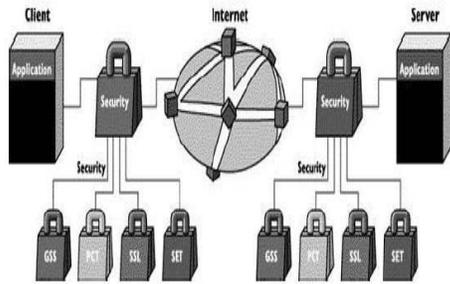


2.1.1 Internet Protocol Security (IPSec)

IPSec[2] adalah suatu algoritma keamanan yang memberikan mekanisme autentifikasi, kerahasiaan data, dan menggunakan suatu management key. Key yang dapat digunakan dapat dilihat pada gambar 2.



Gambar 2. Struktur Key pada IPSec

Setelah diberikan key data yang dikirimkan melalui internet di enkripsi terlebih dahulu dengan menggunakan key, pada sisi penerima data di dekripsi terlebih dahulu oleh server dan kemudian di teruskan ke tujuan.

2.1.2 Crypto IP Encapsulation (CIPE)

Crypto IP Encapsulation (CIPE)[3] adalah sistem IP-in-IP tunnel yang berjalan pada UDP. CIPE merupakan penyederhanaan teknik VPN dari IPSec. Dimana IPSec memerlukan banyak opsi dan memakan sumber yang lebih banyak.

CIPE link selalu menggunakan 2 endpoint. CIPE bekerja seperti sistem dial-up PPP, dimana pada CIPE digunakan 128-bit key yang digunakan untuk mengenkripsi data.

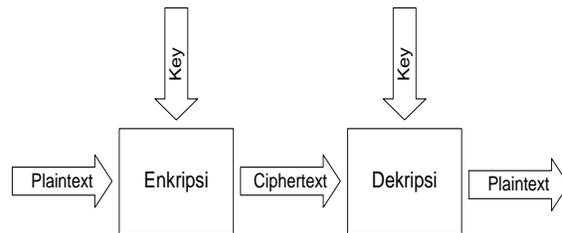
2.2 Kriptografi

Kriptografi (cryptography) merupakan ilmu dan seni penyimpanan pesan, data, atau informasi secara aman. Kriptografi (Cryptography) berasal dari bahasa Yunani yaitu dari kata Crypto dan Graphia yang berarti penulisan rahasia. Kriptografi adalah suatu ilmu yang mempelajari penulisan secara rahasia. Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut Cryptology. Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah.

Dalam menjaga kerahasiaan data, kriptografi mentransformasikan data jelas (plaintext) ke dalam bentuk data sandi (ciphertext) yang tidak dapat dikenali. Ciphertext inilah yang kemudian dikirimkan oleh pengirim (sender) kepada penerima (receiver). Setelah sampai di penerima, ciphertext tersebut ditransformasikan kembali ke dalam bentuk plaintext agar dapat dikenali.

Proses tranformasi dari plaintext menjadi ciphertext disebut proses Encipherment atau enkripsi (encryption), sedangkan proses mentransformasikan kembali ciphertext menjadi plaintext disebut proses dekripsi (decryption).

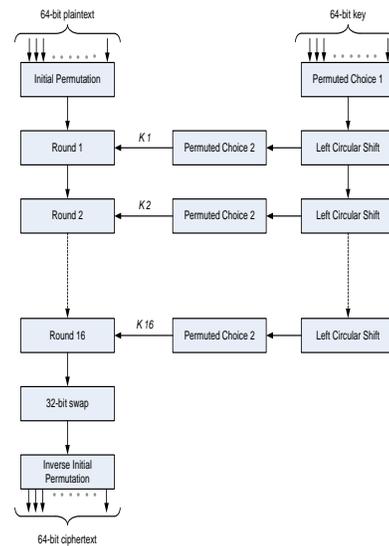
Untuk mengenkripsi dan mendekripsi data. Kriptografi menggunakan suatu algoritma (cipher) dan kunci (key). Cipher adalah fungsi matematika yang digunakan untuk mengenkripsi dan mendekripsi. Sedangkan kunci merupakan sederetan bit yang diperlukan untuk mengenkripsi dan mendekripsi data. Secara sederhana dapat digambarkan pada gambar 3.



Gambar 3. Proses Enkripsi dan Dekripsi

2.2.1 Data Encryption Standard (DES)

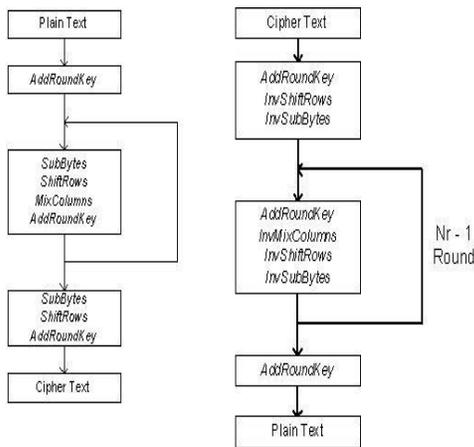
Secara umum algoritma DES[4] terbagi menjadi 3 kelompok dimana kelompok satu dengan lainnya saling berinteraksi dan saling terkait. Gambar 4 menunjukkan kelompok-kelompok tersebut, yaitu: pemrosesan kunci, enkripsi data 64 bit, dan dekripsi data 64 bit. Algoritma DES dirancang untuk menulis dan membaca berita blok data yang terdiri dari 64 bit di bawah control kunci 64 bit. Dalam pembacaan berita, haruslah dikerjakan dengan menggunakan kunci yang sama dengan waktu menulis berita, dengan penjadwalan alamat kunci bit yang diubah sehingga proses membaca adalah kebalikan dari proses menulis



Gambar 4. Algoritma DES

2.2.2 Advanced Encryption Standard (AES)

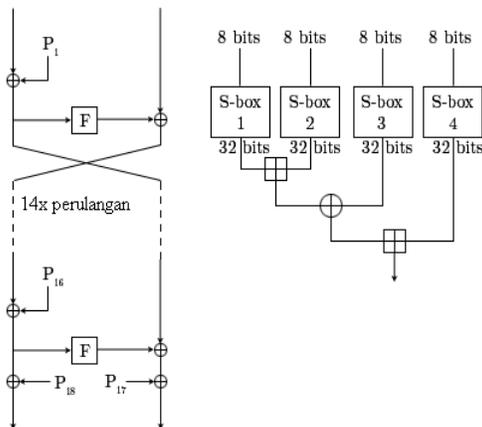
Proses enkripsi pada algoritma AES[5] terdiri dari 4 jenis transformasi bytes, yaitu SubBytes, ShiftRows, MixColumns, dan AddRoundKey. Pada awal proses enkripsi, input yang telah dikopikan ke dalam state akan mengalami transformasi byte AddRoundKey. Setelah itu, state akan mengalami transformasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey secara berulang-ulang sebanyak Nr. Proses ini dalam algoritma AES disebut sebagai round function. Round yang terakhir agak berbeda dengan round-round sebelumnya dimana pada round terakhir, state tidak mengalami transformasi MixColumns.



Gambar 5. Proses Enkripsi dan Dekripsi pada AES

Transformasi cipher dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan inverse cipher yang mudah dipahami untuk algoritma AES. Transformasi byte yang digunakan pada invers cipher adalah InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey.

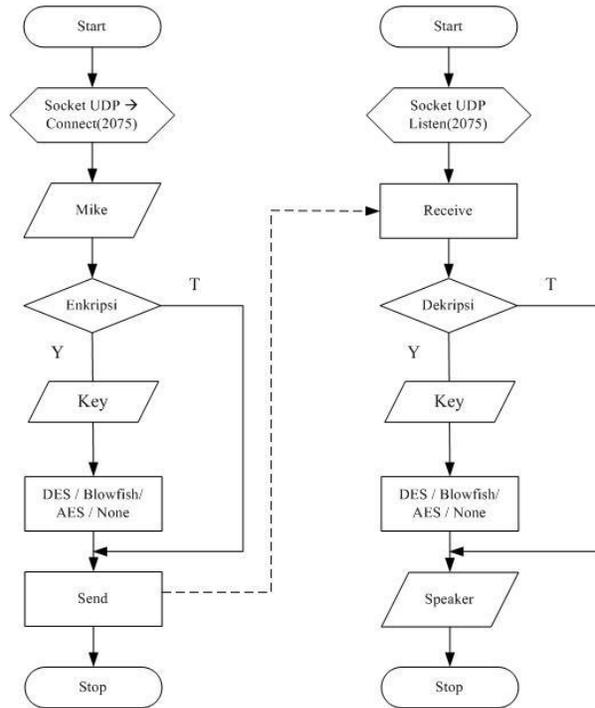
2.2.3 Blowfish



Gambar 6. Algoritma Blowfish dan Fungsi F

Blowfish memiliki 64 bit block dan panjang key antara 32 – 448 bit. Memiliki 16x perulangan Feistel Chiper dan menggunakan S-boxes. Blok diagram metode Blowfish dapat dilihat pada gambar 6.

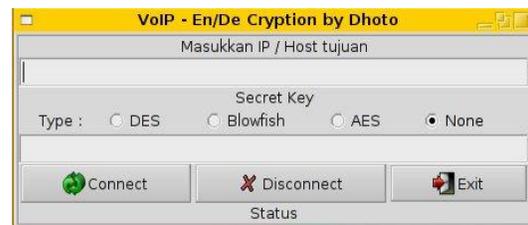
2.3 VoIP Linux dan Kriptografi



Gambar 7. Proses Enkripsi dan Dekripsi pada VoIP

VoIP yang digunakan berjalan di sistem operasi Linux. Dimana menggunakan socket programming dan berjalan di UDP. Suara yang masuk secara Real-Time di kirim ke tujuan, apabila ingin di enkripsi terlebih dahulu maka akan bertambah proses enkripsi, begitu juga pada sisi penerima. Kriptografi yang digunakan adalah DES, Blowfish dan AES.

Untuk Graphical User Interface (GUI), digunakan pemrograman GTK[8]. Tampilan GUI aplikasi VoIP yang digunakan tampak pada gambar 8.



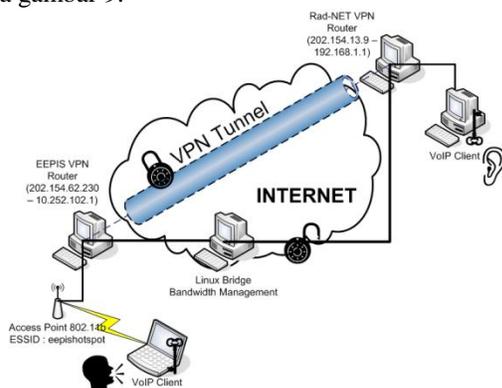
Gambar 8. GUI Aplikasi VoIP dengan GTK

2.4 Wireless LAN 802.11b

Wireless LAN[9] adalah Local Area Network yang menggunakan gelombang radio sebagai carinya. Koneksi terakhir dengan pengguna menggunakan wireless, dimana dalam jangkauan tertentu dapat memberikan koneksi jaringan. Area yang dicakup bisa dalam ruangan atau seluruh kampus. Pada backbone jaringan tetap menggunakan infrastruktur kabel, yang terhubung dengan beberapa akses point yang menghubungkan pengguna dengan jaringan yang ada. IEEE 802.11b[10], adalah standarisasi untuk WI-FI. Standar ini digunakan pada infrastruktur Wireless LAN, untuk IEEE 802.11b menggunakan frekuensi 2.4 GHz sebagai carinya.

III. BENTUK EKSPERIMEN

Pada eksperimen ini digunakan Jalur Internet yang terhubung antara EEPIS dengan Internet Service Provider (ISP), dalam eksperimen ini ISP yang digunakan adalah RAD-Net. Di sisi EEPIS dibangun sebuah VPN Router dengan sistem operasi Linux, dan di sisi RAD-Net juga dibangun sebuah VPN Router. Selain itu disisi EEPIS juga dibangun sebuah Linux Bridge yang berguna sebagai pengatur Bandwidth. Pada sisi jaringan EEPIS client terhubung dengan Access Point Wireless LAN dengan ESSID : eepishotspot. Topologi jaringan pada eksperimen ini dapat dilihat pada gambar 9.



Gambar 9. Topologi Jaringan

Aplikasi VoIP dengan Kriptografi diinstall di PC VoIP Client. Dengan perjanjian terlebih dahulu, kata kunci yang digunakan sebagai key harus sama. Percobaan dilakukan dalam beberapa mode kriptografi, yang pertama tanpa enkripsi, kemudian dengan metode DES, Blowfish dan AES.

Pada Linux bridge digunakan teknik Hierarchical Token Bucket (HTB)[11] dan Class Base Queueing (CBQ)[12] sebagai pengatur Bandwidth. Untuk memonitoring trafik jaringan digunakan

protokol Simple Network Management Protocol (SNMP).

Spesifikasi PC Router yang digunakan adalah Pentium 4, 2.8GHz dengan memory 256MByte, Ethernet 100Mbps, sistem operasi yang digunakan Debian GNU/Linux[13]. Sedangkan spesifikasi VoIP Client adalah Laptop Compaq Presario, Pentium 4, 2.4GHz dengan Memory 256MByte dan kartu Ethernet 100Mbps.

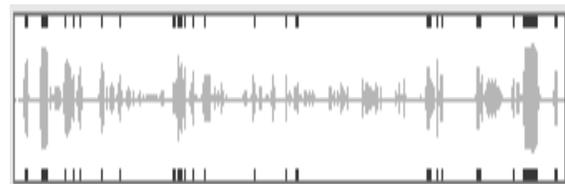
IV. HASIL PERCOBAAN

4.1 Analisa Keamanan VPN

Pada percobaan keamanan VPN, tools yang digunakan adalah Tethereal[14] dan Sniffit[15] yang dipasang pada Linux Bridge. Dimana hasil yang didapatkan adalah dengan menggunakan VPN baik IPsec maupun CIPE, kedua tools tersebut tidak dapat mendeteksi adanya data yang lewat dari VoIP client melainkan komunikasi antar VPN Router. Apabila tanpa menggunakan VPN, tools masih dapat menangkap adanya komunikasi antar VoIP Client.

4.2 Gambar Analisa Sinyal VoIP

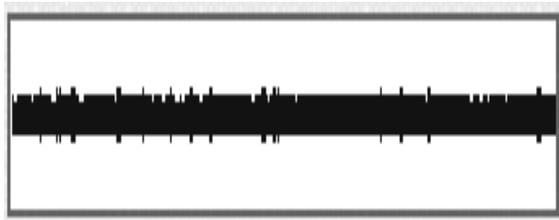
Analisa sinyal VoIP ini dilakukan dengan mengambil simple gambar sinyal yang telah direkam, kemudian hasil perekaman file tersebut dikirim melalui VoIP dengan enkripsi maupun tanpa menggunakan enkripsi. Pengujian sinyal ini dilakukan pada tiga kondisi yaitu sinyal yang dikirimkan dengan VoIP tanpa enkripsi, sinyal yang dikirimkan dengan VoIP dimana pada sisi pengirim dienkripsi tetapi pada penerima tidak di dekripsi, dan sinyal dikirim dengan menggunakan VoIP dimana pada sisi pengirim dienkripsi dan pada sisi penerima didekripsi. Hasil gambar sinyal VoIP dapat dilihat pada gambar 10-13.



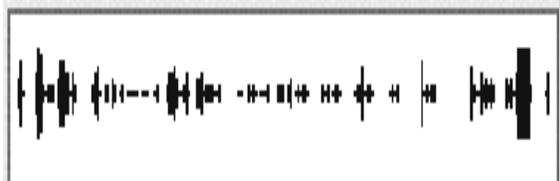
Gambar 10. Sinyal asli yang dikirimkan



Gambar 11. Sinyal VoIP yang diterima tanpa proses enkripsi dan dekripsi



Gambar 12. Sinyal VoIP yang Terenkripsi



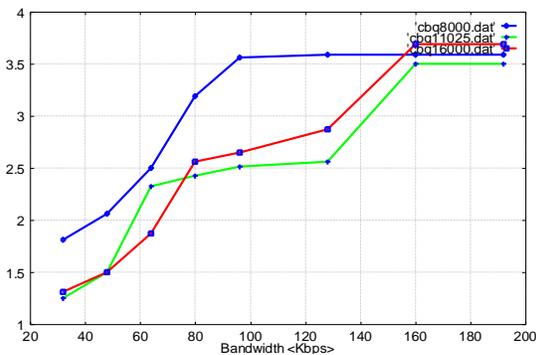
Gambar 13. Sinyal VoIP terenkripsi yang telah didekripsi kembali

Pada gambar 13, saat pengiriman di sisi pengirim sinyal dienkrif terlebih dahulu baru dikirimkan, dan pada sisi penerima sinyal didekripsikan kembali agar bisa didengarkan. Hasil sinyal yang telah didekripsikan hampir sama dengan sinyal aslinya sehingga bisa didengarkan meskipun ada delay.

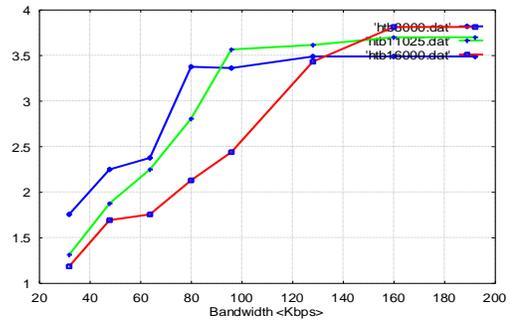
4.3 Analisa Mean Opinion Score (MOS)

Pada analisa MOS, digunakan bandwidth manager CBQ dan HTB dilakukan dengan tahapan bandwidth yang berbeda dari 16kbps hingga 256kbps dengan tingkat kenaikan sebesar 16 kbps.

Dengan memperdengarkan suara hasil percobaan dan melakukan survey, maka didapat nilai MOS yang terlihat pada gambar 14 dan 15.



Gambar 14. Grafik MOS terhadap bandwidth dengan bandwidth manager CBQ



Gambar 15. Grafik MOS terhadap bandwidth dengan bandwidth manager HTB

Gambar 14 dan 15, menunjukkan bahwa intelligibility suara yang diwakili nilai MOS, naik seiring dengan bertambahnya bandwidth. Disana juga nampak bahwa pada saat kebutuhan bandwidth belum terpenuhi (suara terputus-putus), dengan bandwidth yang sama suara dengan frekwensi sampling lebih tinggi intelligibility-nya lebih rendah daripada suara dengan frekwensi sampling lebih rendah. Namun pada saat kebutuhan bandwidthnya telah terpenuhi (suara tidak terputus-putus), dengan bandwidth yang sama suara dengan frekwensi sampling lebih tinggi intelligibility-nya lebih tinggi daripada suara dengan frekwensi sampling lebih rendah.

V. KESIMPULAN

Adapun simpulan yang diperoleh dari model ini adalah sebagai berikut:

1. Pada VoIP Sistem Operasi Linux dengan jaringan nir-kabel 802.11b terdapat korelasi terhadap bandwidth dan intelligibility suara.
2. Teknologi VPN dan Kriptografi dapat digunakan sebagai salah satu cara untuk mengamankan data pada komunikasi VoIP.
3. Antara VPN-IPSec dan VPN-CIPE, sama-sama memiliki kemampuan untuk mengamankan data, tetapi sebaiknya menggunakan CIPE karena lebih mudah dalam setting penggunaan dan opsi.
4. Sinyal hasil enkripsi bentuknya tidak beraturan atau berbeda dengan sinyal aslinya sehingga suara yang telah terenkripsi tersebut tidak dapat disadap. Komunikasi suara melalui jaringan komputer, terbukti apabila bandwidth yang tersedia lebih sempit dari bandwidth yang dibutuhkan, maka suara yang diterima menjadi terputus-putus dan ada delay.

DAFTAR PUSTAKA

- [1] RFC 2401, "Security Architecture for the Internet Protocol".
- [2] Racoon IPSec-Tools Internet Key Exchange (IKE), <http://ipsec-tools.sourceforge.net/>
- [3] CIPE, Crypto IP Encapsulation, <http://sites.inka.de/~bigred/devel/cipe.html>
- [4] National Bureau of Standards, "Data Encryption Standard", FIPS PUB 46 (January 1977).
- [5] "AES", <http://csrc.nist.gov/CryptoToolkit/aes/>
- [6] B. Schneier, Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish), 1994
- [7] Sritrusta Sukaridhoto, Titon Dutono, Nonot Harsono, Iwan Sarif, Deni Kurniawan, "Teknik Keamanan pada VoIP dengan Virtual Private Networking dan Kriptografi Serta Korelasi Bandwidth dan Intelligibility Suara", Proceeding of Indonesian Conference on Telecommunication 2005 (ICTEL 2005) Vol. 1 Thn 2005 hal 175-180.
- [8] GIMP Toolkit, <http://www.gtk.org>
- [9] Wireless LAN – wikipedia, http://en.wikipedia.org/wiki/Wireless_lan
- [10] IEEE802.11b, <http://en.wikipedia.org/wiki/802.11b>
- [11] Martin Devera, "HTB Manual User" <http://luxik.cdi.cz/~devik/qos/>
- [12] Bert Hubert, "Linux Advanced Routing and Traffic Control", <http://www.lartc.org>
- [13] Debian, The Universal Operating System, <http://www.debian.org>
- [14] Ethereal: A Network Protocol Analyzer, <http://www.ethereal.com>
- [15] Sniffit a packet sniffer, <http://reptile.rug.ac.be/~coder/sniffit/sniffit.html>
- [16] Vivien Arif, Titon Dutono, Sritrusta Sukaridhoto, "Studi Korelasi Bandwidth dan Intelligibility Suara (Modul Telephony)", Tugas Akhir EEPIS-ITS, 2005.
- [17] Kasiani, Sritrusta Sukaridhoto, Nonot Harsono, "Aplikasi Sistem Keamanan Pada VoIP menggunakan Algoritma Advanced Encryption Standard(AES)", Tugas Akhir EEPIS-ITS, 2005.
- [18] Yeni Ika Setyorini, Sritrusta Sukaridhoto, Nonot Harsono, "Aplikasi Sistem Keamanan Pada VoIP menggunakan Algoritma Blowfish", Tugas Akhir EEPIS-ITS, 2005.
- [19] Wingga Latuayu Hidayat, Sritrusta Sukaridhoto, Iwan Sarif, "Implementasi VPN-IPSec pada Jaringan EEPIS-ITS", Tugas Akhir EEPIS-ITS, 2005.
- [20] Radian Glorifia, Sritrusta Sukaridhoto, Iwan Sarif, "Implementasi VPN-CIPE pada Jaringan EEPIS-ITS", Tugas Akhir EEPIS-ITS, 2005.
- [21] Awan Asmara Frima, Sritrusta Sukaridhoto, Mochamad Zen Samsono Hadi, "Implementasi VPN-MPLS pada Jaringan EEPIS-ITS", Tugas Akhir EEPIS-ITS, 2005.
- [22] Syaiful Riszal, Titon Dutono, Sritrusta Sukaridhoto, "Studi Korelasi Bandwidth dan Intelligibility Suara (Modul Bandwidth Management)", Tugas Akhir EEPIS-ITS, 2005.
- [23] Dimas Arya Wahyu K, Sritrusta Sukaridhoto, Aries Pratilarso, "Pembuatan Prototipe BTS untuk Komunikasi Wireless LAN", Tugas Akhir EEPIS-ITS, 2005
- [24] Miftahuddin Darwadi, Sritrusta Sukaridhoto, Nonot Harsono, "Aplikasi Sistem Keamanan Pada VoIP menggunakan Algoritma Data Encryption Standard(DES)", Tugas Akhir EEPIS-ITS, 2005.