

ABSTRAK

APLIKASI KEAMANAN DATA *MULTIMEDIA MESSAGE SERVICE* (MMS) PADA *MICROSOFT OFFICE FILE* MEMANFAATKAN ALGORITMA *RIVEST-SHAMIR ADLEMAN* (RSA) DAN *BLOWFISH* BERBASIS ANDROID

Oleh:

Abdul Aziz

1210705001

Penggunaan *Multimedia Message Service* (MMS) pada telepon seluler menjadi salah satu pilihan dalam melakukan pertukaran data. Permasalahannya, celah keamanan terbesar pada pertukaran data melalui MMS yaitu pesan yang dikirimkan akan disimpan di *Multimedia Messaging Service Center* (MMSC) dan *operator* atau orang yang mempunyai hak akses penuh dapat melihat *file* yang dikirimkan. Dengan alasan tersebut butuh metode yang dapat mengamankan data MMS agar tidak diketahui oleh orang yang tidak berhak yaitu salah satunya dengan kriptografi. Kriptografi yang dipakai menggunakan algoritma *hybrid* yaitu dalam penelitian ini menggabungkan antara algoritma kunci simetris *Blowfish* yang memakai satu kunci mempunyai kelebihan dalam kecepatan operasi, dan algoritma kunci asimetris *Rivest-Shamir Adleman* (RSA) yang memakai dua kunci yaitu kunci publik dan kunci privat mempunyai tingkat keamanan yang lebih tinggi. Estimasi waktu yang dicapai dalam melakukan enkripsi, baik menggunakan algoritma *Blowfish* maupun algoritma RSA ternyata tidak bergantung pada besar ukuran *plaintext*-nya ataupun panjang kunci yang dipakai.

Kata kunci : MMS, Simetris, Asimetris, *Blowfish*, RSA

UNIVERSITAS ISLAM NEGERI
SUNAN GUNUNG DJATI
BANDUNG