Bachtiyar Muclis Arief, 2016, **Kriptanalisis Algoritma Kriptografi RSA menggunakan *Hybrid* Jaringan Syaraf Tiruan *Extreme Learning Machine* dengan *Harmony Search* dan *Simulated Annealing***, skripsi ini dibawah bimbingan Drs. Edi Winarko, M.Cs dan Auli Damayanti, S.Si, M.Si, Prodi S1-Matematika, Departemen Matematika, Fakultas Sains dan Teknologi, Universitas Airlangga, Surabaya.

## ABSTRAK

Pada skripsi ini membahas kriptanalisis algoritma kriptografi RSA menggunakan *Hybrid* jaringan syaraf tiruan *Extreme Learning Machine* (ELM) dengan *Harmony Search* (HS) dan *Simulated Annealing* (SA). Jaringan syaraf tiruan ELM diterapkan untuk mendapatkan plainteks dari cipherteks yang telah dienkripsi melalui proses RSA. Algoritma RSA didesain dan diimplementasikan pada sistem untuk mendapatkan sampel cipherteks yang akan diuji. Dalam mendekripsikan cipherteks RSA jaringan syaraf tiruan yang didesain pada sistem membutuhkan informasi kunci publik dan beberapa parameter pada pelatihan jaringan syaraf tiruan dan metode metaheuristik ELM-HS-SA. Cipherteks yang didapatkan dari hasil enkripsi algoritma kriptografi RSA beserta kunci publiknya dimanfaatkan sebagai data pelatihan pada jaringan syaraf tiruan. Kemudian dengan melakukan simulasi pembelajaran data cipherteks dari algoritma RSA, maka dapat dibangun dengan jaringan syaraf tiruan yang di *hybrid* dengan metode metaheuristik HS dan SA untuk mencari pola keterkaitan antara cipherteks plainteks supaya mendapatkan plainteksnya kembali. HS dan SA digunakan untuk mengoptimalkan MSE yang merupakan fungsi tujuan dari penelitian ini. Berdasarkan hasil pengujian yang telah dicapai, didapatkan bahwa hasil kriptanalisis dengan ELM-HS-SA dengan menggunakan bantuan software NetBeans 8.1 berhasil mendeteksi cipherteks RSA menjadi plainteks awalnya dengan tingkat keakuratan yang tinggi dan ELM-HS-SA mampu mencapai *error* untuk proses klasifikasi sebesar 7.4088697215769630E-15.

**Kata Kunci: Kriptanalisis, Kriptografi, RSA, Jaringan Syaraf Tiruan, Klasifikasi, Extereme Learning Machine, Harmony Search, Simulated Annealing**