ABSTRACT

ASYMMETRY CRYPTOSYSTEM AND GENERATING PUBLIC KEY USING RADIAL BASIS FUNCTION NEURAL NETWORK

By

NURUL HAYATY
13/354958/PPA/04327

Security is very important part and can not be separated in a computer system and networks. The computer system is currently growing through network connections that are also expanding to make individuals and organizations more easily communicate and get information. Meanwhile, opportunities for parties who are not authorized to obtain confidential information becomes higher.

One of the security methods is using cryptography. Key distribution symmetry of insecurity through the channels of communication gave rise to asymmetry of cryptography in 1976.

Computational Cryptography has some similarities with neural network computing that is equally has the link between data input and data output. Neural network of Radial Bassis Function (RBFNN) is unique algorithm because the algorithm is hybrid method using combination of supervised and unsupervised learning methods. Plaintext represents the input layers, hidden layer represents the public key, the private key represents the weighs between the hidden layer to the output layer, and decrypted plaintext results represent the output layer.

Based on the results of the research are constructed using the approach of neural network of Radial Basis Functions with function Gaussian activation can be used to encode the message and return it to its original form.

Keyword : Cryptography, asymmetry, neural network, Radial Basis Function, Gaussian function.

INTISARI

KRIPTOSISTEM KUNCI ASIMETRI DAN PEMBANGKITAN KUNCI PUBLIK MENGGUNAKAN JARINGAN SYARAF TIRUAN *RADIAL BASIS FUNCTION*

Oleh

NURUL HAYATY
13/354958/PPA/04327

Keamanan menjadi suatu bagian yang sangat penting dan tidak dapat dipisahkan dalam suatu sistem komputer dan jaringan. Sistem komputer saat ini yang semakin berkembang melalui hubungan jaringan yang juga semakin meluas menjadikan individu maupun organisasi semakin mudah dalam berkomunikasi dan mendapatkan informasi. Sementara itu, peluang bagi pihak-pihak yang tidak berwenang untuk mendapatkan informasi yang bersifat rahasia menjadi semakin tinggi.

Salah satu metode pengamanan yang dapat dilakukan adalah dengan menggunakan kriptografi. Ketidakamanan pendistribusian kunci simetri melalui saluran komunikasi memunculkan kriptografi asimetri pada tahun 1976.

Komputasi kriptografi memiliki beberapa kesamaan dengan komputasi jaringan syaraf tiruan yaitu sama-sama memiliki keterkaitan antara data masukan dan data keluaran. Jaringan syaraf tiruan *Radial Basis Function* (RBF) merupakan algoritma yang cukup unik karena algoritma ini menggunakan metode *hybrid* yang merupakan kombinasi antara metode pembelajaran tak terawasi (*unsupervised*) dan pembelajaran terawasi (*supervised*). *Plaintext* merepresentasikan *input layer*, kunci publik merepresentasikan *hidden layer*, kunci privat merepresentasikan bobot-bobot antara *hidden layer* dengan *output layer*, dan *Plaintext* hasil dekripsi merepresentasikan *output layer*.

Berdasarkan hasil penelitian kriptosistem yang dibangun menggunakan pendekatan jaringan syaraf tiruan *Radial Basis Function* dengan fungsi aktivasi Gaussian dapat digunakan untuk menyandikan pesan dan mengembalikannya ke bentuk semula.

Kata kunci : Kriptografi, asimetri, jaringan syaraf tiruan, *Radial Basis Function*, fungsi Gaussian.