Jurnal Ilmiah KURSOR
Menuju Solusi Teknologi Informasi
Vol. 1, No. 2, Juli 2005
ISSN 0216 - 0544

PEMBUATAN SISTEM ENKRIPSI PADA SISTIM INFORMASI JARINGAN KOMPUTER BERBASIS INTERNET

Bain Khusnul Khotimah, ST

Jurusan Teknik Informatika
Fakultas Teknik Universitas Trunojoyo

Email: bain@trunojoyo.ac.id

ABSTRAK

Pengamanan system informasi pada umumnya dikategorikan menjadi dua yaitu pencegahan (*preventif*) dan pengobatan (*recovery*). Usaha pencegahan dilakukan agar sistem informasi tidak memiliki lubang keamanan, sementara usaha-usaha pengobatan dilakukan apabila lubang keamanan sudah dieksploitasi. Pengamanan sistem informasi dapat dilakukan melalui beberapa layer yang berbeda pada protocol TCP/IP yang digunakan, yang ditempatkan pada server. Dimana secara fisik sistem ini diamankan dengan menggunakan "firewall" yang memisahkan sistem anda dengan Internet. Penggunaan teknik enkripsi dapat dilakukan di tingkat aplikasi sehingga data-data anda atau e-mail anda tidak dapat dibaca oleh orang yang tidak berhak. Agar data tidak dapat disadap oleh orang lain, maka data yang hendak dikirim di acak (enkripsi) terlebih dahulu. Mekanisme Enkripsi yang akan digunakan pada penelitian ini adalah mekanisme yang menggunakan kunci publik. Pada mekanisme kunci publik, terdapat 2 macam kunci yaitu kunci privat dan kunci publik. Kunci publik di hasilkan (*generate*) oleh kunci privat milik kita. Untuk selanjutnya kunci publik di sebar ke setiap orang yang akan berkomunikasi dengan kita. Di internet terdapat beberapa server kunci publik yang menyimpan kunci publik dari orang yang terdaftar di server tersebut. Publik key berfungsi untuk meng-enkripsi, dan data hasil enkripsi ini hanya bisa dibuka oleh kunci privat yang menghasilkan kunci publik peng-enkripsi tadi. Sedangkan untuk membuka file asli dengan menggunakan kunci privat. Cara ini yang disebut sebagai Sistem Kriptografi Asimetris.

Kata Kunci : *kunci, privat, publik , server, enkripsi, deskripsi*

1. PENDAHULUAN

Masalah keamanan merupakan salah satu aspek penting dari sebuah system informasi. Sayang sekali masalah keamanan ini sering kali kurang mendapat perhatian dari para pemilik dan pengelola sistem informasi. Seringkali masalah keamanan berada di urutan kedua, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila menggangu performansi dari sistem, seringkali keamanan dikurangi atau ditiadakan. Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual. Dengan perkembangan yang pesat di bidang teknologi komputer dan telekomunikasi, sangat penting nilai sebuah informasi menyebabkan seringkali informasi diinginkan hanya boleh diakses oleh orang-orang tertentu. Jatuhnya informasi ke tangan pihak lain (misalnya pihak lawan bisnis) dapat menimbulkan kerugian bagi pemilik informasi. Sebagai contoh, banyak informasi dalam sebuah perusahaan yang hanya diperbolehkan diketahui oleh orang-orang tertentu di dalam perusahaan tersebut, misalnya informasi tentang produk yang sedang dalam development, sehingga algoritma-algoritma dan teknik-

teknik yang digunakan untuk menghasilkan produk tersebut sangatlah rahasia. Untuk itu keamanan dari sistem informasi yang digunakan harus terjamin dalam batas yang dapat diterima. Jaringan komputer, seperti LAN dan Internet, memungkinkan untuk menyediakan informasi secara cepat. Ini salah satu alasan perusahaan atau organisasi mulai berbondong-bondong membuat LAN untuk system informasinya dan menghubungkan LAN tersebut ke Internet. Terhubungnya LAN atau komputer ke Internet membuka potensi adanya lubang keamanan (*security hole*) yang tadinya bisa ditutupi dengan mekanisme keamanan secara fisik. Ini sesuai dengan pendapat bahwa kemudahan (kenyamanan) mengakses informasi berbanding terbalik dengan tingkat keamanan sistem informasi itu sendiri. Semakin tinggi tingkat keamanan, semakin sulit (tidak nyaman) untuk mengakses informasi. Keamanan itu tidak dapat muncul demikian saja, dia harus direncanakan. Demikian pula di sisi pengamanan sebuah sistem informasi. Jika tidak kita budgetkan di awal, kita akan dikagetkan dengan kebutuhan akan adanya perangkat pengamanan (firewall, Intrusion Detection System, anti virus, Dissaster Recovery Center, dan seterusnya). Setiap orang yang berada pada jalur data tersebut, dimungkinkan untuk membaca data tersebut. Pembacaan data yang bukan tujuannya ini dikenal sebagai *sniff*. Program sniffer adalah program yang dapat digunakan untuk menyadap data dan informasi melalui jaringan komputer. Di tangan seorang admin, program sniffer sangat bermanfaat untuk mencari (*debug*) kesalahan di jaringan atau untuk memantau adanya serangan. Di tangan cracker, program sniffer dapat digunakan untuk menyadap password (jika dikirimkan dalam bentuk *clear text*) yang solusinya bisa diatasi dengan program enkripsi dan deskripsi untuk memproteksi data tersebut.

1.1. Rumusan Masalah

Berdasarkan pada permasalahan yang telah dijelaskan pada bagian latar belakang diatas, maka yang menjadi permasalahan adalah bagaimana membuat sistem pengamanan informasi yang bagus dengan menggunakan kriptografi, enkripsi, dan dekrtipsi (baik dengan menggunakan private-key maupun dengan menggunakan public-key).

2. TINJAUAN PUSTAKA

2.1. Protokol TCP/IP

TCP/IP adalah protokol yang tersedia untuk layanan aplikasi berorientasi internet dan intranet. TCP/IP sendiri sebenarnya merupakan suite dari gabungan beberapa protokol. Di dalamnya terdapat protokol TCP, IP, SMTP, POP, dan sebagainya. TCP (Transmission Control Protokol) melakukan transmisi data persegmen, artinya paket data dipecah dalam jumlah yang sesuai dengan besaran paket, kemudian dikirim satu persatu hingga selesai. Agar pengiriman data sampai dengan baik, maka pada setiap paket pengiriman, TCP akan menyertakan nomor seri (sequence number). Komputer mitra yang menerima paket tersebut harus mengirim balik sebuah sinyal *ACKnowledge* dalam satu periode yang ditentukan. Bila pada waktunya sang mitra belum juga memberikan ACK, maka terjadi " time out " yang menandakan pegiriman paket gagal dan harus diulang kembali. Model protocol TCP disebut sebagai *connection oriented protocol.*

2.2. Tcp Port

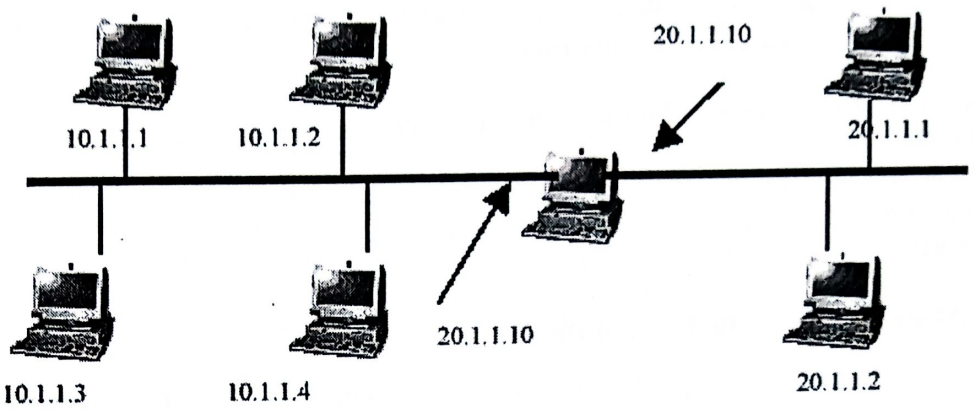
Port merupakan pintu masuk datagram dan paket data. Port data dibuat mulai dari 0 sampai dengan 65.536. Port 0 sampai dengan 1024 disediakan untuk layanan standar, seperti FTP, TELNET, Mail, Web dan lainnya. Port ini lebih dikenal dengan nama *well known* port. Dapat dilihat contoh port pada table dibawah.

No Port	Keterangan
21	FTP
110	POP3
23	Telnet
25	SMTP
80	HTTP/ Web

2.3. Proses Routing

Paket data yang akan dikirim dari satu jaringan ke jaringan lainnya dilakukan dengan proses *routing*. *Routing* selain bertugas menyampaikan paket data dari satu jaringan kejaringan lainnya, *routing* juga memilih " jalan terdekat " untuk mencapai suatu tujuan. Komponen untuk melakukan *routing* ini disebut dengan *router*.

Dalam Windows NT dapat berfungsi sebagai router dengan menyediakan minimal 2 network interface card (network interface dapat berbentuk Ethernet, token ring atau serial interface). Dalam hal ini windows NT disebut sebagai *multihomed compute*.



Gambar 1. Proses *Routing*

2.3.1. *Static Routing VS Dynamic Routing*

Router yang mempunyai table *routing* yang dikelola secara manual disebut *static router* yang ditunjukkan dalam Table yang berisi daftar jaringan yang dapat dicapai oleh router tersebut. *Static router* dapat mempelajari jaringan yang berada disekelilingnya secara terbatas (bila hanya 2 jaringan), tapi bila terdapat banyak jaringan, maka administrator harus mengelola table *routing* tersebut secara cermat. *Dynamic routing* adalah fungsi dari *routing* protocol yang berkomunikasi dengan router lainnya untuk dapat saling meremajakan (*update*) table *routing* yang ada. Dengan demikian, administrator tidak perlu melakukan *updating* jalur (*path*). Dynamic *routing* umumnya digunakan untuk jaringan komputer yang besar dan kompleks. Beberapa protocol yang digunakan dalam *dynamic routing* antara lain RIP (*Routing Information Protokol*) dan OSPF (*Open Shortest path First*).

2.4. Dasar-Dasar Keamanan Sistem Informasi

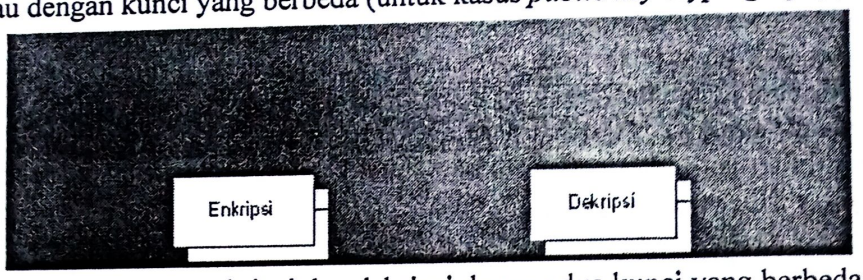
2.4.1. Terminologi

Kriptografi (*cryptography*) merupakan ilmu dan seni untuk menjaga pesan agar aman. (Cryptography is the art and science of keeping messages *secure*. "*Crypto*" berarti "*secret*" (rahasia) dan "*graphy*" berarti "*writing*". Para pelaku atau praktisi kriptografi disebut cryptographers. Sebuah algoritma kriptografik (cryptographic algorithm), disebut cipher, merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi. Biasanya kedua persamaan matematik (untuk enkripsi dan dekripsi) tersebut memiliki hubungan matematis yang cukup erat. Proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut *plaintext*) menjadi pesan yang tersembunyi (disebut *ciphertext*) adalah enkripsi (*encryption*). *Ciphertext* adalah pesan yang sudah tidak dapat dibaca dengan mudah. Menurut ISO 7498-2, terminologi yang lebih tepat digunakan adalah "*encipher*".Proses sebaliknya, untuk mengubah *ciphertext* menjadi *plaintext*, disebut dekripsi (*decryption*). Menurut ISO 7498-2, terminologi yang lebih tepat untuk proses ini adalah "*decipher*". *Cryptanalysis* adalah seni dan ilmu untuk memecahkan *ciphertext* tanpa bantuan kunci. *Cryptanalyst* adalah pelaku atau praktisi yang menjalankan *cryptanalysis*. *Cryptology* merupakan gabungan dari *cryptography* dan *cryptanalysis*.

2.4.2. Enkripsi

Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak. Dengan enkripsi data anda disandikan (*encrypted*) dengan menggunakan sebuah kunci (*key*). Untuk membuka (*decrypt*) data tersebut digunakan juga sebuah

kunci yang dapat sama dengan kunci untuk mengenkripsi (untuk kasus *private key* Enkripsi *cryptography*) atau dengan kunci yang berbeda (untuk kasus *public key cryptography*).



Gambar 2. Proses enkripsi dan dekripsi dengan dua kunci yang berbeda.

Secara matematis, proses atau fungsi enkripsi (*E*) dapat dituliskan sebagai:
E (M) = C (1)
dimana: M adalah plaintext (message) dan C adalah ciphertext.
Proses atau fungsi dekripsi (*D*) dapat dituliskan sebagai:
D(C) = M (2)

2.4.3. Algoritma dari Enkripsi dan Dekripsi.

Algoritma dari enkripsi adalah fungsi-fungsi yang digunakan untuk melakukan fungsi enkripsi dan dekripsi. Algoritma yang digunakan menentukan kekuatan dari enkripsi, dan ini biasanya dibuktikan dengan basis matematika. Berdasarkan cara memproses teks (*plaintext*), *cipher* dapat dikategorikan menjadi dua jenis: *block cipher* and *stream cipher*. Block *cipher* bekerja dengan memproses data secara blok, dimana beberapa karakter/data digabungkan menjadi satu blok. Setiap proses satu blok menghasilkan keluaran satu blok juga. Sementara itu stream cipher bekerja memproses masukan (karakter atau data) secara terus menerus dan menghasilkan data pada saat yang bersamaan.

2.4.4. Kunci yang digunakan dan panjangnya kunci.

Kekuatan dari penyandian bergantung kepada kunci yang digunakan. Beberapa algoritma enkripsi memiliki kelemahan pada kunci yang digunakan. Untuk itu, kunci yang lemah tersebut tidak boleh digunakan. Selain itu, panjangnya kunci, yang biasanya dalam ukuran *bit*, juga menentukan kekuatan dari enkripsi. Kunci yang lebih panjang biasanya lebih aman dari kunci yang pendek. Jadi enkripsi dengan menggunakan kunci 128-bit lebih sukar dipecahkan dengan algoritma enkripsi yang sama tetapi dengan kunci 56-bit. Semakin panjang sebuah kunci, semakin besar keyspace yang harus dijalani untuk mencari kunci dengan cara *brute force attack* atau coba-coba karena keyspace yang harus dilihat merupakan pangkat dari bilangan 2. Jadi kunci 128-bit memiliki keyspace 2128, sedangkan kunci 56-bit memiliki keyspace 256. Artinya semakin lama kunci baru bisa ketahuan.

2.4.4.1. Plaintext.

Plaintext adalah pesan atau informasi yang akan dikirimkan dalam format yang mudah dibaca atau dalam bentuk aslinya.

2.4.4.2. Ciphertext.

Ciphertext adalah informasi yang sudah dienkripsi. Kembali ke masalah algoritma, keamanan sebuah algoritma yang digunakan dalam enkripsi atau dekripsi bergantung kepada beberapa aspek. Salah satu aspek yang cukup penting adalah sifat algoritma yang digunakan. Apabila kekuatan dari sebuah algoritma sangat tergantung kepada pengetahuan (tahu atau tidaknya) orang terhadap algoritma yang digunakan, maka algoritma tersebut disebut "restricted algorithm". Apabila algoritma tersebut bocor atau ketahuan oleh orang banyak, maka pesan-pesan dapat terbaca. Tentunya hal ini masih bergantung kepada adanya kriptografer yang baik. Jika tidak ada yang tahu, maka sistem tersebut dapat dianggap aman (meskipun semu). Meskipun kurang aman, metoda pengamanan dengan *restricted algorithm* ini cukup banyak digunakan karena mudah implementasinya dan tidak perlu diuji secara mendalam. Contoh penggunaan metoda ini adalah enkripsi yang menggantikan huruf yang digunakan untuk mengirim pesan dengan huruf lain. Ini disebut dengan "*substitution cipher*".

2.4.4.3. Multiple-letter encryption

Untuk meningkatkan keamanan, enkripsi dapat dilakukan dengan mengelompokkan beberapa huruf menjadi sebuah kesatuan (unit) yang kemudian dienkripsi. Ini disebut *multiple-letter encryption*. Salah satu contoh multiple-letter encryption adalah "*Playfair*".

2.4.4.4. Data Encryption Standard (DES)

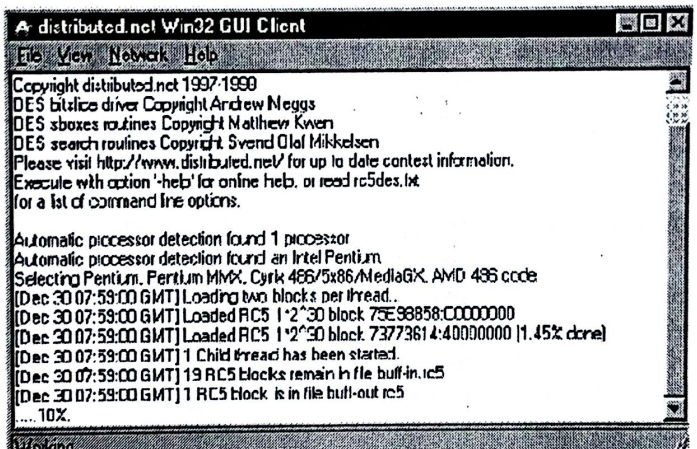
DES, atau juga dikenal sebagai *Data Encryption Algorithm* (DEA) oleh ANSI dan DEA-1 oleh ISO, merupakan algoritma kriptografi simetris yang paling umum digunakan saat ini. Ia dikenal sebagai Federal Information Processing Standard. Aplikasi yang menggunakan DES antara lain:

- enkripsi dari password di sistem UNIX
- berbagai aplikasi di bidang perbankan

2.4.4.5. Memecahkan DES

DES merupakan block chiper yang beroperasi dengan menggunakan blok berukuran 64-bit dan kunci berukuran 56-bit. Brute force attack dengan mencoba segala kombinasi membutuhkan 256 kombinasi atau sekitar 7x1017 atau 70 juta milyar kombinasi. DES dengan penggunaan yang biasa (*cookbook mode*) dengan panjang kunci 56 bit saat ini sudah dapat dianggap tidak aman karena sudah berhasil dipecahkan dengan metoda coba-coba (*brute force attack*).

Ada berbagai group yang mencoba memecahkan DES dengan berbagai cara. Salah satu group yang bernama *distributed.net* menggunakan teknologi Internet untuk memecahkan problem ini menjadi sub-problem yang kecil (dalam ukuran blok). Pengguna dapat menjalankan sebuah program yang khusus dikembangkan oleh tim ini untuk mengambil beberapa blok, via Internet, kemudian memecahkannya di computer pribadinya. Program yang disediakan meliputi berbagai operating system seperti Windows, DOS, berbagai variasi Unix, Macintosh. Blok yang sudah diproses dikembalikan ke *distributed.net* via Internet.



Gambar 3. peragaan client distributed.net untuk Windows 98

Perlu diingat bahwa group seperti EFF merupakan group kecil dengan budget yang terbatas. Dapat dibayangkan sistem yang dimiliki oleh *National Security Agency* (NSA) dari pemerintah Amerika Serikat1. Tentunya mereka dapat memecahkan DES dengan lebih cepat.

3. PEMBAHASAN

3.1. *Hash function - integrity checking*

Salah satu cara untuk menguji integritas sebuah data adalah dengan memberikan "checksum" bahwa data tersebut tidak berubah. Cara yang paling mudah dilakukan adalah dengan menjumlahkan karakter-karakter atau data-data yang ada sehingga apabila terjadi perubahan, hasil penjumlahan menjadi berbeda. Cara ini tentunya mudah dipecahkan dengan menggunakan kombinasi data yang berbeda akan tetapi menghasilkan hasil penjumlahan yang sama.

Pada sistem digital biasanya ada beberapa mekanisme pengujian integritas seperti antara lain:

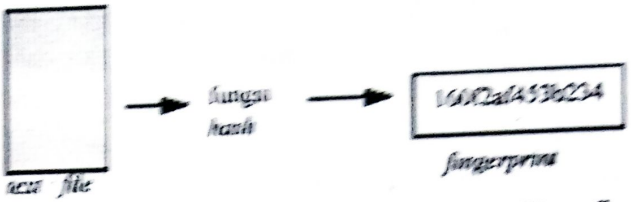
- parity checking
- checksum

• hash function

Hash function merupakan fungsi yang bersifat satu arah dimana jika kita masukkan data, maka dia akan menghasilkan sebuah "*checksum*" atau "*fingerprint*" dari data tersebut. Ada beberapa hash function yang umum digunakan, antara lain:

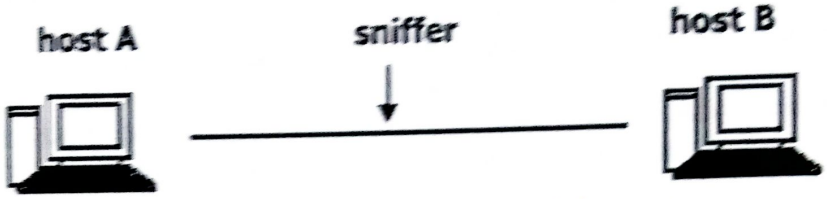
• MD5

• SHA



Gambar 4. Penggunaan fungsi hash yang menghasilkan fingerprint

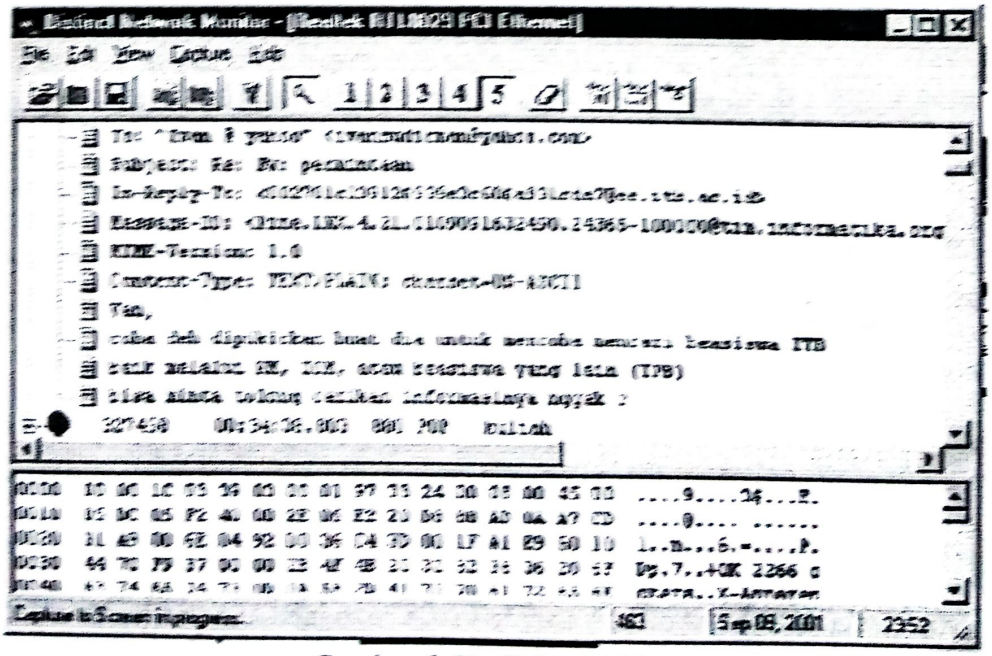
3.2. Sniffer



Gambar 5. Sniff Dalam Komunikasi Komputer

Program Sniffer yang digunakan adalah Network Monitor dari Distinct Corporation (http://www.distinct .com). Program ini merupakan versi trial yang berumur 10 hari. Di dalam komunikasi TCP/IP atau yang menggunakan model komunikasi 7 layer OSI, sebuah komputer akan mengirim data dengan alamat komputer tujuan. Pada sebuah LAN dengan topologi *bus* atau *star* dengan menggunakan hub yang tidak dapat melakukan switch (hub tersebut melakukan *broadcast*), setiap komputer dalam jaringan tersebut menerima data tersebut. Standarnya hanya komputer dengan alamat yang bersesuaian dengan alamat tujuanlah yang akan mengambil data tersebut. Tetapi pada saat sniff, komputer dengan alamat bukan alamat tujuan tetap mengambil data tersebut.

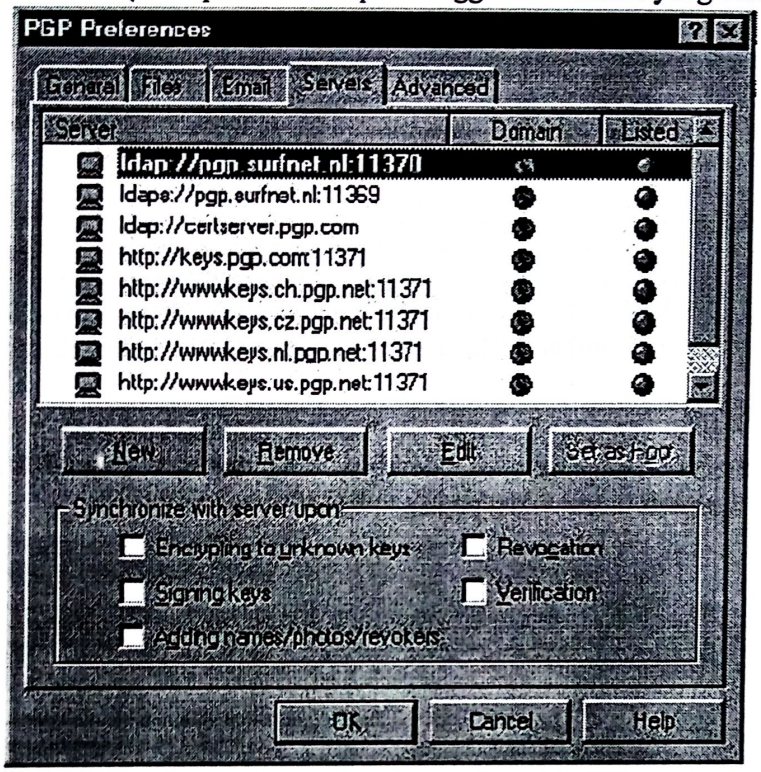
Sebelum melakukan sniff, pertama kali adalah membuka adapter (ethernet card), agar mengambil semua data yang melewatinya, sekalipun bukan sebagai alamat tujuan. Biasanya data yang melewati Adapter akan sangat banyak, untuk mempermudah pencarian, kegunakan fasilitas filter seperti terlihat. Hasil dari sniff pada protokol POP (Post Office Propotocol), dapat dilihat pada gambar 6.



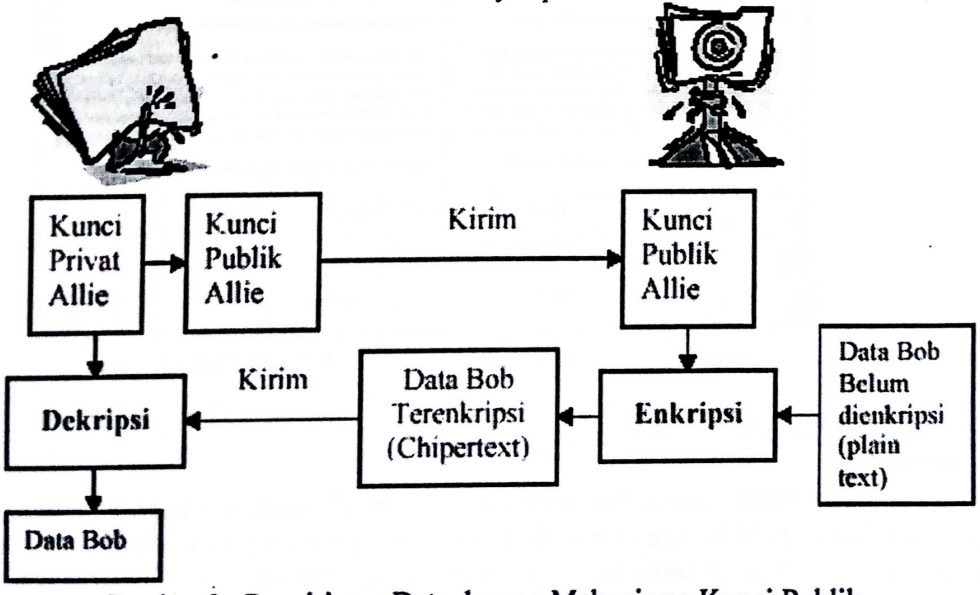
Gambar 6. Hasil data akhir

3.3. Pengacakan Data

Agar data tidak dapat disadap oleh orang lain, maka data yang hendak dikirim di acak (enkripsi) terlebih dahulu. Mekanisme Enkripsi yang akan digunakan pada percobaan ini adalah mekanisme yang menggunakan kunci publik. Pada mekanisme kunci publik, terdapat 2 macam kunci yaitu kunci privat dan kunci publik. Kunci publik di hasilkan (*generate*) oleh kunci privat milik kita. Untuk selanjutnya kunci publik di sebar ke setiap orang yang akan berkomunikasi dengan kita. Di internet terdapat beberapa server kunci publik, yang menyimpan kunci publik dari orang yang terdaftar di server tersebut. Publik key berfungsi untuk meng-enkripsi, dan data hasil enkripsi ini hanya bisa dibuka oleh kunci privat yang menghasilkan kunci publik peng-enkripsi tadi. Cara ini juga merupakan Sistem Kriptografi Asimetris. (Enkripsi dan dekripsi menggunakan kunci yang berbeda).



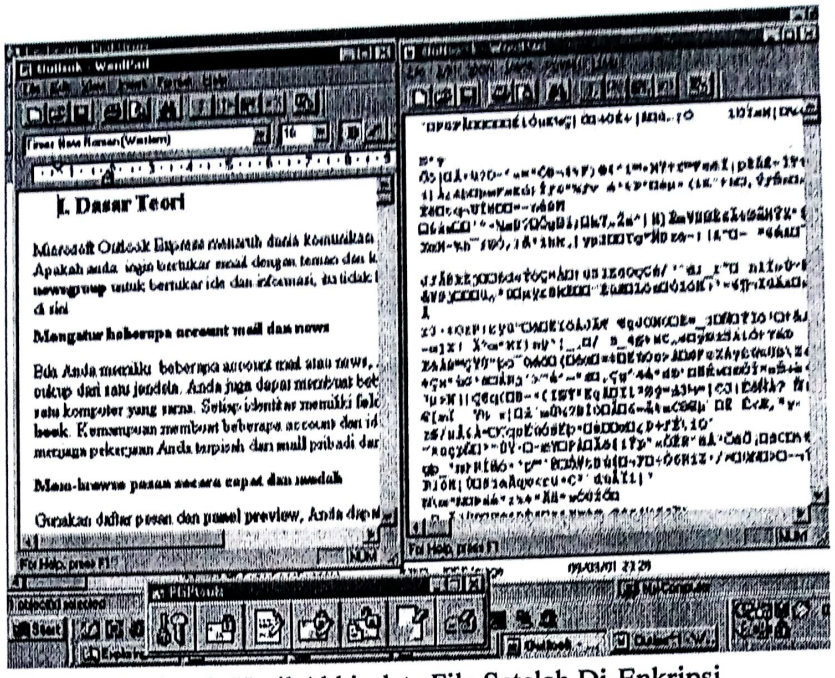
Gambar 7 : Server Penyimpan Kunci Publik



Gambar 8 . Pengiriman Data dengan Mekanisme Kunci Publik

3.4. Pembuatan Kunci Publik

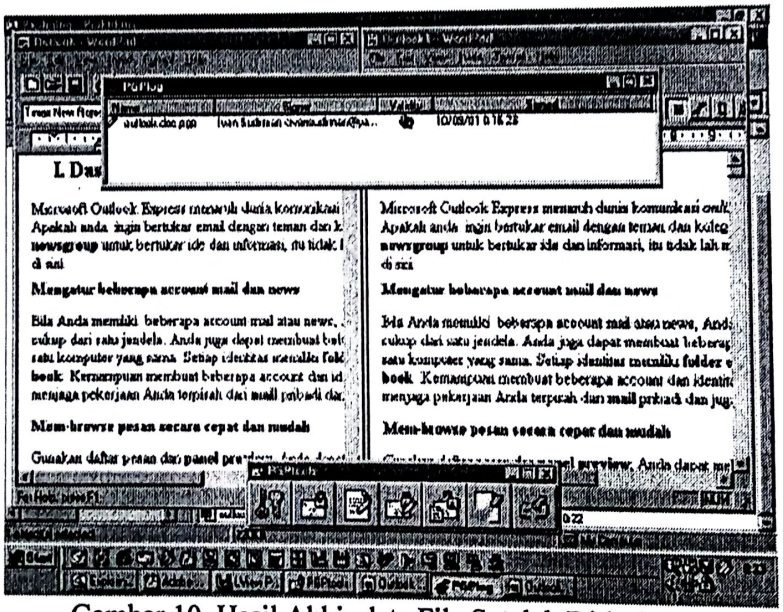
Langkah pertama sebelum dapat melakukan komunikasi dengan data yang ter-acak, adalah membuat kunci publik.



Gambar 9. Hasil Akhir data File Setelah Di-Enkripsi

3.5. Dekripsi File

Kebalikan dari enkripsi adalah dekripsi, dan untuk mendeteksi file dipe rlukan kunci privat.Hasilnya seperti ditunjukkan pada gambar 10



Gambar 10. Hasil Akhir data File Setelah Dideskripsi

4. KESIMPULAN DAN SARAN

4.1. Kesimpulan

Data yang telah diproteksi sebelum dikirim di acak (enkripsi) terlebih dahulu dengan menggunakan kunci publik. Kunci publik di hasilkan (*generate*) oleh kunci privat milik kita. Untuk selanjutnya kunci publik di sebar ke setiap orang yang akan berkomunikasi dengan kita. Di internet terdapat beberapa server kunci public yang menyimpan kunci publik dari orang yang terdaftar di server tersebut. Publik key berfungsi untuk meng-enkripsi, dan data hasil enkripsi ini hanya bisa dibuka oleh kunci privat yang menghasilkan kunci publik peng-enkripsi tadi. Dimana proses yang digunakan dalam penelitian diatas adalah pembuatan program mulai dari Inisialisasi, alamat e-mail, panjang kunci, masa berlakunya kunci, unci privat, pemilihan bilangan acak, pemilihan kunci public

yang telah dibuat dan pengiriman kunci public ke server. Sehingga yang bertugas untu membuka dan mengakses file atau data hanya orang yang berkepentingan saja, dan itupun harus ijin.

4.2. Saran

Sistem proteksi keamanan data selain menggunakan enkripsi dan deskripsi data diatas, masih banyak cara lain yang bisa digunakan misalnya dengan cara Port Scanning dan Blocking data yang ditempatkan pada layer protocol. Sehingga setiap system proteksi mempunyai kelebihan dan kekurangan, tergantung dari setiap kebutuhan layanan system proteksi itu sendiri.

5. DAFTAR PUSTAKA

1. Richard H. Baker, "Network Security: how to plan for it and achieve it,"McGraw-Hill International, 1995.
2. Tim Berners-Lee, "Weaving the Web: the past, present and future of the world wide web by its inventor," Texere, 2000
3. www. Ilmukomputer.com