KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

PALCOMTECH PALEMBANG

SKRIPSI

APLIKASI KEAMANAN EMAIL MENGGUNAKAN ALGORITMA ELGAMAL BERBASIS OPEN SOURCE PADA PT MEDCO E&P INDONESIA

OLEH :

SANDRO FEBRIYANSYAH

012080041

Untuk Memenuhi Sebagian dari Syarat-Syarat

Guna Mencapai Gelar Serjana Komputer

2012

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

PALCOMTECH PALEMBANG

SKRIPSI

APLIKASI KEAMANAN EMAIL MENGGUNAKAN ALGORITMA ELGAMAL BERBASIS OPEN SOURCE PADA PT MEDCO E&P INDONESIA

OLEH :

SANDRO FEBRIYANSYAH

012080041

Untuk Memenuhi Sebagian dari Syarat-Syarat

Guna Mencapai Gelar Serjana Komputer

2012

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

PALCOMTECH PALEMBANG

HALAMAN PENGESAHAN PEMBIMBING

NAMA	**: Sandro Febriyansyah**
NOMOR POKOK	**: 012080041**
PROGRAM STUDI	**: Teknik Informatika**
JENJANG PENDIDIKAN	**: Strata Satu (S1)**
KONSENTRASI	**: Jaringan**
JUDUL LAPORAN	**: Aplikasi Keamanan Email Menggunakan Algoritma Elgamal Berbasis Open Source Pada PT Medco E&P Indonesia**

PALEMBANG, September 2012

Menyetujui,	**Mengetahui,**
Pembimbing Skripsi,	**Ketua STMIK,**
R.M. Nasrul Halim, S.Kom.	**Rudi Sutomo, S.Kom, M.Si.**
NIDN : 0202128201	**NIP : 028.PCT.08**

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

PALCOMTECH PALEMBANG

HALAMAN PENGESAHAN PENGUJI

NAMA : **Sandro Febriyansyah**

NOMOR POKOK : **012080041**

PROGRAM STUDI : **Teknik Informatika**

JENJANG PENDIDIKAN : **Strata Satu (S1)**

KONSENTRASI : **Jaringan**

JUDUL LAPORAN : **Aplikasi Keamanan Email Menggunakan Algoritma Elgamal Berbasis Open Source Pada PT Medco E&P Indonesia**

Tanggal : 22 September 2012	**Tanggal :22 September 2012**
Penguji 1 :	**Penguji 2 :**
Ganda Hutasoit,S.E.,M.M.	**Rudi Sutomo, S.Kom, M.Si.**
NIDN. 0206055401	**NIDN. 0222057501**

Menyetujui,

Ketua STMIK,

Rudi Sutomo, S.Kom, M.Si.

NIP : 028.PCT.08

MOTTO DAN PERSEMBAHAN

"Hai orang-orang yang beriman apabila kamu mengadakan pembicaraan rahasia. Janganlah kamu membicarakan dengan perbuatan dosa, permusuhan dan perbuatan durhaka kepada Rasul. Dan bicarakanlah tentang membuat kebajikan dan taqwa. Dan bertaqwalah kepada Allah yang kepadaNyalah kamu dikembalikan."

Qs. Al-Mujaadillah (58): 9

"Tidak ada sistem keamanan yang benar-benar aman.
Jadi, persulitlah memasukinya dan merusak didalamnya."

Kupersembahkan untuk:

- ♠ *Tuhan Yang Maha Esa*
- ♠ *Ayah dan Ibuku Tercinta*
- ♠ *Kakakku Tersayang*
- ♠ *Teman Seperjuangan*
- ♠ *Almamater*

KATA PENGANTAR

Puji dan syukur Penulis panjatkan kehadirat Tuhan Yang Maha Esa, atas segala berkat dan karunia-Nya sehingga Penulis dapat menyelesaikan laporan tugas akhir atau skripsi ini dengan baik. Judul laporan ini adalah "Aplikasi Keamanan Email Menggunakan Algoritma Elgamal Berbasis Open Source". Skripsi ini disusun untuk memenuhi salah satu syarat guna memperoleh gelar Sarjana Komputer Jurusan Teknik Informatika pada Sekolah Tinggi Manajemen Informatika dan Komputer PalComTech Palembang.

Adapun selama penulisan dan penyusunan skripsi ini, Penulis mendapatkan banyak bimbingan, bantuan, dan dukungan dari banyak pihak. Oleh karena itu, sudah menjadi kewajiban bagi Penulis untuk mengucapkan terima kasih kepada Ketua STMIK PalComTech, Bapak Rudi Sutomo, S.Kom, M.Si., kepada Ketua Program Studi Teknik Informatika, Bapak D Tri Octafian, S.Kom., dan dosen pembimbing Bapak R.M. Nasrul Halim, S.Kom.

Penulis berharap skripsi ini dapat bermanfaat dan berguna bagi para pembaca, Penulis menyadari bahwa skripsi ini masih mempunyai banyak kekurangan sehingga membutuhkan banyak saran dan kritik yang membangun untuk menghasilkan sesuatu yang lebih baik. Terima kasih.

Palembang, September 2012

Penulis

DAFTAR ISI

BAB IV METODE PENELITIAN

BAB V HASIL DAN PEMBAHASAN

DAFTAR TABEL

DAFTAR GAMBAR

ABSTRAK

APLIKASI KEAMANAN EMAIL MENGGUNAKAN ALGORTIMA ELGAMAL BERBASIS OPEN SOURCE

Febriyansyah, Sandro. 2012. (012080041) . **Apliksi Keamanan Email Menggunakan Algoritma Elgamal Berbasis Open Source Pada PT Medco E&P Indonesia.** Skripsi. Jurusan Teknik Informatika. STMIK PalComTech Palembang. Pembimbing: R.M. Nasrul Halim, S.Kom.

Kata kunci: Kriptografi, Algoritma Elgamal, Keamanan Email.

Keamanan merupakan salah satu aspek terpenting dari suatu sistem informasi. Masalah kemanan sering kali kurang mendapat perhatian dari para perancang dan pengelola sistem informasi. Seringkali masalah keamanan berada diurutan setelah tampilan, atau bahkan diurutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila tidak mengganggu performa dari sistem, seringkali masalah keamanan tidak begitu dipedulikan bahkan ditiadakan.

Rancangan yang dibangun adalah aplikasi email client untuk keamanan email menggunakan kriptografi dengan algoritma elgamal, dengan aplikasi email client ini depat melakukan proses enkripsi dan dekripsi pesan dengan merubah pesan asli (*plaintext*) kedalam bentuk sandi (*ciphertext*) sehingga pesan lebih terjamin kerahasiaannya.

BAB I

PENDAHULUAN

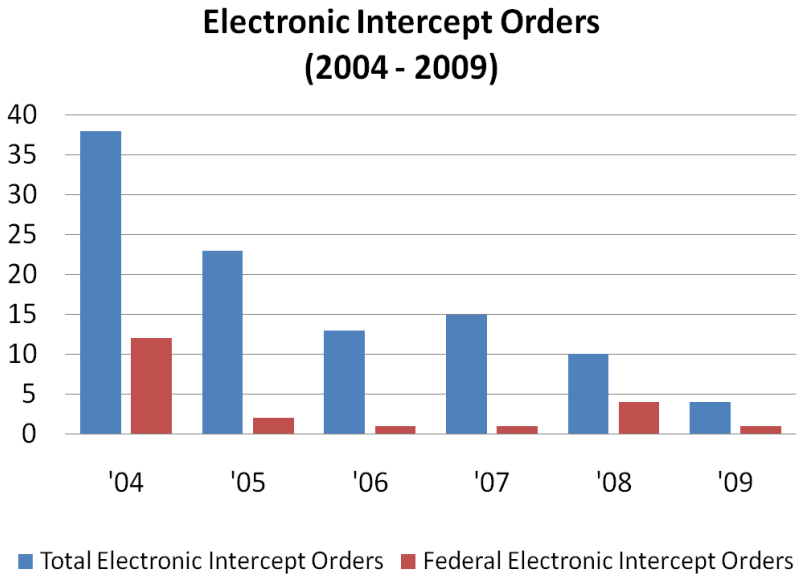
1.1. Latar Belakang

Keamanan merupakan salah satu aspek terpenting dari suatu sistem informasi. Masalah kemanan sering kali kurang mendapat perhatian dari para perancang dan pengelola sistem informasi. Seringkali masalah keamanan berada diurutan setelah tampilan, atau bahkan diurutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila tidak mengganggu performa dari sistem, seringkali masalah keamanan tidak begitu dipedulikan bahkan ditiadakan.

Pertukaran informasi menjadi sangat penting karena suatu komunikasi data jarak jauh belum tentu memiliki jalur transmisi yang aman dari penyadapan sehingga keamanan informasi menjadi bagian penting dalam dunia informasi itu sendiri. Terdapat data-data yang tidak terlalu penting, sehingga apabila publik mengetahui data tersebut, pemilik data tidak terlalu dirugikan. Tetapi apabila pemilik data adalah pihak militer atau pemerintah, keamanan dalam pertukaran informasi menjadi sangat penting karena data yang mereka kirim kebanyakan adalah data-data rahasia yang tidak boleh diketahui oleh publik.

Berikut ini contoh kejahatan email yang terjadi di pemerintahan Amerika. Setiap tahunnya kantor pengadilan Amerika Serikat menyusun laporan statistik penyadapan atau pencegatan email yang terjadi

sepanjang tahun 2004 sampai dengan 2009. Dapat dilihat pada statistik pencegatan email pada tahun 2004 jumlah email yang dicegat atau disadap kurang lebih 37%, 12% diantaranya merupakan pesan yang dikirim yang berhubungan dengan kerahasiaan Negara. Dapat dibayangkan seandainya pesan Negara tersebut disadap atau jatuh ketangan pihak ketiga, contohnya ketangan teroris.



Gambar 1.1 Statistik Kejahatan Email
(Sumber : http://paranoia.dubfire.net)

Metode penyandian yang pertama kali dibuat masih menggunakan metode algoritma rahasia. Metode ini menumpukan keamanannya pada kerahasiaan algoritma yang digunakan. Namun metode ini tidak efesien saat digunakan untuk berkomunikasi dengan banayak orang. Oleh karena itu seseorang harus membuat algoritma baru apabila akan bertukaran informasi rahasia dengan orang lain.

Karena penggunaannya yang tidak efesien maka algoritma rahasia mulai ditinggalkan dan dikenalkan suatu metode baru yang disebut dengan algoritma kunci. Metode ini tidak menumpukan keamanan pada algoritmanya, tetapi pada kerahasiaan kunci yang digunakan pada proses penyandian. Algoritmanya dapat diketahui, digunakan dan dipelajari oleh siapapun. Metode algoritma kunci mempunyai tingkat efisiensi dan keamanan yang lebih baik dibandingkan dengan algoritma rahasia. Sampai sekarang algoritma kunci masih digunakan secara luas di internet dan terus dikembangkan keamanan yang lebih baik.

Algoritma El-Gamal merupakan salah satu dari algoritma kunci. algoritma ini dikembangkan pertama kali oleh Taher El-Gamal pada tahun 1985. Sampai saat ini, algoritma El-Gamal masih dipercaya sebagai metode penyandian, seperti aplikasi PGP dan GnuPG yang dapat digunakan untuk pengamanan e-mail dan tanda tangan digital. Pada tahun 1994 pemerintah Amerika Serikat mengadopsi Digital Signature Standard, sebuah mekanisme penyandian yang berdasar pada algoritma El-Gamal.

PT Medco E&P Indonesia yang dulunya bernama PT Exspan Nusantara merupakan perusahaan yang bergerak di bidang industri minyak dan gas bumi. Industri perminyakan merupakan industri yang komplek, yaitu terdiri dari berbagai usaha yang saling mendukung satu sama lainnya. Sebagai anak perusahaan PT Medco Energy Internasional,

Tbk., PT Medco E&P Indonesia merupakan perusahaan nasional yang telah berhasil menempatkan diri sejajar dengan perusahaan minyak dan gas Internasional yang beroperasi di Indonesia. Perusahaan ini memiliki beberapa wilayah operasi di seluruh Indonesia seperti wilayah Sumatra Selatan memiliki dua daerah operasi bagian barat yaitu Lapangan (Stasiun Semoga) dan daerah Timur yaitu Lapangan (Stasiun Kaji Semoga). Lapangan Kaji Semoga Blok Rimau sendiri terletak di Desa Bonot, Kecamatan Lais, Kabupaten Musi Banyuasin, Provinsi Sumatra Selatan.

PT Medco E&P Indonesia (Rimau Asset) menggunakan berbagai saranah komunikasi untuk pertukaran informasi yang digunakan dalam menunjang efisiensi perusahaan yaitu salah satunya adalah email. email digunakan sebagai sarana pengiriman data baik itu hanya dalam ruang lingkup Rimau Asset (internal), maupun pengiriman keluar (eksternal).

Pada PT Medco E&P Indonesia (Rimau Assets) jumlah *account email* yang digunakan sebanyak 364 *acount* dengan *scope* pekerjaan *sharing* informasi meliputi dua *domain* utama (medcoenergi.com dan energibiz.com). standarisasi keamanan selama ini menggunakan *protocol* SSL dengan enkripsi 128 bit.

Standar keamanan ini sebenarnya sudah cukup untuk pertukaran informasi secara umum, tetapi masih belum optimal untuk pengiriman data-data yang sifatnya sensitive atau rahasia. Sehingga penulis

berkeinginan untuk mengangkat judul skripsi " **Aplikasi Keamanan Email dengan Algoritma El-Gamal Berbasis Open Source pada PT Medco E&P Indonesia (Rimau Asset) ".**

1.2.Rumusan Masalah

Dari paparan latar belakang diatas terdapat beberapa rumusan masalah yang harus di pecahkan pada penelitian ini yaitu, Bagaimana cara membuat dan merancang aplikasi pengamanan email menggunakan algoritma El-Gamal pada PT Medco E&P Indonesia (Rimau Assets) ?

1.3.Batasan Masalah

Pada penelitian ini diberikan pembatasan masalah agar penelitian ini lebih fokus, lebih spesifikasi hanya membahas pada :

a. Enkripsi dan dekripsi email hanya berupa text.
b. Algoritma yang digunakan adalah algoritma El-Gamal.
c. Bahasa pemrograman yang digunakan adalah PHP.
d. *Database* yang digunakan berupa MYSQL.
e. Sistem operasi yang digunakan adalah *Linux Debian Squeeze 6*.

1.4.Tujuan Penelitian

Penelitian ini mempunyai tujuan agar dapat membuat dan mengimplementasikan aplikasi keamanan email dengan algoritma El-Gamal.

1.5.Manfaat Penelitian

Adapun manfaat yang duharapkan dapat diperoleh dari penyusunan skripsi ini adalah :

1. Bagi Penulis
   a. Dapat mengimplementasikan ilmu yang didapat dari perkuliahan khususnya ilmu keamanan komputer, dan mengimplementasikan algoritma El-Gamal dalam pembuatan aplikasi keamanan email untuk enkripsi dan dekripsi email.
   b. Untuk memenuhi syarat kelulusan strata satu (S1) Teknik Informatika Palcomtech Palembang.
   c. Untuk memperkenalkan gambaran umum perusahaan yang diperlukan mahasiswa dalam memasuki dunia kerja.
2. Bagi PT Medco E&P Indonesia Blok Rimau Asset

   Dapat membantu dalam mengamankan email dengan proses kriptografi dengan algorima El-Gamal dari penyadapan email dari pihak-pihak yang tidak punya kepentingan,
3. Bagi Akademik

   Dapat dijadikan referensi dan perbandingan dalam pengembangan aplikasi berikutnya.

1.6.Sistematika Penulisan

Untuk memperoleh gambaran yang mudah dimengerti dan komperehensif mengenai isi dalam penulisan skripsi ini, secara global dapat dilihat dari sistematika pembahasan skripsi dibawah ini :

BAB I PENDAHULUAN

Bab ini merupakan bab pendahuluan yang di dalamnya berisi tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

BAB II GAMBARAN UMUM PERUSAHAAN

Dalam bab ini akan membahas tentang sejarah singkat, visi dan misi, struktur organisasi dan aktivitas perusahaan.

BAB III TINJAUAN PUSTAKA

Pada bab ini di bahas tentang beberapa landasan teori yang harus di pahami sebelum membahas bagian inti dari penelitian ini, yaitu tentang kriptografi, Email Client, web server dan Al goritma El-Gamal dan penelitian terdahulu.

BAB IV METODE PENELITIAN

Pada bab ini akan menjelaskan mengenai waktu dan lokasi penelitian, jenis data yang digunakan, teknik pengumpulan data, jenis penelitian, alat dan teknik pengembangan sistem.

BAB V HASIL DAN PEMBAHASAN

Bab ini menjelaskan tentang implementasi dari sistem yang telah dibuat ke dalam bentuk sebuah program aplikasi secara keseluruhan.

BAB VI PENUTUP

Bab ini merupakan penutup, yang di dalamnya berisi simpulan dan rangkuman dari pembahasan penelitian ini, serta berisi saran yang diharapkan dapat bermanfaat untuk pengembangan pembuatan program aplikasi selanjutnya.

BAB II

GAMBARAN UMUM

2.1.Profil Perusahaan

2.1.1. Sejarah Perusahaan

PT Medco E&P Indonesia merupakan suatu perusahaan swasta yang bergerak di bidang eksplorasi dan produksi minyak dan gas bumi. Perusahaan ini memiliki beberapa wilayah kerja pertambangan di berbagai wilayah di seluruh Indonesia seperti wilayah South Sumatra memiliki dua daerah operasi yaitu operasi bagian Barat yaitu lapangan (Stasiun Soka) dan daerah Timur yaitu lapangan (Stasiun Kaji Smoga). Selain eksplorasi dan produksi minyak dan gas bumi, PT Medco juga bergerak dibidang eksplotasi minyak dan gas bumi. Saat ini, rata-rata produksi minyak mentah PT Medco E&P perhari skitar 36.000 BOPD (*Barrel Oil per Day*).

1. Tahun 1912

   Pendirian PT Medco E&P Indonesia dimulai pertama kali ketika Standart *Oil of New Jersey* (Exxon) mendirikan *Nederlands Koninklijk Petroleum Maaschaappij* (NKPM) di Indonesia.

2. Tahun 1933

   Pada tanggal 07 September 1933 terjadinya penggabungan perusahaan antara *Exxon* dengan *Socony*

Vacuum (Mobil Oil) dan mengubah nama NKPM menjadi *Standart Oil Company* (Stanvac) yang disingkat menjadi SVPM atau SVCS.

3. Tahun 1961

   SVPM atau SVCS di Indonesia berubah nama menjadi PT Stanvac Indonesia, dimana pengelolaan dan operasi kerja dilaksanakan oleh Exxon International Company (EIC) yang beroperasi di New Jersey, Amerika Serikat.

4. Tahun 1986

   Ditemukannya lapangan minyak baru yang diantaranya adalah Tabuan, Jene, Lagan dan Tanjung Laban mulai produksi. Berikutnya dua lapangan baru lainnya di Sumatra Selatan, yaitu Pian dan Panglero ditemukan.

5. Tahun 1987

   Lapangan minyak di Block Rimau, Sumatra Selatan mulai berproduksi, perusahaan Stanvac kembali menemukan lapangan baru, masing-masing Serdang dan Langkap di Sumatra Selatan dan Paya Rumbai (Parum) di Riau, sekaligus dimulai pengembangan lapangan *Jene Extension Area*.

6. Tahun 1995

   Pada tanggal 22 November 1995, karena dianggap tidak dapat lagi memproduksi minyak mentah sesuai target yang diinginkan (25.000 barrel minyak mentah per hari), maka

40.000 lembar saham PT Stanvac Indonesia, yang semula dimiliki bersama *Exxon Corporation* dan *Mobil Oil Corporation*, secara keseluruhan dijual kepada sebuah perusahaan swasta nasional yang berdiri pada tahun 1992, yaitu *Medco Energy Corporation*.

7. Tahun 1996-1998

   PT Exspan Sumatra menemukan cadangan minyak yang besar di Lapangan Kaji-Semoga, tepatnya di Kabupaten Musi Banyuasin, Sumatra Selatan. Pada April 1997, Lapangan Kaji-Semoga mulai beroperasi. Stasiun pengumpulan minyak dan seluruh fasilitas penunjangnya diresmikan pada tahun 1998.

   PT Exspan Kalimantan dan PT Exspan Sumatera disatukan menjadi PT Exspan Nusantara. Pada awal tahun ini ekspor minyak pertama dari Lapangan kaji-Semoga dimulai. Pengiriman dilakukan melalui barge dari Stasiun Tengguleng sebelum dikirim keluar negeri. Sekitar 450.000 barrel minyak setiap bulan diekspor. Pada tahun yang sama PT Exspan Nusantara berhasil menemukan tambahan cadangan minyak sebesar 10 MMBO serta gas sebesar 237 BCF.

8. Tahun 2000

   Pada awal tahun 2000, dimulainya ekspor minyak pertama yang berasal dari Lapangan Kaji-Semoga dengan

pengiriman minyak mentah sebesar 450.000 barrel per bulan. Pada tanggal 05 Juli 2000, terjadi penggabungan PT Exspan Sumatera dan PT Exspan Kalimantan menjadi sebuah perusahaan yang bernama PT Exspan Nusantara yang berorientasi sebagai perusahaan Internasional.

9. Tahun 2003

   PT Exspan Nusantara mencapai produk rata-rata harian sebanyak 86.000 BOPD ditambah 70 MMCFD gas. PT Exspan Nusantara berkomitmen mendukung kebijakan energi nasional melalui beberapa penandatanganan perjanjian jual beli gas dan memasok gas alam ke beberapa instalasi pembangkit listrik PT PLN (Persero) di Sumatra Selatan.

10. Tahun 2004

    Pada awal tahun 2004, PT Exspan Nusantara melakukan penandatanganan perjanjian jual beli gas, diantaranya dengan PT PLN (Persero), PT Krakatau Steel, dan PT Pertamina (Persero). Mulai tanggal 19 April 2004, PT Exspan Nusantara memiliki indentitas baru dengan merubah nama menjadi PT Medco E&P Indonesia. Perubahan ini merupakan konsekuensi dari kerangka perubahan strategis yang sedang berlangsung di dalam induk perusahaan, PT Medco Energi Indonesia, Tbk dengan target untuk menjadi yang terdepan sebagai penyediaan energi.

11. Tahun 2007

Pada tahun 2007, PT Medco E&P Indonesia Rimau Asset mengimplementasikan sistem Manajemen Kesehatan Kerja berbasis ISRS7 dan berhasil mendapatkan sertifikasi ISRS7 Level 3 pada bulan Desember 2008 dan ditargetkan untuk mencapai Level 5 pada Desember 2010.

12. Tahun 2010

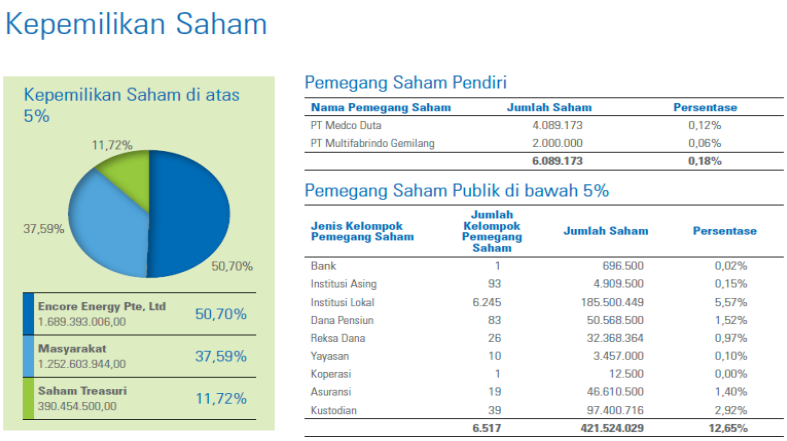
Diakhir tahun 2009, PT Medco E&P Indonesia Rimau Asset masih terus konsisten untuk memproduksi minyak dan gas alam dengan didukung oleh proses-proses pendukung lainnya termasuk sarana-sarana (Kaji, *office*, *compressor plant*, *warehouse*, *waste treatment center*, *workshop*, mess, kantin, dan sebagainya) dan juga sumber daya manusia yang ada.

Saat ini PT Medco E&P Indonesia memiliki wilayah kerja yang meliputi 16 area blok yang tersebar di 8 provinsi di Indonesia yaitu :

1. Sumatera Utara, yaitu Blok Asahan di Kabupaten Langkat.
2. Riau, yaitu Blok Kampar di Kabupaten Indaragiri Hulu, Indaragiri Hilir dan Palalawan.
3. Sumatera Selatan, yaitu Blok Western extention, Blok eastern extention, Blok Lematang, Blok Rimau di Kabupaten Musi Banyuasin, Musi Rawas, Banyuasin, Lahat, Muara Enim.

4. Bangka Belitung, yaitu di Bangka.
5. Jawa Timur, yaitu Blok Tuban, Blok Madura di Kabupaten Tuban, Bangkalan, Sampang, Pamekasan, dan Sumenep.
6. Kalimantan Timur, yaitu Blok Samboja, Blok Sanga-Sanga, Blok Tarakan, Blok Simenggaris, Blok Mengarai di Kabupaten Kutai Kartanegara, Bulungan, Tarakan, Nunukan.
7. Sulawesi Tengah, yaitu Blok Tomori di Kabupaten Luwuk dan Morowali.
8. Papua, yaitu Blok Yapen, Rambebai di Kabupaten Yapen.

Adapun kepemilikan saham dari PT Medco Energi dapat dilihat dari gambar 2.1.



Gambar 2.1 : Kepemilikan Saham PT Medco Energi
(Sumber : Diolah Sendiri)

2.1.2. Visi dan Misi PT Medco E&P Indonesia (Rimau Asset)

Berikut ini visi dan misi yang menjadi pedoman kegiatan PT Medco E&P Indonesia :

1. Visi

   Diakui sebagai perusahaan energi terkemuka di dunia dengan integritas tertinggi serta menjadi perusahaan energi pilihan.

2. Misi

   Mencari dan mengembangkan secara inovatif sumber daya energi untuk mengingkatkan manfaat bagi semua pihak yang berkepentingan (*stakeholders*) sejalan dengan standar etika dan standar lingkungan tertinggi.

Visi dan Misi yang telah disebutkan diatas menunjukkan bahwa PT Medco E&P Indonesia bertekad untuk diakui oleh masyarakat dunia sebagai perusahaan yang terhormat, memegang teguh etika bisnis dan nilai moral (universal) yang tinggi, mentaati perundangan yang berlaku, terpandang dan setara dengan perusahaan energy lain yang terkemuka.

Visi dan Misi tersebut juga menerangkan bahwa dalam melaksanakan usahanya, PT Medco E&P Indonesia senantiasa memberikan kesempatan yang seluas-luasnya kepada para pekerja untuk melakukan eksperimen dan inovasi, berusaha menghasilkan produk-produk yang dihargai dan dinilai tinggi oleh para stakeholders, bekerja dengan penuh kepedulian, tanggung jawab social, dan berpegang pada standar etika dan lingkungan tertinggi

demi peningkatan kesejahteraan bersama, baik *stakeholders*, manajemen, pekerja, maupun masyarakat disekitar operasinya.

Dalam menerapkan Visi dan Misinya, PT Medco E&P Indonesia didukung oleh pekerja tetap yang keseluruhannya adalah warga Indonesia. Dengan personalia dari masing-masing wilayah kerja yang diatur secara unik, dimana pemusatan perekrutan pekerja tetap (karyawan staff dan non-staff) diatur oleh bagian personalia Jakarta dan perekrutan pekerja kontrak oleh HRD lapangan atau pun menjadi salah satu perusahaan swasta Nasional terkemuka yang bergerak pada sector pertambangan minyak bumi dan gas alam.

Dalam mewujudkan Visi dan Misi perusahaan PT Medco E&P Indonesia memiliki batasan moral dalam bekerja yang disebut tata nilai perusahaan. Adapun tata nilai yang dimiliki perusahaan ini adalah kejujuran, kepedulian, semangat belajar, semangat inovatif, semangat bekerja tim, dapat dipercaya, dan diandalkan.

2.2.Struktur Organisasi

2.2.1. Bagian/Unit Kerja

Struktur organisasi merupakan suatu cara yang berguna untuk mengetahui tugas dan tanggung jawab, merupakan hal penting bagi suatu perusahaan dalam rangka menjalankan usahanya agar tujuan perusahaan dapat tercapai dengan baik.

Dengan struktur organisasi yang baik, tugas dan tanggung jawab dapat dilihat dengan jelas sehingga dapat mempermudah orang-orang yang ada didalam suatu perusahaan itu untuk melaksanakan tugas dan tanggung jawabnya masing-masing. Adapun bentuk struktur organisasi untuk setiap perusahaan tergantung kepada besar atau kecilnya perusahaan dan pembagian tugas yang sesuai dengan kegiatan perusahaan. Pada perusahaan yang kecil tentu organisasinya relatif sederhana dibandingkan dengan perusahaan yang besar, maka untuk membantu pelaksanaan operasional perusahaan perlu merancang suatu struktur organisasi perusahaan. Secara umum tidak ada struktur organisasi yang ideal, namun demikian struktur oganisasi harus ada dan diperlukan.

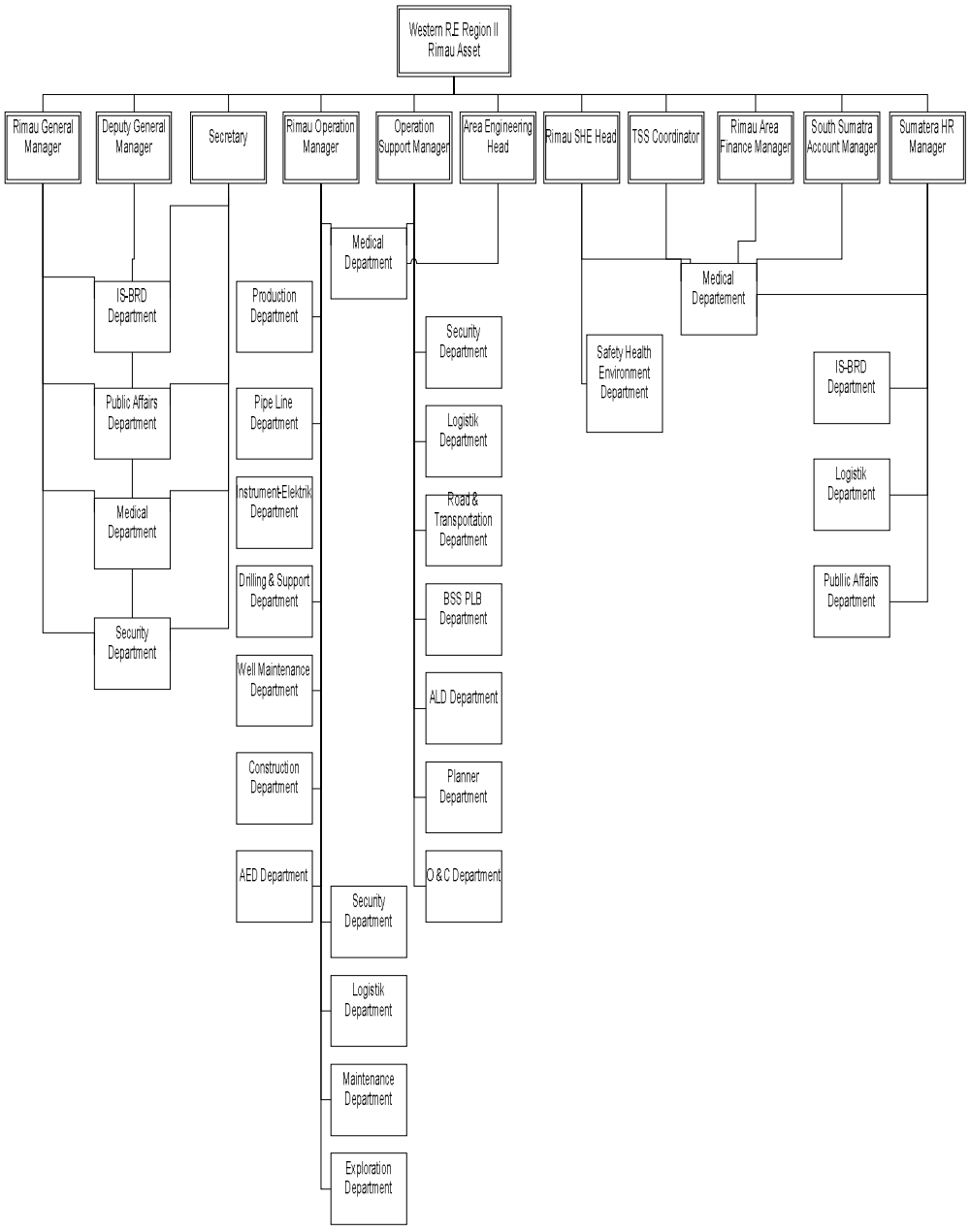
Struktur organisasi berguna untuk mengetahui :

a) Posisi dari masing – masing individu.
b) Bagian-bagian yang terdapat didalam perusahaan.
c) Wewenang dan tanggung jawab masing-masing bagian.

Struktur organisasi suatu perusahaan harus mempunyai sifat fleksibel sehingga dapat berubah sesuai dengan kebutuhan perusahaan pada saat itu. Selain itu struktur organisasi mempunyai tujuan yang takkala pentingnya dalam mencapai suatu tujuan perusahaan.

STRUKTUR ORGANISASI PT MEDCO E&P INDONESIA

Blok Rimau Asset



Gambar 2.2 Struktur Organisasi PT Medco E&P Indonesia

(Sumber : PT Medco E&P Indonesia Blok Rimau Asset)

2.3.Tugas Wewenang

1. *Rimau General Manager*

Tugas dan wewenang *General Manager* meliputi :

a. Memimpin kegiatan pelaksanaan perusahaan.
b. Merencanakan dan menyiapkan rapat tinjauan perusahaan.
c. Menjalin hubungan kerjasama dengan berbagai perusahaan.

2. *Deputy General Meneger*

Memiliki tugas dan tanggung jawab sebagai berikut :

a. Bersama General Manager Regional memimpin para Manager bagian di Kantor Regional, Manager Cabang dan Manager Unit untuk menyusun sasaran, rencana kerja, dan anggaran Kantor Regional yang merupakan Bagian Rencana Kerja dan Anggaran Perusahaan.
b. Memberikan penugasan, pengendalian dan penilaian kerja, kepada para Asisten Manager.
c. Membantu General Manager Regional dalam melaksanakan kegiatan operasional di Kantor Regional, Cabang dan Unit.
d. Meminpin penyelenggaraan kegiatan Kantor Regional.
e. Mewakili General Manager Regional dalam melaksanakan tugas-tugasnya apabila General Manager berhalangan.
f. Memimpim penyelenggaraan pengelolaan (penerbitan atau pelaporan, pendistribusian, penyimpangan, dan pemeliharaan) data dan informasi di Kantor Regional.

3. *Secretary*

Tugas dan wewenang *Secretary* meliputi :

a. Memberikan masukan dari aspek hukum kepada direksi , berkaitan dengan operasional dan perkembangan usaha perusahaan.
b. Menyelenggarakan database dan menyimpan dokumen asli perusahaan.
c. Mengkoordinasikan pengurusan izin-izin usaha perusahaan.
d. Mebangun jaringan kerjasama yang saling menguntungkan dengan berbagai pihak stake holder.
e. Mengkomunikasikan kebijakan perusahaan dan atau pemerintah kepada pihak internal maupun eksternal.

4. *Rimau Operation Manager*

Operation manager adalah kepala untit kerja yang bertanggungjawab atas pelaksanaan tugas dan wewenang yang berkaitan dengan teknis operasional kantor cabang PT Medco E&P Indonesia tepatnya Blok Rimau Asset.

5. *Operation Support Manager*

Tugas dan wewenang *operation Support Manager* meliputi :

a. Memantau infrastruktur dan sistem pendukung perusahaan.
b. Membuat target perencanaan operasional perusahaan.
c. Memiliki akses kesemua peralatan pendukung perusahaan.

6. *Area Engineering Head*

Tugas dan wewenang *engineering head* meliputi :

a. merencanakan, mengembangkan dan mengawasi semua kegiatan Pemeliharaan untuk memastikan keandalan dan efisiensi di operasi produksi.
b. Menyediakan dukungan teknis untuk semua unit seperti yang diminta.

7. Rimau SHE Head

Rimau SHE (*Safety Health Environment*) Head bertanggung jawab atas segala sesuatu mengenai *Safety* atau Keselamatan Kerja, *Healt* atau Kesehatan Kerja, dan *Environment* atau Pemeliharaan Lingkungan Kerja.

8. TSS Coordinator

Tugas dan tanggung jawab *TSS Coordinator* adalah melakukan proses estimasi, pengembangan perencanaan dan spesifikasi produk, merchandising, dan material marketing yang dibutuhkan.

9. Rimau Area Finance Manager

Tugas dan wewenang Rimau Area Finance Manager :

a. Bertanggung jawab penuh terhadap segala bentuk transaksi keuangan di kantor PT Medco E&P Indonesia.
b. Mengelolah dana yang didapat dari nasabah.
c. Mengawasi arus keperusahaan.

10. South Sumatra Acount Manager

Tugas dan wewenang *Acount Manager* meliputi :

a. Mengajukan anggaran penerimaan dan pengeluaran secara periodik.
b. Melakukan penelitian, penilaian, dan pengendalian pengadaan dana secara utuh, tepat pada waktunya.
c. Bertanggung jawab atas penggajian karyawan.

11. Sumatra HR Manager

a. Mengkoordinasikan pengembangan struktur organisasi yang efektif, analisi kompetensi dan pengembangan manajemen.
b. Sebagai konsultan dalam pengembangan organisasi dan rencana usaha perusahaan.
c. Memastikan target departemen dan individu dilingkungan HRD tercapai.

Untuk meningkatkan kinerja operasional perusahaan, di setiap organisasi memiliki beberapa depertemen pendukung yang memiliki peranan masing-masing, yaitu sebagai berikut :

a. Production Department

Prodaction Departement merupakan depertemen yang bertanggung jawab atas perkembangan (Peningkatan dan Penurunan) produksi, pengolahan hasil produksi minyak dan gas serta kelancaran operasional di Blok Rimau

b. *Pipe Line Department*

Merupakan departemen yang bertanggung jawab atas aliran minyak melalui pipa dari sumur-sumur ke stasiun-stasiun.

c. *Instrument – Elektrik Department*

Merupakan departemen yang bertanggung jawab atas permesinan dan kelistrikan.

d. *Safety Health Environment Department*

SHE (*Safety Health Environment*) merupakan departemen yang bertanggung jawab atas segala sesuatu mengenai *Safety* atau Keselamatan Kerja, *Healt* atau Kesehatan Kerja, dan *Environment* atau Pemeliharaan Lingkungan. Depetemen ini berwewenang untuk merumuskan program K3, dan mengadakan investigasi apabila terjadi kecelakaan, kelestarian lingkungan operasi dan sekitarnya.

e. *Drilling & Support Department*

Merupakan departemen yanag bertanggung jawab atas kegiatan pengeboran sumur-sumur minyak bumi.

f. *Well Maintenance Department*

Merupakan departemen yang bertanggung jawab atas pemeliharaan fasilitas-fasilitas produksi seperti pemeliharaan pompa, pemeliharaan sumur pompa, pemeliharaan sumur-sumur ring service.

g. *Construction Department*

Merupakan departemen yang bertangggung jawab atas pembangunan fasilitas-fasilitas pendukung produksi.

h. Medical Department

Meruakan departemen yang bertanggung jawab dalam hal pemeriksaan dan pengobatan pekerja, serta melakukan usaha-usaha kesehatan untuk menjaga dan meningkatkan derajat kesehatan pekerja.

i. AED Department

Area Engineering Department merupakan departemen yang bertanggung jawab atas perancangan teknis stasiun maupun fasilitas penunjang operasi.

j. Security Department

Merupakan departemen yang bertanggung jawab atas keamanan pekerja dan operasional perusahaan di Sumatera Selatan.

k. Logistik Department

Merupakan departemen yang bertanggung jawab atas pengadaan barang dan jasa serta pengadaan atau penyimpanan barang-barang untuk keperluan operasi diseluruh wilayah kerja Medco E&P Rimau Asset.

l. Road & Transportation Department

Merupakan departemen yang bertanggung jawab melayani perpindahan dan transportasi kebutuhan operasi, seperti pemindahan semua alat besar dan kecil menjadi kebutuhan operasi perusahaan.

m. *Maintenance Department*

Merupakan departemen yang bertugas dan bertanggung jawab atas pemeliharaan fasilitas-fasilitas penunjang produksi dan operasional perusahaan.

n. *BSS PLB Department*

Basic Share Service Palembang merupakan departemen yang bertanggung jawab atas pelayanan terhadap klien.

o. *IS – BRD Department*

IS-BRD Departement merupakan departemen yang bertanggung jawab atas sistem informasi, komputerisasi dan publikasi perusahaan.

p. *Exploration Department*

Depertamen yang bertanggung jawab mencari lokasi sumber minyak baru mulai koordinatnya hingga aktualnya di wilayah Sumatera Selatan.

q. *ALD Department*

Artificial Lift Department merupakan departemen yang bertanggung jawab atas pengembangan design sumur minyak (Well) sesuai dengan kebutuhan dan teknologi.

r. *Public Affairs Department*

*Public Affai*rs merupkan departemen yang bertanggung jawab mengatur hubungan dengan masyarakat dan pihak-pihak seperti pemerintahan daerah dan media masa.

s. *Planner Department*

Planner Department merupakan departemen yang bertanggung jawab untuk merancang dan merencanakan konsep dan perkembangan produksi dan operasional perusahaan.

t. *O & C Department*

Office and Camp Department merupakan departemen yang bertanggung jawab atas pemeliharaan perkantoran dan camp pekerja.

BAB III

TINJAUAN PUSTAKA

3.1 Teori Pendukung

3.1.1 Komunikasi Data

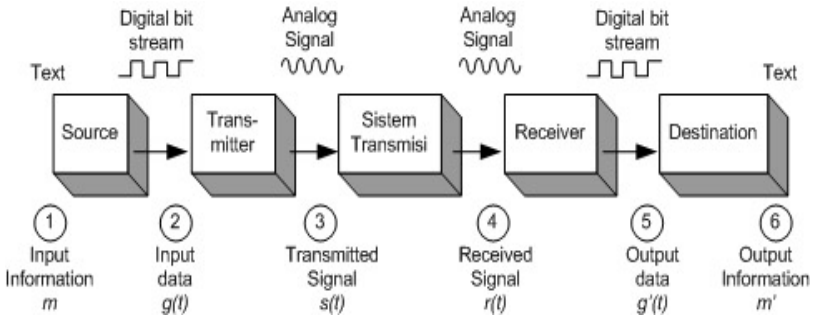
Menurut Sutanta (2005:6) Source adalah sumber program yang berisi beberapa perintah yang akan dikerjakan oleh komputer.

Menurut Sutanta (2005:6) Transmiter adalah pemancar atau perangkat I/O.

Menurut Sutanta (2005:6) Sistem Transmisi sistem yang berfungsi untuk konversi torsi dan kecepatan (putaran) dari mesin menjadi torsi dan kecepatan yang berbeda-beda untuk diteruskan ke penggerak akhir. Konversi ini mengubah kecepatan putar yang tinggi menjadi lebih rendah tetapi lebih bertenaga, atau sebaliknya.

Menurut Sutanta (2005:6) Receiver adalah perangkat penerima informasi atau sinyal.

Menurut Sutanta (2005:6) Destination adalah berarti tujuan. Tujuan dari suatu proses. Misalnya kemana lalu lintas jaringan ditujukan oleh pengirim (source).



Gambar 3.1 Model Komunikasi Data Sederhana
(Sumber :Diolah Sendiri)

Komunikasi data adalah transmisi atau proses pengiriman atau penerimaan data dari dua atau lebih device (sumber), melalui beberapa media transmisi pengiriman data.

3.1.2 Media Transmisi

Media transmisi bekerja dengan cara menghubungkan antar terminal satu dengan terminal lainnya, dengan cara mengirimkan atau menerima sinyal atau glombang elektromagnetik. Yani (2008:38).

1. **Kabel**

   Saat ini ada beberapa tipe dan jenis kabel yang digunakan untuk suatu jaringan. Kabel *twisted pair* (ada dua tipe, UTP dan STP), coaxial, dan fiber optic adalah yang paling popular.

A. Kabel Twisted Pair

a. STP (*Shielded Twisted Pair*), yaitu kabel *twisted pair* yang setiap pasangnya diberi perlindungan lagi.

b. UTP (*Unshielded Twisted Pair*), yaitu kabel *twisted pair* yang tidak diberi perlindungan untuk setiap kabelnya.

Tabel 3.1 Daftar Kabel Twisted Pair

Kabel	Tipe	Feature
Cat 1	UTP	Analog (biasanya digunakan diperangkat telepon. Pada umumnya jalur ISDN (Integrated Service Digital Networks) digunakan untuk menghubungkan modem dengan line telepon).
Cat 2	UTP	Up to 1 Mbits (seiring digunakan pada topologi ring)
Cat 3	UTP/STP	16 Mbits data transfer (sering digunakan pada topologi token ring atau 10BaseT).
Cat 4	UTP,STP	20 Mbits data transfer (biasanya digunakan pada topologi token ring).
Cat 5	UTP,STP UP TO 100 MHZ	100 Mbits data transfer/22 db
Cat 5e	UTP,STP UP TO 100 MHZ	1 Gigabit Ethernet up to 100 meters – 4 copperpairs (kedua jenis CAT5 sering digunakan pada topologi token ring 16 Mbps, Ethernet 10 Mbps, atau pada FastEthernet 100 Mbps).
Cat 6	UP TO 155 MHZ 250	2,5 Gigabit Ethernet up to 100 meter atau 10 Gigabits/ up to

	MHZ	25 meter
Cat 7	UP TO 200 MHZ 700 MHZ	Giga-Ethernet / 20.8 db (Gigabit Ethernet)

B. Kabel Coaxial

Kabel ini lebih sederhana, berisikan kawat tembaga sebagai intinya dan di sekelilingnya dilapisi dengan bahan penyekat, diluarnya dilapisi lagi dengan bahan konduktor yang dianyam atau dijalin.

Ada dua tipe kabel *coaxial* sebagai berikut :

a. *Coaxial baseband*, yang biasanya digunakan untuk transmisi digital dengan resistansi 50 ohm.
b. *Coaxial broadband*, biasanya digunakan untuk transmisi analog dengan resistansi 75 ohm.

Kabel *coaxial* memiliki daya transmisi yang cukup jauh, yaitu sebagai berikut :

a. 200 meter dengan kecepatan 10 Mbps (10Base2-thin *coaxial* RG58, RG54, dengan impedensi 75 Ohm *broadband ethernet*).
b. 500 meter dengan kecepatan 10 Mbps (10Base5-Thick *Coaxial)*.

C. Fiber Optik

Prinsip kerja serat optik adalah mentranformasikan data dengan pulsa cahaya. Pulsa cahaya dapat digunakan untuk mensinyalkan bit 0 (nol). Jenis transmisi menggunakan optik memiliki tiga komponen utama, yaitu media transmisi, sumber cahaya, dan *detector*.

Media transmisi menggunakan serat kaca yang sangat halus atau silica yang terfusi. Sumber cahaya yang digunakan memanfaatkan *Light Emitting Diode* (LED) atau *laser Diode*. Keduanya memamcarkan cahaya jika diberi arus listrik, media detektornya menggunakan *photodiode* yang berfungsi untuk menggenerasikan pulsa elektrik bila ada cahaya yang menyorotnya.

3.1.3 Klasifikasi Jaringan

Pada dasarnya jaringan komputer dapat dibedakan berdasarkan luasan area yang dapat dijangkau oleh jaringan itu sendiri. Hal ini berarti luasan area dapat ditentukan berdasarkan jarak atau jangkauan dari jaringan itu. Namun dengan berkembangnya teknologi dari jaringan komputer, ada pertimbangan lain yang dapat mengubah penggolongan tersebut. Misalnya saja pertimbangan mengenai peralatan yang digunakan,

fasilitas dan beberapa hal lain. Alat-alat yang menjadi pertimbangan antara lain *router, gateway, bridge* dan *repeater*. Semua peralatan tersebut dipertimbangkan, karena dari alat inilah dapat terlihat jangkauan area jaringan dan luas segmen yang digunakan. (Yani,2008:6).

Berdasarkan kriteria diatas, ada empat kelompok jaringan yang dapat disimpulkan sebagai berikut :

a. *Local Area Network* (LAN)

Local Area Network biasanya menghubungkan atara komputer satu dengan komputer lainnya, atau bisa juga *node* satu dengan *node* lainnya. Daerah jangkauan LAN yang tidak terlalu jauh, misalnya saja dalam suatu ruangan atau dalam satu area dengan radius antara 100 sampai 2.000 m, tergantung dari kabel yang digunakan.

b. *Interconection Network (Internetwork)*

Inter-network adalah pengembangan dari jaringan local. Misalnya pada suatu kantor besar, komputer setiap departemen akan digabungkan menjadi satu dengan departemen yang lainnya, berarti administrator jaringan menggabungkan dua jaringan local yang ada.

c. *Metropolitan Area Network* (MAN)

MAN biasanya meliputi area yang lebih besar dari LAN, misal antar wilayah dalam satu propinsi. Dalam hal ini jaringan MAN menghubungkan beberapa buah jaringan-jaringan kecil kedalam lingkuangan area yang lebih besar, sebagai contoh jaringan kantor cabang sebuah bank didalam sebuah kota besar dihubungkan atara satu dengan lainnya.

d. *Wide Area Network* (WAN)

Jaringan komputer ini merupakan gabungan ketiga jaringan diatas, yang telah mengalami pengembangan infrastruktur jaringan sehingga jarak cakupannya semakin jauh (antar kota, provinsi, bahkan Negara).

3.1.4 Topologi Jaringan

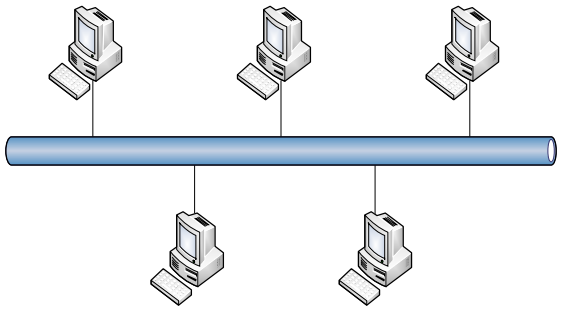
Topologi menggambarkan metode yang digunakan untuk melakukan pengabelan secara fisik dari suatu jaringan. Topologi jaringan adalah susunan atau pemetaan *interkoneksi* antara *node*, dari suatu jaringan, baik secara fisik (*rill*) dan logis (v*irtual*). (Sopandi,2008:27).

1. Topologi Fisik Jaringan

Topologi fisik jaringan adalah cara yang digunakan untuk menghubungkan *workstation-workstation* didalam LAN tersebut. Sebenarnya ada banyak topologi jaringan komputer, namun yang sering didengar pada umumnya berkisar pada tiga bentuk *(topology*) jaringan komputer,yaitu *Bus, Ring* dan *Star*.

a. Topologi *Bus* atau *Linier*

Topologi linier bus merupakan topologi yang banyak dipergunakan pada masa penggunaan kabel *Coaxial*. Dengan menggunakan *T-Connector* (dengan *terminator* 500 ohm pada ujung *network*), maka komputer atau perangkat jaringan lainnya bisa dengan mudah dihubungkan satu sama lain.

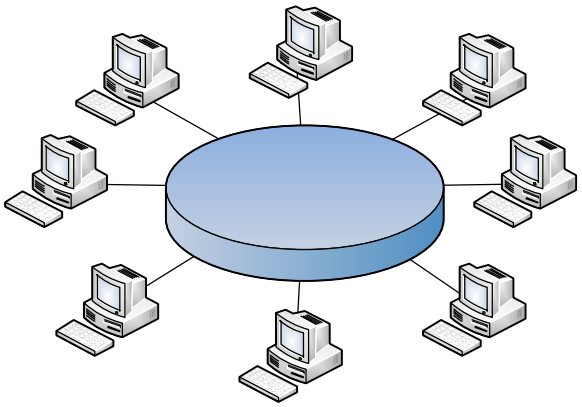


Gambar 3.2 Topologi Bus atau Linier
(Sumber : Diolah Sendiri)

b. Topologi *Ring*

Topologi ini memanfaatkan kurva tertutup, artinya informasi dan data serta *traffic* disalurkan sedemikian rupa

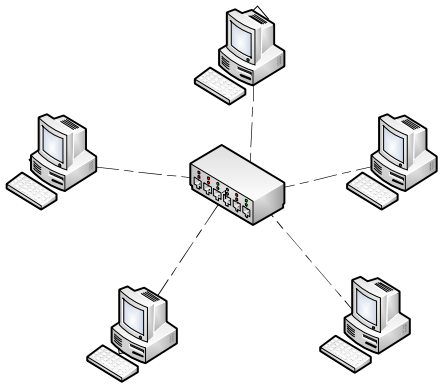
sehingga masing-masing *node.* Umumnya fasilitas ini memanfaatkan *fiber optic* sebagai sarananya (walaupun ada juga yang menggunakan *twisted pair).*



Gambar 3.3 Topologi Ring
(Sumber : Diolah Sendiri)

c. Topologi *Star*

Topologi ini banyak dipergunakan diberbagai tempat, karena kemudahan untuk menambah, mengurangi atau mendeteksi kerusakan jaringan yang ada. Selain itu, permasalahan panjang kabel yang harus sesuai (matching) juga tidak menjadi suatu yang penting lagi.



Gambar 3.4 Topologi Star
(Sumber : Diolah Sendiri)

2. Topologi Logic

Dilihat dari *metode accsess*, topologi jaringan ini terdiri dari :

1. *Ethernet*

   Dikembangkan *Xerox Corp* pada tahun 70-an dan menjadi popular pada tahun 80-an karena diterima sebagai standar IEEE 802.3. *Ethernet* bekerja berdasarkan *broadcast network*, dimana setiap *node* menerima setiap trasmisi data yang dikirim oleh sebuah *node* menggunakan metode CSMA/CD (*Carrier Sense Multipleacces/Collision Detection) baseband*.

   Cara kerja *Ethernet* :

   a. Sebelum mengirimkan paket data, setiap *node* melihat apakah *network* juga sedang mengirimkan paket data.

Jika *network busy node* akan menunggu sampai tidak ada sinyal lagi yang dikirim oleh *network.*

b. Jika *network* sepi barulah *node* itu mengirimkan paketnya. Jika pada saat yang sama terdapat dua *node* yang mengirimkan data, maka terjadi *collision*. Jika terjadi *collision* kedua node mengirimkan sinyal jam ke *network* dan semua *node* berhenti mengirimkan paket data dan kembali menunggu. Kemudian secara *random*, node-node itu kembali menunggu dan mengirimkan data. Paket yang mengalami *collision* akan dikirimkan kembali saat ada kesempatan.
c. Kecepatan 10 mbps dan menurun seiring semakin banyaknya *node* yang terpasang semakin banyak kemungkinan tabrakan.

Jika dilihat dari kecepatannya, *Ethernet* terbagi menjadi empat jenis, yakni sebagai berikut :

a. 10 Mbit/detik, yang sering disebut *Ethernet* (standar yang digunakan: 10Base2, 10Base5, 10BaseT, 10BaseF).
b. 100 Mbit/detik, yang sering disebut *Fast Ethernet* (standar yang digunakan: 100BaseFX, 100BaseT, 100BaseT4, 100BaseTX).

c. 1000 Mbit/detik atau 1 Gbit/detik, yang sering disebut sebagai *Gigabit Ethernet* (standar yang digunakan: 1000BaseCX, 1000BaseLX, 1000BaseSX, 1000BaseT).
d. 10000 Mbit/detik atau 10 Gbit/detik. Standar ini belum banyak di implementasikan

2. *Token Ring*

Berdasarkan standar IEEE 802.5 yang dikembangkan oleh IBM untuk menghindari *collision* tidak menggunakan *collision detection* melainkan *token passing scheme*, *token passing scheme* dapat dijelaskan secara sederhana: sebuah token bebas mengalir pada setiap node melalui *network.* Token mengalir di *network* dalam satu arah dan setiap station di poll satu persatu (kecepatan 4 mbps dan 16 mbps).

Ada tiga pengembangan dari *Token Ring* dasar: *Token Ring Full Duplex, Switched Token Ring*, dan *100VG-AnyLAN*. *Token Ring Full Duplex* menggunakan *bandwidth* dua arah pada jaringan *komputer*. *Switched Token Ring* menggunakan *switch* yang mentransmisikan data diantara segmen LAN (tidak dalam device LAN tunggal). Sementara, standar 100VG-AnyLAN dapat mendukung

baik format *Ethernet* maupun *Token Ring* pada kecepatan 100 mbps.

3. *ARC net*

   ARCnet topologi adalah kombinasi *star* dan *bus*. Jenis kabel adalah RG-62 A/U koaksial (93 ohm), UTP atau serat optik. Sebuah jaringan bisa menggunakan kombinasi dari media ini. Konektor yang digunakan meliputi BNC, RJ-45, dan yang lainnya. Panjang segmen maksimum adalah 600 meter dengan RG-62 A/U, 121 meter dengan UTP, 3485 meter dengan serat optic, dan 30 meter dari satu pusat (hub) pasif.

4. *FDDI*

   FDDI (*Fiber Distributed Data Interchange)* adalah standar komunikasi data menggunakan kabel *fiber optic* (serat optik), bekerja berdasarkan dua ring konsentrik, masing-masing berkecepatan 1200 mbps, dengan menggunakan *token passing scheme*. Salah satu ring dapat berfungsi sebagai *backup* atau dibuat menjadi pengirim saja (mengirim dan menerima data dalam arah yang berbeda), jumlahnya bisa mencapai 100 node dengan jarak sampai dengan 200 km. FDDI tidak kompatibel dengan *Ethernet* namun *Ethernet* dapat dienkapsulasi dalam paket FDDI, FDDI bukan standar IEEE.

3.1.5 Protokol Jaringan

Protokol pada suatu jaringan merupakan aturan dalam melakukan pengiriman data berupa blok-blok data dari sebuah *node* jaringan ke *node* jaringan yang lain. (Mulyanta, 2008 : 5).

A. *Internet Protocol* (IP)

IP *address* yaitu sistem pengalamatan di *network* yang direpresentasikan dengan sederetan angka berupa kombinasi 4 deret bilangan antara 0 sampai dengan 255 yang masing-masing dipisahkan oleh tanda titik (.), mulai dari 0.0.0.1 hingga 255.255.255.255 .

IP *address* digunakan sebagai alamat dalam hubungan antar *host* di internet sehingga merupakan sebuah sistem komunikasi yang *universal* karena merupakan metode pengalamatan yang telah diterima di seluruh dunia. Dengan menentukan IP *address* berarti kita telah memberikan identitas yang *universal* bagi setiap interadce komputer. Jika suatu komputer memiliki lebih dari satu *interface* (misalkan menggunakan dua *ethernet*) maka kita harus memberi dua IP *address* untuk komputer tersebut masing-masing untuk setiap *interface*nya. (Sopandi, 2006 : 55).

B. Format Penulisan IP Address

IP address terdiri dari bilangan biner 32 bit yang dipisahkan oleh tanda titik setiap 8 bitnya. Tiap 8 bit ini disebut

sebagai *oktet*. Bentuk IP address dapat dituliskan sebagai berikut :

xxxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx

Jadi IP *address* ini mempunyai range dari 00000000.00000000.00000000.00000000 sampai 11111111.11111111.11111111.11111111. Notasi IP *address* dengan bilangan *biner* seperti ini susah untuk digunakan, sehingga sering ditulis dalam 4 bilangan desimal yang masing-masing dipisahkan oleh 4 buah titik yang lebih dikenal dengan "notasi desimal bertitik". Setiap bilangan *desimal* merupakan nilai dari satu *oktet* IP *address*. (Sopandi, 2006 : 57).

C. Pembagian Kelas IP Address V.4

a. Kelas A

Bit pertama IP *address* kelas A adalah 0, dengan panjang net ID 8 bit dan panjang *host* ID 24 bit. Jadi *byte* pertama IP *address* kelas A mempunyai range dari 0-127. Jadi pada kelas A terdapat 127 *network* dengan tiap *network* dapat menampung sekitar 16 juta *host* (255x255x255). (Sopandi, 2006 : 58).

b. Kelas B

Dua bit IP *address* kelas B selalu diset 10 sehingga *byte* pertamanya selalu bernilai antara 128-191. *Network* ID adalah 16 bit pertama dan 16 bit sisanya adalah *host* ID

sehingga kalau ada komputer mempunyai IP *address* 167.205.26.161, *network* ID = 167.205 dan *host* ID = 26.161. Pada. IP *address* kelas B ini mempunyai range IP dari 128.0.xxx.xxx sampai 191.155.xxx.xxx, yakni berjumlah 65.255 *network* dengan jumlah *host* tiap *network* 255 x 255 *host* atau sekitar 65 ribu *host*. (Sopandi, 2006 : 58).

c. Kelas C

IP *address* kelas C mulanya digunakan untuk jaringan berukuran kecil seperti LAN. Tiga bit pertama IP *address* kelas C selalu diset 111. Network ID terdiri dari 24 bit dan *host* ID 8 bit sisanya sehingga dapat terbentuk sekitar 2 juta *network* dengan masing-masing *network* memiliki 256 *host*. (Sopandi, 2006 : 59).

d. Kelas D

IP a*ddress* kelas D digunakan untuk keperluan *multicasting*. 4 bit pertama IP *address* kelas D selalu diset 1110 sehingga *byte* pertamanya berkisar antara 224-247, sedangkan bit-bit berikutnya diatur sesuai keperluan *multicast group* yang menggunakan IP *address* ini. Dalam multicasting tidak dikenal istilah *network* ID dan *host* ID. (Sopandi, 2006 : 59).

e. Kelas E

IP *address* kelas E tidak diperuntukkan untuk keperluan umum. 4 bit pertama IP *address* kelas ini diset 1111 sehingga *byte* pertamanya berkisar antara 248-255. (Sopandi, 2006 : 59).

3.1.6 Perangkat Jaringan

Perangkat jaringan adalah semua komputer, *peripheral*, *interface card* dan perangkat tambahan yang terhubung ke dalam suatu sistem jaringan komputer untuk melakukan komunikasi data sebagai berikut :

1. *Server*

   Server merupakan pusat kontrol jaringan komputer. Biasanya berupa komputer berkecepatan tinggi dengan kapasitas RAM yang besar dan memiliki *space hardisk* cukup besar pula. Sistem operasi yang digunakan merupakan sistem operasi khusus yang dapat memberikan berbagai layanan bagi *workstation.*

2. *Workstation*

   Semua komputer yang terhubung dengan jaringan dapat dikatakan sebagai *workstation*. Komputer ini yang melakukan akses ke *server* guna mendapat layanan yang telah disediakan oleh *server.*

3. *Network Interface Card (NIC)*

NIC sering disebut *Ethernet Card*, digunakan untuk menghubungkan sebuah komputer ke jaringan. NIC memberikan suatu koneksi fisik antara kabel jaringan dengan bus internal komputer.

4. *Hub*

Hub merupakan komponen jaringan yang digunakan didalam jaringan 10Mbps tradisional untuk menghubungkan komputer-komputer dalam jaringan skala kecil (LAN). Pada perangkat hub, semua anggota jaringan yang terhubung dengan perangkat ini melakukan transmisi data pada jaringan (*collision domain*). Ini berarti, jika lebih dari satu komputer mengirim data kejaringan secara bersama, maka tidak satupun komputer yang dapat memanfaatkan 100% *bandwidth* jaringan yang tersedia.

5. *Switch*

Switch atau lebih dikenal dengan istilah LAN *switch* merupakan perluasan dari konsep *bridge*. Ada dua arsitektur dasar yang digunakan pada *switch*, yaitu *cut-through* dan *store-and-forward*. Secara tipikal berikut kelebihan dari switch :

a. Mampu menginspeksi paket-paket data yang mereka terima.

b. Mampu menentukan sumber dan tujuan paket yang melaluinya.

c. Mampu memforward paket-paket dengan tepat.

Switch terbagi menjadi dua tipe utama; *switch* layer-2 dan layer-3. *Switch* layer-2 bekerja pada layer *datalink model OSI* dan berdasarkan teknologi *bridging*. *Switch* tipe ini membangun koneksi logika antar port berdasarkan pada alamat MAC. *Switch layer*-3 beroperasi pada layer-3 dari OSI model dan berdasarkan teknologi *routing*.

6. *Repeater*

Repeater bekerja meregenarasi atau memperkuat sinyal-sinyal yang masuk. Pada *Ethernet* kualitas transmisi data hanya dapat bertahan dalam *range* waktu dan jangkauan terbatas, yang selanjutnya mengalami degradasi. *Repeater* akan berusaha mempertahankan integritas sinyal dan mencegah degradasi sampai paket data menuju tujuan. Adapun kelemahan *repeater*, perangkat ini tidak dapat melakukan *filter traffic* jaringan.

7. *Bridge*

Bridge adalah perangkat yang berfungsi menghubungkan *topologi bus*, dan digunakan untuk memecah jaringan yang besar. *Bridge* bekerja pada *layer data-link dari model OSI*. *Bridge* bekerja dengan mengenali alamat MAC asal

yang mentransmisikan data kejaringan dan secara otomatis membangun sebuah table *internal*.

8. *Router*

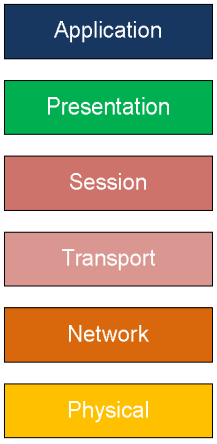
Router bekerja dengan cara yang mirip dengan *switch* dan *bridge*. Perbedaannya, *router* merupakan penyaring atau *filter* lalu litas data. Penyaringan dilakukan dengan menggunakan protokol tertentu. *Router* pada dasarnya merupakan piranti pembagi jaringan secara logical bukan fisikal. *Router* bekerja pada *layer network* dari model OSI untuk memindahkan paket antar jaringan menggunakan alamat logikalnya. *Router* memiliki tabel *routing* yang melakukan pencatatan terhadap semua alamat jaringan yang diketahui dan lintasan yang mungkin dilalui serta waktu tempuhnya. *Router* bekerja hanya jika *protocol* jaringan yang dikonfigurasikan adalah *protocol* yang *routable* seperti TCP/IP.

3.1.7 Model Referensi dan OSI Standarisasi

OSI (*Open System Interconection*) adalah salah satu standar protokol jaringan yang dikembangkan oleh ISO (*International Standardization Organization*). Untuk menyelenggarakan komunikasi berbagai macam vendor komputer diperlukan sebuah aturan baku yang standar dan disetujui berbagai pihak. Seperti halnya dua orang yang berlainan bangsa, maka untuk

berkomunikasi memerlukan penerjemah atau satu bahasa yang di mengerti oleh kedua belah pihak. Dalam dunia komputer dan telekomunikasi interpreter indentik dengan protokol. Untuk itu maka badan dunia yang menangani masalah standarisasi ISO membuat aturan baku yang dikenal dengan nama model referensi OSI (*Open System Interconnection*). Dengan demikian diharapkan semua vendor perangkat telekomunikasi haruslah berpedoman dengan model referensi ini dalam mengembangkan protokolnya.

Model referensi OSI terdiri dari tujuh lapisan, mulai dari lapisan fisik sampai dengan aplikasi. Model referensi ini tidak hanya berguna untuk produk-produk LAN saja, tetapi dalam membangun jaringan Internet sekalipun sangat diperlukan. Menurut Hasrul (2011:33).



Gambar 3.5 OSI Model
(Sumber : Diolah Sendiri)

Adapun ketujuh lapisan OSI tersebut adalah sebagai berikut :

1. **Lapisan ke-7** *Application Layer*

   Berfungsi sebagai antarmuka dengan aplikasi fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan, dan kemudian membuat pesan-pesan kesalahan, protokol yang berada dalam lapisan ini adalah HTTP, FTP, SMTP, dan NFS.

2. **Lapisan ke-6** *Presentation Layer*

   Berfungsi untuk mentranslasikan data yang hendak di transmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan. Protokol yang berada dalam level ini adalah perangkat lunak *redirector (redirector software),* seperti layanan *Workstation* (dalam Windows NT) dan juga *Network Shell* (semacam *Virtual Network Computing* (VNC) atau *Remote Desktop Protocol* (RDP)).

3. **Lapisan ke-5** *Session Layer*

   Berfungsi untuk mendefinisikan bagaiman koneksi dapat dibuat, dipelihara, atau dihancurkan. Selain itu, dilevel ini juga dilakukan resolusi nama.

4. **Lapisan ke-4** *Transport Layer*

   Berfungsi untuk memecah data kedalam paket-paket data serta memberikan nomor urut ke paket-paket tersebut sehingga dapat disusun kembali pada sisi tujuan setelah

diterima. Selain itu, pada level ini juga membuat sebuah tanda bahwa paket diterima dengan sukses (*acknowledgement*), dan mentransmisikan ulang terhadap paket-paket yang hilang ditengah jalan.

5. **Lapisan ke-3** *Network Layer*

   Berfungsi untuk mendefenisikan alamat-almat IP, membuat *header* untuk paket-paket, dan kemudian melakukan *routing* melalui *internetworking* dengan melakukan *router* dan *switch* layer-3.

6. **Lapisan ke-2** *Data Link Layer*

   Berfungsi untuk menentukan bagaimana bit-bit data dikelompokan menjadi format yang disebut sebagai *frame*. Selain itu, pada level ini terjadi koreksi kesalahan, *flow control*, pengalamtan perangkat keras (seperti halnya *Media Accsess Control Address* (MAC Address)), dan menentukan bagaimana perangkat-perangkat jaringan seperti *hub, bridge, repeater,* dan *switch* layer 2 beroperasi. Spesifikasi IEEE 802, membagi level ini menjadi dua level anak, yaitu lapisan *Logical Link Control* (LLC) dan lapisan *Media Accsess Control* (MAC).

7. **Lapisan ke-1** *Phsyical Layer*

   Berfungsi untuk mendefenisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur

jaringan (seperti halnya *Ethernet* atau *Token Ring*), topologi jaringan dan pengabelan. Selain itu, level ini juga mendefenisikan bagaimana *Network Interface Card* (NIC) dapat berinteraksi dengan media kabel atau radio.

Standarisasi masalah jaringan tidak hanya dilakukan oleh ISO saja, tetapi juga diselenggarakan oleh badan dunia lainnya seperti *International Telecomunocation Union* (ITU), *Americal National Standard Institute* (ANSI), *National Committee for Information Teknologi Standardization* (NCITS), bahkan juga oleh lembaga asosiasi profesi IEEE (*Institute of Electrical and Electronics Engineers)* dan ATM-Forum di Amerika. Pada prakteknya bahkan vendor-vendor produk LAN bahkan memakai standar yang dihasilkan IEEE.

3.1.8 Web Server

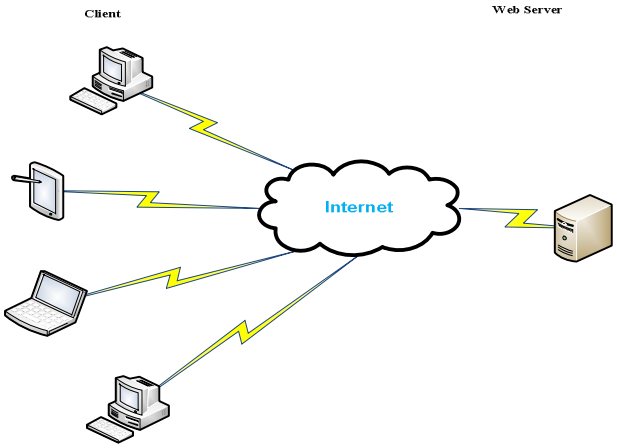
Web Server adalah potongan perangkat lunak yang mendukung berbagai protokol Web, seperti HTTP, HTTPS, dan lain – lain untuk memproses permintaan *client* (Simarmata, 2010:88).

Ada dua komponen dasar di dalam arsitektur web, yaitu *browser web* dan *server web*. *browser web* menawarkan antarmuka grafis untuk pengguna dan bertanggung jawab untuk komunikasi dengan *server web*. Protokol komunikasi antara *browser* dan *server web* mengikuti protokol HTTP yang distandarisasi.

Antarmuka antar pengguna dan *browser* adalah bahasa HTML yang terstandarisasi. Sedangkan komunikasi antara browser dan server menggunakan protokol HTTP. HTTP disebut *client / server*, dengan arti bahwa *browser* adalah *client* dan *server web* adalah *server* (Simarmata, 2010:54).

A. Cara Kerja Web Server

Web server menunggu permintaan dari *client* yang menggunakan *browser* seperti *Internet Explorer, Mozilla Firefox*, *Opera* dan program *browser* lainnya. Jika ada permintaan dari *browser*, maka *web server* akan memproses permintaan itu kemudian memberikan hasil prosesnya berupa data yang diinginkan kembali ke browser. Data ini mempunyai format yang standar, disebut dengan format SGML (Standar general markup language). Data yang berupa format ini kemudian akan ditampilkan oleh browser sesuai dengan kemampuan browser tersebut (Winarno 2010:200).



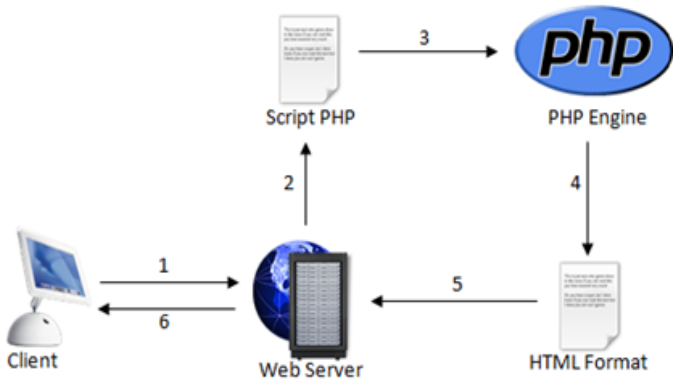
Gambar 3.6 Cara Kerja Web Server
(Sumber : Diolah Sendiri)

3.1.9 PHP (*Hypertext Preprocessor*)

Menurut Sidik (2012:4). PHP memiliki beberapa pandangan dalam mengartikannya, akan tetapi kurang lebih PHP dapat diartikan sebagai PHP: Hypertext Preeprocesor. Ini merupakan bahasa yang hanya dapat berjalan pada *server* dan hasilnya dapat ditampilkan pada *client*.

PHP adalah produk *Open Source* yang dapat digunakan secara gratis tampa harus membayar untuk menggunakannya.

Interpereter PHP dalam mengeksekusi kode PHP pada sisi *server* (disebut *server-side*), sedangkan tampa adanya *interpereter* PHP, maka semua skrip dan aplikasi PHP yang dibuat tidak dapat dijalankan. Proses eksekusi kode PHP yang dilakukan oleh *Apache Web Server* dan *interpereter* secara diagram dapat digambarkan sebagai berikut.



Gambar 3.7 Struktur Pembacaan Web Server
(Sumber : Diolah Sendiri)

PHP merupakan bahasa standar yang digunakan dalam dunia *web site*, PHP adalah bahasa pemrograman yang berbentuk skrip yang diletakan didalam server web. Jika dilihat dari sejarah mulanya PHP diciptakan dari ide *Rasmus Lerdof* untuk kebutuhan pribadinya, skrip tersebut sebenarnya dimaksudkan untuk digunakan sebagai keperluan membuat *web site* pribadi, akan tetapi kemudian dikembangkan lagi sehingga menjadi sebuah bahasa yang disebut "*Personal Home Page*", inilah awal mula munculnya PHP sampai saat ini.

3.1.10 MYSQL (*My Structured Query Lenguage*)

Menurut Nugroho (2008:91). MySQL (*My Structured Query Lenguege*) atau yang biasa dibaca mai-se-kuel adalah sebuah program pembuat dan pengelola database atau yang sering disebut dengan DBMS (*DataBase Management System*), sifat dari DBS ini adalah *Open Source*.

MySQL sebenarnya produk yang berjalan pada *platform Linux*, dengan adanya perkembangan dan banyaknya pengguna, serta lisensi dari *database* ini adalah *Open Source*, maka para pengembang kemudian merilis versi *Windows*.

Selain itu MySQL juga merupakan program pengakses *database* yang bersifat jaringan, sehingga dapat digunakan untuk aplikasi *Multi User* (Banyak Pengguna). Kelebihan lain dari MySQL adalah menggunakan bahasa *query* (permintaan) standar SQL (*Structured Query Lenguage*). SQL adalah suatu bahasa permintaan yang terstruktur, SQL telah distandarkan untuk semua program pengakses *database* seperti *Oracle*, *PosgreSQL, SQL Server* dan lain-lain.

Sebagai sebuah program penghasil *database*, MySQL tidak mungkin berjalan sendiri tampa adanya sebuah aplikasi pengguna (*Interface*) yang berguna sebagai program aplikasi pengakses database yang dihasilkan. MySQL dapat didukung oleh hampir semua program aplikasi baik yang *Open Source* seperti PHP maupun yang tidak *Open Source* yang ada *platform Windows* seperti *Visual Basic, Delphi* dan lainya.

DBS yang menggunakan bahasa SQL :

a. MySQL

b. MSQL

c. PosgreSQL

d. Oracle

e. SQL Server 97, 2000, dan lain-lain

f. Inaterbase, dan lain-lain

Program-program aplikasi yang mendukung MySQL :

a. PHP (Page Hipertext Preprosesor)

b. Borland Delphi, Borland C++ Builder

c. Visual Basic 5.0/6.0 dan .Net

d. Visual FoxPro

e. Cold Fusion, dan masih banyak lagi.

MySQL memiliki layar utama seperti layar DOS, yaitu memiliki prompt utama yang disebut mysql>. Sehingga akan kesulitan bagi pembaca yang baru pertama dan belum mengenal perintah DOS. Nugroho (2008).

3.1.11 Apache

Menurut Winarno (2010). *Apache* merupakan *web server* yang paling banyak dipergunakan di *internet.* Program ini pertama kali didesain untuk sistem operasi lingkungan UNIX. Namun demikian, pada beberapa versi berikutnya *Apache* mengeluarkan yang dapat dijalankan dengan basis *Microsoft Windows* NT.

Apache mempunyai program pendukung yang cukup banyak. Hal ini, memberikan layanan yang cukup lengkap bagi penggunanya.

B. Keuntungan *Web Server Apache*

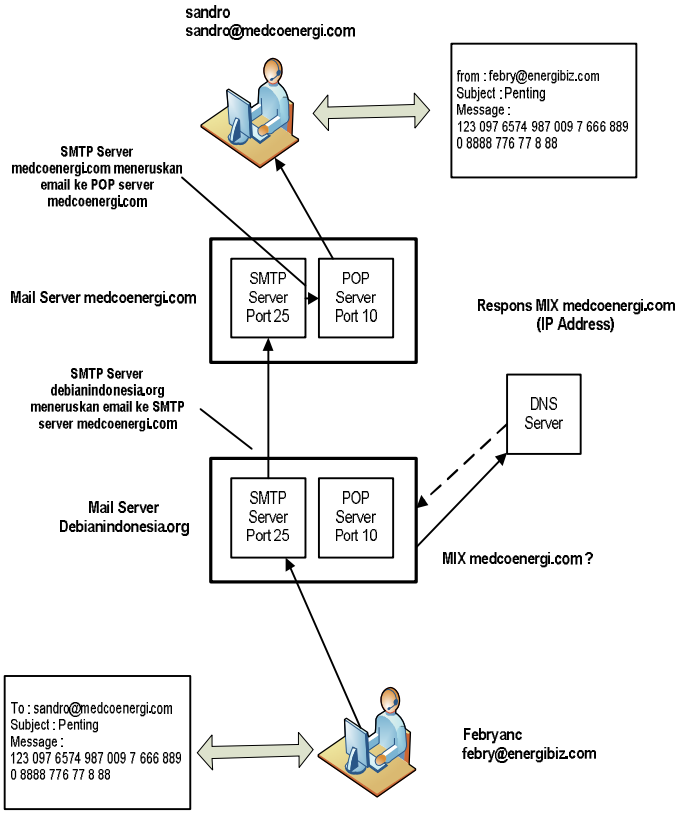
1. *Apache* termasuk dalam katagori *freeware.*
2. Mampu beroperasi berbagai *platform* sistem operasi.
3. Kemudahan dalam mengatur konfigurasinya. *Apache* mempunyai hanya empat *file* konfigurasi.
4. Mudah dalam menambahkan *peripheral* lainnya ke dalam *platform web server*.

3.1.12 E-mail (*Elektronik Mail*)

Menurut Azikin (2011). *Email* merupakan aplikasi internet untuk komunikasi dua arah. *Email* juga dapat dianalogikan dengan pengiriman surat yang lazim digunakan saat ini melalui kantor pos, atau melalui jasa pengiriman surat atau barang. Pengiriman email dilakukan melalui perangkat elektronik seperti komputer atau HP/PDA.

Proses pengiriman atau penerimaan *email* melibatkan protokol *Simple Mail Transfer Protocol* (SMPT) dan *Post Office Protocol version 3* (POP 3). Protocol SMTP bertugas untuk proses pengiriman email (*outgoing mail*) dan POP3 bertugas untuk proses penerimaan email (*ingoing mail*).

Proses pengiriman *email* secara detail dapat dilihat dari gambar berikut yang melibatkan beberapa komponen *server* seperti DNS *Server*, *mail Server* meliputi *Mail Transfer Agent* (MTA), dan POP3 server.



Gambar 3.8 Cara Kerja Emil
(Sumber : Diolah Sendiri)

3.1.13 Keamanan Informasi

A. Aspek-Aspek Keamanan Komputer

Menurut Ariyus (2009:12). Keamanan computer meliputi beberapa aspek diantaranya :

a. *Authentication* : agar penerima informasi dapat memastikan keaslian pesan tersebut datang dari orang yang dimintai informasi. Dengan kata lain informasi tersebut benar-benar dari orang yang dikehendaki.
b. *Integrity* : keaslian pesan yang dikirim melalui sebuah jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi oleh orang yang tidak berhak dalam perjalanan informasi tersebut.
c. *Nonrepudiation* : merupakan hal yang bersangkutan dengan orang yang mengirim. Si pengirim tidak dapat mengelah bahwa dialah yang mengirim informasi tersebut.
d. *Authority* : informasi yang berada pada system jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak atas akses tersebut.
e. *Confidentiality* : merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Confidentiality biasanya berhubungan dengan informasi yang diberikan kepada pihak lain.
f. *Privacy* : merupakan lebih kearah data-data yang sifatnya private (pribadi).
g. *Availability* : ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. System informasi

yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi.

h. *Access Control* : aspek ini berhubungan dangan cara pengaturan akses kepada informasi. Hal ini biasanya berhubungan dengan masalah authentication dan juga privacy. Access Control sering kali dilakukan menggunakan kombinasi user id dan password atau dengan menggunakan mekanisme lainnya.

B. Aspek-Aspek Ancaman Keamanan

a. Interruption

Merupakan suatu ancaman terhadap availability. Informasi dan data yang ada dalam system computer dirusak dan dihapus sehingga jika dibutuhkan, data atau informasi tersebut tidak ada lagi.

b. Interception

Merupakan ancaman terhadap kerahasiaan (secrecy). Informasi yang ada disadap atau orang yang tidak berhak mendapatkan akses ke computer di mana informasi tersebut disimpan.

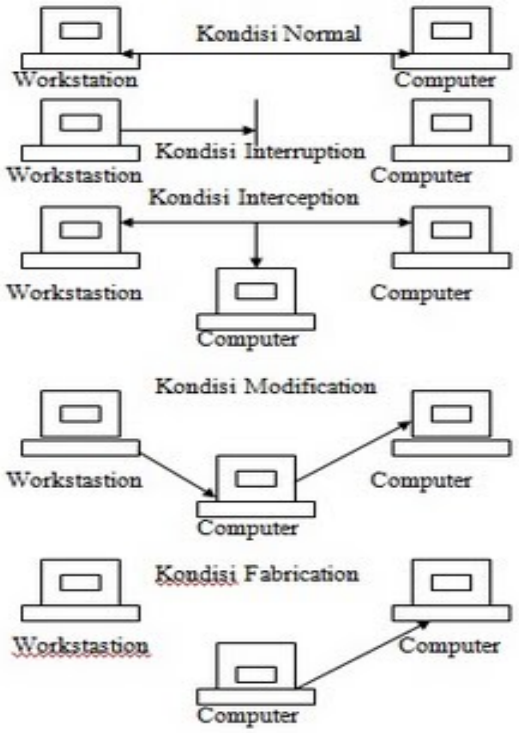
c. Modifikasi

Merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil menyadap lalu lintas informasi

yang sedang dikirim dan diubah sesuai keinginan orang tersebut.

d. Fabrication

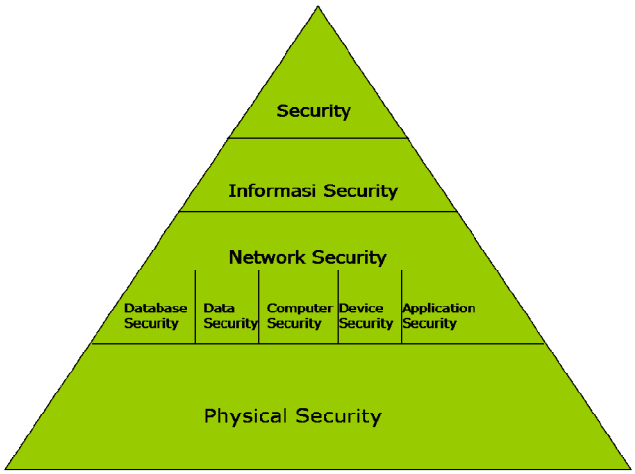
Merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil meniru (memalsukan) suatu informasi yang ada sehingga orang yang menerima informasi tersebut menyangka informasi tersebut berasal dari orang yang dikehendaki oleh si penerima informasi tersebut.



Gambar 3.9 Aspek-Aspek Ancaman Keamanan
(Sumber : Diolah Sendiri)

C. Metedologi Keamanan

Keamanan computer memiliki cabang yang sangat banyak. Dalam masalah keamanan, pertimbangan-pertimbangan untuk mengamankan system harus diperhatikan, seperti keamanan database, keamanan data, keamanan computer, keamanan perangkat komputer, keamanan aplikasi, keamanan jaringan, dan keamanan informasi.



Gambar 3.10 *Security Methodology*
(Sumber : Diolah Sendiri)

Metodologi keamanan computer merupakan sesuatu yang sangat penting dalam masalah keamanan komputer karena semua elemen saling berkaitan.

a. Keamanan-**Level 0**

Keamanan fisik merupakan keamanan tahap awal dari computer security. Jika keamanan fisik tidak terjaga dengan baik, maka data-data, bahkan hardware computer sendiri, tidak dapat diamankan.

b. Keamanan-**Level 1**

Pada gambar diatas, peringkat terdiri dari database security, data security, keamanan dari PC itu sendiri, device, dan application.

c. Keamanan-**Level 2**

Keamanan level 2 adalah network security. Computer yang terhubung dengan jaringan, baik itu LAN, WAN, maupun Internet, sangat rawan dalam masalah keamanan karenan computer server bisa diakses menggunakan computer client, baik itu merusak data, mencuri data, maupun melakukan perbuatan-perbuatan lainnya.

d. Keamanan-**Level 3**

Keamanan level 3 adalah information security. Maksud dari keamanan informasi disini adalah keamanan informasi-informasi yang kadang tidak begitu dipedulikan oleh administrator atau pegawai, seperti memberikan password keteman, kertas-kertas bekas transaksi.

e. Keamanan-**Level 4**

Keamanan level 4 merupakan keamanan secara keseluruhan dari computer. Jika level 1-3 sudah dapat dikerjakan dengan baik, maka otomatis keamanan level 4 sudah terpenuhi. Akan tetapi jika salah satu dari level

tersebut belum bisa terpenuhi, maka masih ada lubang keamanan yang bisa diakases.

D. Mencegah

Mencegah terjadinya suatu serangan terhadap system. Dengan demikian kita perlu memperhatikan desain dari system, aplikasi yang dipakai, dan human (admin).

a. Desain Sistem

Desain system yang baik tidak meninggalkan lobang-lobang yang memungkinkan terjadinya penyusupan setelah system tersebut siap dijalankan.

Salah satu contoh kesalahan dari desain system adalah algoritma enkripsi Ceasar cipher, dimana karakter digeser 3 huruf atau beberapa huruf. Meskipun diimplementasikan dengan programming yang sangat teliti dan secanggih apapun, siapa pun yang mengetahui algoritma nya dapat memecahkan enkripsi tersebut.

b. Aplikasi yang Dipakai

Aplikasi yang dipakai sudah diperiksa dengan seksama untuk mengetahui apakah program yang dipakai dalam system tersebut tidak memiliki backdoor (system dapat diakses tampa harus melalui prosedur yang seharusnya) dan apakah aplikasi sudah mendapatkan kepercayaan dari banyak orang.

c. Manajemen

Pada dasarnya untuk membuat suatu system yang secure tidak lepas dari bagaimana mengelola suatu system dengan baik. Dengan demikian, persyaratan gold practice standard seperti Standard Operating Procedure (SOP) dan Security Policy harusnya diterapkan di samping memikirkan hal teknologinya.

d. Manusia (Administrator)

Manusia adalah salah satu yang sangat penting, tetapi sering kali dilupakan dalam pengembangan teknologi informasi. Begitu juga dalam pengembangan system keamanan.

3.1.14 Kriptografi

Cryptography berasal dari Bahasa Yunani. Menurut bahasanya, istilah tersebut terdiri dari kata *kripto* dan *graphia*. *Kripto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan). Menurut *teminologinya*, *cryptography* adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain. (Ariyus,2009:77).

1. komponen kriptografi

pada dasarnya, kriptografi terdiri dari beberapa komponen seperti

a. *Enkripsi*

Enkripsi merupakan hal yang sangat penting dalam kriptografi sebagai pengamanan atas data yang dikirim agar rahasianya terjaga. Pesan aslinya disebut plaintext yang diubah menjadi kode-kode yang tidak dimengerti.

b. *Dekripsi*

Merupakan kebalikan dari enkripsi, pesan yang telah dienkripsi dikembalikan kedalam bentuk asalnya (plaintext), yang disebut dekripsi pesan.

c. Kunci

Kunci yang dimaksud disini adalah kunci yang dipakai untuk melakukan *enkripsi* dan *dekripsi*. Kunci terbagi menjadi dua bagian, yakni kunci pribadi (*private key*) dan kunci umum (*public key*).

d. *Chipertext*

Merupakan suatu pesan yang sudah melalui proses enkripsi. Pesan yang ada pada *chipertext* tidak bisa dibaca karena memiliki karakter-karakter yang tidak bermakna.

e. Plaintext

Sering juga disebut *cleartext*; merupakan suatu pesan yang bermakna yang ditulis atau diketik dan

plaintext itulah yang akan diproses menggunakan algortima kriptografi agar menjadi *ciphertext*.

f. Pesan

Pesan bisa berupa data atau informasi yang dikirim (melalui kurir ataupun saluran komunikasi data) atau yang disimpan di dalam media perekam (kertas, *storage*, dan sebagainya).

g. *Cryptanalysis*

Bisa diartikan sebagai analisis sandi atau suatu ilmu untuk mendapatkan plaintext tampa harus mengetahui kunci secara wajar. Jika suatu chipertext berhasil menjadi plaintext tanpa harus menggunakan kunci yang sah, maka proses tersebut dinamakan breaking code yang dilakukan oleh para *cryptanalys*.

h. System kriptografi kunci simetris dan tak simetris

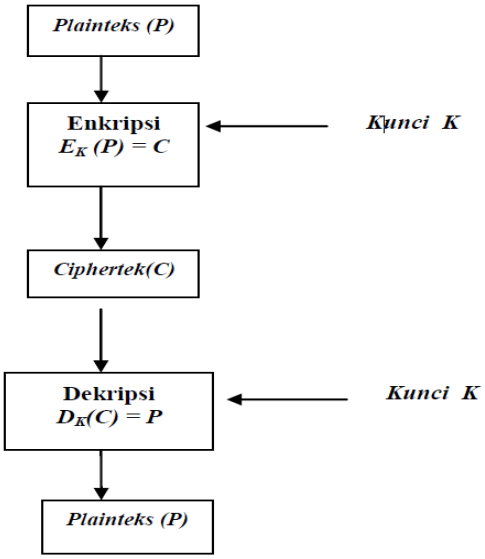
Sistem kriptografi merupakan kumpulan yang terdiri dari plaintext, ciphertext, kunci, enkripsi serta dekripsi.(Stinson, 2006 :1)

Berdasarkan kunci yang digunakan dalam proses enkripsi dan dekripsi, kriptografi dapat dibedakan menjadi kriptografi kunci simetri dan kriptografi kunci tak simetri. Kriptografi kunci tak

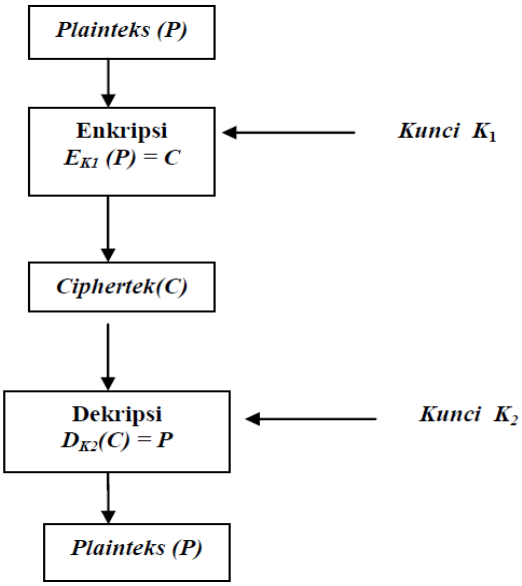
simetri ini sering disebut dengan kriptografi kunci publik.

Kriptografi kunci simetri, sering disingkat menjadi kriptografi simetri, kunci yang digunakan pada proses enkripsi dan dekripsi adalah sama. Oleh karena itu, sebelum saling berkomunikasi kedua belah pihak harus melakukan kesepakatan dalam menentukan kunci yang akan digunakan. Keamanan menggunakan sistem ini terletak pada kerahasiaan kunci yang akan digunakan. Sedangkan dalam sistem kriptografi kunci publik, kunci yang digunakan dalam proses enkripsi dan dekripsi berbeda. Sistem ini terdapat dua buah kunci, yaitu kunci publik dan kunci privat. Kunci publik digunakan untuk proses enkripsi, dan kunci privat digunakan untuk mendekripsikan pesan. Kunci publik bersifat tak rahasia, sedangkan kunci privat hanya boleh diketahui oleh penerima pesan.

Dibawah ini akan diberikan gambar tentang skema kriptografi simetri dan kriptografi kunci public.



Gambar 3.11 Skema Kriptografi Simetris
(Sumber : Diolah Sendiri)



Gambar 3.12 Skema Kriptografi Kunci Publik
(Sumber : Diolah Sendiri)

3.1.15 Algoritma El-Gamal

Menurut Ariyus (2008:163). ELGamal adalah suatu *public key cryptosystem* yang dibuat pada tahun 1985. Algoritma ElGamal digunakan untuk melakukan *enkripsi* dan tanda tangan digital. Keamanan dari algoritma ElGamal terletak pada susahnya perhitungan logaritma yang terpisah pada GF (p) ketika p merupakan bilangan prima yang besar. Faktorisasi utama dari logaritma yang terpisah dianjurkan untuk diimplementasikan pada RSA dan ElGamal *cryptosystem*.

Pada RSA *cryptosystem*, penggunaan mempunyai tiga bilangan integer e, d dan n, dimana n = pq dengan dua bilangan prima yang besar p dan q, dan ed=1 (mod φ (n)), φ menjadi fungsi Euler totient. Pengguna A memiliki kunci public yang berisi dua (e_A,n_A) dan kunci rahasia d_A; yang sama, penguna B memiliki (e_B,n_B) dan d_B, untuk mengenkripsi pesan m ke B, A, pengguna B menggunakan kunci public untuk mendapatkan teks-kode $c \equiv meB\ (mod\ nB)$, jika A ingin mengirim yang sudah ditanda-tangani ke B, A menanda-tangani pesan m menggunakan kunci rahasia d_A seperti $c \equiv mdA\ (mod\ nA)$.

System ElGamal memilih satu bilangan prima p dan dua bilangan acak g dan x, g < P dan x < p, jika x adalah kunci rahasia. Bilangan acak g adalah akar dari modulo p. kunci public digambarkan oleh y, g dan p, dengan perhitungan $y \equiv$

$gx\ (mod\ p)$. Untuk mengenkripsi pesan m, 0 < m _ p-1, pertama mengambil suatu bilangan acak k seperi gcd (k, p -1) = 1. Teks-kode dienkripsikan dengan dua penanda (r,s) seperti di bawah ini:

$r \equiv gk\ (mod\ p)$

$s \equiv (ykm\ (mod\ p))(m\ (mod\ p-1))$

Untuk mendekripsi pesan m, dibagi s dengan r_x seperti $\frac{s}{rx} \equiv m\ (\mathrm{mod}\ p-1)$ dan untuk mendapatkan tanda tangan dari pesan m, yang pertama dilakukan adalah memilih suatu bilangan acak k seperti gcd $(k, p-1) = 1$ dan menghitung $m \equiv xr + ks\ (mod\ p-1)$ menggunakan algoritma Euclidean yang diperluas unruk memacahkan S. teknik perhitungan dasar untuk enkripsi dan tanda tangan digital menggunakan algoritma ElGamal dengan dua kunci cryptosystem. Algoritma enkripsi ElGamal seperti berikut ini :

Kunci umum :

p (bilangan prima)

$g, x < p$ (dua bilangan acak)

$y \equiv gx\ (mod\ p)$

$y, g\ dan\ p$: kunci publik

Kunci rahasia :

$x < p$

Enkripsi :

k : bilangan acak gcd $(k, p-1) = 1$

$r \equiv gk\ (mod\ p)$

$s \equiv (yk\ (mod\ p))(m\ (mod\ p-1))$

Dekripsi :

$m \equiv \frac{s}{rx}\ (\ mod\ p\ ), 0_{m_p} - 1$

Contoh :

Enkripsi ElGamal diasumsikan sebagai berikut :

p = 11 (bilangan prima)

g = 4 (bilangan acak g < p)

x = 8 (kunci rahasia x < p)

kemudian dihitung :

$y \equiv g^x\ (mod\ p) \equiv 4^8\ (mod\ 11) \equiv 9$

Kunci public adalah y = 9, q = 4 dan p = 11. Kunci rahasia x = 8. Untuk mengenkripsi pesan m = 5, pertama pilih bilangan acak k = 7, $\gcd(k, p-1) = \gcd(7,10) = 1$ dengan perhitungannya :

$r \equiv g^k\ (mod\ p) \equiv 4^7\ (mod\ 11) \equiv 5$

$s \equiv (y^x\ (mod\ p))(m\ (mod\ p-1))$

$\equiv (\ 9^7\ (mod\ 11))(5\ (mod\ 10) \equiv 4\ \times 5\ \equiv 20$

Untuk mendekripsi pesan m, pertama dihitung :

$r_x (mod\ p) \equiv 58\ (mod\ 11) \equiv 4$

Dan rasionya:

$$m \equiv \frac{s}{r_x\ (mod\ p)} \equiv 20/4 \equiv 5$$

Pesan m sudah selesai dienkripsi dengan menggunakan algoritma enkripsi ElGamal.

3.1.16 Debian

a. Pengertian Debian

Menurut Ahmad (2005:8) Debian adalah distribusi yang mengutamakan kestabilan dan keandalan meskipun mengorbankan aspek kemudahan dan kemutakhiran program. Debian menggunakan .deb dalam paket instalasi programnya.

b. Sejarah Debian

Pertama kali debian diperkenalkan oleh Ian Murdoch, seorang mahasiswa dari Universitas Purdue, Amerika Serikat, pada tanggal 16 Agustus 1993, Nama Debian berasal dari kombinasi nama mantan-kekasihnya [DEB]ra dan namanya sendiri [IAN] Murdoch. Pada awalnya, Ian memulainya dengan memodifikasi distribusi SLS (Softlanding Linux Sistem). Namun, dia tidak puas dengan SLS yang telah dimodifikasi olehnya sehingga dia berpendapat bahwa lebih baik membangun sistem (distribusi Linux) dari nol (Dalam hal ini, Patrick Volkerding juga berusaha memodifikasi SLS. Dia

berhasil dan distribusinya dikenal sebagai Slackware. Proyek debian tumbuh lambat pada awalnya dan merilis versi 0.9x di tahun 1994 dan 1995. Kemudian deb adalah perpanjangan dari paket perangkat lunak Debian format, dan nama yang paling sering digunakan untuk paket-paket binari seperti itu. Seperti Deb istilah bagian dari Debian, itu berasal dari nama Debra, kemudian pacar dan sekarang mantan istri pendiri Debian Ian Murdock.

c. Kelebihan Debian

1. Debian adalah distribusi yang mengutamakan kestabilan dan keandalan.
2. Debian adalah sistem operasi yang *free,* legal dan dapat dikembangkan dengan paket-paket pendukungnya.
3. Debian sejak awal dapat berjalan pada beberapa processor, sampai *release* terbaru, debian dapat berjalan pada 11 arsitektur processor.
4. Debian memiliki kernel independent yang dapat mendukung banyak kernel, sehingga jika suatu saat kernel linux tidak *free* lagi, maka debian dapat menggunakan kernel lain yang masih *free.*
5. Keunikan debian adalah aturan *release* distro debian, jika ada versi baru pada debian, versi lama tetap dapat diakses,

sedangkan versi terbaru bisa dengan mudah digunakan siapa saja.

3.2 Hasil Penelitian Terdahulu

Tabel 3.2 Hasil Penelitian Terdahulu

No	Nama Peneliti	Judul Penelitian & Tahun	Hasil Penelitian
1	Agus Perdamean	Implementasi Algoritma El Gamal dan Digital Signature untuk Pengamanan Data Pada CV. Tridian Hariwangsa Tahun 2011	Dengan steganoraphy, keamanan pesan yang dikirim berupa pesan yang dimasukan kedalam image, sehingga orang yang tidak bertanggung jawab yang bermaksud mengambil pesan tersebut akan mengalami kesulitan untuk melakukan pelepasan pesan yang telah dimasukan kedalam images.
2	Abdul Ghafur	Implementasi Algoritma ElGamal untuk Pengamanan Email Tahun 2010	Semua karakter pada body email dapat dienkripsi dan didekripsi dengan sempurna dengan algoritma elgamal, hasil chiperrtext dari proses enkripsi kriptografi menggunakan algortima elgamal ini lebih panjang dari plaintext nya, namun tidak mempengaruhi terhadap proses pengiriman email, kelebihan dari algoritma elgamal adalah proses enkripsi pada plaintext yang sama akan menghasilkan chippertext yang berbeda, namun pada proses dekripsinya menghasilkan plaintext yang sama.

BAB IV

METODE PENELITIAN

4.1. Lokasi dan Waktu Penelitian

Lokasi dan waktu penelitian yang dilakukan penulis pada penelitian di PT Medco E & P Indonesia Blok Rimau Asset (Kaji-Semoga).

4.1.1. Lokasi Penelitian

Penelitian dilakukan di salah satu stasiun cabang PT Medco E&P Indonesia, yaitu di lapangan Kaji Semoga Blok Rimau tepatnya pada Departemen ISBRD yang terletak kurang lebih 111 KM dari kota Palembang, tepatnya di Desa Bonot, Kecamatan Lais, Kabupaten Musi Banyuasin, Provinsi Sumatera Selatan. Lapangan Kaji Semoga ini terletak pada koordinat 1044’ , 21,94’’ Bujur Timur dan 002 49 14,43’’ Lintang Selatan.

4.1.2. Waktu Penelitian

Waktu penelitian berjalan selama 1 (satu) bulan, mulai dari tanggal 23 April sampai dengan tanggal 23 Mei 2012.

4.2. Jenis Data

Dalam penelitian ini dibutuhkan data-data yang relevan dan objektif untuk bisa menganalisis masalah dan menyelesaikan permasalahan yang diteliti, dalam penulisan skripsi ini penulisan menggunakan beberapa jenis data dalam pengumpulan data, yang terdiri dari:

4.2.1. Data Primer

Menurut Kuncoro (2009:148), data Primer adalah data yang diperoleh dengan survei lapangan yang mengunakan semua metode pengumpulan data original.

Data primer dalam penulisan skripsi ini didapat oleh penulis secara langsung dari Pembina riset pada PT Medco E&P Indonesia Blok Rimau Asset tepatnya pada Departemen ISBRD yaitu data-data yang berupa topologi jaringan, system pengiriman email, jumlah account yang memiliki akses email, dan security policy yang terkait masalah email.

4.2.2. Data Sekunder

Menurut Kuncoro (2009:148), data Sekunder adalah data yang telah dikumpulkan oleh lembaga pengumpul data dan dipublikasikan kepada masyarakat pengguna data.

Data sekunder dalam penulisan skripsi ini didapat oleh penulis dari PT Medco E&P Indonesia Blok Rimau Asset berupa sejarah singkat, visi dan misi, serta struktur organisasi perusahaan.

4.3. Teknik Pengumpulan Data

Adapun metode pengumpulan data yang digunakan dalam penyusunan tugas laporan ini, yaitu :

a. Metode Pengamatan (Observasi)

Menurut Made (2006:37), *observasi* adalah metode pengumpulan data dimana penulis laporan atau kolaboratornya mencatat informasi sebagaimana yang mereka saksikan selama disana.

Metode ini dilakukan penulis dengan cara mengamati bagaimana metode yang digunakan pada *Mail Server* di PT Medco E&P Indonesia Blok Rimau Asset.

b. Metode Wawancara (*interview*)

Menurut Made (2006:37), wawancara adalah proses memperoleh keterangan untuk tujuan membuat laporan dengan cara tanya jawab dan tatap muka antara sipenanya atau pewawancara dengan sipenjawab atau *responder*.

Metode wawancara ini dilakukan penulis tanya jawab langsung dengan kepala umum Departemen ISBRD yaitu bapak Trisakti Herlambang. pada PT Medco E&P Indonesia Blok Rimau Asset, mengenai metode pengiriman email.

4.4. Jenis Penelitian

Dalam hal ini jenis penelitian yang dipilih penulis yaitu jenis penelitian eksploratif (*exploratife research*). Penelitian eksploratif merupakan penelitian yang bertujuan untuk memberikan arahan bagi penelitian selanjutnya.

Dalam praktek, penelitian eksploratife bisa dilakukan dengan empat prosedur, yaitu :

a. Teknik informan kunci (*key-informant technique*)

Metode ini dilakukan dengan cara mencari dan mewawancarai beberapa orang ahli atau informan kunci dibidang yang berhubungan dengan situasi yang akan diteliti.

b. *Focus Group Interview* atau *Focus Group Discussion* (FGD)

Cara ini dilakukan dengan cara membuat forum diskusi yang biasanya terdiri dari 8 sampai 12 orang. Forum diskusi ini diberi suatu topik yang disesuaikan dengan penelitian yang dibuat dalam situasi yang informal dengan dipimpin oleh seorang moderator yang sudah terlatih dengan baik (well-trained).

c. Analisis Data Sekunder (*Secondary-data Analysis*)

Penelitian eksploratif juga bisa mengambil data sekunder, yaitu pengumpulan data dari data yang sudah dipublikasikan. Dengan cara ini, akan menghemat waktu dan biaya yang diperlukan.

d. Metode Studi Kasus (*Case Study Method*)

Metode studi kasus merupakan pengujian yang mendalam terhadap unit yang berkepentingan, seperti pelanggan atau konsumen, took, penjual,

perusahaan, dan area pasar. Dengan metode ini, si peniliti bisa memperoleh informasi secara detail tentang subjek yang diteliti.

4.5. Teknik Pengembangan Sistem

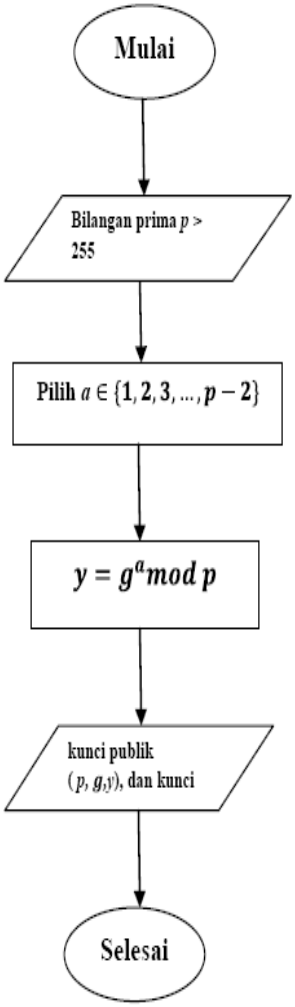
Alur dan teknik pengembangan sistem terdiri dari alur pembuatan kunci, alur enkripsi pesan dan alur dekripsi pesan.

4.5.1. Alur Pengembangan Aplikasi Keamanan Email

4.5.1.1. Model Alur Proses

Model Alur Proses menggunakan *Flowchart*, yang menggambarkan alur pengembangan aplikasi keamanan email. *Flowchart* menggambarkan secara grafik dari langkah-langkah dan urut-urutan prosedur dari suatu program. Flowchart menolong analis dan programmer untuk memecahkan masalah kedalam segmen-segmen yang lebih kecil dan menolong dalam menganalisis alternatif-alternatif lain dalam pengoperasian.

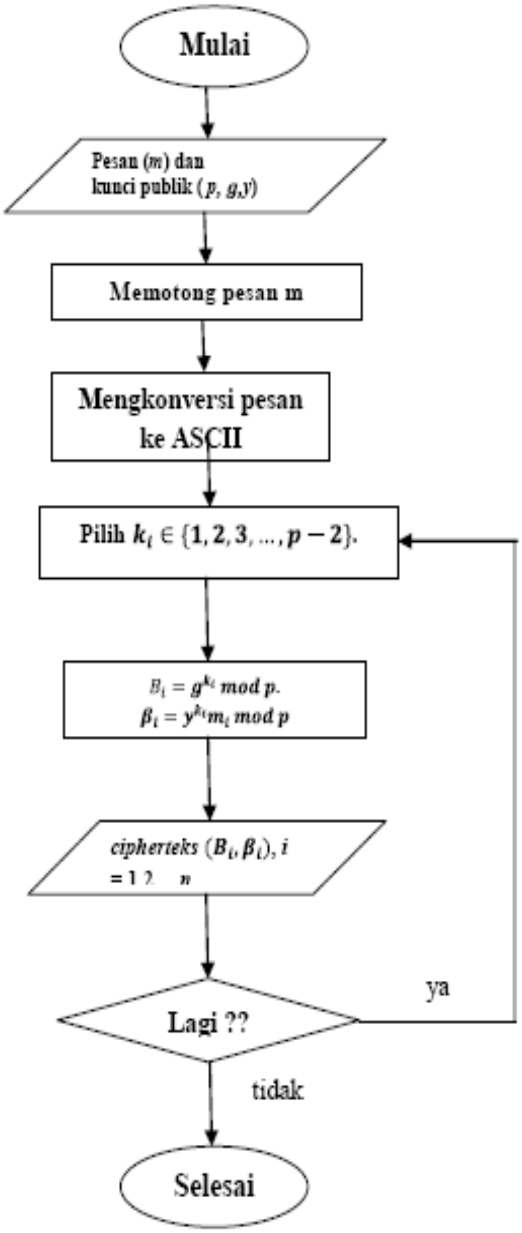
A. Alur pembentukan Kunci



Gambar 4.1 Proses Pembentukan Kunci

(Sumber : Diolah Sendiri)

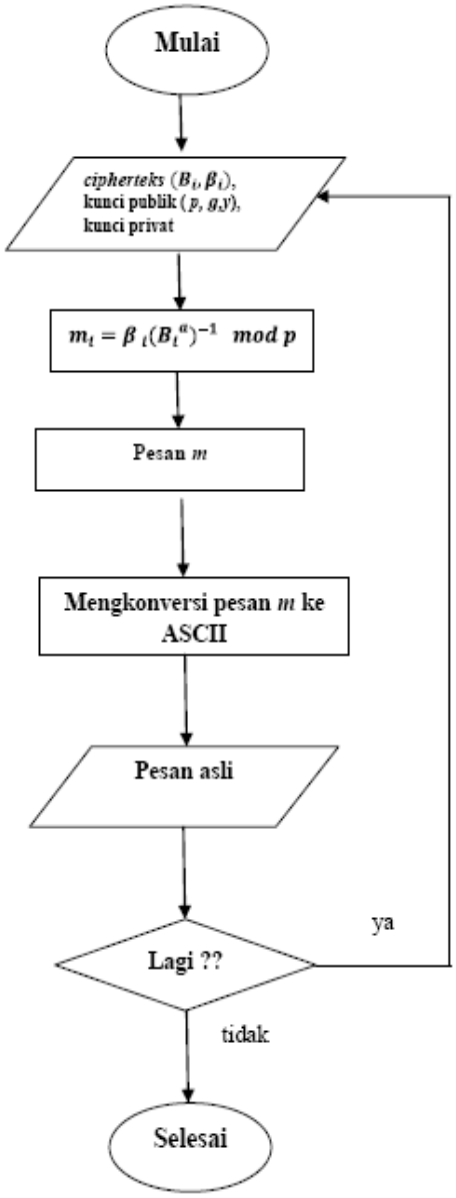
B. Alur Enkripsi Pesan



Gambar 4.2 Proses Enkripsi

(Sumber : Diolah Sendiri)

C. Alur Dekripsi Pesan

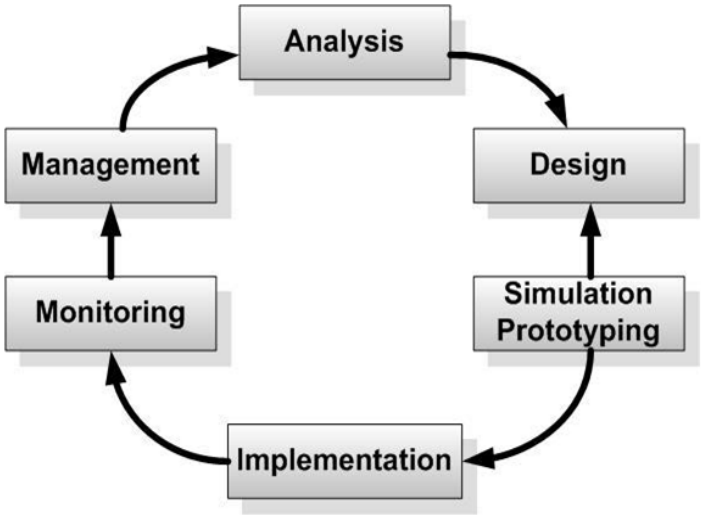


Gambar 4.3 Proses Dekripsi

(Sumber : Diolah Sendiri)

4.5.2. Teknik Pengembangan Sistem

Teknik pengembangan sistem yang penulis gunakan yaitu NDLC (*Network Development Life Cycle).*



Gambar 4.4 *Network Development Life Cycle* (NDLC)

(Sumber Diolah Sendiri)

1. Analisis

Tahap awal ini dilakukan untuk menganalisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan user, dan analisa topologi atau jaringan yang sudah ada saat ini. Metode yang bisa digunakan pada tahap ini diantaranya :

a. Wawancara

Wawancara dilakukan dengan pihak terkait melibatkan dari struktur manajemen atas sampai ke level bawah atau operator agar mendapatkan data yang konkrit dan lengkap.

Dalam hal ini wawancara secara langsung dengan Pembina riset pada PT Medco E&P Indonesia Blok Rimau Asset tepatnya pada Departemen ISBRD yaitu data-data yang berupa topologi jaringan, system pengiriman email, jumlah account yang memiliki akses email, dan security policy yang terkait masalah email.

b. Survey Langsung Kelapangan

Pada tahap analisis juga biasanya dilakukan survey langsung kelapangan untuk mendapatkan hasil sesungguhnya dan gambaran seutuhnya sebelum masuk ke tahap desain, survey biasa dilengkapi dengan alat ukur atau metode yang sesuai kebutuhan untuk mengetahui detail yang dilakukan.

c. Membaca Manual atau Blueprint Dokumentasi

Pada analisis awal ini juga dilakukan dengan mencari informasi dari manual-manual atau blueprint dokumentasi yang mungkin pernah dibuat sebelumnya. Sudah menjadi keharusan

dalam setiap pengembangan suatu sistem dokumentasi menjadi pendukung akhir dari pengembangan tersebut, begitu juga pada project *network*, dokumentasi menjadi syarat mutlak setelah sistem selesai dibangun.

d. Menelaah Setiap Data yang Didapat dari Data-data Sebelumnya

Maka perlu dilakukan analisa data tersebut untuk masuk ke tahap berikutnya. Adapun yang bisa menjadi pedoman dalam mencari data pada tahap analisis ini adalah ;

1. *User*

Jumlah *user*, kegiatan yang sering dilakukan, level teknis *user.*

2. Media *Hardware* dan *Software*

Peralatan yang ada, status jaringan, ketersedian data yang dapat diakses dari peralatan, aplikasi *software* yang digunakan

a. Data :

Jumlah pelanggan atau pegawai , jumlah inventaris sistem, sistem keamanan yang sudah ada dalam mengamankan data, media *web server* yang digunakan.

b. *Network* :

Konfigurasi jaringan, protocol, monitoring *network* yang ada saat ini, harapan dan rencana pengembangan kedepan.

c. Perencanaan fisik :

Masalah tata letak, ruang khusus *hardware*, sistem keamanan yang ada, dan kemungkinan akan pengembangan kedepan**.**

2. Desain

Dari data-data yang didapatkan sebelumnya, tahap Desain ini akan membuat gambar desain topologi jaringan interkoneksi yang akan dibangun, diharapkan dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan yang ada.

Desain ini dilakukan penulis dengan cara mendesain topologi yang digunakan, yaitu topologi *star*.

3. *Simulation Prototype*

beberapa *networker's* akan membuat dalam bentuk simulasi dengan bantuan Tools khusus di bidang network seperti *Packet Tracert, Netsim*, dan sebagainya, hal ini dimaksudkan untuk melihat kinerja awal dari network yang akan dibangun dan sebagai bahan presentasi. karena keterbatasan perangkat lunak simulasi ini, banyak para *networker's* yang hanya menggunakan alat Bantu tools VISIO untuk membangun topology yang akan didesain.

4. Implemensi

Tahapan ini akan memakan waktu lebih lama dari tahapan sebelumnya. Dalam implementasi *networker's* akan menerapkan semua yang telah direncanakan atau didesain sebelumnya. dan ditahap inilah akan diuji dilapangan untuk menyelesaikan masalah teknis dan non teknis.

5. Monitoring

setelah implementasi tahapan monitoring merupakan tahapan yang penting, agar jaringan komputer dan komunikasi dapat berjalan sesuai dengan keinginan dan tujuan awal dari user pada tahap awal analisis, maka perlu dilakukan kegiatan monitoring. Monitoring bisa berupa melakukan pengamatan pada ;

a. Infrastruktur hardware : dengan mengamati kondisi reliability atau kehandalan sistem yang telah dibangun.

b. Memperhatikan jalannya paket data di jaringan (pewaktuan, latency, peektime,troughput)

6. Manajemen

Manajemen atau pengaturan, salah satu yang menjadi perhatian khusus adalah masalah Policy, kebijakan perlu dibuat

untuk membuat atau mengatur agar sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama dan unsur *reliability* terjaga. *Policy* akan sangat tergantung dengan kebijakan level *management* dan strategi bisnis perusahaan tersebut. IT sebisa mungkin harus dapat mendukung atau *alignment* dengan strategi bisnis perusahaan.

BAB V

HASIL DAN PEMBAHASAN

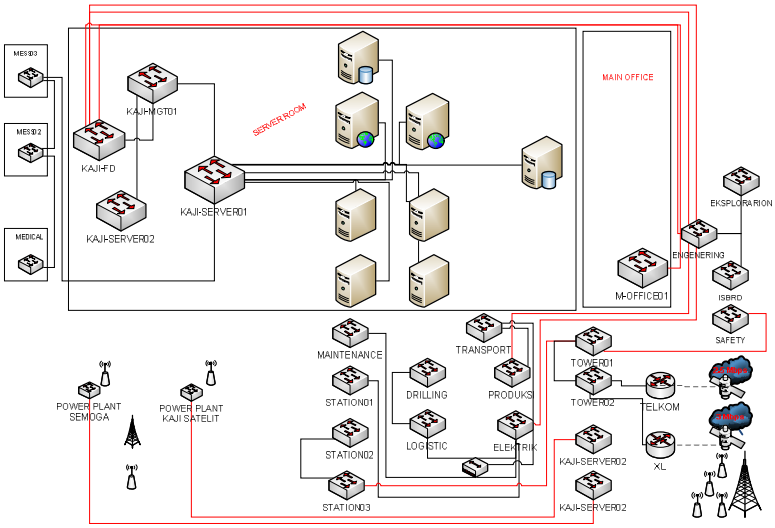
5.1 Hasil Penelitian

5.1.1 Analisis Sistem yang Digunakan

1. Prosedur dan Topologi Jaringan

Prosedur jaringan komputer pada PT. Medco E&P Indonesia Blok Rimau Asset (Kaji-Semoga) memiliki jaringan yang dihubungkan menggunakan pemancar satelit dari Provider XL (3 Mbps) dan Telkom (2,5 Mbps).

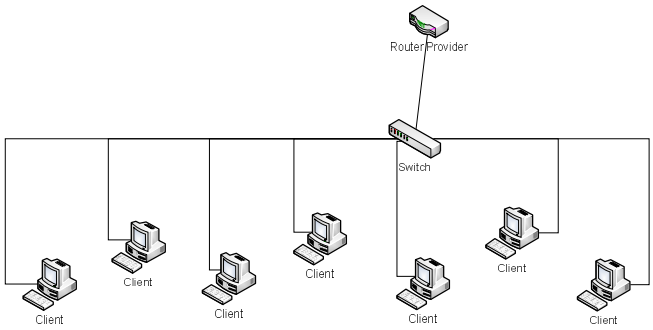
Dibawah ini gambar umum dari topologi jaringan yang sudah tersedia pada PT. Medco E&P Indonesia Blok Rimau Asset.



Gambar 5.1. Topologi Jaringan PT. Medco E&P Indonesia
(Sumber : Diolah Sendiri)

2. Terminologi Jaringan

Pada PT Medco E&P Indonesia Blok Rimau Asset sendiri menggunakan topologi jaringan star. pada dasarnya kinerja jaringan pada PT Medco E&P Indonesia sendiri memfokuskan pada kantor pusat dimana setiap kali ingin melakukan koneksi kekantor cabang yang lain otomatis system yang ada akan langsung merouting ke kantor pusat lalu bisa terkoneksi ke kantor cabang yang ingin di hubungi. Jadi kantor pusat tersebut di ibaratkan sebagai switch sebagai jembatan penghubung ke kantor cabang yang ada dan terminology yang digunakan saat ini adalah LAN (*Local Area Network*).



Gambar 5.2. Terminologi Jaringan PT. Medco E&P Indonesia
(Sumber : Diolah Sendiri)

3. Teknologi Jaringan

Teknologi jaringan yang digunakan pada PT Medco E&P Indonesia Blok Rimau Asset (Kaji-Semoga) yaitu menggunakan teknologi BTS (*Base Transceiver Station)*

dengan menggunakan Tower SST (*Self Supporting Tower*) dari provider Telkom (2,5 Mbps) dan XL (3 Mbps).

4. Sistem Operasi

   Sistem Operasi yang digunakan pada PT Medco E&P Indonesia pada ruang lingkup Departemen ISBRD menggunakan Sistem Operasi Windows Server 2008, dan Windows Xp sebagai Sistem Operasi client.

5.1.2 Permasalahan dan Kendala

PT Medco E&P Indonesia (Rimau Asset) menggunakan berbagai saranah komunikasi untuk pertukaran informasi yang digunakan dalam menunjang efisiensi perusahaan yaitu salah satunya adalah email. email digunakan sebagai sarana pengiriman data baik itu hanya dalam ruang lingkup Rimau Asset (*internal*), maupun pengiriman keluar (*eksternal*).

Pada PT Medco E&P Indonesia (Rimau Assets) jumlah *account email* yang digunakan sebanyak 364 *acount* dengan *scope* pekerjaan sharing informasi meliputi dua *domain* utama (medcoenergi.com dan energibiz.com). standarisasi keamanan selama ini menggunakan *protocol* SSL dengan enkripsi 128 bit.

Standar keamanan ini sebenarnya sudah cukup untuk pertukaran informasi secara umum, tetapi masih belum optimal untuk pengiriman data-data yang sifatnya sensitive atau rahasia.

5.1.3 Alternatif Solusi Masalah

Untuk meningkatkan keamanan dari *email* pada PT Medco E&P Indonesia Blok Rimau Asset, maka penulis berkeinginan merancang sebuah aplikasi *email client* yang dapat digunakan dalam mengenkripsi dan dekripsi email, sehingga kerahasiaan *email* dapat lebih terlindungi.

5.2 Sistem yang Diusulkan

5.2.1 Kelebihan Sistem Aplikasi

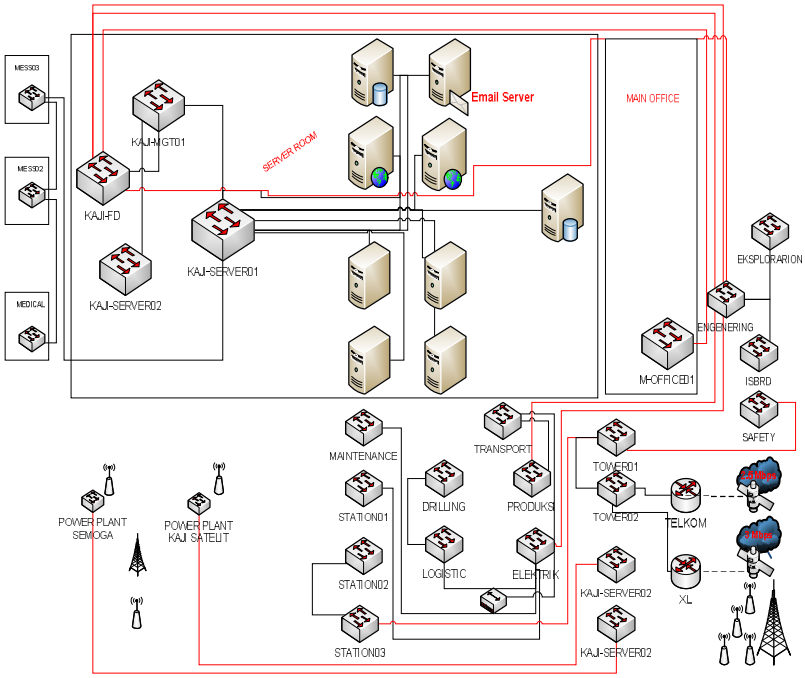
Sistem aplikasi keamanan email yang penulis rancang memiliki kelebihan, yaitu email yang akan dikirim setelah di enkripsi akan berupa kode-kode yang seakan tidak memiliki makna, dan email yang dienkripsi dapat dikembalikan lagi kedalam bentuk text aslinya (*plaintext*) setelah melakukan proses dekripsi dengan menggunakan algoritma elgamal.

Jadi dengan aplikasi email client ini keamanan email lebih dapat terjaga kerahasiaannya.

5.2.2 Prosedur dan Topologi Jaringan

Prosedur yang akan dirancang oleh penulis yaitu membangun aplikasi *email client* untuk pengamanan email yang terhubung dengan *mail server*.

Dibawah ini gambaran umum dari topologi jaringan yang dirancang oleh penulis.



Gambar 5.3. Prosedur Topologi Jaringan
(Sumber : Diolah Sendiri)

5.2.3 Terminologi Jaringan

Pada penelitian ini penulis menggunakan terminologi jaringan LAN (*Local Area Network*) dalam merancang terminologi jaringan yang diusulkan.

5.2.4 Kebutuhan Spesifikasi

Dalam implementasi aplikasi ini, ruang lingkup yang digunakan meliputi ruang lingkup perangkat keras (*Hardware*) dan perangkat lunak (*Software*).

1. Perangkat Keras (*Hardware*)

Perangkat keras (*Hardware)* yang digunakan dalam pengembangan aplikasi pengamanan email dengan algoritma El-Gamal dan uji cobanya adalah :

Tabel 5.1. Spesifikasi Perangkat Keras (*Hardware*)

Jenis Perangkat	Spesifikasi
Processor	Processor Intel Pentium IV 1.6 Ghz
Hardisk	40 GB
Memory	512 MB
Monitor	14”

2. Perangkat Lunak (*Software*)

Adapun perangkat lunak (*Software*) yang digunakan dalam pengembangan aplikasi pengamanan email dengan algoritma El-Gamal ini adalah sebagai berikut :

a) Sistem Operasi *Linux Debian Squeeze*

b) Bind9 (*DNS Server*)

c) Apache

d) Mysql-Server

e) PHP5

5.2.5 Analisis Sistem Aplikasi Email

1. Analisis Data

Data yang di gunakan sebagai obyek penelitian dalam system aplikasi pengaman email ini adalah sebuah pesan email yang berupa teks-teks biasa (*plaintext*) yang akan dikirim ke penerima, akan di rubah menjadi kode-kode (*chipertext*) yang sulit dipahami dan dimengerti dengan proses enkripsi dengan algoritma El-Gamal, kemudian akan dirubah menjadi teks-teks kembali seperti semula (*plaintext*) oleh penerima pesan dengan proses dekripsi dengan algoritma El-Gamal juga.

2. Analisi Aplikasi

Aplikasi yang akan dibangun pada penelitian ini yaitu sebuah *email client* yang sederhana namun di lengkapi dengan proses enkripsi dan dekripsi menggunakan algoritma El-Gamal pada email yang akan dikirim yang berfungsi untuk mengamankan email.

Ada dua spesifikasi dari program yang akan di bangun pada penelitian ini yaitu :

a. *Email client* yang digunakan untuk mengirimkan *email* yang telah terenkripsi ke *email server* oleh pengirim dan kemudian mendekripsikan *email* tersebut.
b. Pengaman *email* yang berupa kriptografi El-Gamal yang mempunyai fungsi dua garis besar yaitu pertama untuk mengekripsi pesan dari pesan asli (*plainteks*) ke bentuk kode-

kode (*chiperteks*) dengan kunci publik dan kedua untuk mendekripsikan pesan dari pesan yang hanya berupa kode-kode saja (*chipertext*) menjadi kembali pesan aslinya (*plaintext*) dengan menggunakan kunci privat. Hal ini dilakukan untuk proses pengamanan email tersebut.

3. Dekripsi Sistem

Proses pengamanan *email* pada system ini terdiri dari beberapa proses garis besar,yaitu :

a. Pembentukan kunci publik yang terdiri dari tiga kunci (p, g, y), dan privat (x) untuk proses enkripsi dan dekripsi, dengan mengambil acak bilangan prima dan sebuah bilangan *generator*.

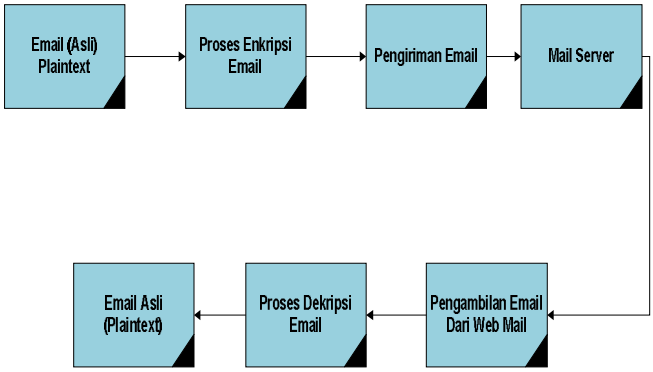
b. Konsep pembentukan kunci dilakukan dengan konsep pertemanan, dimana setiap teman mempunyai kunci publik masing masing untuk melakukan enkripsi pesan yang akan dikirim kepadanya oleh sang pembuat pesan. kunci publik ini boleh disebarkan kepada teman- temannya yang akan mengirim pesan kita.

c. Setelah mendapatkan kunci publik teman, selanjutnya melakukan pemasangan kunci public tersebut pada aplikasi, selanjutnya melakukan proses enkripsi terhadap pesan yang akan dikirim yang berupa teks-teks (*plaintext)* dengan kunci

publik algoritma El- Gamal menjadi *chipertext* yang berupa kode-kode untuk mengamankan email dari para penyadap di internet dan dikirim kepada teman kita yang akan dikirimi pesan.

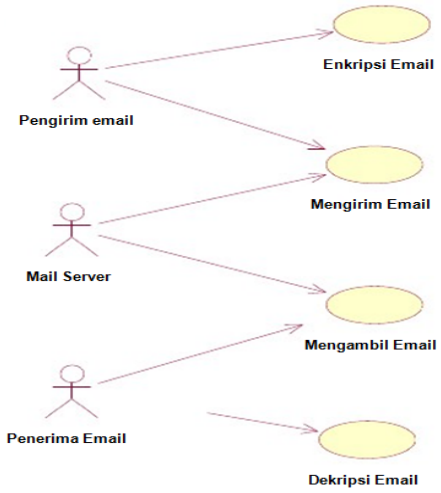
d. Melakukan dekripsi terhadap *email* yang sudah di ambil dari *email server* dengan kunci privat algoritma El-Gamal milik kita, karena teman kita mengenkripsi email dengan kunci publik kita. Dari *chiperteks* yang masih berwujud kode-kode menjadi *plainteks* atau teks asalnya sebelum di ekripsi.

Dikripsi ini secara jelas penulis gambarkan dalam bentuk diagram blok di bawah ini:



Gambar 5.4. Diagram Blok Pengamanan Email Dengan Algoritma ElGamal
(Sumber : Diolah Sendiri)

4. Analisi Use Case



Gambar 5.5. *Analisi Usecase*
(Sumber : Diolah Sendiri)

Diagram *usecase* yang terdapat pada Gambar 5.2 terdapat Tiga aktor dalam proses pengaman *email* dengan algoritma El-Gamal, dimana aktor pertama sebagai pengirim *email* atau *mail sender*, seperti yang telah di gambarkan pada diagram, *usecase* pengirim *email* ini melakukan dua proses, proses pertama melakukan enkripsi terhadap *email* yang akan di kirim kepada penerima *email*, pengenkripsian *email* dilakukan dengan kunci publik yang telah diberikan oleh penerima *email* sebelumniya sedangkan privat key-nya di simpan sendiri oleh penerima email untuk mengenkripsi *email* yang akan dikirim kepadanya, Proses kedua yang dilakukan oleh pengirim *email* yaitu mengirim email kepada penerima setelah mengenkripsi email.

Aktor yang kedua yaitu *server mail* yaitu perangkat lunak yang mendistribusikan *file* atau informasi sebagai respons atas permintaan yang dikirim via email. *Mail server* ini sebagai mediator antara penerima dan pengirim pesan, sebelum sampai kepenerima email, email yang dikirimkan oleh pengirim akan melewati *server mail* ini. Oleh karena itu email yang akan dikirim kepenerima perlu diamankan. Agar orang lain tidak bisa mengaksesnya.

Aktor yang ketiga yaitu penerima atau *mail receiver* , aktor ini melakukan dua proses proses juga, yaitu: mengmbil email dari *server mail* dengan *email client* yang sudah dihubungkan dengan fungsi email di php. Proses selanjutnya mendekripsi pesan dengan menggunakan kunci privat untuk mendapatkan email yang asli.

5. Proses Penyandian Kriptografi

Berikut ini diberikan sistem kriptografi ElGamal yang untuk selanjutnya penulisan penotasian akan mengacu pada sistem kriptografi ElGamal berikut:

Diberikan bilangan prima p dan sebuah elemen primitip $g \in \mathbb{Z}_p$.

Ditentukan :

$p = \mathbb{Z}_p$, C= $\mathbb{Z}_p$ X $\mathbb{Z}_p$dan $x \epsilon \{0,1,2,3,\dots.,p-2\}$ didefenisikan

$$k = \{(p, g, y): y = g^x \ mod \ p\}$$

Nilai p,g,y dipublikasikan dan nilai x dirahasiakan. Untuk $k = (p, g, y, x)$ $plaintext\ m \in \mathbb{Z}_p$ dan untuk satu bilangan acak rahasia $k = \{0,1,2, \dots , p-2\}$ di defenisikan:

$$e_k\ (m,k) = (a,b)$$

Dengan

$$a = g^k \ (mod \ p)$$

Dan

$$b = y^k \ . m \ (mod \ p)$$

Untuk $a, b \in \mathbb{Z}_p$, didefenisikan

$$d_k \ (a, b) = b \ . (a^x)^{-1} \ (mod \ p)$$

Secara singkat dapat dituliskan besaran-besaran dalam kriptografi ElGamal yang untuk selanjutkan akan dijadikan acuan penotasian dalam penulisan skripsi ini adalah:

a) Bilangan prima, p (bersifat tidak rahasia)

b) Bilangan acak, g $(g < p)$ (bersifat tidak rahasia)

c) Bilangan acak, x $(x < p)$ (bersifat rahasia)

d) $y = g^x \ mod \ p$ (kunci public)

e) m merupakan plaintext (bersifat rahasia)

f) $a \ dan \ b$ merupakan ciphertext (bersifat rahasia)

A. Pembuatan Kunci (*Generate Key*)

Membangkitkan pasangan kunci yang terdiri dari kunci rahasia dan kunci umum adalah proses pertama yang harus dilakukan dalam kriptografi ElGamal. Prosedur yang pertama dilakukan adalah memilih sembarang bilangan prima *p*.

Selanjutnya memilih dua bilangan acak, elemen primitif g dan x dengan syarat $g < p$ dan $x \epsilon \{0,1,2,\dots,p-2\}$. Maka dapat kita hitung $y = g^x \, mod \, p$.

Kunci umum kriptografi ElGamal berupa pasangan 3 bilangan (tripel), yaitu (p, g, y), dengan $y = g^x \, mod \, p$. Sedangkan kunci rahasia kriptografi ElGamal berupa pasangan bilangan, yaitu (x, p).

Kriptografi ElGamal menggunakan bilangan bulat prima dalam proses perhitungan penyandiannya, maka pesan harus dikonversi ke dalam suatu bilangan bulat. Berdasarkan sistem kriptografi ElGamal di atas dapat di buat algoritmanya sebagai berikut:

Algoritma 3.1. (Algoritma Pembentuk Kunci)

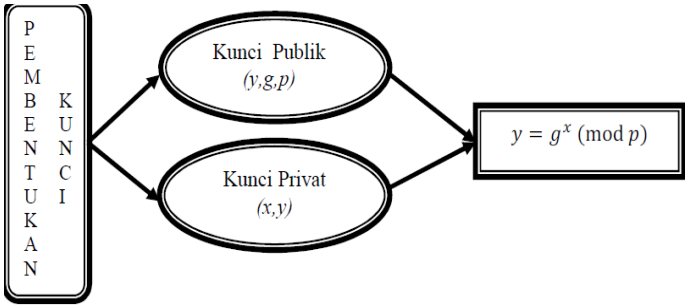
Input : bilangan prima aman p dan elemen primitive $g \in \mathbb{Z}_p$

Output : kunci public (p, g, y) dan kunci private *(x,p).*

Langkah :

1) Pilih sembarang bilangan prima p
2) Pilih dua bilangan acak, g dan x dengan syarat $(p > g)$ dan $x \in \{0,1,2,\dots,p-2\}$ atau $1 \leq x \leq p-2$
3) Hitung $y = g^x \bmod p$
4) Publikasikan nilai p,g dan y serta nilai x.

Untuk lebih jelasnya tentang segala sesuatu yang diperlukan dalam pembentukan kunci kriptografi ElGamal. Dapat dilihat skemanya sebagai berikut:



Gambar 5.6. Proses Pembentukan Kunci

(sumber : Diolah Sendiri)

Contoh :

Misalkan Sandro dan Amel akan saling berkomunikasi lewat sebuah email dimana email tersebut adalah sebuah email yang sangat penting dan hanya mereka saja yang boleh tahu akan isi email tersebut, yang isi pesannya adalah sebagai

berikut “AMBIL BARANGNYA BESOK MALAM JAM 9”. Oleh karena itu Sandro harus membuat sebuah pasangan kunci publik dan kunci privat. Maka dipilihlah bilangan prima (*p*), dan bilangan acak (*g,x*), dan melakukan perhitungan menggunakan rumus berikut :

$$y = g^x \, mod \, p$$

Dengan *p=2521, x=1175,* dan *g=2*

Maka didapatkan $y = 2^{1175} \, mod \, 2521 = 2127$

Maka Sandro mendapatkan pasangan kunci public (*y,g,p*) = (2127, 2, 2521), dan kunci privat (*x,p*)=(1175, 2521).

B. Enkripsi Pesan

Pada proses ini pesan di enkripsi menggunakan kunci publik *(y,g,p)* dan sebarang bilangan acak rahasia $k \in \{0,1,2,\dots,p-2\}$. Misalkan m seperti yang telah dimisalkan sebelumnya adalah pesan yang akan dikirim atau pesan dalam bentuk plainteks. Selanjutnya, m diubah ke dalam blok-blok karakter dan setiap karakter dikonversikan pada bilangan bulat, sehingga diperoleh plainteks $m_1, m_2, .., m_n$ dengan $m_1 \in \{0,1,2,\dots,p-$

$2\}, i = 1,2,\dots,n$. Proses enkripsi pada algoritma ElGamal dilakukan dengan menghitung:

$$a = g^x \bmod p$$

Dan

$$b = y^k . m \bmod p$$

Dengan $k \in \{0,1,2,\dots,p-2\}$ acak. Diperoleh ciphertext (*a*,*b*).

Dalam proses enkripsi, kunci privat adalah bilangan acak *k*. Bilangan acak *k* ditentukan oleh pihak pengirim dan harus dirahasiakan, jadi hanya pengirim saja yang mengetahuinya. Bilangan acak *k* hanya digunakan saat melakukan enkripsi saja jadi tidak perlu disimpan.

Algoritma 3.2. (Algoritma Enkripsi)

Input : pesan yang akan dienkripsi dan kunci publik (*p*,*g*,*y*)

Output : ciphertext (*a*,*b*), *i = 1,2,…,n*

Langkah :

1) Susun plainteks menjadi blok-blok $m_1, m_2, \dots, m_n$ sedemikian hingga setiap blok mempresentasikan nilai di dalam selang $[0, p-1]$.

2) Pilih bilangan acak *k*, yang ada pada selang $1 \leq x \leq p-2$

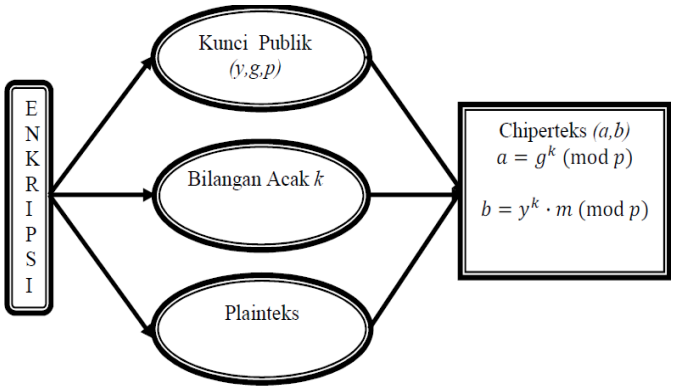
3) Setiap blok *m* di enkripsi dengan rumus

$$a = g^x \bmod p$$

$$b = y^k . m \ (mod \ p)$$

4) Diperoleh chiperteks (*a*,*b*)

Pasangan *a* dan *b* adalah sebuah *chiperteks* untuk blok pesan *m*. jadi, ukuran *chiperteks* dua kali ukuran *plainteks* nya. Untuk lebih jelasnya tentang segala sesuatu yang diperlukan dalam proses enkripsi. Dapat dilihat skema berikut:



Gambar 5.7. Proses Enkripsi Pesan
(Sumber : Diolah Sendiri)

Contoh :

Amel ingin mengirim pesan “AMBIL BARANGNYA BESOK MALAM JAM 9”. Maka yang perlu dilakukan amel dalam mengenkripsi pesan adalah :

a) Memotong pesan menjadi blok-blok karakter.

b) Menkonversikan blok-blok karakter kedalam bilangan bulat kode ASCII (lihat lampiran 1) Kode ASCII (*American Standard for Information Interchange*), merupakan representasi numerik dari karakter-karakter yang digunakan pada komputer, serta mempunyai nilai minimal 0 dan maksimal 255. Berdasarkan sistem kriptografi ElGamal di atas, maka harus digunakan bilangan prima yang lebih besar dari 255. Kode ASCII berkorespondensi 1-1 dengan karakter pesan.

Tabel 5.2. Konversi Pesan Kedalam Kode ASCII

i	Karakter	Plaintext *m*	Kode ASCII
1	A	m_1	65
2	M	m_2	77
3	B	m_3	66
4	I	m_4	73
5	L	m_5	76
6	<spasi>	m_6	32
7	B	m_7	66
8	A	m_8	65
9	R	m_9	82
10	A	m_{10}	65
11	N	m_{11}	78
12	G	m_{12}	71
13	N	m_{13}	78
14	Y	m_{14}	89
15	A	m_{15}	65
16	<spasi>	m_{16}	32
17	B	m_{17}	66

18	**E**	m_{18}	**69**
19	**S**	m_{19}	**83**
20	**O**	m_{20}	**79**
21	**K**	m_{21}	**75**
22	**<spasi>**	m_{22}	**32**
23	**M**	m_{23}	**77**
24	**A**	m_{24}	**65**
25	**L**	m_{25}	**76**
26	**A**	m_{26}	**65**
27	**M**	m_{27}	**77**
28	**<spasi>**	m_{28}	**32**
29	**J**	m_{29}	**74**
30	**A**	m_{30}	**65**
31	**M**	m_{31}	**77**
32	**<spasi>**	m_{32}	**32**
33	**9**	m_{33}	**57**

c) Mengenkripsi pesan menggunakan kunci publik dan memilih bilangan bulat acak *k* untuk setiap karakter.

Dengan $k_i \in \{1,2,..,p-2\}; \quad i = 1,2,..33.$ Kemudian hitung nilai $a = g^k \bmod p$ dan $b = y^k . m \ (mod\ P)$ sebagai berikut :

Tabel 5.3. Perhitungan Enkripsi

i	m_i	k_i	$a = 2^k \bmod 2521$	$b = 2127^k . m \ (mod\ p)$
1	**65**	**1843**	**600**	**638**
2	**77**	**1404**	**28**	**184**
3	**66**	**1414**	**941**	**1145**
4	**73**	**1572**	**2197**	**2267**
5	**76**	**146**	**112**	**2452**
6	**32**	**1299**	**195**	**2512**
7	**66**	**990**	**1209**	**219**
8	**65**	**729**	**1654**	**1212**
9	**82**	**478**	**217**	**1718**
10	**65**	**1317**	**2284**	**1296**

11	**78**	**876**	**2430**	**1512**
12	**71**	**791**	**560**	**1440**
13	**78**	**1148**	**1084**	**842**
14	**89**	**307**	**305**	**454**
15	**65**	**481**	**1736**	**836**
16	**32**	**569**	**2281**	**729**
17	**66**	**1251**	**2004**	**2478**
18	**69**	**1373**	**1614**	**295**
19	**83**	**1652**	**108**	**2512**
20	**79**	**802**	**2346**	**128**
21	**75**	**752**	**520**	**1906**
22	**32**	**909**	**1968**	**2278**
23	**77**	**791**	**560**	**603**
24	**65**	**782**	**395**	**2298**
25	**76**	**544**	**197**	**1489**
26	**65**	**444**	**1406**	**289**
27	**77**	**567**	**2461**	**425**
28	**32**	**789**	**140**	**1338**
29	**74**	**910**	**1415**	**1131**
30	**65**	**1123**	**1085**	**1805**
31	**77**	**921**	**1291**	**258**
32	**32**	**1188**	**1753**	**2015**
33	**57**	**1531**	**465**	**1969**

Berdasarkan Tabel 5.2 diperoleh chipperteks : (*a*,*b*), *i {1,2,3,..,33},* sebagai berikut :

(600,638) (28,184) (941,1145) (2197,2267) (112,2452) (195,2512) (1209,219) (1654,1212) (217,1718) (2284,1296) (2430,1512) (560,1440) (1084,842) (305,454) (1736,836) (2281,729) (2004,2478) (1614,295) (108,2512) (2346,128) (520,1906) (1968,2278) (560,603) (395,2298) (197,1489) (1406,289) (2461,425) (140,1338) (1415,1131) (1085,1805) (1291),258) (1753,2015) (465,1969).

Selanjutnya Sandro mengirim email yang berupa *chipperteks* diatas kepada Amel.

Salah satu kelebihan dari algoritma El-Gamal adalah suatu *plainteks* yang sama akan di enkripsi menjadi *chipperteks* yang berbeda beda walaupun hurufnya sama. Hal ini dikarenakan pemilihan bilangan *k* yang acak. Akan tetapi, walaupun chipperteksnya yang diperoleh berbeda beda, tetapi pada proses dekripsi akan di peroleh plainteks yang sama.

C. Dekripsi Pesan

Setelah menerima *cipherteks* (*a*,*b*), proses selanjutnya adalah mendekripsi *cipherteks* menggunakan kunci publik *p* dan kunci rahasia *x*. Dapat ditunjukkan bahwa *plainteks m* dapat diperoleh dari *cipherteks* menggunakan kunci rahasia *x*.

Diberikan (*p*,*g*,*y*) sebagai kunci publik dan *x* sebagai kunci privat pada kriptografi ElGamal. Jika diberikan *cipherteks* (*a*,*b*), maka

$$m = b \,.\, (a^x)^{-1} \pmod{p}$$

Dengan *m* adalah *plaintext.*

Bukti :

Diketahui kunci publik (*p*,*g*,*y*) dan kunci privat *x* pada kriptografi elgamal. Diberikan *ciphertext* (*a*,*b*), dari persamaan diatas diperoleh bahwa :

$$b.(a^x)^{-1} \equiv (y^k \,.m).(a^x)^{-1}(mod\ p)$$

$$\equiv y^k \,.m\,.a^{-1}\ (mod\ p\ )$$

$$\equiv (g^x)^{\,k}\,.m\,.(g^k)^{-x}\ mod\ p$$

$$\equiv g^{k.x}\,.m\,.g^{-x.k}\ (mod\ p)$$

$$\equiv m.g^0\ (mod\ p)$$

$$\equiv m\ (mod\ p\ )$$

Dengan demikian didapat :

$$b\,.(a^x)^{-1} \equiv m\ (mod\ p)$$

$$m = b\,.(a^x)^{-1}\ mod\ p$$

Karena $\mathbb{Z}_p$ mempunyai orde $p-1$ dari $x \in \{0,1,2,..,p-2\}$, maka :

$$(a^x)^{-1} = a^{-x} = a^{p-1-x}\ (mod\ p)$$

Algortima 3.3. (Algoritma Dekripsi)

Input : ciphertext (*a*,*b*), kunci publik (*p*,*g*,*y*), dan kunci privat *x*.

Output : pesan asli.

Langkah :

1) Gunakan kunci privat x untuk mendeskripsikan a dan b menjadi plainteks m dengan persamaan $m = b|a^x \ (mod\ p)$
2) Diperoleh plaintext $m_1, m_2, \dots, m_n$

Dalam menghitung algoritma deskripsi harus di ingat beberapa catatan berikut ini:

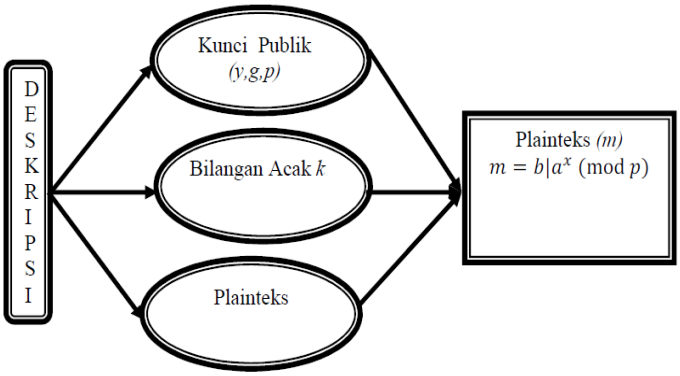
1) $(a^x)^{-1} = a^{-x} = a^{p-1-x} \ (mod\ p)$. Harus diingat bahwa "-1" menyatakan invers modulo.
2) $a^x \equiv g^{k.x} \ (mod\ p)$ maka

   $b|a^x \equiv y^k \,.\, m|a^x$

   $\equiv g^{x.k} \,.\, m|a^{x.k}$

   $\equiv m \ (mod\ p)$
3) *Plainteks* dapat ditemukan kembali dari pasangan *chiperteks* (*a*,*b*).

Untuk lebih jelasnya tentang segala sesuatu yang diperlukan dalam proses enkripsi dapat di lihat dalam skema berikut:



Gambar 5.8. Proses Dekripsi Pesan
(Sumber : Diolah Sendiri)

Kriptografi ElGamal diciptakan untuk mengamankan pesan atau informasi-informasi rahasia yang tidak boleh diketahui oleh pihak-pihak yang tidak berhak.

Kriptografi ElGamal adalah bagian dari kriptografi kunci-publik yang berarti dalam mengamankan pesannya menggunakan dua buah kunci. Untuk mengubah pesan menjadi plainteks yang dinamakan kunci publik dan mengubah plainteks menjadi chiperteks yang dinamakan kunci privat. Pihak yang membuat kunci publik dan kunci rahasia adalah penerima, sedangkan pihak pengirim hanya mengetahui kunci publik yang diberikan oleh penerima, dan kunci publik tersebut digunakan untuk mengenkripsi pesan. Jadi, pemegang kendali keamanan penuh adalah penerima pesan. Maka dengan menggunakan kriptografi

kunci public adalah tidak ada permasalahan pada distribusi kunci apabila jumlah pengirim sangat banyak serta tidak ada kepastian keamanan jalur yang digunakan.

Contoh :

Amel telah mendapatkan chiperteks pesan rahasia dari Sandro, maka Amel melakukan proses deskripsi menggunakan kunci privatnya sebagai berikut:

Tabel 5.4. Perhitungan Dekripsi

i	a	b	$m_i = b.a^{1345} \bmod 2521$	Karakter
1	600	638	65	A
2	28	184	77	M
3	941	1145	66	B
4	2197	2267	73	I
5	112	2452	76	L
6	195	2512	32	<spasi>
7	1209	219	66	B
8	1654	1212	65	A
9	217	1718	82	R
10	2284	1296	65	A
11	2430	1512	78	N
12	560	1440	71	G
13	1084	842	78	N
14	305	454	89	Y
15	1736	836	65	A
16	2281	729	32	<spasi>
17	2004	2487	66	B
18	1614	295	69	E
19	108	2512	83	S
20	2346	128	79	O
21	520	1906	75	K

22	**1968**	**2278**	**32**	**<spasi>**
23	**560**	**603**	**77**	**M**
24	**395**	**2298**	**65**	**A**
25	**197**	**1489**	**76**	**L**
26	**1406**	**289**	**65**	**A**
27	**2461**	**425**	**77**	**M**
28	**140**	**1338**	**32**	**<spasi>**
29	**1415**	**1131**	**74**	**J**
30	**1085**	**1805**	**65**	**A**
31	**1291**	**258**	**77**	**M**
32	**1753**	**2015**	**32**	**<spasi>**
33	**465**	**1969**	**57**	**9**

Jadi, setelah melakukan proses deskripsi dengan kunci privat yang dimilikinya. Amel dapat mengetahui pesan yang sebanarnya yaitu "AMBIL BARANGNYA BESOK MALAM JAM 9".

6. Rancangan Database

Untuk menyimpan dan mengamankan data-data dalam aplikasi *email client* yang penulis buat, seperti *account* dan data-data teman pada *email client*, kami buat *database* supaya data data data tersebut aman dan terstruktur.

Aplikasi database yang kami gunakan dalam tugas akhir ini yaitu phpMyAdmin file databasenya "**admin**". Berikut ini nama-nama tabel yang digunakan beserta *field-field* yang terdapat pada masing-masing tabel.

a. Tabel *Administrator*

Tabel 5.5. *Fields* Tabel *Administrator*

No	Fields	Type	Size
1	idAdmin	int	11
2	namaAdmin	varchar	30
3	Username	varchar	50
4	Email	varchar	50
5	Password	varchar	30
6	waktu	Datetime	-
7	petugas	varchar	30

b. Tabel Arsip Pesan

Tabel 5.6. Tabel *Fields* Arsip Pesan

No	Fields	Type	Size
1	idPesan	Int	11
2	Subject	Varchar	100
3	Pesan	Text	
4	Pesan_enkripsi	Text	
5	Pesan_dekripsi	Text	
6	Pengirim	Varchar	50
7	Tujuan	Varchar	50
8	waktu	datetime	

c. Tabel *Key* (kunci)

Tabel 5.7. Tabel *Fields Key* (kunci)

No	Fields	Type	Size
1	Y	Int	11
2	P	Int	11
3	G	Int	11
4	X	int	11

d. Tabel *User*

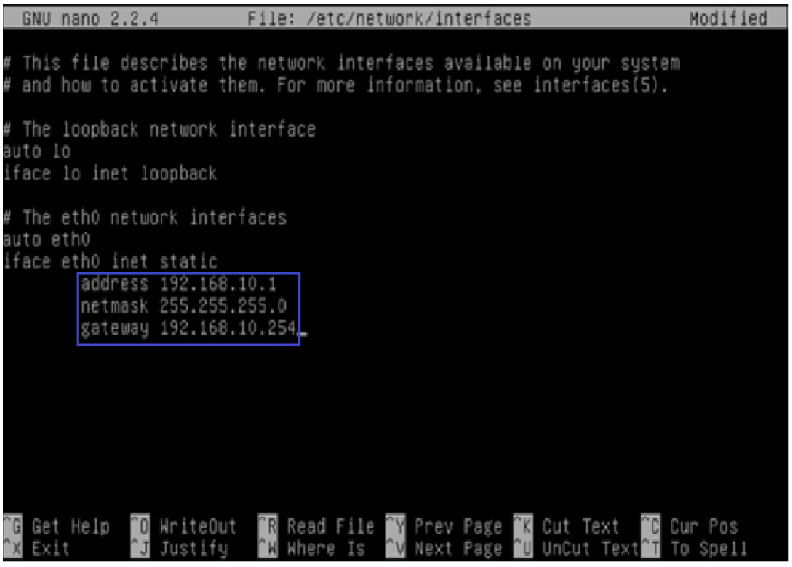
Tabel 5.8. Tabel *Fields User*

No	Fields	Type	Size
1	User_id	Int	11
2	Nama	Varchar	30
3	Username	Varchar	30
4	Password	Varchar	30
5	email	Varchar	50

5.2.6 Dokumentasi dan Konfigurasi

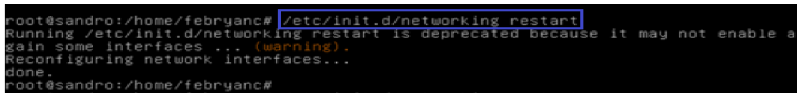
1. Konfigurasi IP *Address*

   Untuk memasukan alamat IP pada *ethernet*, edit file *interfaces* dengan perintah **#nano /etc/network/interfaces**. Tambahkan IP *Adress* seperti *script* di bawah ini.



Gambar 5.9. Menambahkan IP Address
(Sumber : Diolah Sendiri)

Agar konfigurasi tersebut dapat langsung dijalankan, *service networking* harus direstart terlebih dahulu.



Gambar 5.10. Restart Kartu Jaringan
(Sumber : Diolah Sendiri)

2. Konfigurasi DNS Server

A. Install Bind9 (*Berkeley Internet Name Domain versi* 9)

```
root@sandro:/home/febryanc# apt-get install bind9
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  bind9-host bind9utils dnsutils libbind9-60 libdns69 libisc62 libisccc60
  libisccfg62 liblwres60
Suggested packages:
  bind9-doc resolvconf ufw rblcheck
The following packages will be upgraded:
  bind9 bind9-host bind9utils dnsutils libbind9-60 libdns69 libisc62
  libisccc60 libisccfg62 liblwres60
10 upgraded, 0 newly installed, 0 to remove and 37 not upgraded.
Need to get 1,680 kB of archives.
After this operation, 0 B of additional disk space will be used.
Do you want to continue [Y/n]? y
```

Gambar 5.11. Install Bind9
(Sumber : Diolah Sendiri)

B. Konfigurasi

Berikut file-file penting yang akan dikonfigurasi dalam DNS Server :

- /etc/bind/named.conf
- file forward
- file reverse
- /etc/resolv.conf

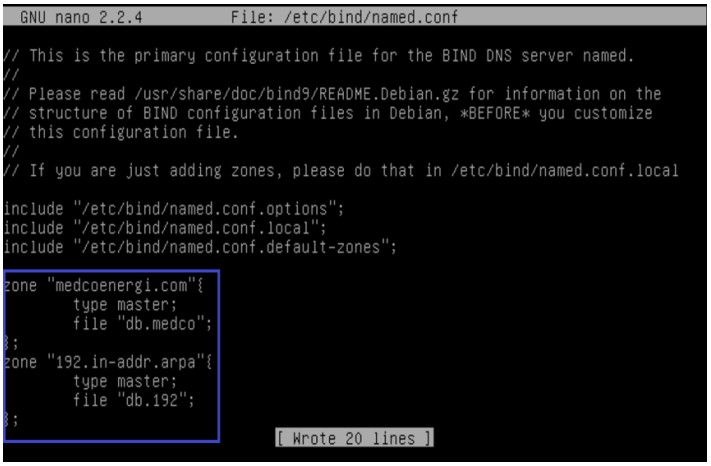
a. Membuat zona domain

Untuk membuat zona domain baru cukup edit file **named.conf** yang berada didirektory **/etc/bind/**.

```
root@sandro:/home/febryanc# nano /etc/bind/named.conf_
```

Gambar 5.12. Membuat Zona DNS
(Sumber : Diolah Sendiri)

Setelah itu tambahkan *script* seperti gambar di bawah ini.



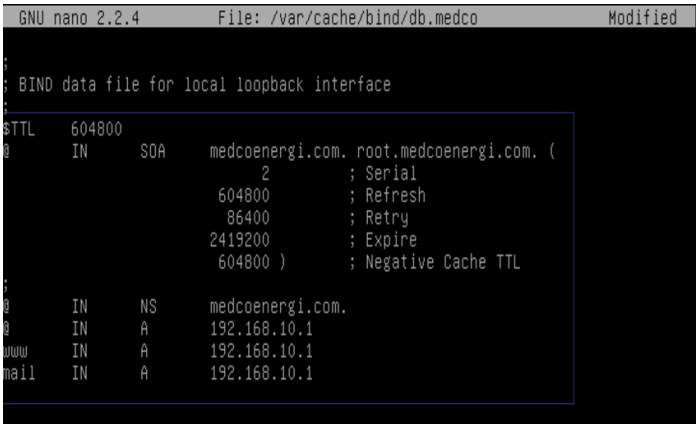
Gambar 5.13. Script Zone DNS
(Sumber : Diolah Sendiri)

b. File forward

Forward berfungsi untuk konversi dari DNS ke Ip *Address*. ketika kita ketik **www.medcoenergi.com** melalui Web Browser, maka akan muncul *website* dari *server* medcoenergi.

Buat file konfigurasi untuk file forward dari DNS tersebut, dan letakan di direktori **/var/cache/bind/.**

Edit file forward yang telah dibuat tadi, lalu edit file tersebut dengan perintah #nano /var/cache/bind/db.medco. lalu edit script seperti gambar di bawah ini.

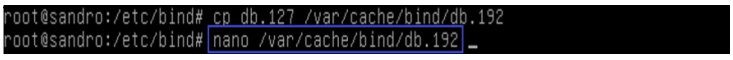


Gambar 5.14. File Forward
(Sumber : Diolah Sendiri)

c. File reverse

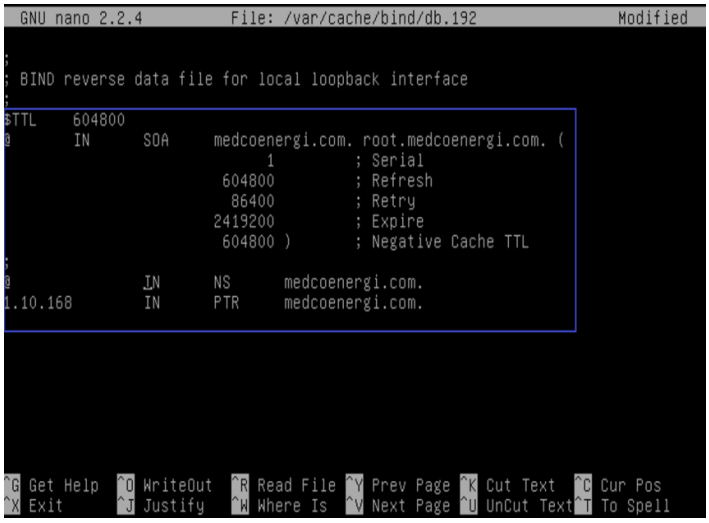
Reverse berfungsi untuk konversi IP *Address* ke DNS. Misalnya jika kita mengetikan IP Address http://192.168.10.1 pada *Web Browser*, secara otomatis akan *redirect* ke alamat **www.medcoenergi.com**.

Buat dan edit file *reverse* yang berada dalam direktori **/var/cache/bind/**.



Gambar 5.15 File Reverse
(Sumber : Diolah Sendiri)

Masukan *script* seperti gambar di bawah ini.



Gambar 5.16 Script File Reverse
(Sumber : Diolah Sendiri)

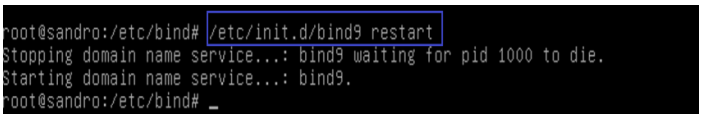
Tambahkan DNS dan *nameserver* dari *server* medcoenergi tersebut pada file **resolv.conf**. Agar dapat diakses melalui computer *localhost.*

Gambar 5.17 Menambahkan Nameserver
(Sumber : Diolah Sendiri)

Tambahkan *name server* seperti script di bawah ini.

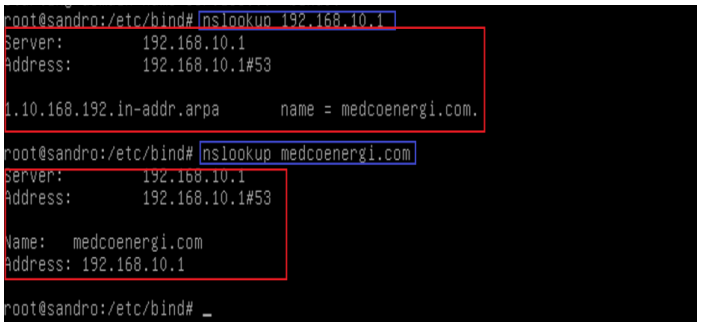
Gambar 5.18 Script File Resolv.conf
(Sumber : Diolah Sendiri)

Terakhir, *restart daemon* dari bind9.



Gambar 5.19 Perintah Restart Bind9
(Sumber : Diolah Sendiri)

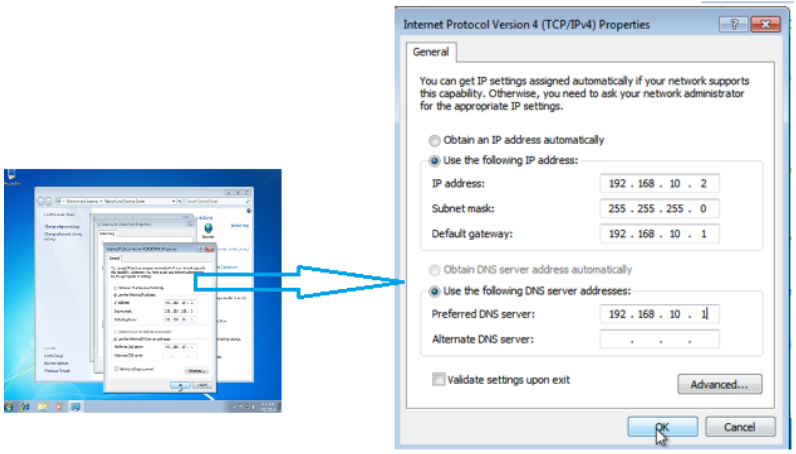
Test apakah DNS *Server* tersebut berhasil atau tidak, dengan perintah nslookup dari komputer Localhost ataupun dari komputer client.



Gambar 5.20 Test DNS Server
(Sumber : Diolah Sendiri)

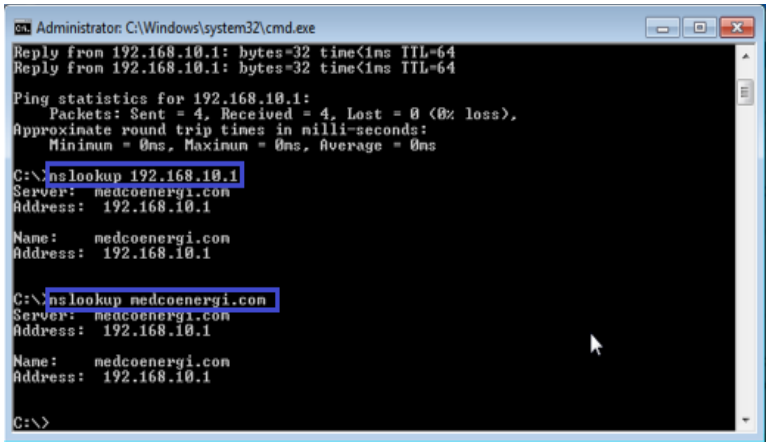
C. Pengujian DNS Server Pada *Client*

Menambahkan IP *Address* pada sisi *client* dengan ip *address* 192.168.10.2, netmask 255.255.255.0, dan DNS Server 192.168.10.1.



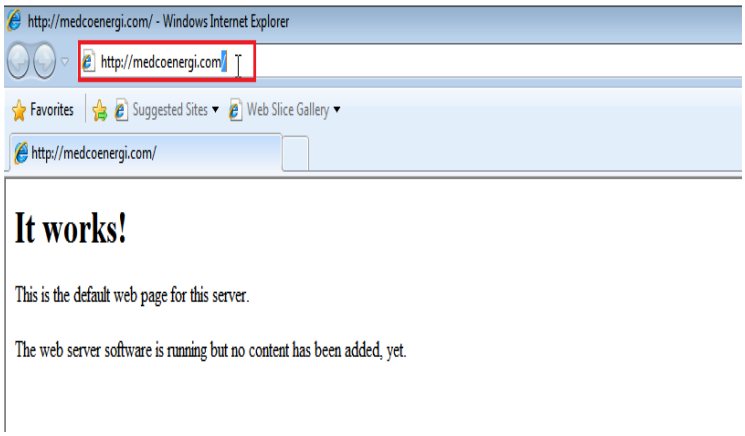
Gambar 5.21 IP Address Client
(Sumber : Diolah Sendiri)

Testing DNS *Server* dengan perintah nslookup (**nslookup 192.168.10.1** , **nslookup medcoenergi.com**).



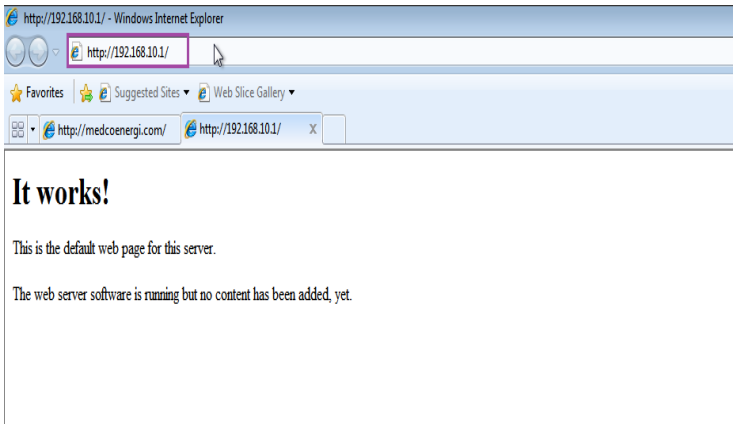
Gambar 5.22 Testing DNS Server
(Sumber : Diolah Sendiri)

Testing DNS *Server* melalui *web browser* dengan domain "medcoenergi.com".



Gambar 5.23 Testing DNS Melalui Web Browser (medcoenergi.com)
(Sumber : Diolah Sendiri)

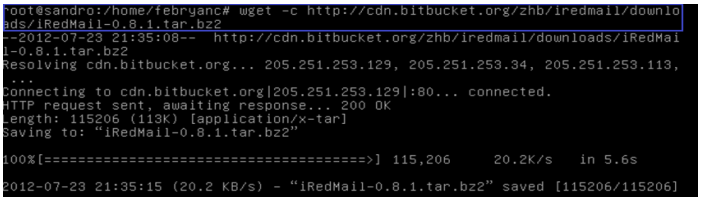
Testing DNS *Server* melalui *web browser* dengan *file reverse* domain "192.168.10.1".



Gambar 5.24 Testing DNS Melalui Web Browser (192.168.10.1)
(Sumber : Diolah Sendiri)

D. Install dan Konfigurasi *Web Mail* (Roundcube)

1. Download iRedMail

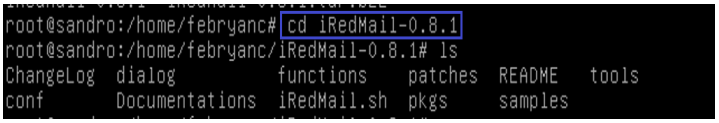


Gambar 5.25 Download iRedMail
(Sumber : Diolah Sendiri)

2. Ekstrak file iRedMail dengan perintah **#tar xjf**

Gambar 5.26 Ekstrak File iRedMail
(Sumber : Diolah Sendiri)

3. Pindah ke directory iRedMail

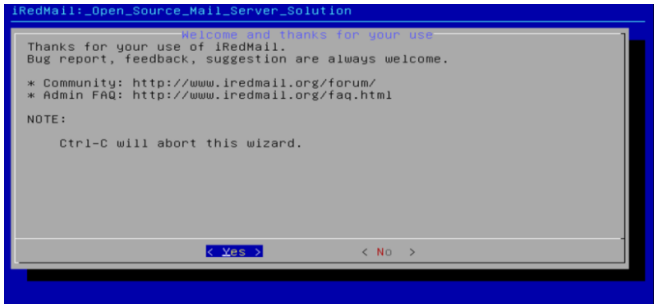


Gambar 5.27 Pindah Kedirektori iRedMail
(Sumber : Diolah Sendiri)

4. Install iRedMail **#bash iRedMail.sh**

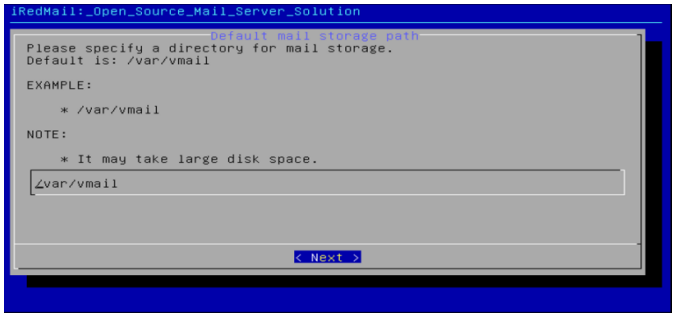
Gambar 5.28 Menjalankan iRedMail Instalation
(Sumber : Diolah Sendiri)

a. *Welcome and thanks for your use*



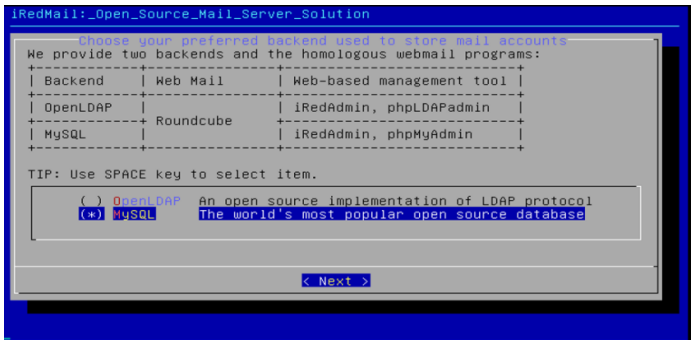
Gambar 5.29 Halam Utama Konfigurasi iRedMail
(Sumber : Diolah Sendiri)

b. *Directory* tempat penyimpanan *mailbox*.



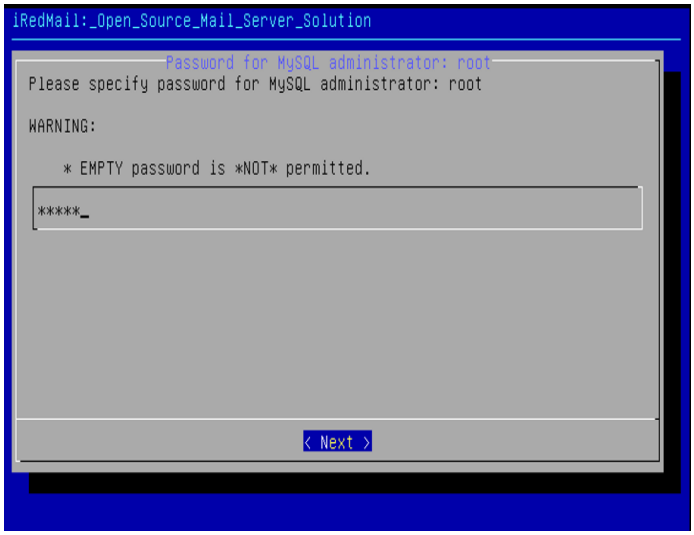
Gambar 5.30 Direktori Tempat Penyimpanan Mailbox
(Sumber : Diolah Sendiri)

c. Memilih *database administrator* yang akan digunakan.



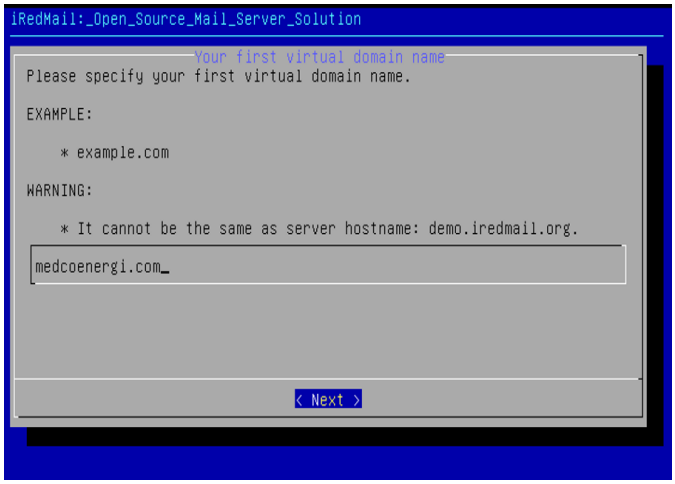
Gambar 5.31 Database yang Digunakan (Mysql)
(Sumber : Diolah Sendiri)

d. Masukan *password* untuk *administrator*.



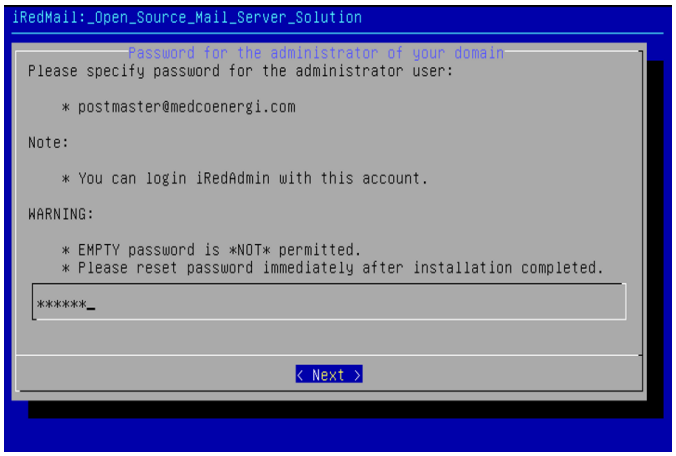
Gambar 5.32 Password Administrator Database
(Sumber : Diolah Sendiri)

e. Memasukan *domain* yang akan digunakan (medcoenergi.com).



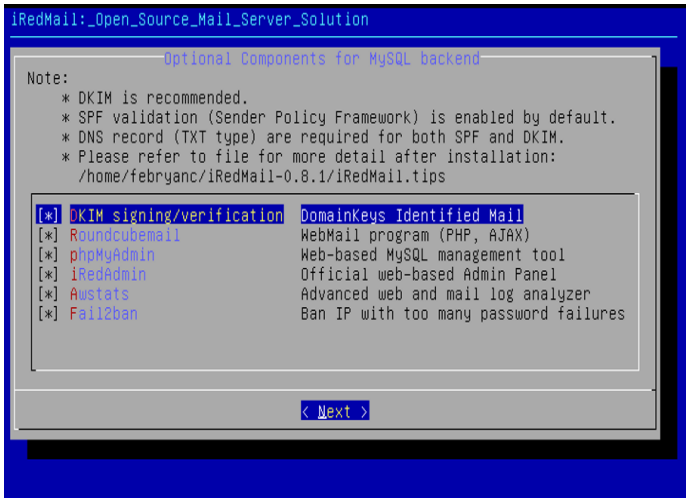
Gambar 5.33 Domain yang Digunakan
(Sumber : Diolah Sendiri)

f. Masukan *password administrator* yang akan digunakan.



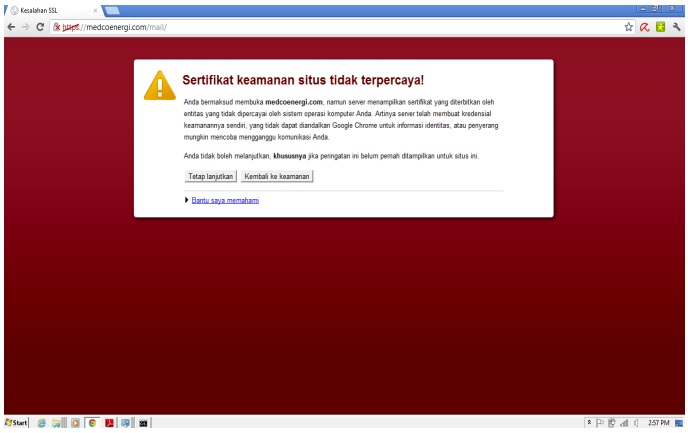
Gambar 5.34 Password Administrator Mail
(Sumber : Diolah Sendiri)

g. Memilih komponen-komponen penunjang dari mysql.



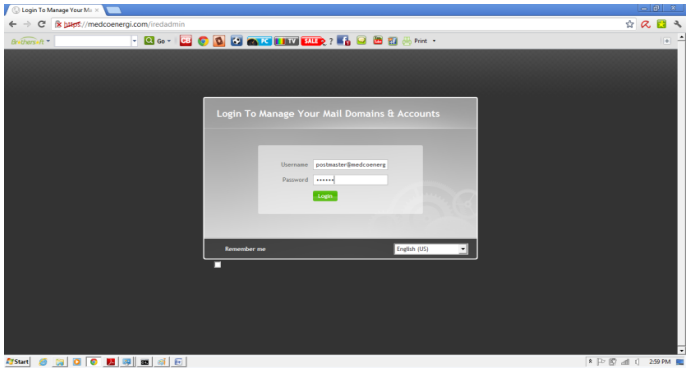
Gambar 5.35 Aplikasi Pendukung
(Sumber : Diolah Sendiri)

h. Pengujian web mail dari sisi client dengan domain (medcoenergi.com/mail).



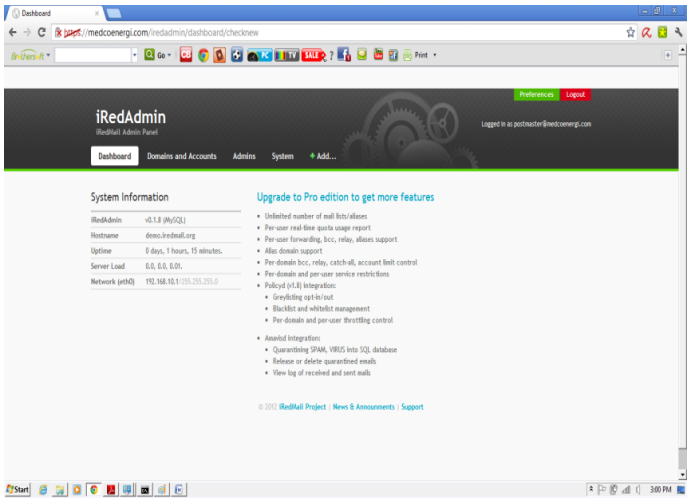
Gambar 5.36 Sertifikat SSL
(Sumber : Diolah Sendiri)

i. Login ke administrator untuk menambahkan user dari web mail, menambahkan domain untuk email, dan menambahkan administrator. Masuk ke domain (medcoenergi.com/iredadmin), untuk login default menggunakan user_default@domain.com (postmaster@medcoenergi.com).



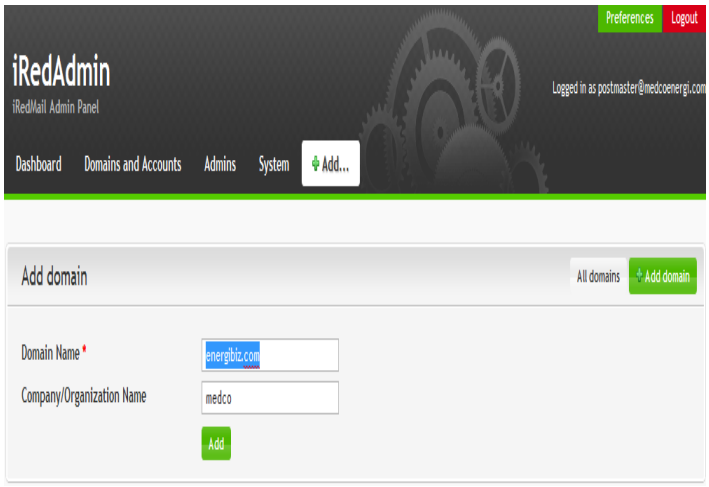
Gambar 5.37. Halaman Login Administrator
(Sumber : Diolah Sendiri)

j. Halaman utama (Dashboard) dari antarmuka web mail administrator.



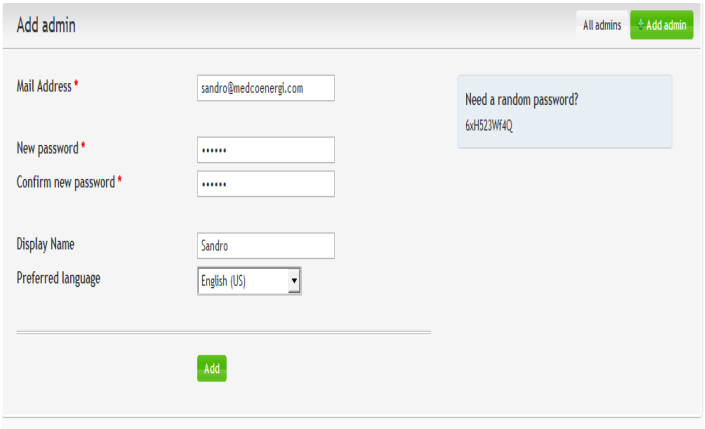
Gambar 5.38 Dashboard Administrator
(Sumber : Diolah Sendiri)

k. Menambahkan domain baru yaitu (energibiz.com).



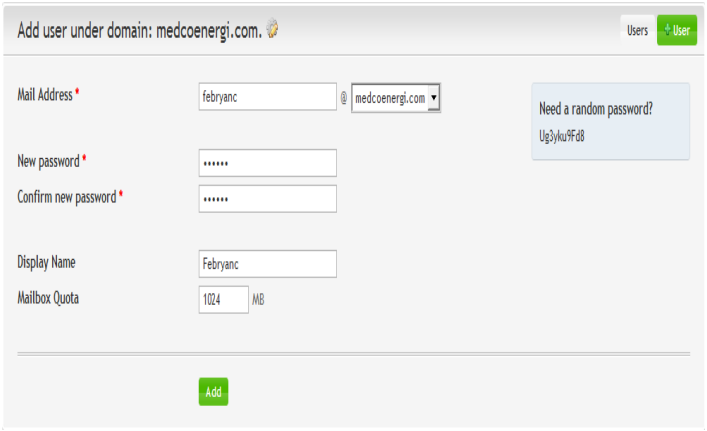
Gambar 5.39 Menambahkan Domain Baru
(Sumber : Diolah Sendiri)

l. Menambahkan admin baru untuk memenage lalu lintas dari client (sandro.febriyansyah@medcoenergi.com).



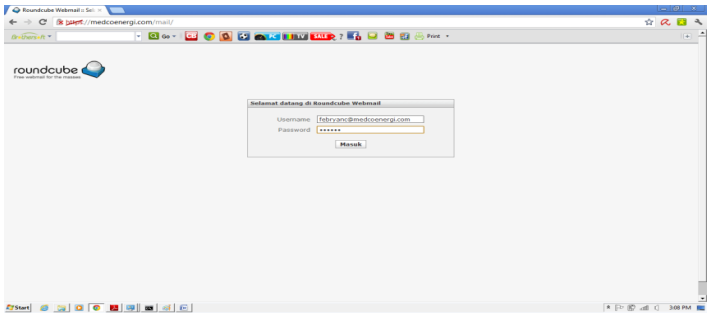
Gambar 5.40 Menambahkan Administrator
(Sumber : Diolah Sendiri)

m. Menambahkan user pengguna baru untuk login ke web mail (medcoenergi.com/mail/).



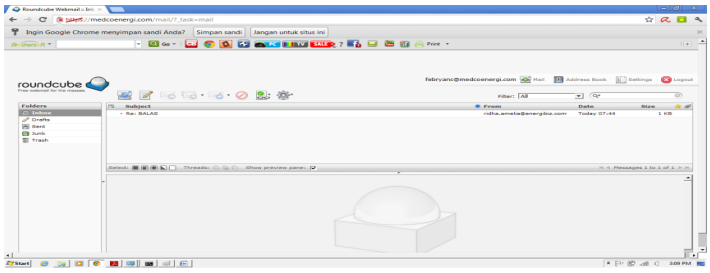
Gambar 5.41 Menambahkan User
(Sumber : Diolah Sendiri)

n. Halaman login web mail (roundcube)



Gambar 5.42 Halaman Login User
(Sumber : Diolah Sendiri)

o. Dashboard roundcube (web mail)



Gambar 5.43 Dashboard User
(Sumber : Diolah Sendiri)

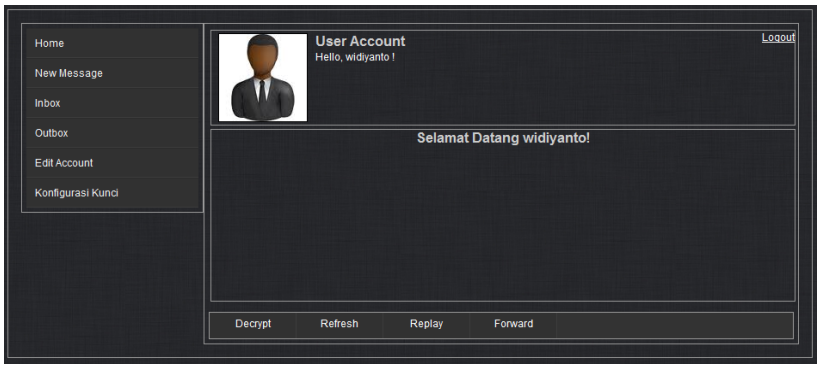
5.3 Implementasi Sistem Aplikasi

5.3.1 Halaman Login User

Login USer
Username :
Password :
Login

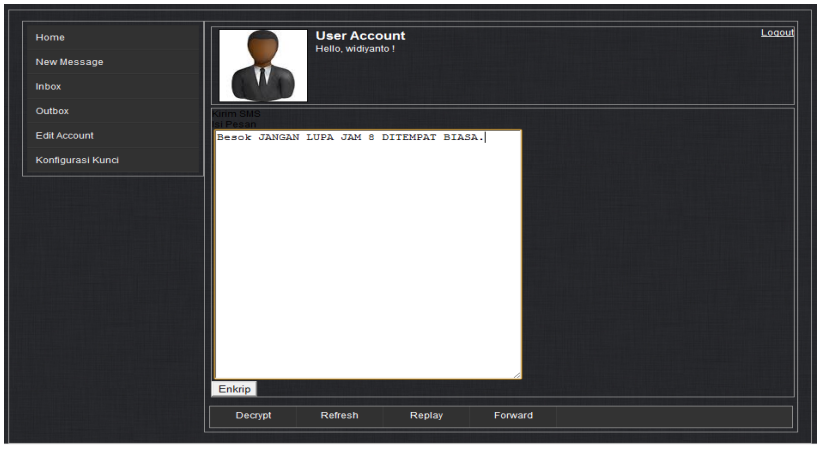
Gambar 5.44 Halaman Login
(Sumber : Diolah Sendiri)

5.3.2 Halaman Utama Aplikasi Email Client



Gambar 5.45 Halaman User
(Sumber : Diolah Sendiri)

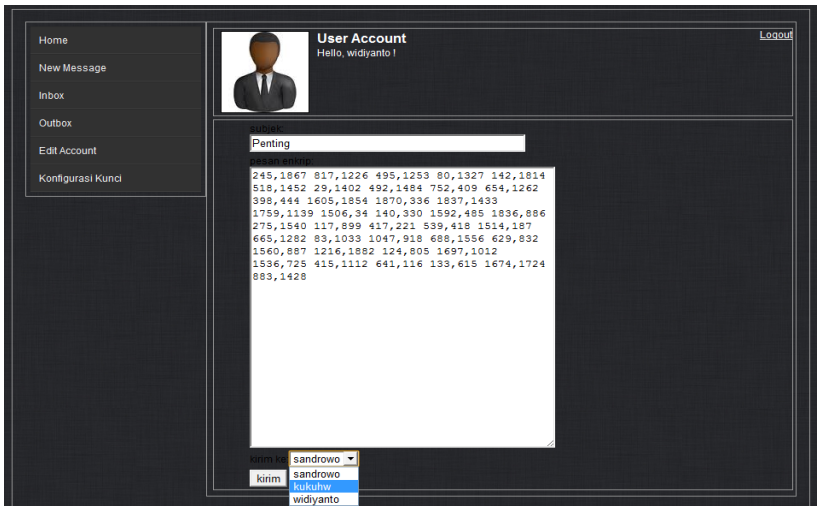
5.3.3 Pesan Baru (*New Message*)



Gambar 5.46 Halaman New Message
(Sumber : Diolah Sendiri)

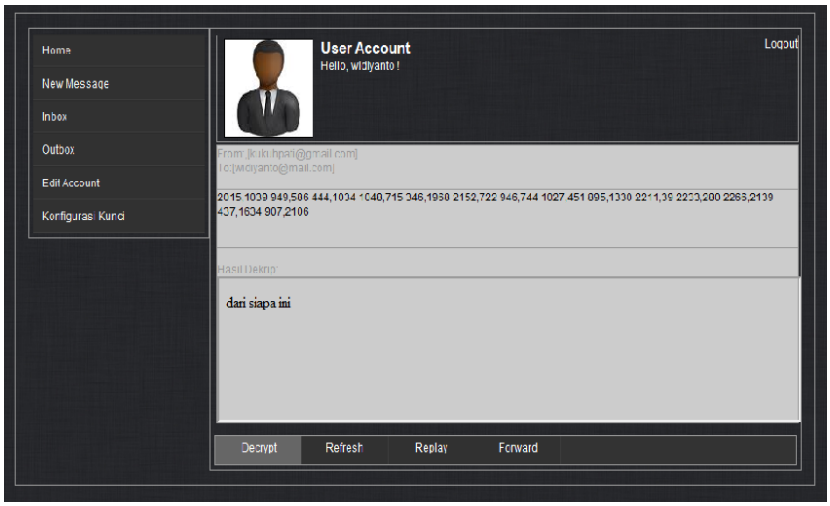
Pada halaman ini (new message) digunakan untuk melakukan pengiriman pesan baru dan langsung melakukan proses enkripsi terhadap pesan.

5.3.4 Enkripsi Pesan



Gambar 5.47 Halaman Enkripsi Pesan
(Sumber : Diolah Sendiri)

5.3.5 Proses Dekripsi



Gambar 5.48. Halaman Dekripsi
(Sumber : Diolah Sendiri)

5.3.6 Generate Kunci

Gambar 5.50 Generate Key
(Sumber : Diolah Sendiri)

BAB VI

PENUTUP

6.1 Simpulan

Kesimpulan yang dapat diambil dari penulis setelah menyelesaikan pembuatan skripsi ini adalah :

1. Pada PT medco E&P Indonesia Blok Rimau Asset, standarisaasi keamanan email selama ini menggunakan ptotocol SSL dengan enkripsi 128 bit. Standar keamanan ini sebenarnya sudah cukup untuk pertukaran informasi secara umum, tetapi masih belum optimal untuk pengiriman data-data yang sifatnya sensitive atau rahasia.
2. Untuk meningkatkan keamanan email pada PT Medco E&P Indonesia Blok Rimau Asset maka dari itu penulis mengusulkan suatu sistem aplikasi email client untuk keamanan email. Dengan aplikasi keamanan email ini pesan yang dikirim dapat dijaga kerahasiaannya, dengan melakukan proses pengubahan text asli (plaintext) kedalam bentuk sandi (ciphertext).
3. Aplikasi email client yang penulis buat menggunakan algoritma ElGamal untuk melakukan proses enkripsi dan dekripsi. Kriptografi ElGamal, mendasarkan kekuatannya pada masalah logaritma diskrit dan dalam proses pembuatan kuncinya

menggunakan bilangan prima. Pemecahan masalah logaritma diskrit yang cukup menyulitkan dan bilangan prima yang besar menambah kekuatan keamanan kriptografi ElGamal. Kelebihan dari algoritma El-Gamal adalah proses enkripsi pada *plaintext* yang sama akan menghasilkan *chippertext* yang berbeda, namun pada proses dekripsinya menghasilkan *plaintext* yang sama. Dan salah satu kelemahannya adalah perhitungan kuncinya yang memerlukan waktu yang cukup lama.

6.2 Saran

Berikut adalah beberapa saran untuk penggunaan dan pengembangan system aplikasi yang akan datang, berdasar pada hasil perancangan, implementasi dan ujicoba yang telah dilakukan penulis :

1. Untuk tetap menjaga keamanan *chippertext* hasil enkripsi dengan algoritma elgamal, kunci publik harus tetap di jaga dari manupulasi orang-orang yang tidak bertanggung jawab.
2. Untuk penelitian selanjutnya diharapka dapat mengimplementasikan algoritma ElGamal untuk aplikasi tanda tangan digital dan pertukaran kunci. Seperti pada transaksi *online*, *internet banking*, lembaga intelejen, militer dan sebagainya, alat-alat telekomunikasi seperti telepon seluler (*handphone*) dan jaringan komunikasi nirkabel (*wireless*).

3. Dapat mengimplementasikan algoritma El-Gamal menggunakan pemerograman lain seperti, *Java, C/C++, Visual Basic, Delphi* dan sebagainya.
4. Perlu dilakukan penelitian yang lebih mendalam untuk *plaintext* berupa file data, *Image* (citra), *video* dan sebagainya.
5. Teknologi keamanan yang di terapkan pada PT Medco E&P Indonesia masih berjalan pada *layer Application*, disarankan untuk penelitian berikutnya dapat melakukan pengembangan algoritma elgamal tersebut agar dapat berjalan secara *transparent* pada *layer transport*.

DAFTAR PUSTAKA

Ariyus, Donny. 2009. *Keamanan Multimedia.* Yogyakarta : Andi.

Ariyus, Donny. 2006. *Computer Security.* Yogyakarta : Andi.

Ariyus, Donny. 2008. *Pengantar Ilmu Kriptografi*. Yogyakarta : Andi.

Azikin, Askari. 2011. *Debian GNU/Linux.* Bandung : Informatika.

Ashari, Ahmad., Bernard, R.S., Wilfridus, B.T.H. 2010. *Linux System Administrator.* Bandung : Informatika.

Ghafur, Abdul. 2009. Implementasi Keamanan Email dengan Algortima ElGamal. Skripsi Mahasiswa Universitas Negeri Malang.

Hamidah, Siti Nur. 2009. *Konsep Matematis dan Proses Penyandian Kriptografi ElGamal.* Skripsi Mahasiswa Universitas Negeri Malang.

Kuncoro, Mudrajad. 2009. *Metode Riset Untuk Bisnis & Ekonomi*. Jakarta : Erlangga.

Nugroho, Bunafit. 2007. *Latihan Membuat Aplikasi Web PHP dan Mysql dengan Dreamweaver MX (6, 7, 2004) dan 8.* Yogyakarta : Gava Media.

Sidik, Betha. 2012. *Pemrograman Web PHP*. *Bandung* : Informatika.

Sopandi, Dede. 2008. *Instalasi dan Konfigurasi Jaringan Komputer*. Bandung : Informatika.

Stallings, William. 2001. *Komunikasi Data dan Komputer : Dasar-Dasar Komunikasi Data*. Jakarta : Selemba Teknik.

Yugianto, Gin-Gin dan Oscar Rachman. *Router Teknologi, Konsep, Konfigurasi dan Troubleshooting*. Bandung : Informatika.

Yani, Ahmad. 2008. *Panduan Menjadi Teknisi Jaringan Komputer*. Bandung : Kawan Pustaka.