ABSTRAK

Kerahasiaan data adalah hal yang penting dalam komunikasi data. Ada beberapa algoritma enkripsi yang biasa digunakan seperti, DES, Triple DES, Blowfish, IDEA, dsb. Algoritma-algoritma tersebut begitu rumit dan sulit dimengerti, memang itu alasannya, 'tampilan keamanan', semakin sulit suatu algoritma dimengerti, maka semakin aman. Namun, bagi para pemakai, mereka tidak memikirkan seberapa sulit algoritmanya, yang penting data mereka aman. Ada dua syarat keamanan suatu sistem enkripsi, yaitu *true random bits* dan *key space* yang sangat besar untuk algoritma enkripsi tersebut. Jika dua syarat tersebut dipenuhi, tidak masalah seberapa kompleks algoritma enkripsinya. Bahkan semakin sederhana semakin baik, karena semakin sederhana, maka semakin sedikit proses komputasinya, dan semakin sedikit waktu yang dibutuhkan untuk mengeksekusinya

Tugas Akhir ini membahas algoritma One Time Pad (OTP), yang terkenal sederhana dan '*unbreakable*', pada data yang bertipe alphanumerik serta bagaimana kemungkinan pengulangan kunci simetrik yang digenerate. Algoritma OTP ini dipadukan dengan algoritma RSA dan Md5 untuk keamanan kunci dan tanda tangan digital.

Sistem pada Tugas Akhir ini dibangun pada sistem operasi Windows Server 2003, mail server Kerio versi 5.5.0 dan tools pembantu lainnya, serta dengan bahasa pemrograman Java.

Sistem e-mail OTP yang dipadukan dengan RSA dan MD5 ini menawarkan kemudahan dan keamanan dengan key yang tidak berulang pada ukuran *message* tertentu.

Kata kunci: OTP, kriptografi, kerahasiaan data, e-mail