

PENAMBAHAN FITUR ENKRIPSI *RIVEST CODE 6* WEBSOCKET UNTUK PENGAMANAN ALIRAN DATA MESSAGING

Husnul Atho' Mubarak
(14.04.1.1.1.00100)

Pembimbing 1 : Dwi Kuswanto, S.Pd., M.T.

Pembimbing 2 : Yoga Dwitya Pramudita, S.Kom., M.Cs.

ABSTRAK

Protokol *websocket* menyediakan komunikasi *realtime* dua arah. Namun dengan menerapkan protokol *websocket*, ancaman keamanan akan lebih banyak. Salah satu serangan yang sering terjadi adalah *packet monitoring* yang dilakukan oleh pihak-pihak tidak bertanggung jawab. Untuk menjaga kerahasiaan dan keaslian data dari serangan tersebut. Salah satu teknik yang dapat digunakan untuk pengamanan data yaitu dengan menerapkan metode enkripsi. Pada penelitian ini metode enkripsi yang digunakan adalah *Rivest Code 6* (RC6) metode tersebut memiliki performa tinggi dalam prosesnya menggunakan operasi-operasi primitif, sehingga tidak terlalu mempengaruhi kinerja protokol *websocket*. Hasil dari uji coba *avalanche effect* didapatkan total perubahan untuk algoritma *Rivest Code 6* (RC6) berdasarkan *plaintext* sebesar 28.29% dan berdasarkan kunci sebesar 52.28%. Sedangkan untuk *Transport Layer Security* (TLS) didapatkan total perubahan untuk berdasarkan *plaintext* sebesar 42.50% dan berdasarkan kunci 53.19%. Hasil uji coba performa kecepatan pengiriman pesan didapatkan nilai rata-rata keseluruhan waktu pengiriman pesan sebesar 10673 *millisecond* untuk *Transport Layer Security* (TLS) dan 6964 *millisecond* untuk *Rivest Code 6* (RC6). *Library websocket* hasil modifikasi juga mampu melakukan komunikasi terenkripsi pada kondisi *link* komunikasi dengan tingkat probabilitas *packet loss* dibawah 12%.

Kata Kunci : Protokol *websocket*, keamanan data, performa kecepatan dan enkripsi RC6.

[HALAMAN INI SENGAJA DI KOSONGKAN]