

ABSTRAK

Keamanan data adalah suatu hal yang sangat perlu diperhatikan dalam dunia komunikasi dan kriptografi adalah solusinya. Algoritma RSA merupakan algoritma kriptografi simetris yang masih memiliki ketahanan dari ancaman sampai saat ini. Kunci RSA dengan panjang 1024 bit dapat memakan waktu 1.43×10^{213} tahun jika menggunakan *brute force*.

Dalam tugas akhir ini, akan diterapkan algoritma RSA pada aplikasi *chatting*, dimana dengan menerapkan mekanisme kriptografi akan menutup celah keamanan yang ada pada aplikasi pesan instan tersebut. Dengan penerapan aplikasi dapat dihasilkan mekanisme komunikasi yang aman untuk dipakai dalam komunikasi penting agar tidak disadap pihak yang tidak bertanggung jawab. Hasil penerapan algoritma menambah tingkat keamanan dari data yang dikirimkan. Text yang dikirim berubah menjadi ciphertext acak yang hanya dapat didekripsi pada saat sampai ditujuan.

Kata Kunci: *Cryptography, RSA, Chat Encrypted, Client-Server Chat.*