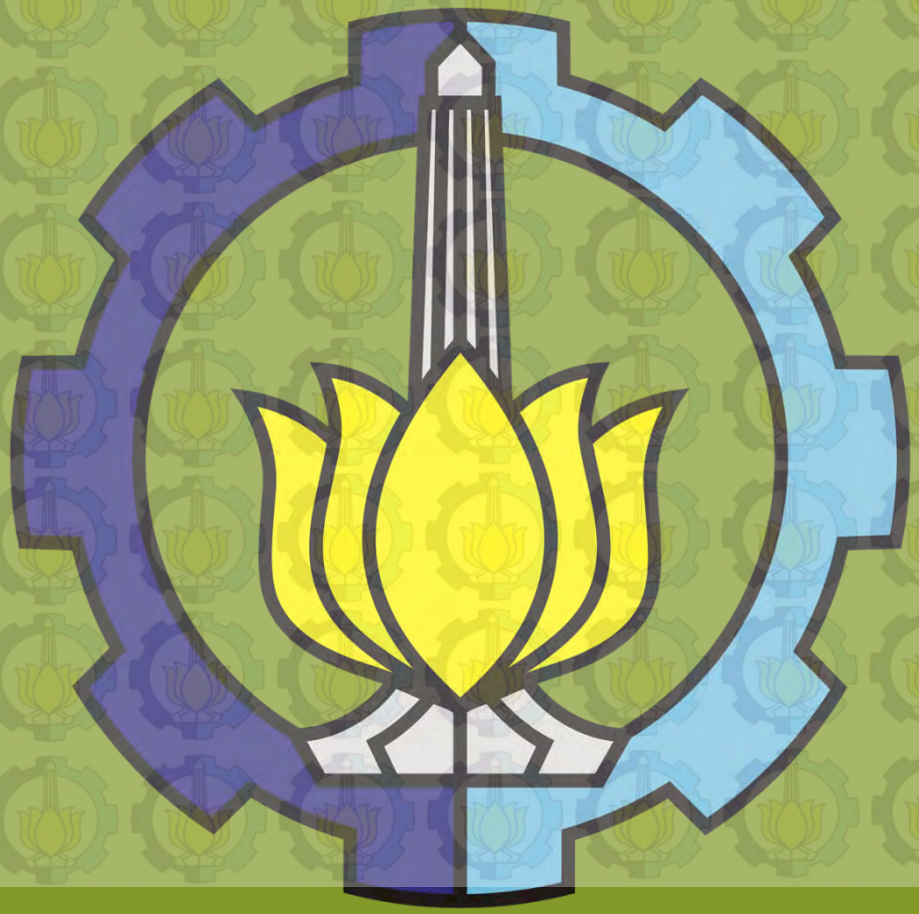
PERANCANGAN SISTEM KRIPTANALISIS RSA DENGAN MENGGUNAKAN JARINGAN SYARAF TIRUAN BACK PROPAGATION



Ujian Tugas Akhir

Oleh:
Edi Krisnayana
(1210100074)

Dosen Pembimbing:
Dr. Darmaji, S.Si, MT

Latar Belakang

Keamanan

↓

Kriptorafi

↓

Kriptanalisis

Rumusan Masalah

Permasalahan yang dihadapi dalam tugas akhir ini dapat dirumuskan sebagai berikut:

1. Bagaimana penerapan Jaringan Syaraf Tiruan Back Propagation dalam pengembangan kriptanalisis cipherteks RSA.
2. Bagaimana efektivitas Jaringan Syaraf Tiruan Back Propagation untuk kriptanalisis RSA.
3. Bagaimana perilaku Jaringan Syaraf Tiruan Back Propagation dalam mengklasifikasikan pola cipherteks RSA.

Batasan Masalah

Dalam penelitian tugas akhir ini, permasalahan yang akan dibahas dibatasi ruang lingkup pembahasannya antara lain:

1. Bilangan prima untuk kunci dibatasi maksimal 10 digit.
2. Kunci publik RSA (E,N) untuk proses krptanalisisis dengan Jaringan Syaraf Tiruan harus diketahui.
3. Perancangan Sistem kriptanalisis RSA menggunakan Jaringan Syaraf Tiruan.
4. Back Propagation diimplementasikan menjadi sebuah program dengan bahasa pemrograman *java*.

Tujuan

Tujuan dari penelitian tugas akhir ini antara lain:

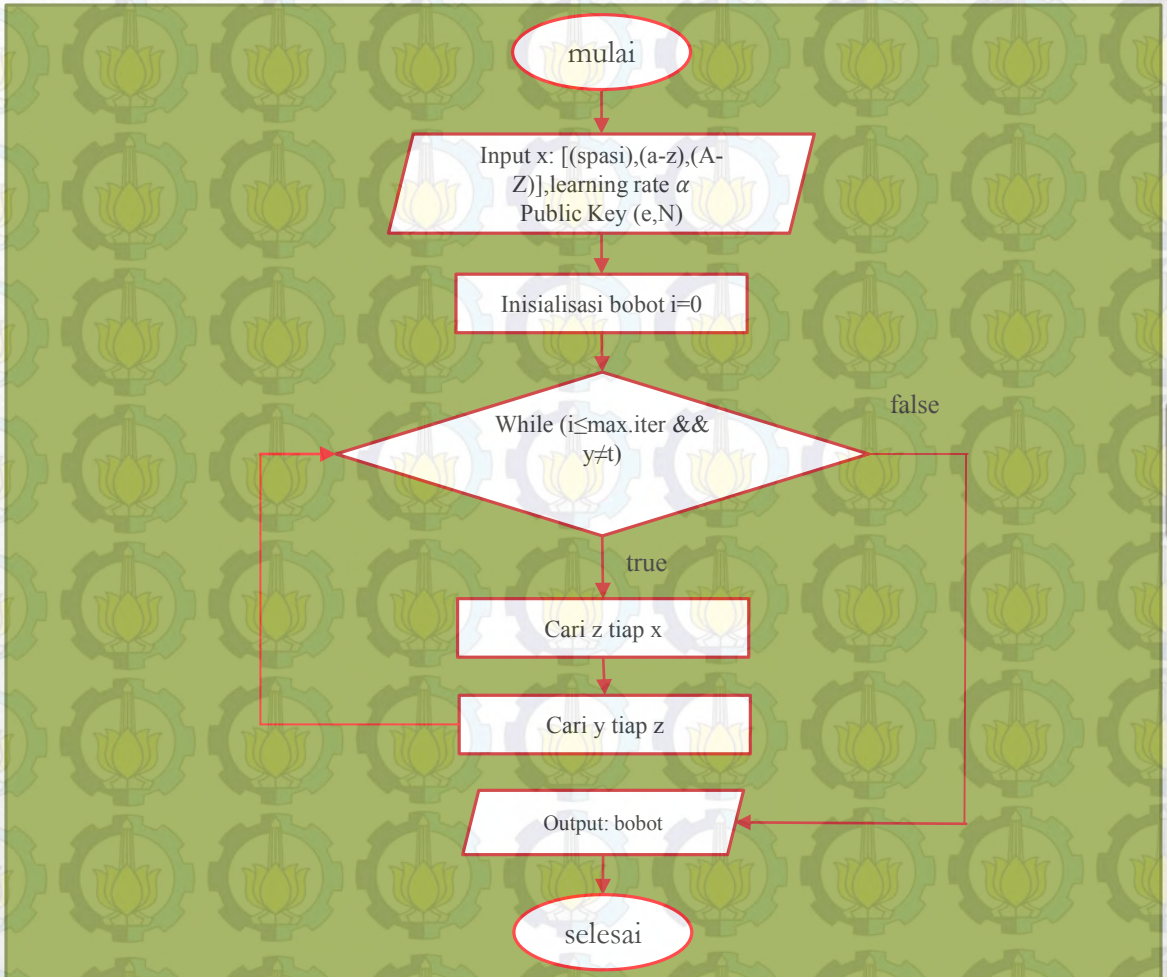
1. Mendapatkan proses pembelajaran cipherteks RSA dengan Jaringan Syaraf Tiruan yang tepat sehingga cipherteks tersebut dapat kembali ke plainteks awalnya.
2. Menunjukkan apakah jaringan syaraf tiruan mampu untuk melakukan kriptanalisis RSA.
3. Mendapatkan program komputer (*source code*) untuk enkripsi dekripsi RSA sekaligus mengkriptanalisis cipherteksnya dengan Jaringan Syaraf Tiruan.

Manfaat

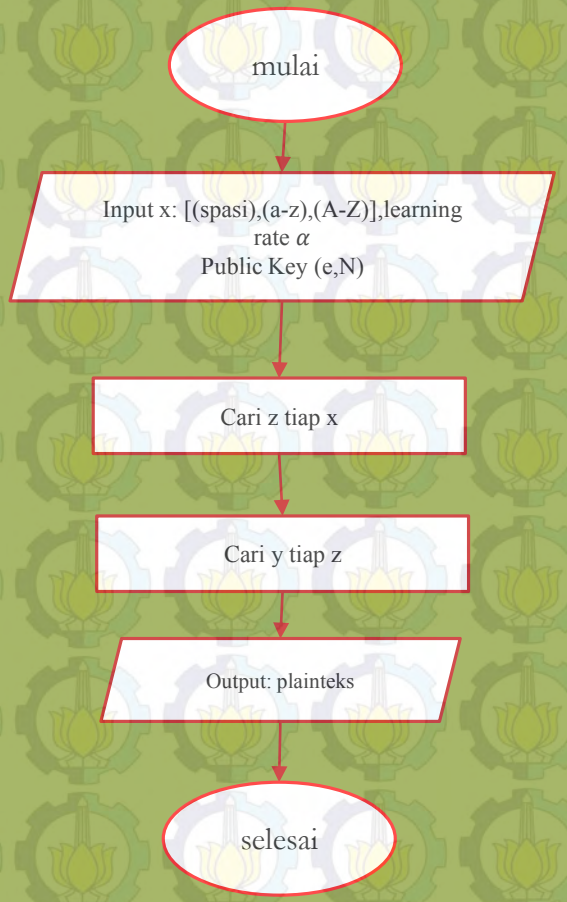
Manfaat yang dapat diperoleh dari tugas akhir yang diusulkan ini antara lain:

1. Memberikan informasi bagi pihak yang ingin mengembangkan sistem kriptanalisis RSA.
2. Dapat digunakan untuk mengembangkan/membuat aplikasi-aplikasi sistem yang berbasis Jaringan Syaraf Tiruan.
3. Sebagai pembanding waktu lama komputasi RSA dengan Jaringan Syaraf Tiruan.

Proses Pembelajaran



Dekripsi dengan Back Propagation



Hasil Pembelajaran

Hasil pembelajaran untuk mendekripsikan cipherteks yang memiliki public key (e,N) = (6345151585 63,786735800415560985 59) menggunakan data karakter[(spasi), A-Z, a-z].

α	Target error	Epoch yang dicapai	Waktu Training (detik)
0,2	0	182.478	2985,314
0,4	0	95.290	1598,552
0,6	0	65.710	1571,969
0,8	0	52.652	1108,223
1	0	45.820	848,615

Hasil Pengenalan

Plainteks "Algortima RSA dijabarkan pada tahun 1977 oleh tiga orang : Ron Rivest, Adi Shamir dan Len Adleman dari Massachusetts Institute of Technology. Huruf RSA itu sendiri berasal dari inisial nama mereka (Rivest-Shamir-Adleman). Clifford Cocks, seorang matematikawan Inggris yang bekerja untuk GCHQ, menjabarkan tentang sistem equivalen pada dokumen internal pada tahun 1973. Penemuan Clifford Cocks tidak terungkap hingga tahun 1997 karena alasan top-secret classification. Algoritma tersebut dipatenkan oleh Massachusetts Institute of Technology pada tahun 1983 di Amerika Serikat sebagai U.S. Patent 4.405.829. Paten tersebut berlaku hingga 21 September 2000. Semenjak Algoritma RSA dipublikasikan sebagai aplikasi paten, regulasi di sebagian besar negara-negara lain tidak memungkinkan penggunaan paten. Hal ini menyebabkan hasil temuan Clifford Cocks di kenal secara umum, paten di Amerika Serikat tidak dapat mematenkannya. "

Hasil Pengenalan

No	Kriteria	Hasil Data
1	Waktu enkripsi dengan RSA (detik)	0,188
2	Waktu deskripsi dengan RSA (detik)	0,062
3	Waktu deskripsi dengan JST (detik)	0,109
4	Plainteks berhasil dikenali dengan JST (karakter)	924
5	Plainteks gagal dikenali dengan JST (karakter)	0
6	Akurasi pengenalan (%)	100

Kesimpulan

1. Pengaruh learning rate dalam training.
2. Tingkat keberhasilan Back Propagation
3. Waktu pendekripsian.

Daftar Pustaka

1. Ariyus, Dony. 2005. **Kriptografi Keamanan Data dan Komunikasi**. Yogyakarta : Penerbit Graha Ilmu.
2. Fausett, Laurene. 1994. **Fundamentals of Neural Network.** New Jersey : Printice-Hall Inc.
3. Adyaksyah, Rimico. 2013. **Perancangan Sistem Kriptanalisis RSA Menggunakan Jaringan Syaraf Tiruan Perceptron.** Surabaya : Institut Teknologi Sepuluh Nopember.

TERIMA KASIH