IMPLEMENTASI ALGORITMA RSA TERHADAP KEAMANAN DATA

SKRIPSI

SETO PRIYANGGORO

DEPARTEMEN MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS AIRLANGGA
SURABAYA
2008

Seto Priyanggoro, 2008, *Implementasi Algoritma RSA Terhadap Keamanan Data,* Skripsi ini di bawah bimbingan Drs. Eto Wuryanto, DEA dan Dra. Inna Kuswandari, M.Si, Departemen Matematika, Fakultas Sains dan Teknologi, Universitas Airlangga.

ABSTRAK

Tujuan skripsi ini adalah untuk menyelesaikan permasalahan keamanan data atau dokumen menggunakan algoritma kriptografi RSA sekaligus membuat programnya.

Algoritma RSA adalah algoritma kriptografi asimetris yang komponen kuncinya dibangun dari 2 buah bilangan prima yang berbeda. Untuk membangun sebuah kunci yang tepat diperlukan bantuan operasi matematis karena data yang diproses berbentuk numerik, bilangan prima yang dibangkitkan akan melalui beberapa tahapan perhitungan sampai didapatkan pasangan kunci yang aman. Proses pembentukan kunci pada algoritma RSA diawali dengan membangkitkan bilangan prima acak, lalu yang kedua membangkitkan pasangan kunci publik, dan yang ketiga membangkitkan pasangan kunci privat. Proses enkripsi pada algoritma RSA diawali dengan menerima pasangan kunci publik, lalu menghitung cipherteks dari data asli, proses dekripsinya dimulai dengan mengambil pasangan kunci privat untuk kemudian menghitung nilai plainteks dari data aslinya.

Skripsi ini menggunakan data berekstensi *.txt dalam prosesnya. Data teks yang telah diuji adalah data berukuran 12 bytes dan 5 kilobytes. Proses kriptografi dilakukan dengan bantuan program C++ Builder 6, ukuran data hasil enkripsi lebih besar daripada data aslinya, sedangkan ukuran data hasil dekripsi relatif sama dengan data aslinya.

Kata kunci : RSA, enkripsi, dekripsi, algoritma asimeris, kriptografi, bilangan prima.

Seto Priyanggoro, 2008. *The Implementation of RSA Algorithm for Data Security.* This *skripsi* was under guidance of Drs. Eto Wuryanto, DEA and Dra. Inna Kuswandari, M.Si. Department of Mathematics, The Faculty of Science and Technology, Airlangga University

ABSTRACT

The purpose of this *skripsi* is to solve data security problem using RSA cryptography algorithm and also write a computer program from it's algorithm.

RSA algorithm is asymmetric cryptography algorithm which is build from two different prime number for the keys components. To build a right key it is need a help from mathematics operation because the processing data is in numerical form. The generated prime number will through a few calculation steps until a pair of safe keys is obtain. The keys generation process on RSA algorithm is begin with random prime number generation. And then the second is generate a pair of public keys, and the third steps is generate a pair of private keys. The encryption process is start with accept a pair of public keys, and then calculate cyphertext value from original data. The decryption process is start with taking a pair of private keys and then calculate plaintext value from cyphertext to get original data.

This *skripsi* is using *.txt data extension in whole process. The data text that have been tested is 12 byte and 5 kilobytes data, the cryptography process is done by C++ Builder 6 program, the encrypted data size is larger than its original data, while the decrypted data size is relatively same from the original data

Kata kunci : RSA, enkripsi, dekripsi, algoritma asimeris, kriptografi, bilangan prima.