

ABSTRAK

Komunikasi pada zaman modern seperti sekarang meliputi berbagai macam cara seperti video, telepon, langsung, dan melalui teks yang dikirimkan dari perangkat ke perangkat lainnya. Banyak pengguna obrolan berbasis teks ini memerlukan privasi obrolannya aman dari orang lain termasuk peretas yang ingin membaca dan mengetahui obrolan tanpa izin dari pengguna.

Untuk memperkuat keamanan dan kerahasiaan obrolan pengguna dari seorang peretas, obrolan seorang pengguna sebaiknya diamankan dengan teknologi pengamanan yang baik, salah satunya yaitu dengan metode kriptografi berbasis *lattice*, metode pengamanan ini merupakan metode terbaru untuk mengamankan kerahasiaan suatu data, dimana metode ini memiliki model enkripsi dua kunci sehingga sulit untuk dimengerti oleh para peretas.

Berdasarkan pemaparan diatas, maka dikembangkan sebuah aplikasi obrolan dengan keamanan kriptografi berbasis lattice sehingga dapat membuat pengguna lebih merasa nyaman dan aman ketika menggunakan aplikasi. Khususnya untuk aplikasi obrolan

Kata kunci: kriptografi, lattice, obrolan, keamanan, android.