BAB IV

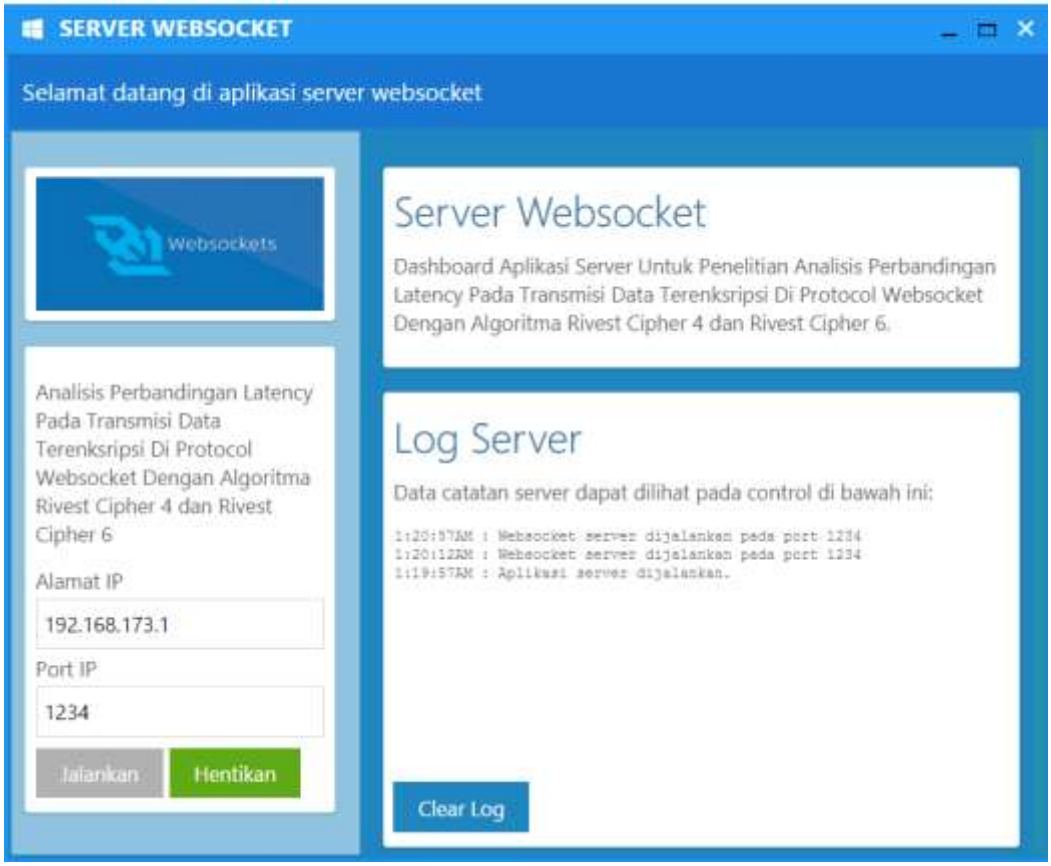
HASIL DAN UJI COBA

IV.1. Tampilan Hasil

Analisa berdasarkan penjelasan mengenai algoritma RC4 dan RC6, dapat diketahui beberapa perbedaan mendasar antara RC6 dengan RC4. RC6 menggunakan 4 register berukuran b/4-bit, sedangkan RC4 bekerja pada tingkat dasar, mari kita state-array 4 bit. Hal ini dikarenakan akan sulit menggambarkan proses RC4 secara manual dengan state-array 256 bit. RC6 menggunakan 4 register karena dirancang untuk memenuhi spesifikasi AES, yaitu kemampuan beroperasi dalam mode 128 bit. Dengan 4 register kerja, maka besar masing-masing register kerja yang diperlukan hanya 32 bit (4 × 32 = 128 bit) dijelaskan mengenai tampilan hasil dari Analisis Perbandingan Latency Pada Transmisi Data Terenkripsi di Protokol Websocket Dengan Algoritma RC4 Dan RC6 yang dapat dilihat sebagai berikut :

IV.1.1. Tampilan *Server Websocket*

Tampilan *server websocket* untuk menjalankan alamat ip dan port ip dapat terlihat seperti pada gambar IV.1 berikut :



Gambar IV.1. Tampilan *Server Websocket*

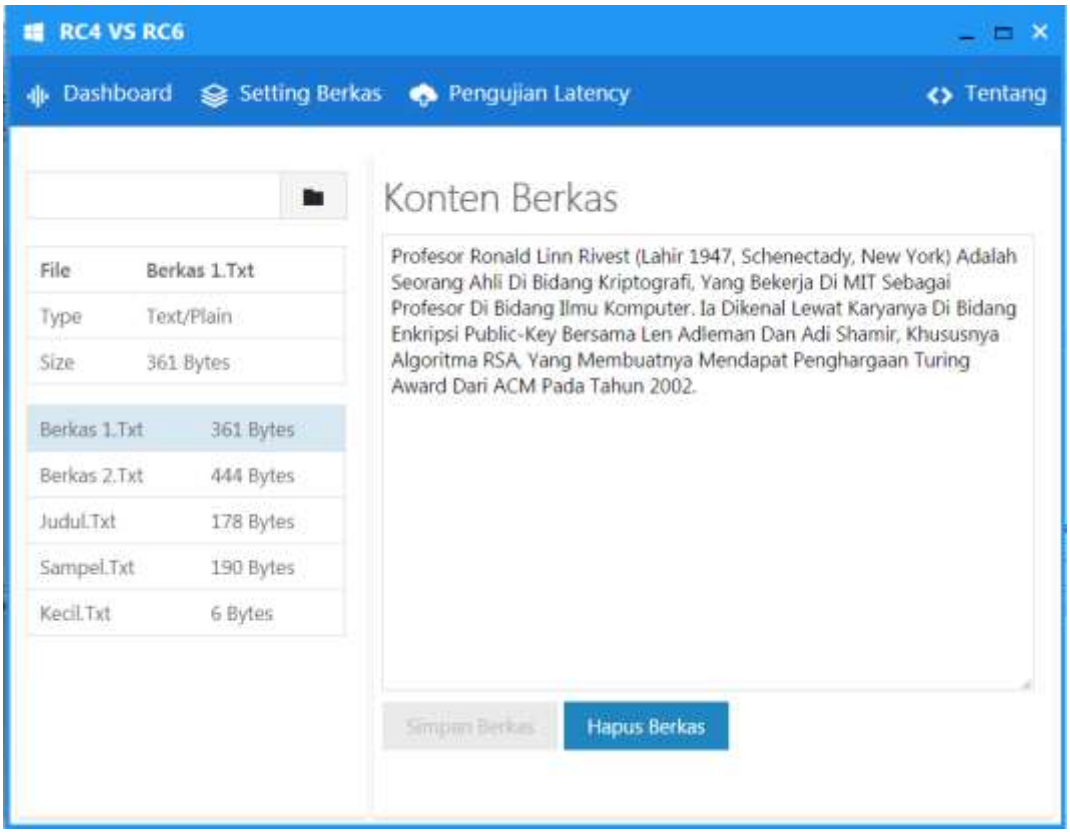
IV.1.2. Tampilan Dashboard

Tampilan dashboard untuk menu utama aplikasi dapat terlihat seperti pada gambar IV.2 berikut :

Gambar IV.2. Tampilan *Dashboard*

IV.1.3. Tampilan *Form* Setting Berkas

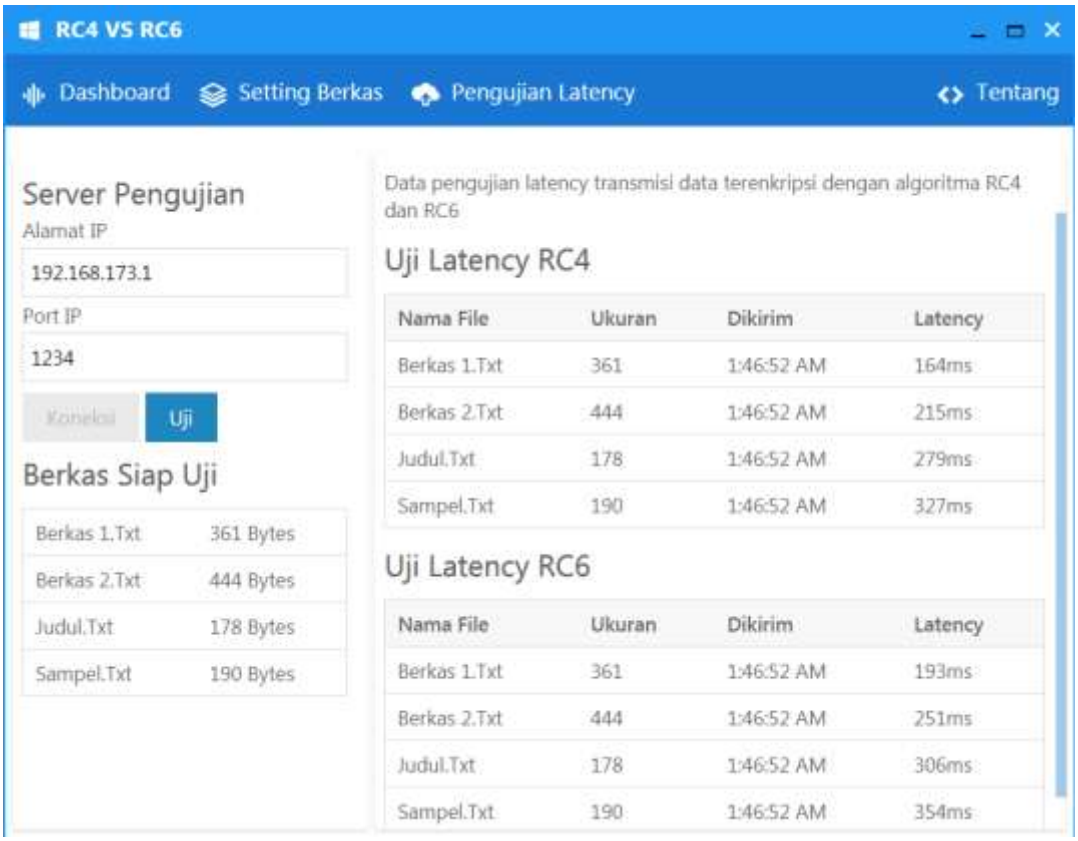
Tampilan *Form* setting berkas untuk mengetahui kapasitas berkas yang telah di ambil dapat terlihat seperti pada gambar IV.3 berikut :



Gambar IV.3. Tampilan *Form* Setting Berkas

IV.1.4. Tampilan *Form* Pengujian Latency

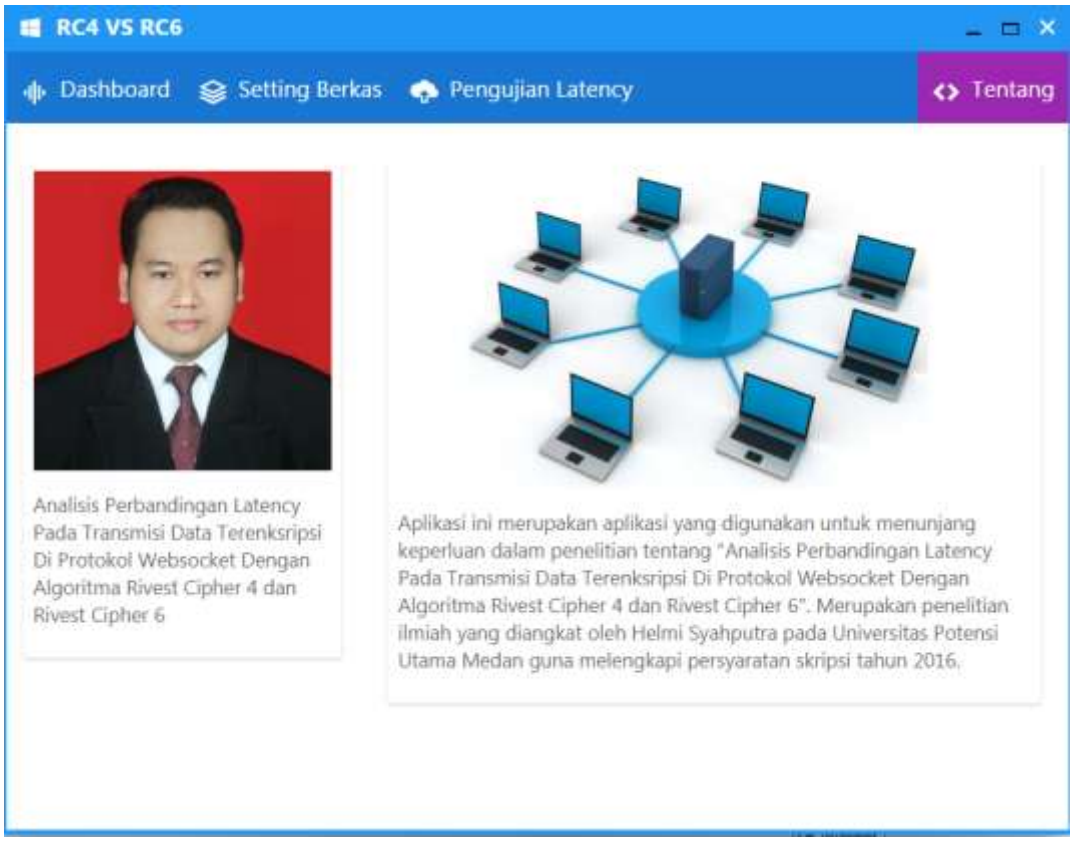
Tampilan *Form* pengujian latency untuk melakukan pengolahan pengujian latency dapat terlihat seperti pada gambar IV.4 berikut :



Gambar IV.4. Tampilan *Form* Pengujian Latency

IV.1.5. Tampilan *Form* Tentang

Serangkaian kegiatan untuk melihat tentang aplikasi dapat terlihat seperti pada gambar IV.5 berikut :



Gambar IV.5. Tampilan *Form* Tentang

IV.2. Pembahasan

Studi kasus RC4 proses pertama dalam algoritma RC-4 adalah Key Scheduling Algorithm. KSA ini merupakan inisialisasi untuk pentabelan S-BOX dan kunci. RC4 mempunyai sebuah S-Box, S0,S1,...,S255, yang berisi permutasi dari bilangan 0 sampai 255. Terdapat dua indeks yaitu i dan j yang diinisialisasi dengan bilangan nol. Untuk menghasilkan random byte langkahnya adalah sebagai berikut :

For i ← 0 to 255

S[i] ← i

Dalam operasi selanjutnya, RC-4 akan mengubah isi kotak-S tergantung kunci K dengan operasi sebagai berikut :

j=0

for i ← 0 to 255

j ← (j +S[i] +K[i]) mod 256

pertukarkan isi S[i] dan isi S[j]

Dengan demikian berakhirlah proses KSA. Untuk selanjutnya untuk membangkitkan kunci enkripsi, dilakukan proses PRGA atau Pseudo Random Generation Algorithm.

Algoritma PRGA adalah sebagai berikut :

i ← 0

j← 0 i ←(i + 1) mod 256

j ←(j + S[i]) mod 256

pertukarkan isi S[i] dan S[j]

k = S [S[i] + S [j]] mod 256

perhatikan bahwa k kecil merupakan kunci yang langsung beroperasi terhadap plaintext, sedangkan K besar adalah kunci utama induk.

Bila terdapat plaintext P, maka operasi enkripsi berupa :

C = P XOR k

IV.2.1. Spesifikasi Uji Coba Program

Uji coba terhadap sistem bertujuan untuk memastikan bahwa sistem sudah berada pada kondisi siap pakai. Instrumen yang digunakan untuk melakukan pengujian ini yaitu dengan menggunakan:

1. Satu unit laptop dengan spesifikasi sebagai berikut:
    a. Processor Intel Core I3

b. Memory 2 Gb

c. Hardisk 500 Gb

2. Perangkat Lunak dengan spesifikasi sebagai berikut:

a. Java

b. iReport

c. MySQL Server Versi 10

Pengujian program dilakukan untuk mengetahui tingkat keakuratan data dan informasi yang dihasilkan oleh program yang telah dirancang, adapun data yang diuji adalah :

1. *Performance* program yang dirancang untuk menyesuaikan kenyamanan *user* dalam mengakses sistem.
2. Keakuratan informasi dari *input*, proses dan *output* pada sistem.

IV.2.2. Hasil Uji Coba

Setelah melakukan uji coba terhadap sistem, maka dapat disimpulkan hasil yang didapatkan yaitu:

1. Sistem memiliki *Performance* yang relatif stabil.
2. Sistem telah menghasilkan informasi yang *valid*.
3. Antarmuka yang sederhana dapat mempermudah pengguna dalam mempelajari sistem ini.
4. Kebutuhan akan informasi laporan sangat cepat disajikan.

Tabel. IV.1 Blackbox Testing

No	Form	Keterangan	Hasil
1	Jalankan alamat IP dari server untu menjalakan server websocket	Sistem akan menjalankan setelah menekan jalan form server	[√] Jalankan [ ] Hentikan
2	Pilih berkas yang akan di setting	Sistem	[√] diterima

	berkas	memproses berkas yang ada di form setting berkas	[ ] ditolak
3	Pengujian latency untuk memperbandingkan RC4 dan RC6	Sistem akan melakukan pengujian di form pengujian latency	[√] Koneksi [ ] Uji

IV.3. Kelebihan dan Kekurangan Sistem

Setiap sistem memiliki kelebihan dan kekurangan, berikut ini adalah kelebihan dan kekurangan sistem yang telah dibuat.

IV.3.1. Kelebihan Sistem

Kelebihan sistem ini diantaranya yaitu :

1. Waktu yang dibutuhkan untuk proses *start-up* relatif singkat.
2. *Performance* sistem relatif stabil.
3. Sistem mampu menghasilkan informasi yang sesuai dengan yang diharapkan.
4. Algoritma enkripsi RC4 dan RC6 merupakan algoritma enkripsi yang cukup aman dan memiliki performa tinggi.

IV.3.2. Kekurangan Sistem

Adapun kekurangan sistem yang telah dibuat diantaranya yaitu :

1. Sistem ini belum memiliki modul yang lengkap.

Sistem ini belum memiliki akses *online* sehingga penyebaran informasi data tidak bekerja dengan efektif.