IMPLEMENTASI ALGORITMA RSA (RIVEST-SHAMIR-ADLEMAN) PADA LAYANAN *CHATTING* BERBASIS LAN (*LOCAL AREA NETWORK*)

[1]Dony Catur Dermawan. [2]Ari Eko W.,S.T.,M.Kom., [3]Triawan Adi C.,M.Kom.
Jurusan Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Jember
Email : donycad2212@gmail.com

ABSTRAK

Pertukaran pesan (*chatting*) sudah luas digunakan oleh berbagai kalangan. Pesan yang dikirimkan sering berisi informasi yang penting. Masalah keamanan informasi pesan (*chatting*) seringkali kurang mendapat perhatian dari perancang dan pengelola informasi. Dalam pencegahannya dapat digunakan algoritma kriptografi kunci publik sehingga pesan (*chatting*) yang akan dikirimkan diamankan dan dirahasiakan. Salah satu metode kriptografi kunci publik yang paling aman dalam jaringan digunakan algoritma RSA (Rivest-Shamir-Adleman). Tujuan penelitian ini adalam mengimplementasikan algoritma RSA (Rivest-Shamir-Adleman) pada layanan *chatting* berbasis LAN *(Local Area Network)* sebagai solusi untuk mengamankan pesan yang dikirimkan. Selanjutnya pesan (*chatting*) yang terenkripsi dikirimkan melalui jaringan untuk dideskripsi menjadi pesan plainteks. Jika hasilnya dapat dideskripsikan oleh penerima maka pesan yang dikirimkan terjamin keasliannya. Pesan yang dikirimkan melalui jaringan, pesan tersebut sangat sulit dideskripsi tanpa mengetahui kunci privat.

Kata kunci : *chatting*, RSA (Rivest-Shamir-Adleman), Kriptografi