Abstrak

Digital signature adalah proses pemberian nilai kriptografis pada sebuah dokumen, dimana nilai kriptografis ini bergantung pada dokumen dan pengirimnya. Jadi untuk setiap dokumen yang berbeda dan/atau pengirim yang berbeda maka nilai kriptografis yang dihasilkan untuk *digital signature* berbeda.

Tugas akhir ini membahas pembubuhan *digital signature* untuk file executable JAR. pembubuhan digital signature ini menggunakan fungsi hash untuk mendapatkan *message digest* dari file yang kemudian diencrypt menggunakan algoritma *digital signature* RSA.

Fungsi hash yang digunakan dalam aplikasi ini menggunakan algoritma MAC, dimana algoritma ini menggabungkan algoritma fungsi hash satu arah yaitu MD5 dengan sebuah kunci rahasia, sehingga walaupun algoritma MD5 telah dikriptanalisis maka *message digest* tetap aman karena kriptanalis harus mengetahui kunci rahasia yang dibutuhkan.

Dalam tugas akhir ini dibangun dua aplikasi. Berbasis PC dan berbasis *mobile device*. Aplikasi berbasis PC akan menyediakan fasilitas upload file executable JAR beserta penambahan *digital signature* ke dalamnya dan juga fasilitas download dan pengecekan terhadap file executable JAR yang telah diupload. Sedangkan aplikasi berbasis mobile device hanya akan menyediakan fasilitas download file executable JAR beserta pengecekan terhadap digital signature di dalamnya.

Tugas akhir ini dapat memperlihatkan *digital signature success* jika dalam pengujian yang dilakukan tidak merubah file dan kunci sedikit pun. Sedangkan *digital signature failed* jika salah satu atau kedua-duanya mengalami perubahan.

Kata kunci: *Digital Signature, MAC algotrithm, RSA algorithm*