ABSTRACT

Data secrecy is an important thing in data communication. There is some encryption algorithms that usually use like DES, Triple DES, Blowfish, IDEA, etc. Those algorithms is so complicative dan hard to be understand, that is the reason, 'security appearance', more difficult to be understand, more save. But, on the user side, they do not care how difficult the algorithm that they use, they just care their data safety. There is two security recuirements in an encyption system, true random bits and very big key space for that ancryption algorithm. If both recuirement fulfilled, no matter how complex the encryption algorithm. Even the simplier is better, because simplier an algorithm result in fewer computation process, and fewer time to execute.

This Final Project disscuss about One Time Pad (OTP) algorithm, which has been known simple and 'unbreakable', on the alphanumerik data and also how the possibility of the generate key repetition. This algorithm fused with RSA algorithm and MD5 algorithm for key security and digital signature.

The final project system is build on Windows Server 2003 operating system, Kerio Mail server version 5.5.0, and other supporting tool, and also with Java programming language.

One Time Pad e-mail system which fused with RSA and MD5 offerring easy and secure mail system with 'one time' key on certain message sizes.

Key words: OTP, cryptography, data secrecy, e-mail