

## Abstrak

Tugas akhir ini melakukan mekanisme untuk meyakinkan penerima SMS bahwa pengirim SMS merupakan pengirim yang sebenarnya, yaitu dengan mengimplementasikan *digital signature* dalam pengiriman dan penerimaan SMS menggunakan algoritma RSA dan fungsi *hash* MD5. *Digital signature* mencakup aspek keamanan nirpenyangkalan yang mengakibatkan pengirim SMS tidak dapat menyangkal telah mengirim SMS, otentikasi yang meyakinkan penerima SMS tentang identitas pengirim SMS, dan integritas data yang menyatakan bahwa isi pesan asli dari pengirim SMS dan tidak dimanipulasi.

Dalam tugas akhir ini telah dibuat suatu aplikasi untuk membuat *digital signature* dengan algoritma RSA dan fungsi *hash* MD5 untuk keperluan pengiriman SMS. Teknologi yang dilakukan dalam pembuatan aplikasi adalah J2ME. Tujuan dari penggunaan *digital signature* pada aplikasi SMS adalah untuk meyakinkan otentikasi pengirim pesan, menjaga integritas pesan, dan juga mencegah penyangkalan dari pengirim pesan.

Dalam tugas akhir ini telah dilakukan pengujian pembuatan dan verifikasi *digital signature*. Dari hasil pengujian didapatkan bahwa semakin besar peningkatan panjang bit kunci, maka waktu pembuatan dan verifikasi *digital signature* juga meningkat secara eksponensial. Peningkatan panjang bit kunci juga menyebabkan peningkatan ukuran tanda tangan yang dihasilkan.

**Kata kunci:** SMS, *digital signature*, algoritma RSA, fungsi *hash* MD5, waktu pembuatan dan verifikasi, ukuran tanda tangan.