PERANCANGAN SISTEM KRIPTANALISIS RSA DENGAN MENGGUNAKAN JARINGAN SYARAF TIRUAN BACK PROPAGATION

Nama Mahasiswa : Edi Krisnayana
NRP : 1210 100 074
Jurusan : Matematika FMIPA-ITS
Dosen Pembimbing : Dr. Darmaji S.Si., M.T.

Abstrak

Jaringan Syaraf Tiruan BackPropagation digunakan untuk mendapatkan plainteks dari cipherteks yang sudah dienkripsi melalui proses RSA. Algoritma RSA didesain dan diimplementasikan pada sistem untuk mendapatkan sampel ciperteks yang akan diuji. Dalam mendekripsi cipherteks RSA, jaringan syaraf tiruan yang didesain pada sistem hanya membutuhkan informasi kunci publik yang dimiliki cipherteks. Kunci publik tersebut dibutuhkan untuk pembelajaran algoritma Back Propagation. Cipherteks yang didapatkan dari hasil enkripsi algoritma RSA digunakan sebagai input untuk proses pembelajaran jaringan syaraf tiruan. Kemudian dengan melakukan simulasi pembelajaran data cipherteks dari algoritma RSA, maka dapat dibangun jaringan syaraf tiruan untuk mencari pola keterkaitan antara cipherteks dengan plainteks untuk mendapatkan plainteksnya kembali. Perilaku jaringan syaraf tiruan dengan arsitektur Back Propagation yang berbeda dalam training data cipherteks merupakan analisis yang dilakukan pada penelitian ini.

Kata kunci: *Jaringan Syaraf Tiruan Back Propagation, Kriptanalisis, Kriptografi, RSA.*

RSA CRYPTANALYSIS SYSTEM DESIGN USING BACK PROPAGATION NEURAL NETWORK

Student Name	: Edi Krisnayana
NRP	: 1210 100 074
Major	: Mathematics FMIPA-ITS
Advisor	: Dr. Darmaji S.Si., M.T.

Abstract

Backpropagation Neural Network is used to obtain the plaintext from the ciphertext which is encrypted via RSA process. RSA algorithm is designed and implemented in the system to get ciperteks sample to be tested. In RSA decrypt ciphertext, artificial neural networks are designed in the system only requires the public key information held ciphertext. The public key is needed for Back Propagation learning algorithm. Ciphertext obtained from the results of the RSA encryption algorithm is used as input for the neural network learning process. Then by performing a simulation study of data from the ciphertext RSA algorithm, it can be constructed artificial neural networks to search for patterns of relationship between plaintext to ciphertext to get back plainteksnya. The behavior of neural networks with different architectures in Back Propagation training is a ciphertext of data analysis conducted in this study.

Kata kunci: *Back Propagation Neural Network, Cryptanalysis,Cryptography, RSA.*