KATA PENGANTAR

Puji syukur ke hadirat Allah SWT, atas nikmat, hidayah serta kasih sayang-Nya sehingga penulis dapat menyelesaikan skripsi dengan judul "**IMPLEMENTASI DAN ANALISIS APLIKASI TRANSFER FILE ANTAR PC MENGGUNAKAN ALGORITMA RC4 128 BIT DAN AES 128 BIT**". Hanya kepada-Nya kita menyembah dan memohon. Serta sholawat terhadap junjungan Rasulullah Muhammad SAW, keluarga, sahabat serta seluruh umatnya. Skripsi ini disusun untuk memenuhi sebagian persyaratan memperoleh gelar Sarjana Komputer di Jurusan Program Teknologi Informasi dan Ilmu Komputer Universitas Brawijaya Malang.

Tidak banyak yang bisa penulis sampaikan kecuali ungkapan terima kasih kepada berbagai pihak yang telah memberikan bimbingan, arahan, dan dukungan hingga penulisan skripsi ini dapat terselesaikan. Pada kesempatan kali ini, penulis mengucapkan banyak terima kasih kepada:

1. Bapak Ir. Sutrisno, M.T, Bapak Ir. Heru Nurwasito, M.Kom, Bapak Himawat Aryadita, S.T, M.Sc, dan Bapak Eddy Santoso, S.Kom selaku Ketua, Wakil Ketua 1, Wakil Ketua 2 dan Wakil Ketua 3 Program Teknologi Informasi dan Ilmu Komputer Universitas Brawijaya.
2. Bapak Drs. Marji, M.T dan Bapak Issa Arwani, S.Kom, M.Sc selaku Ketua dan Sekretaris Program Studi Teknik Informatika Universitas Brawijaya.
3. Bapak Aswin Suharsono, selaku Dosen Pembimbing I yang telah banyak meluangkan waktunya untuk memberikan arahan, masukan, dan bimbingan kepada penulis selama penyusunan skripsi ini.
4. Bapak Barlian Henryranu Prasetio ST., MT, selaku Dosen Pembimbing II yang telah banyak meluangkan waktunya untuk memberikan arahan, masukan, dan bimbingan kepada penulis selama penyusunan skripsi ini.
5. Ungkapan terima kasih dan penghargaan yang sangat special penulis haturkan dengan rendah hati dan rasa hormat kepada kedua orang tua penulis yang tercinta, Ayahanda H. Widji Suroyo, SH. MH. dan ibunda Hj. Nuraini, Amd Kep. serta kakak Firly Wulandari, SE. dan kakak Endi

Suhendri SE. serta adik penulis Frizky Winanda yang dengan segala pengorbanan tak akan pernah penulis lupakan atas jasa-jasa mereka. Do'a restu, nasehat dan petunjuk dari mereka kiranya merupakan dorongan moril yang paling efektif bagi kelanjutan studi penulis hingga saat ini.

6. Keluarga Besar Bapak H. Agus Rus Herudjianto, ST. dan Hj. Eny Hariyanti, SE serta Kiki Harfiqi dan Hardhika O., yang terus memberikan dorongan moral agar terselesaikannya skripsi ini.
7. Seorang terkasih dan tercinta Ravi Indracahya K. P., ST. yang telah memberikan banyak dukungan moral, doa dan memberikan inspirasi.
8. Harfinda Avrilida Fajrin, ST., Denisa Novinda A.P., ST., Lipo Pamuncak, ST., Muhammad Fadhli Madjid ST. dan Rega Putra Permana ST., yang selalu memberikan dorongan semangat dan do'a serta selalu ada saat penulis membutuhkan bantuan mereka.
9. Segenap Bapak dan Ibu Dosen Teknik Informatika yang telah membantu selama kegiatan belajar, semoga ilmu yang telah diajarkan dapat bermanfaat dikemudian hari.
10. Teman-teman LEGENDARY TIF, seluruh angkatan 2007, yang merupakan angkatan penuh cerita yang secara langsung maupun tidak langsung memberikan dukungan moral.

Penulis menyadari bahwa skripsi ini masih jauh dari kesempurnaan, maka saran yang konstruktif dari semua pihak sangat diharapkan demi penyempurnaan selanjutnya. Semoga skripsi ini dapat bermanfaat bagi semua pihak, khususnya bagi penulis dan para pembaca pada umumnya.

Malang, 10 April 2013

Penulis

ABSTRAK

Aplikasi transfer file sangat menguntungkan bagi masyarakat luas, dengan adanya aplikasi ini maka komunikasi data akan lebih efisien dibandingkan menggunakan *bluetooth, flashdisk* maupun *email* karena bersifat *real time*. Aplikasi ini juga dilengkapi oleh metode keamanan AES 128 bit dan RC4 128 bit, tujuannya adalah untuk memastikan bahwa hanya penerima yang dituju yang dapat membacanya. Dengan adanya kedua algoritma ini, tentunya mempengaruhi performansi pengiriman data, sehingga diperlukan suatu pengujian dan analisis untuk mengetahui kualitas data yang dihasilkan oleh masing-masing algoritma. Parameter Quality of Service (QoS) yang diujikan adalah *throughput* dan *delay* (waktu pengiriman). Pengukuran QoS tersebut mengunakan *tools wireshark* 1.84.

Berdasarkan parameter *throughput,* nilai *throughput* tertinggi tanpa enkripsi adalah 3472,490 kbps. Sedangkan, setelah diterapkan algoritma RC4 128 bit adalah 3427,112 kbps dan nilai AES 128 bit yaitu 3414,162 kbps. Nilai *delay* total terendah pada RC4 128 bit adalah 8.886 s dan tertinggi adalah 201,067 s, sedangkan nilai *delay* total terendah pada AES 128 bit yaitu 59.184 s dan tertinggi adalah 1418,613 s. Secara keseluruhan, algoritma RC4 128 bit merupakan algoritma yang performansinya jauh lebih baik daripada menggunakan AES 128 bit dengan *throughput* yang lebih besar, serta waktu pengiriman yang lebih sedikit

Kata Kunci : RC4, AES, 128, Bit, *Throughput, Delay*

ABSTRACT

File transfer application is very beneficial for wider community, with this application, the data communication be more efficient than using bluetooth, flash disk, or e-mail because it's real time. The algorithm that used to create this application is AES 128 bit and RC4 128 bit, the purpose is to ensure that only the intended receiver that can read. With the two algorithm, of course affect the performance of data transmission and thus a testing and analysis to determine the quality of the data produced by each algorithm. Quality of service parameters tested is throughput and delay. That Qos measurement using the tools wireshark 1.84

Based on throughput parameters, highest throughput value without encryption is 3472,490 kbps. Where as after applied RC4 128 bit algorithm is 3427,112 kbps and AES 128 bit is 3414,162 kbps. By value total delay RC4 128 bits has the lowest delay is 8,886 s and has the highest delay is 201,067 s. While on the AES 128 bit has the lowest delay is 59,184 s and has the highest delay is 1416,613 s. Over all, RC4 128 bit algorithm has better than AES 128 bit algorithm, because has highest throughput and has lowest total delay.

Key **:** RC4, AES, 128, Bit, *Throughput, Delay*

DAFTAR ISI

halaman

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR ISTILAH

AddRoundKey	Melakukan XOR antara *state* sekarang *round key*.
Ad-Hoc	Kumpulan node *wireless mobile* yang secara dinamis keberadaannya tanpa menggunakan jaringan infrastruktur yang ada.
AES 128 bit	Algoritma yang memproses enkripsi per 128 blok (*Block Cipher)*.
Algoritma	Urutan langkah instruksi untuk menyelesaikan masalah.
Array	Kumpulan data-data beripe sama dan menggunakan nama yang sama
Bit	Ukuran terkecil data dari sebuah komputer.
Block Cipher	Algoritma kriptografi simetrik yang mengenkripsi satu blok *plaintext* dengan jumlah bit tertentu dan menghasilkan blok *ciphertext* dengan jumlah bit yang sama.
Broadcast	Sebuah metode pengiriman data, dimana data dikirim ke banyak titik sekaligus, tanpa melakukan pengecekan apakah titik tersebut siap atau tidak, atau tanpa memperhatikan pakah data itu sampai atau tidak
Byte	Sekumpulan dari bit yang terdiri dari 8 bit.
Ciphertext	Pesan yang telah melalui proses enkripsi
Dekripsi	Mengubah kode-kode yang tidak dimengerti (*ciphertext*) menjadi pesan asli (*plaintext*).
Delay	Waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan (total).
Enkripsi	Mengubah pesan asli (*plaintext*) menjadi kode-kode yang tidak dimengerti (*ciphertext*).

File	Kumpulan byte-byte yang disimpan dalam media penyimpanan
Flowchart	Metode untuk menggambarkan tahap-tahap penyelesaian masalah (prosedur) beserta aliran data dengan simbol-simbol standar yang mudah dipahami
Generate pseudorandom	Suatu urutan nilai yang tidak dapat ditebak polanya dengan mudah, sehingga urutan nilai tersebut dapat dianggap sebagai suatu keadaan acak.
Input	Semua data dan perintah yang dimasukkan ke dalam memori komputer untuk selanjutnya diproses.
Instalasi	Pemasangan sistem operasi pada sistem komputer.
IP	Suatu alamat host/komputer yang berada diperangkat yang akan terhubung ke jaringan, baik itu *wireless* (nirkabel/tanpa kabel) maupun *wired* (kabel).
Key bit array	Kunci enkripsi untuk menentukan sebuah proses enkripsi berubah atau tidak.
Output	Keluaran data setelah diproses.
Packet Loss	Suatu parameter yang menggambarkan kondisi yang menunjukkan jumlah total paket yang hilang.
Password	Kumpulan karakter atau *string* yang digunakan oleh pengguna jaringan atau sebuah sistem operasi yang mendukung banyak pengguna (*multiuser*) untuk memverifikasi identitas dirinya kepada sistem keamanan yang dimiliki oleh jaringan atau sistem tersebut.

Plaintext	Teks ini merupakan pesan yang ditulis yang memiliki makna.
Port	Mekanisme yang mengizinkan sebuah komputer untuk mendukung beberapa sesi koneksi dengan komputer lainnya dan program di dalam jaringan
Protokol	Sebuah aturan atau standar yang mengatur atau mengijinkan terjadinya hubungan, komunikasi, dan perpindahan data antara dua atau lebih titik komputer.
Quality of Services (QoS)	Kemampuan jaringan untuk menyediakan layanan yang lebih baik pada suatu trafik tertentu mulai berbagai macam tekhnologi meliputi jaringan.
RC4 128 bit	Algoritma yang memproses input pada suatu saat (*Stream Cipher)* dan mengenkripsi per 128 bit.
Real time	Kondisi pengoperasian dari suatu sistem perangkat keras dan perangkat lunak yang dibatasi oleh rentang waktu dan memiliki tenggat waktu (*deadline*) yang jelas, relatif terhadap waktu suatu peristiwa atau operasi terjadi.
Sourcecode	Kumpulan pernyataan atau deklarasi bahasa pemrogramman komputer yang ditulis dan dapat di baca manusia
SSID	Nama jaringan bersama di antara semua perangkat dalam jaringan wireless
State	Kumpulan karakter.
Stream Cipher	Sistem sandi simetrik yang proses penyandiannya dilakukan bit-per-bit atau byte-per-byte per satuan waktu tertentu.

SubBytes	Mensubtitusikan 1 sel dengan sel yang sesuai pada S-Box.
Throughput	Kecepatan transfer data efektif, yang diukur dalam bps.
Topologi	Aturan yang menjelaskan hubungan geometris antara unsur-unsur dasar penyusun jaringan, yaitu *node, link*, dan *station*.
Wireshark	Salah satu dari sekian banyak tool *Network Analyzer* yang banyak digunakan oleh *Network administrator* untuk menganalisa kinerja jaringannya terrmasuk protokol didalamnya