dari bahasa Yunani yaitu, *Steganós* yang berarti menyembunyikan dan *Graptos* yang artinya tulisan, sehingga steganografi diartikan sebagai "tulisan tersembunyi (*covered writing*)". Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia (*hiding message*) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia (Munir, 2004).

Proses penyembunyian data kedalam media disebut penyisipan (*embedding*), sedangkan proses sebaliknya disebut ekstraksi.



Gambar 3.5 Proses penyisipan dan ekstraksi dalam steganografi

3.3.1 Sejarah Steganografi

Steganografi sudah dikenal sejak 440 SM. Herodotus (sejarawan Yunani) menyebutkan dua contoh steganografi di dalam kisah "*Histories of Herodotus".* Kisah pertama, pada saat itu, penguasa Yunani kuno, Histiaeus sedang ditawan oleh Raja Darius di Susa. Histiaeus ingin mengirim pesan rahasia kepada menantunya, Aristagoras, di Miletus. Oleh karena itu, Histiaeus mencukur habis rambut budaknya dan menuliskan (*tato*) pesan rahasia yang ingin dikirim di kepala budak tersebut. Setelah rambut budak tumbuh cukup lebat, barulah budak tersebut dikirim ke Miletus untuk menyampaikan pesan. Kisah kedua, Demeratus mengirimkan peringatan akan serangan Yunani yang selanjutnya dengan menuliskan pesan tersebut di atas sebuah papan kayu dan melapisinya dengan lilin. Lembaran pesan akan ditutup dengan lilin, untuk melihat isi pesan, pihak penerima harus memanaskan lilin terlebih dahulu (Johnson dan Jojadia, 2002).

Teknik steganografi sudah ada sejak 4000 tahun yang lalu di kota Menet Khufu, Mesir. Awalnya berupa penggunaan *hieroglyphic* yakni menulis menggunakan karakter-karakter dalam bentuk gambar. Ahli tulis menggunakan tulisan Mesir kuno ini untuk menceritakan kehidupan majikannya. Tulisan Mesir kuno tersebut menjadi ide untuk membuat pesan rahasia saat ini. Oleh karena itulah, tulisan Mesir kuno yang menggunakan gambar dianggap sebagai steganografi pertama di dunia (Ariyus, 2009).

Teknik steganografi yang lain adalah tinta yang tidak tampak (*invisible ink*) yaitu dengan menggunakan air sari buah jeruk, urin atau susu sebagai tinta untuk menulis pesan. Cara membacanya adalah dengan dipanaskan di atas api. Tinta yang sebelumnya tidak terlihat, ketika tekena panas akan menjadi gelap sehingga dapa dibaca. Teknik ini digunakan oleh bangsa Romawi yang juga digunakan pada Perang Dunia II oleh tentara Jerman (Kahn, 1996).

Bangsa Cina menggunakan cara yang berbeda pula, yaitu manusia sebagai media pembawa pesan. Orang itu akan dicukur rambutnya sampai botak dan pesan akan dituliskan di kepalanya. Kemudian pesan akan dikirimkan ketika rambutnya sudah tumbuh (Fabien, 1999).

3.3.2 Teknik Steganografi

Menurut Ariyus (2009), ada tujuh teknik dasar yang digunakan dalam steganografi, yaitu : 10

a. *Injection*, merupakan suatu teknik menanamkan pesan rahasia secara langsung ke suatu media. Salah satu masalah dari teknik ini adalah ukuran media yang diinjeksi menjadi lebih besar dari ukuran normalnya sehingga mudah dideteksi. Teknik ini sering juga disebut *embedding*.
b. Substitusi, data normal digantikan dengan data rahasia. Biasanya, hasil teknik ini tidak terlalu mengubah ukuran data asli, tetapi tergantung pada file media dan data yang akan disembunyikan. Teknik substitusi bisa menurunkan kualitas media yang ditumpangi.
c. *Trans*form *Domain*, teknik ini sangat efektif. Pada dasarnya, transformasi domain menyembunyikan data pada transform space.
d. *Spread Spectrum*, sebuah teknik pengtransmisian menggunakan *pseudonoise code*, yang independen terhadap data informasi sebagai modulator bentuk gelombang untuk menyebarkan energi sinyal dalam sebuah jalur komunikasi (*bandwidth*) yang lebih besar daripada sinyal jalur komunikasi informasi. Oleh penerima, sinyal dikumpulkan kembali menggunakan replika *pseudo-noise code* tersinkronisasi.
e. *Statistical Method*, teknik ini disebut juga skema *steganographic* 1 bit. Skema tersebut menanamkan satu bit informasi pada media tumpangan dan mengubah statistik walaupun hanya 1 bit. Perubahan statistik ditunjukkan dengan indikasi 1 dan jika tidak ada perubahan, terlihat indikasi 0. Sistem ini bekerja berdasarkan kemampuan penerima dalam membedakan antara informasi yang dimodifikasi dan yang belum.
f. *Distortion*, metode ini menciptakan perubahan atas benda yang ditumpangi oleh data rahasia.
g. *Cover Generation*, metode ini lebih unik daripada metode lainnya karena *cover* object dipilih untuk menyembunyikan pesan. Contoh dari metode ini adalah *Spam Mimic* (Ariyus, 2009).

3.3.3 Tujuan Steganografi

Tujuan dari steganografi adalah menyembunyikan keberadaan pesan dan dapat dianggap sebagai pelengkap dari kriptografi yang bertujuan untuk menyembunyikan isi pesan. Steganografi sebagai suatu teknik penyembunyian informasi pada data digital lainnya dapat dimanfaatkan untuk berbagai tujuan seperti :

a. *Tamper-proofing* dimana steganografi digunakan sebagai alat untuk mengidentifikasikan atau alat indikator yang menunjukkan data *host* telah mengalami perubahan dari aslinya.
b. *Feature location* dimana steganografi digunakan sebagai alat untuk mengidentifikasikan isi dari data digital pada lokasi-lokasi tertentu, seperti contohnya penamaan objek tertentu dari beberapa objek yang lain pada suatu citra digital.
c. *Annotation/caption* dimana steganografi hanya digunakan sebagai keterangan tentang data digital itu sendiri.
d. *Copyright-Labeling* dimana steganografi dapat digunakan sebagai metoda untuk penyembunyian label hak cipta pada data digital sebagai bukti otentik kepemilikan karya digital tersebut.

3.3.4 Media Steganografi

Steganografi menggunakan sebuah berkas yang disebut dengan *cover*, tujuannya sebagai kamuflase dari pesan yang sebenarnya. Steganografi membutuhkan dua properti: wadah penampung (*cover*) dan yang kedua adalah data atau pesan rahasiayang disembunyikan (*hiddentext*). Berkas hasil dari proses steganografi sering disebut sebagai berkas stego (*stegofile*) atau stego objek. Steganografi digital menggunakan media digital sebagai wadah penampung (Christian, 1998).

3.4 Kriptografi

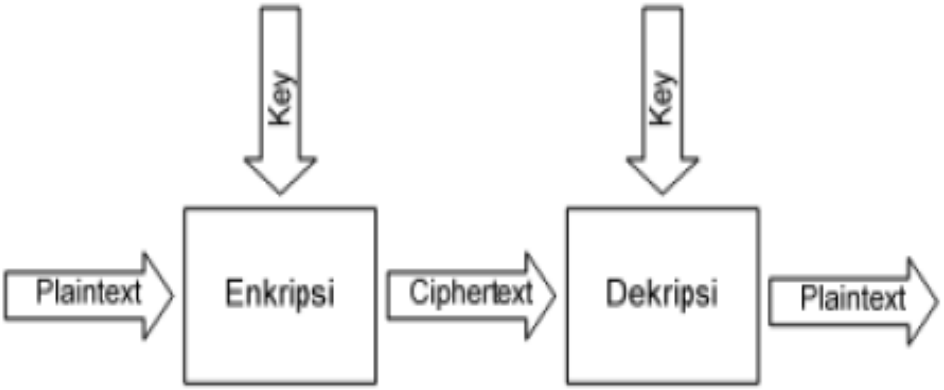
Kriptografi mempunyai peranan penting dalam dunia komputer. Hal ini disebabkan karena banyaknya informasi bersifat rahasia yang disimpan dan dikirmkan melalui media-media komputer. Informasi- informasi ini biasanya berisikan dokumen-dokumen penting dan data keuangan dari suatu instansi yang tidak ingin dibaca oleh pihak lain yang tidak berhak atas informasi tersebut. Oleh sebab itu ilmu kriptografi setiap saat terus dikembangkan oleh orang untuk dapat menjaga keamanan dan kerahasiaan informasi- informasi tersebut.

3.4.1 Definisi Kriptografi

Kriptografi berasal dari dua kata Yunani, yaitu *Crypto* yang berarti rahasia dan *Grapho* yang berarti menulis. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data (Menezes dkk., 1996). Secara umum kriptografi dapat diartikan sebagai ilmu dan seni penyandian yang bertujuan untuk menjaga keamanan dan kerahasiaan suatu pesan. Kriptografi pada dasarnya sudah dikenal sejak lama. Menurut catatan sejarah, kriptografi sudah digunakan oleh bangsa Mesir sejak 4000 tahun yang lalu oleh raja-raja Mesir pada saat perang untuk mengirimkan pesan rahasia kepada panglima perangnya melalui kurir-kurinya.

Orang yang melakukan penyandian ini disebut kriptografer, sedangkan orang yang mendalami ilmu dan seni dalam membuka atau memecahkan suatu algoritma kriptografi tanpa harus mengetahui kuncinya disebut kriptanalis. Kriptologi (*cryptology*) adalah ilmu yang mencakup kriptografi dan kriptoanalisis.

Cryptographic system atau *cryptosystem* adalah suatu fasilitas untuk mengkonversikan plainteks ke chiperteks dan sebaliknya. Kriptografi pada dasarnya terdiri dari dua proses, yaitu proses enkripsi dan proses dekripsi. Proses enkripsi adalah proses penyandian pesan terbuka menjadi pesan rahasia (chiperteks). Chiperteks inilah yang nantinya akan dikirimkan melalui saluran komunikasi terbuka. Pada saat chiperteks diterima oleh penerima pesan, maka pesan rahasia tersebut diubah lagi menjadi pesan terbuka melalui proses dekripsi sehingga pesan tadi dapat dibaca kembali oleh penerima pesan.



Gambar 3.6 Proses Enkripsi dan Dekripsi

Pesan terbuka (plainteks) diberi lambang M, yang merupakan singkatan dari *"Message"*. Plainteks ini dapat berupa teks, foto, atau video yang berbentuk data biner. Plainteks inilah yang nantinya akan dienkripsi menjadi pesan rahasia (chiperteks) yang dilambangkan dengan C. Secara matematis, operasi enkripsi dan dekripsi dapat diterangkan sebagai berikut:

EK (M) = C (Proses Enkripsi) (2.1)

DK (C) = M (Proses Dekripsi) (2.2)

Pada saat proses enkripsi kita menyandikan pesan M dengan suatu kunci K lalu dihasilkan pesan C. Sedangkan pada proses dekripsi, pesan C tersebut diuraikan dengan menggunakan kunci K sehingga dihasilkan pesan M yang sama seperti pesan sebelumnya.

3.4.2 Sejarah Kriptografi

Kriptografi mempunyai sejarah yang panjang dan menakjubkan. Informasi yang lengkap mengenai sejarah kriptografi dapat ditemukan di dalam buku David Kahn yang berjudul *The Codebreakers*. Buku ini menulis secara rinci sejarah kriptografi, mulai dari penggunaan kriptografi oleh Bangsa Mesir 4000 tahun yang lalu (berupa *hieroglyph* pada piramid) hingga penggunaan kriptografi abad ke-20 (Ariyus, 2009).

Sebagian besar sejarah kriptografi merupakan kriptografi klasik, yaitu metode kriptografi yang menggunakan kertas dan pensil atau menggunakan

alat bantu mekanik yang sederhana. Kriptografi klasik secara umum dikelompokkan menjadi dua kategori, yaitu algoritma transposisi (*transposition cipher)* dan algoritma substitusi *(substitution cipher*). Algoritma transposisi adalah algoritma yang mengubah susunan-susunan huruf di dalam pesan, sedangkan algoritma substitusi yaitu mengganti setiap huruf atau kelompok huruf dengan sebuah huruf atau kelompok huruf yang lain.

Penggunaan *transposition cipher* yaitu oleh tentara Sparta di Yunani pada permulaan tahun 500 SM. Mereka menggunakan apa yang dinamakan *scytale* (Gambar 3.7 (a)). *Scytale* terdiri dari sebuah kertas panjang dari daun *papyrus* yang dililitkan pada sebuah silinder dari diameter tertentu (diameter dari silinder merupakan kunci dari penyandian tersebut). Pesan ditulis baris per baris dan secara horisontal (Gambar 3.7. (b)). Apabila pita dilepas, maka setiap huruf akan tersusun secara acak membentuk pesan rahasia (pesan yang tidak dapat dibaca). Agar pesan tersebut dapat dibaca, maka pesan tersebut harus kembali dililitkan ke silinder yang diameternya sama dengan diameter silinder pengirim.

(a) (b)

Gambar 3.7 (a) Sebuah Scytale; (b) Pesan ditulis secara baris per baris

3.4.3 Tujuan Kriptografi

Ada empat tujuan mendasar dari kriptografi yang juga merupakan aspek keamanan informasi (Munir, 2006), yaitu:

a. Kerahasiaan, adalah aspek yang berhubungan dengan penjagaan isi informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka informasi yang telah dienkripsi.
b. Integritas data, adalah aspek yang berhubungan dengan penjagaan dari perubahan data secara tidak sah. 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.
c. Autentikasi, adalah aspek yang berhubungan dengan identifikasi atau pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.
d. Non-repudiation (menolak penyangkalan), adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman suatu informasi oleh yang mengirimkan, atau harus dapat membuktikan bahwa suatu pesan berasal dari seseorang, apabila ia menyangkal mengirim informasi tersebut.

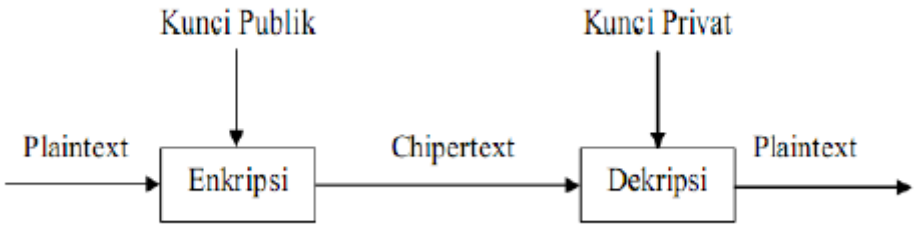
3.4.4 Jenis Kriptografi

Algoritma kriptografi adalah suatu fungsi matematis yang digunakan untuk melakukan enkripsi dan dekripsi. Ada dua macam algoritma kriptografi, yaitu algoritma simetri (*symmetric algorithms*) dan algoritma asimetri (*asymmetric algorithms*).

3.4.4.1 Kriptografi Kunci Asimetri (Kriptografi Kunci Publik)

Kriptografi kunci asimetri yang sering disebut juga kriptografi kunci publik adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Algoritma asimetri ini disebut kunci publik karena kunci untuk enkripsi dapat dibuat publik yang berarti semua orang boleh

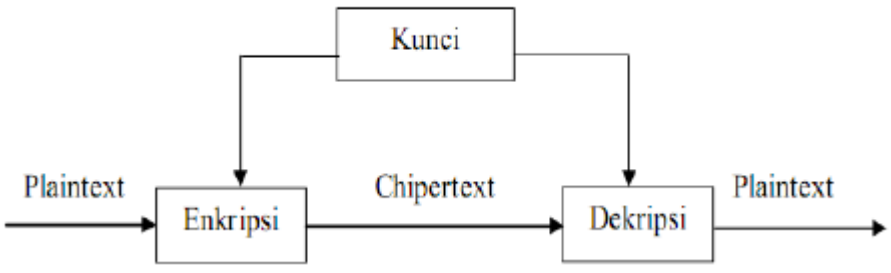
mengetahuinya. Sembarang orang dapat menggunakan kunci enkripsi tersebut untuk mengenkrip pesan namun hanya orang tertentu yaitu calon penerima pesan dan sekaligus pemilik kunci dekripsi yang merupakan pasangan kunci publik, yang dapat melakukan dekripsi terhadap pesan tersebut. Dalam sistem ini, kunci enkripsi disebut kunci publik, sementara kunci dekripsi sering disebut kunci privat.



Gambar 38 Enkripsi kunci asimetri

3.4.4.2 Kriptografi Kunci Simetri

Kriptografi simetri disebut juga sebagai kriptografi konvensional. Kriptografi simetri adalah algoritma kriptografi yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya. Kriptografi simetri sering disebut sebagai algoritma kunci rahasia, algortima kunci tunggal, atau algoritma satu kunci dan mengharuskan pengirim dan penerima menyetujui suatu kunci sebelum mereka dapat berkomunikasi dengan aman. Gambar 3.8 mengilustrasikan kinerja dari proses enkripsi kunci simetri.



Gambar 3.9 Kriptografi Kunci Simetri

Kelebihan Kriptografi Simetri adalah sebagai berikut.

1. Proses enkripsi atau detesis kriptografi simetri membutuhkan waktu yang singkat.
2. Ukuran kunci simetri relatif lebih pendek.
3. Otentikasi pengiriman pesan langsung diketahui dari cipherteks yang diterima, karena kunci hanya diketahui oleh penerima dan pengirim saja.

Kekurangan Kriptografi Simetri adalah sebagai berikut.

1. Kunci simetri harus dikirim melalui saluran komunikasi yang aman, dan kedua entitas yang berkomunikasi harus menjaga kerahasiaan kunci.
2. Kunci harus sering diubah, setiap kali melakasanakan komunikasi.

Masalah utama yang dihadapi kriptografi simetri adalah membuat pengirim dan penerima menyetujui kunci rahasia tanpa ada orang lain yang mengetahuinya.

Salah satu cotoh algoritma kunci simetri adalah algoritma DES. DES sangat digunakan untuk melindungi data dalam dunia elektronika khususnya di bidang perbankan, finansial, dan e-*commerce*.

3.5 Algoritma *Data Encryption Standard* (DES)

Algoritma DES merupakan salah satu algoritma kriptografi simetri. Algoritma DES merupakan algoritma standar untuk kriptografi simetri. Pada sub bab ini penulis akan membahas dasar-dasar dan prinsip kerja dari algoritma DES itu sendiri.

Pertengahan tahun 1973, Pemerintah Amerika Serikat (AS) melalui *National Bureau of Standards* (NBS) mengumumkan kebutuhan akan suatu algoritma sandi yang akan digunakan sebagai standar untuk melindungi kerahasiaan dan keutuhan data-data penting baik yang sedang ditransmisikan maupun yang disimpan.

Algoritma DES merupakan salah satu proposal terbaik tahun 1977. Algoritma DES dikembangkan di IBM di bawah kepemimpinan W. L. Tuchman pada tahun 1972. Algoritma ini didasarkan pada algoritma *Lucifer* yang dibuat oleh *Horst Feistel*. Algoritma ini telah disetujui oleh *National Bureau of Standard* (NBS) setelah penilaian kekuatannya oleh *National Security Agency* (NSA) Amerika Serikat.

DES merupakan salah satu *chiper block* penyandian/kriptografi data yang populer dan telah dijadikan standard enkripsi kunci simetri sejak tahun 1976 dengan ukuran blok 64 bit dan ukuran kuncinya 56 bit. Algoritma DES dibuat di IBM, dan merupakan modifikasi dari algoritma terdahulu yang bernama *Lucifer*. *Lucifer* merupakan algoritma *cipher block* yang beroperasi pada blok masukan 64 bit dan kuncinya berukuran 128 bit (Munir, 2006).

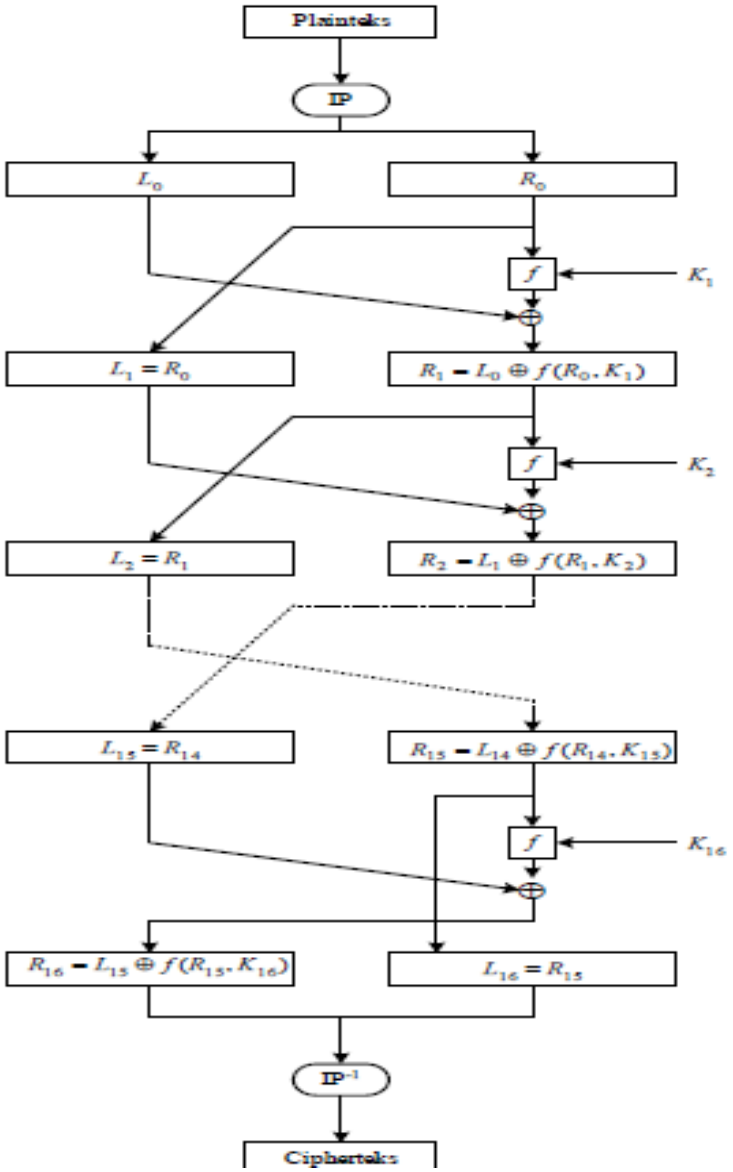
3.5.1 Prinsip Kerja Algoritma DES

Sandi DES adalah hasil pengembangan dari Sandi *Feistel*, dengan demikian wajar bila terdapat Sandi *Feistel* didalamnya. Adapun prinsip kerja dari sandi DES adalah sebagai berikut (Munir, 2006).

1. Persiapan kunci, memecah kunci ke dalam 16 sub kunci.
2. Melakukan prosedur *Feistel* 16 iterasi, dengan menggunakan sub kunci yang telah disediakan, dan menggunakan fungsi yang telah ditentukan.
   Secara detail, yang dikerjakan oleh sandi *Feistel* sebagai berikut.
   a. Plainteks dikonversikan terlebih dahulu dalam biner, kemudian dibagi dan diproses per blok, dimana setiap blok terdiri dari 64 bit.
   b. Untuk setiap blok kemudian dilakukan koversi posisi terhadap Tabel IP (*Initial Permutation*), hasilnya kemudian dibagi menjadi 2 bagian, yaitu 32 bit pada bagian kiri disebut Lo, dan 32 bit di kanan disebut Ro.
   c. Kedua bagian ini kemudian dilakukan iterasi fungsi *f* sebanyak 16 kali (LiRi, $1<i<16$). Secara matematis, satu putaran DES dinyatatakan sebagai berikut: $Li = Ri - 1$, $Ri = Li - 1 \oplus f(Ri - 1, Ki)$ (2.3)
      Ki adalah kunci 48 bit yang terdiri dari 16 macam yang berbeda untuk setiap iterasi.
3. Hasil akhirnya kemudian dibalik, dan dioperasikan dengan invers dari IP (IP-1(R16,L16).

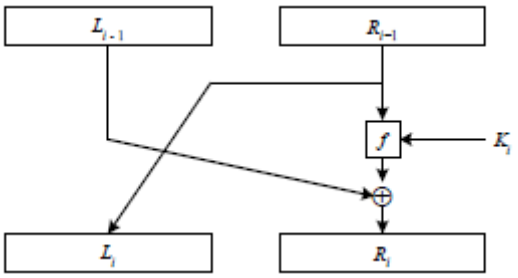
3.5.2 Skema Algoritma DES

Skema algoritma DES ditunjukkan pada Gambar



Gambar 3.10 Algoritma enkripsi dengan DES (Schneier, 1996)

Satu putaran DES merupakan model jaringan *Feistel* (Gambar 3.11).



Gambar 3.11 mengilustrasikan bahwa jika (*L*16, *R*16) merupakan keluaran dari putaran ke-16, maka (*R*16, *L*16) merupakan pra-chiperteks (*pre-ciphertext*) dari enkripsi ini. Chiperteks yang sebenarnya diperoleh dengan melakukan permutasi awal balikan, IP-1 terhadap blok pra-chiperteks.

3.5.3 Pembangkitan Kunci Internal

Pembangkitan kunci internal terjadi selama 16 putaran. Karena terdapat 16 putaran, maka dibutuhkan kunci internal sebanyak 16 buah, yaitu *K*1, *K*2, …, *K*16. Kunci-kunci internal tersebut dapat dibangkitkan sebelum proses enkripsi atau bersamaan dengan proses enkripsi.

Kunci internal dibangkitkan dari kunci eksternal yang diberikan oleh pengguna. Kunci eksternal panjangnya 64 bit atau 8 karakter. Misalkan kunci eksternal yang tersusun dari 64 bit adalah *K*. Kunci eksternal ini menjadi masukan untuk permutasi dengan menggunakan matriks permutasi kompresi PC-1 yang ditunjukkan pada Tabel 1

Tabel 0.3 Matriks PC-1

57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36
63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

Pada permutasi ini, tiap bit kedelapan (*parity bit*) dari delapan *byte* kunci diabaikan. Hasil permutasinya adalah sepanjang 56 bit, sehingga dapat dikatakan panjang kunci DES adalah 56 bit. Selanjutnya, 56 bit ini dibagi menjadi 2 bagian, kiri (C) dan kanan (D), yang masing-masing panjangnya 28 bit disimpan di dalam *C*0 dan *D*0:

*C*0: berisi bit-bit dari *K* pada posisi:

57, 49, 41, 33, 25, 17, 9, 1, 58, 50, 42, 34, 26, 18

10, 2, 59, 51, 43, 35, 27, 19, 11, 3, 60, 52, 44, 36

*D*0: berisi bit-bit dari *K* pada posisi:

63, 55, 47, 39, 31, 23, 15, 7, 62, 54, 46, 38, 30, 22

14, 6, 61, 53, 45, 37, 29, 21, 13, 5, 28, 20, 12, 4

Selanjutnya, kedua bagian digeser ke kiri (*left shift*) sepanjang satu atau dua bit bergantung pada tiap putaran. Operasi pergeseran bersifat *wrapping* atau *round-shift*, aturan pergeseran setiap putaran ditunjukkan pada Tabel 2.

Putaran, *i*	**Jumlah pergeseran bit**
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Misalkan (*Ci*, *Di*) menyatakan penggabungan *Ci* dan *Di*. (*Ci*+1, *Di*+1) diperoleh dengan menggeser *Ci* dan *Di* satu atau dua bit. Setelah pergeseran bit, (*Ci*, *Di*) mengalami permutasi kompresi dengan menggunakan matriks PC-2 yang ditunjukkan pada Tabel 3.

Tabel 0.5 Matriks PC-2

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

Dengan permutasi ini, kunci internal Ki diturunkan dari (Ci, Di) yang dalam hal ini Ki merupakan penggabungan bit-bit Ci pada posisi:

14, 17, 11, 24, 1, 5, 3, 28, 15, 6, 21, 10

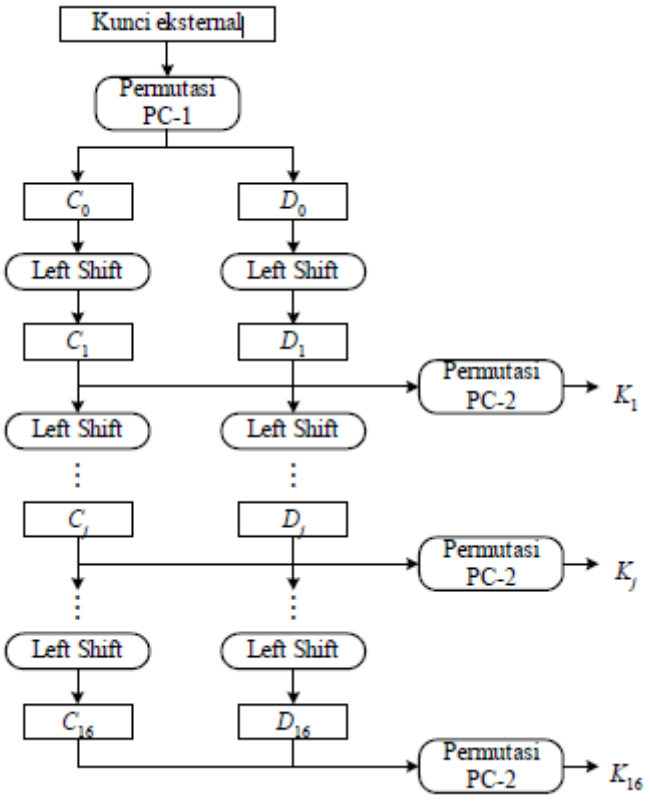
23, 19, 12, 4, 26, 8, 16, 7, 27, 20, 13, 2

dengan bit-bit *Di* pada posisi:

41, 52, 31, 37, 47, 55, 30, 40, 51, 45, 33, 48

44, 49, 39,56, 34, 53, 46, 42, 50, 36, 29, 32

Jadi, setiap kunci internal *Ki* mempunyai panjang 48 bit.



Gambar 3.12 Proses pembangkitan kunci-kunci internal DES (Schneier, 1996)

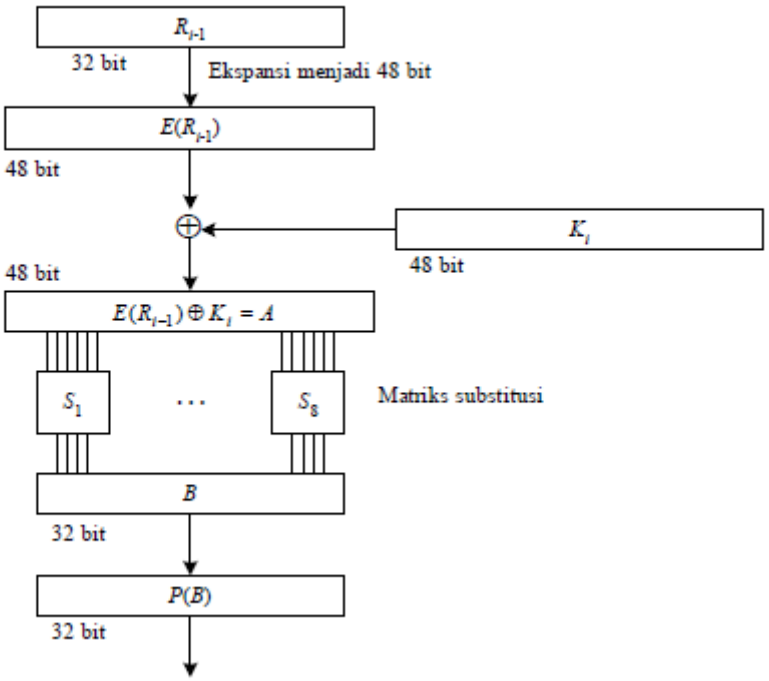
3.5.4 Enkripsi

Proses enkripsi terhadap blok plainteks dilakukan setelah permutasi awal Setiap blok plainteks mengalami 16 kali putaran enkripsi (Gambar 3.10). Setiap putaran enkripsi merupakan jaringan *Feistel* yang secara matematis dinyatakan sebagai berikut:

$Li = Ri - 1$

$Ri = Li - 1 \oplus f(Ri - 1, Ki)$ (2.4)

Diagram komputasi fungsi *f* diperlihatkan pada Gambar 3.13.



Gambar 3.12 Diagram komputasi fungsi *f* (Schneier, 1996)

Notasi *E* adalah fungsi ekspansi yang memperluas blok *Ri* – 1 yang panjangnya 32-bit menjadi blok 48 bit. Fungsi ekspansi direalisasikan dengan matriks permutasi ekspansi yang ditunjukkan pada Tabel 4.

Tabel 0.6 Matriks Permutasi Ekspansi

32	1	2	3	4	5	4	5	6	7	8	9
8	9	10	11	12	13	12	13	14	15	16	17
16	17	18	19	20	21	20	21	22	23	24	25
24	25	26	27	28	29	28	29	30	31	32	1

Selanjutnya, hasil ekpansi, yaitu *E*(*Ri* – 1), yang panjangnya 48 bit di-XOR-kan dengan *Ki* yang panjangnya 48 bit menghasilkan vektor *A* yang panjangnya 48-bit:

E(*Ri* – 1) □ *Ki* = *A* (2.5)

Vektor *A* dikelompokkan menjadi 8 kelompok, masing-masing 6 bit, dan menjadi masukan untuk proses substitusi.

3.5.5 Proses Subtitusi Menggunakan Kotak S-*box*

Proses substitusi dilakukan dengan menggunakan delapan buah kotak-S (*S-box*) yaitu *S*1 sampai *S*8. Setiap kotak-S menerima masukan 6 bit dan menghasilkan keluaran 4 bit.

Kelompok 6-bit pertama menggunakan S1, kelompok 6-bit kedua menggunakan S2, dan seterusnya.

Kotak-*S* di dalam algoritma DES adalah 6 □ 4 *S-box* yang berarti memetakan 6 bit masukan menjadi 4 bit keluaran. Setiap S-*box* terdiri dari suatu tabel ukuran 4 □ 6 (4 baris dan 16 kolom). Setiap baris diberi nomor 0 sampai 3 dan setiap kolom diberi nomor 0 sampai 15. Masukan untuk proses substitusi adalah 6 bit (*b*1*b*2*b*3*b*4*b*5*b*6). Nomor baris dari tabel ditunjukkan oleh *string* bit *b*1*b*6 (menyatakan nilai 0 sampai 3 desimal). Nomor kolom ditunjukkan oleh *string* bit *b*2*b*3*b*4*b*5 (menyatakan nilai 0 sampai 15 desimal).

Contoh:

Misalkan masukan adalah 110100 dan salah satu kotak-*S* yang ada di dalam algoritma DES ditunjukkan pada Tabel 2.7 sebagai berikut

Tabel 5 Contoh proses subtitusi kotak pada kotak S-*box*

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

Nomor baris tabel = 10 (artinya baris 2 desimal). Nomor baris tersebut diperoleh dari yaitu *b1*: 1 dan *b2:* 0.

Nomor kolom tabel = 1010 (artinya kolom 10 desimal). Nomor kolom tersebut diperoleh dari *b2:* 1, *b3*: 0, *b4*: 1 dan *b5*: 0.

Jadi, substitusi untuk 110100 adalah *entry* pada baris 2 dan kolom 10, yaitu 4 desimal atau 0100 dalam bentuk biner.

Kedelapan kotak-S tersebut ditunjukkan pada Lampiran 8.

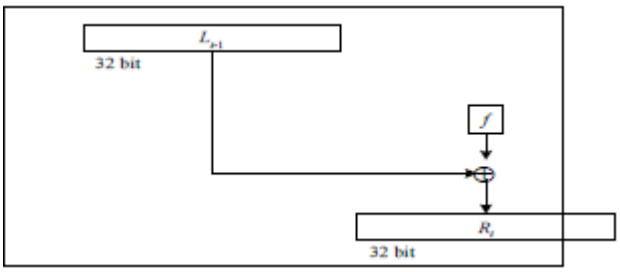
Keluaran proses substitusi adalah vektor *B* yang panjangnya 48 bit. Vektor *B* menjadi masukan untuk proses permutasi. Tujuan permutasi adalah untuk

mengacak hasil proses substitusi kotak-S. Permutasi dilakukan dengan menggunakan matriks permutasi *P* (*P-box*) yang ditunjukkan pada Tabel 6.

Tabel 6 Matriks permutasi P

16	7	20	21	29	12	28	17	1	15	23	26	5	8	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

a. Bit-bit *P*(*B*) merupakan keluaran dari fungsi *f*
b. Akhirnya, bit-bit *P*(*B*) di-XOR-kan dengan *Li* – 1 untuk mendapatkan *Ri* (lihat Gambar 4): *Ri* = *Li* – 1 □ *P*(*B*) (4)
c. Jadi, keluaran dari putaran ke-*i* adalah (*Li*, *Ri*) = (*Ri* – 1, *Li* – 1 □ *P*(*B*)) (5)



Gambar 3.13 Skema perolehan *Ri*

3.5.6 Permutasi Akhir

Permutasi terakhir dilakukan setelah 16 kali putaran terhadap gabungan blok kiri dan blok kanan. Proses permutasi menggunakan matriks permutasi awal balikan (*inverse initial permutation* atau IP-1). Matriks IP-1 ditunjukkan pada Tabel 2.8.

Tabel 7 Matriks IP-1

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

3.5.7 Dekripsi

Proses dekripsi terhadap chiperteks merupakan kebalikan dari proses enkripsi. DES menggunakan algoritma yang sama untuk proses enkripsi dan dekripsi. Jika pada proses enkripsi urutan kunci internal yang digunakan adalah *K*1, *K*2, …, *K*16, maka pada proses dekripsi urutan kunci yang digunakan sebaliknya, yaitu *K*16, *K*15, …, *K*1.

Masing-masing putaran 16, 15, …, 1, menghasilkan keluaran pada setiap putaran *deciphering* sebagai berikut:

$Li = Ri - 1$

$Ri = Li - 1 \square f(Ri - 1, Ki)$ (6)

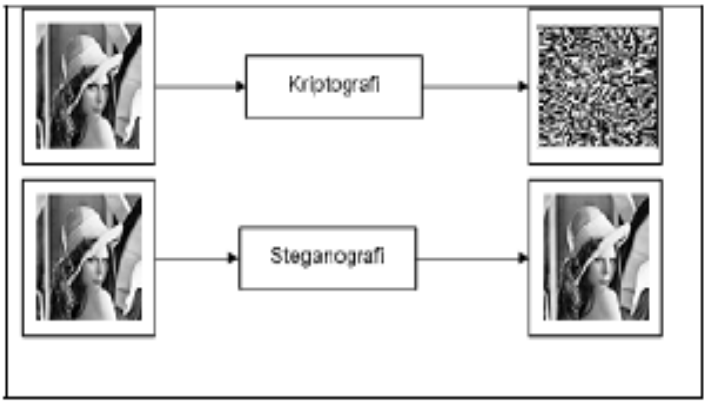
yang dalam hal ini, (*R*16, *L*16) adalah blok masukan awal untuk deciphering. Blok (*R*16, *L*16) diperoleh dengan mempermutasikan chiperteks dengan matriks permutasi IP-1. Pra-keluaran dari *deciphering* adalah adalah (*L*0, *R*0). Dengan permutasi awal IP akan didapatkan kembali blok plainteks semula. Tinjau kembali proses pembangkitan kunci internal pada Gambar 7.

Selama *deciphering*, *K*16 dihasilkan dari (*C*16, *D*16) dengan permutasi PC-2. Tentu saja (*C*16, *D*16) tidak dapat diperoleh langsung pada permulaan *deciphering*. Tetapi karena (*C*16, *D*16) = (*C*0, *D*0), maka *K*16 dapat dihasilkan dari (*C*0, *D*0) tanpa perlu lagi melakukan pergeseran bit. Catatlah bahwa (*C*0, *D*0) yang merupakan bit-bit dari kunci eksternal *K* yang diberikan pengguna pada waktu dekripsi. Selanjutnya, *K*15 dihasilkan dari (*C*15, *D*15) yang diperoleh dengan cara menggeser *C*16 (yang sama dengan *C*0) dan *D*16 (yang sama dengan *C*0) satu bit ke kanan. Sisanya, *K*14 sampai *K*1 dihasilkan dari (*C*14, *D*14) sampai (*C*1, *D*1). Catatlah bahwa (*Ci* – 1, *Di* – 1) diperoleh dengan menggeser *Ci* dan *Di* dengan cara yang sama yang ditunjukkan pada Tabel 2.4, tetapi pergeseran kiri (*left shift*) diganti menjadi pergeseran kanan (*right shift*).

3.5.8 Kelebihan dan Kekurangan Steganografi dan Kriptografi

Steganografi berbeda dengan kriptografi, di mana pihak ketiga dapat mendeteksi adanya data (*chipertext*), karena hasil dari kriptografi berupa data yang berbeda dari bentuk aslinya dan biasanya datanya seolah-olah berantakan,

tetapi dapat dikembalikan ke bentuk semula. Ilustrasi mengenai perbedaan kriptografi dan steganografi ditunjukkan pada Gambar 3.13



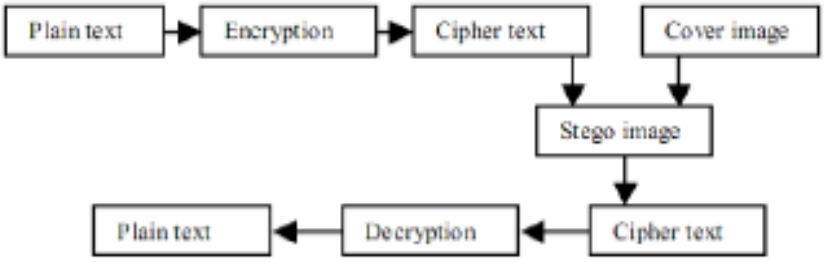
Gambar 3.13 Beda steganografi dan kriptografi (Munir, 2004)

Penyisipan pesan pada citra dapat mempengaruhi kualitas citra tersebut, walau tidak tampak secara kasat mata. Namun melalui pengolahan citra, dapat dideteksi pola-polanya sehingga dapat dicurigai dan memungkinkan untuk dilakukan penyerangan. Penggunaan kriptografi dengan mengubah menjadi bentuk lain memang sangat mudah dicurigai, tetapi pola perubahan pada kriptografi susah diketahui.

Kombinasi steganografi dan kriptografi dapat dilakukan untuk meningkatkan keamanan data (Krenn, 2004). Seandainya citra steganografi dapat dideteksi dan dibongkar, tetapi isinya bukan data asli melainkan data enkripsi dan untuk menhetahui isi pesan masih dipelukan kunci yang benar.

3.5.9 Kombinasi Steganografi dan Kriptografi

Kombinasi steganografi dan kriptografi pada umunya dilakukan dengan proses kriptografi terlebih dahulu kemudian steganografi, yaitu mengenkripsi pesan terlebih dahulu kemudian menyisipkan chiperteks hasil enkripsi ke media *cover* (Raphael dan Sundaram, 2011). Konsep penggabungan kriptografi dan steganografi ditunjukkan pada Gambar 3.14.



Gambar 3.14 Kombinasi Steganografi dan Kriptografi (Raphael dan Sundaram, 2011)

BAB IV
METODE PENELITIAN

4.1 Bahan dan Alat Penelitian

Bahan dan alat penelitian pada penelitian ini diuraikan sebagai berikut.

4.1.1 Bahan Penelitian

Bahan penelitian yang digunakan pada proses penelitian ini bersumber pada jurnal internasional, artikel ilmiah, dan buku-buku pendukung yang terkait dengan steganografi, dan kriptografi algoritma DES.

4.1.2 Alat Penelitian

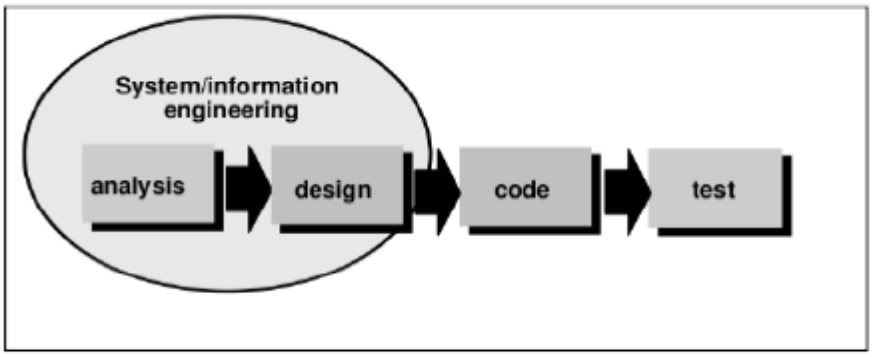
Alat yang digunakan dalam penelitian ini terbagi 2 yaitu, perangkat keras (*hardware*) dan perangkat lunak (*software*).

1. Perangkat Keras, Perangkat keras yang digunakan dalam penelitian ini adalah *notebook* dengan spesifikasi:
   a. *Processor* Intel® CoreTM i3 2.40GHz
   b. Memori RAM 2 GB

2. Perangkat Lunak, yaitu
   a. Sistem operasi Windows
   b. *Software* MATLAB R2009a.

4.2. Jalan Penelitian

Metode yang digunakan dalam penelitian ini yaitu penggabungan steganografi dengan krtipografi. Algoritma kriptografi yang digunakan adalah DES. Terdapat 2 proses didalam steganografi, yaitu *embedding* dan ekstraksi. Pada penelitian ini akan dibangun suatu perangkat lunak stego-kripto dengan model *waterfall* yaitu suatu metode pengembangan *software* yang bersifat sekuensial. Metode *waterfall* ditunjukkan pada Gambar 4.1.



Gambar 4.1 Metode *Waterfall* (Pressman, 2001)

Metode *waterfall* membagi penelitian menjadi 4 tahap yang saling terkait dan mempengaruhi. Empat tahap tersebut yaitu analisa kebutuhan (*analysis*), desain (*design*), pengkodean (*code*) dan pengujian (*test*) (Pressman, 2001).

4.2.1 Analisa Kebutuhan (*analysis*)

Pada tahap analisa kebutuhan dilakukan pengumpulan informasi mengenai proses yang akan digunakan untuk membangun model kombinasi kriptografi dan steganografi yang meliputi:

a. Pencocokan bit

Masukan pada tahap ini adalah pesan dan citra. Langkah-langkah yang dilakukan pada pencocokan bit adalah:

1. Mengkonversi pesan dan citra dalam bentuk biner
2. Mengambil nilai MSB citra
3. Melakukan pencocokan pesan pada MSB citra. Jika bit pesan terdapat pada MSB citra, maka dilanjutkan dengan menyimpan posisi indeks bit. Penyimpanan indeks terdiri dari posisi indeks bit awal (*start*) dan posisi indeks bit akhir (*end*). Jika proses pencocokan tidak terjadi, dilanjutkan proses d) sebagai berikut
4. Membagi pesan menjadi dua bagian sama panjang kiri (L[i]) dan kanan (R[i])
5. Mengulangi langkah yang sama seperti pada nomor b), dengan L[i] dan R[i] sebagai masukan. Jika semua bit pesan terdapat pada citra, maka pencocokan selesai dan dilanjutkan proses f). Jika tidak,

mengulangi langkah c) dengan L[i] dan R[i] sebagai masukkan hingga proses ke-i.

6. Menyimpan semua indeks bit hasil pencocokan
7. Keluaran berupa vektor yang memuat susunan indeks posisi bit.

b. Enkripsi

c. Deksripsi

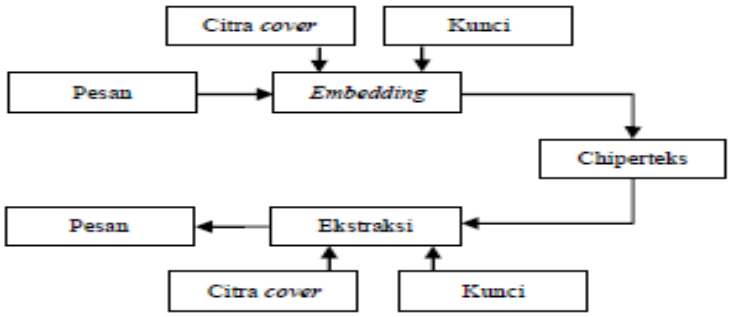
d. Rekonstruksi pesan

Rekonstruksi bertujuan untuk mengembalikan pesan menjadi bentuk semula. Masukan pada tahap ini terdiri dari indeks bit dan citra. Proses yang dilakukan yaitu dengan mengambil susunan bit citra berdasar indeks bit. Hasil keluaran berupa susunan bit pesan. Langkah-langkah yang dilakukan pada proses rekonstruksi adalah:

1. Mengkonversi citra dalam bentuk biner dan mengambil bit MSB citra.
2. Membaca setiap dua indeks isi vektor. Indeks pertama merupakan posisi awal bit (*start*) dan indeks kedua merupakan posisi akhir bit (*end*),
3. Mengambil nilai bit citra berdasarkan langkah b),
4. Mengulangi proses b) dan c) sampai posisi indeks terakhir.
5. Susunan bit yang terbentukakan menghasilkan keluaran berupa susunan bit pesan.

e. Proses *embedding* yang meliputi pencocokan bit dan enkripsi DES

Kombinasi steganografi dan kriptografi pada penelitian ini terdiri dari 2 proses, yaitu proses *embedding* dan ekstraksi yang secara umum dapat dilihat pada Gambar 4.2.

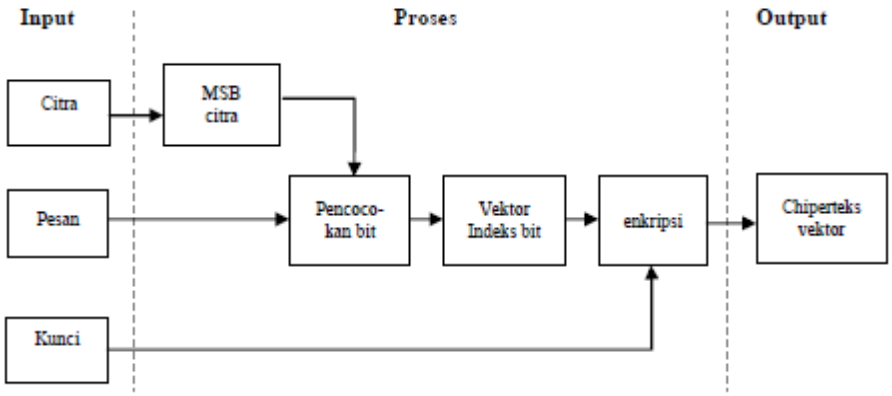


Gambar 4.2 Gambaran umum kombinasi steganografi dan kriptografi

Pada perancangan ini, peneliti mengusulkan metode steganografi yang dikembangkan Challita & Farhat (2011). Pesan tidak dienkrip terlebih dahulu, namun dilakukkan pencocokan antara bit pesan dengan bit citra. Bit citra yang digunakan adalah MSB citra. Hasil pencocokan berupa indeks bit yang kemudian dienkripsi. Untuk mengembalikan pesan, perlu melakukan dekripsi indeks bit dan dilanjutkan rekonstruksi pesan dengan citra yang sama. Proses *embedding* dan ekstraksi pada penelitian ini diuraikan sebagai berikut.

Bagan Proses *Embeeding*

Masukkan proses *embedding* berupa pesan, citra, dan kunci. Pada proses *embeeding* tahap yang dilakukan yaitu mencocokan bit pesan pada bit MSB citra. Hasil pencocokan disimpan dalam vektor yang memuat indeks lokasi bit. Tahap selanjutnya yaitu melakukan proses enkripsi pada vektor tersebut. *Output* yang dihasilkan adalah chiperteks vektor yang telah terenkripsi. Proses *embedding* ditunjukkan pada Gambar 4.3.



Gambar 4.3 Proses Embedding

Langkah-langkah *embedding* adalah sebagai berikut:

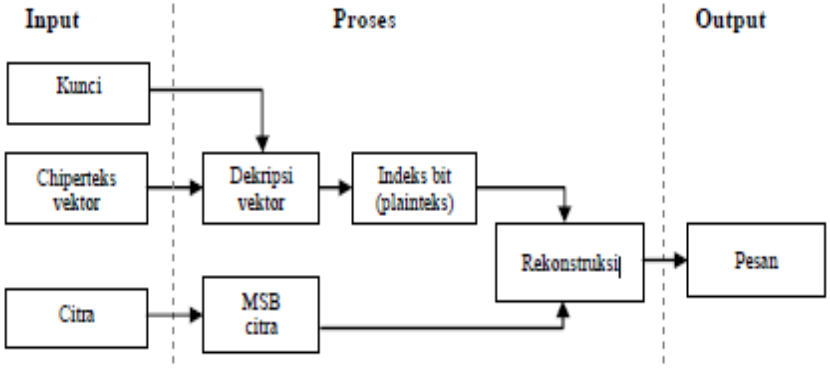
1. Memasukkan *input* berupa citra, pesan, dan kunci.
2. Mengkonversi pesan dan citra dalam bentuk biner.
3. Mencocokan bit pesan dengan bit MSB citra. Posisi bit yang sama disimpan dalam vektor indeks bit.
4. Mengenkripsi vektor indeks bit dengan algoritma DES.

5. Hasil keluaran berupa chiperteks. Chiperteks tersebut memuat vektor indeks bit yang telah terenkripsi.
6. Selesai.

f. Proses ekstraksi yang meliputi dekripsi DES dan rekonstruksi pesan.

Bagan Proses Ekstraksi

Masukkan proses ekstraksi berupa chiperteks vektor, kunci, dan citra. Proses ekstraksi meliputi dekripsi vektor dan dilanjutkan rekonstruksi. Hasil keluaran rekonstruksi berupa pesan semula. Bagan Proses ekstraksi ditunjukkan pada Gambar 4.4.



Gambar 4.4 Proses Ekstraksi

Langkah-langkah proses ekstraksi adalah sebagai berikut:

1. Memasukkan *input* berupa kunci, chiperteks vektor, dan citra.
2. Mendekripsi vektor dengan kunci, hasil dekripsi berupa plainteks indeks bit.
3. Melakukan rekonstruksi pesan dengan mencocokan bit MSB citra berdasar vektor indeks bit.
4. Hasil *output* berupa pesan.
5. Selesai.