Perancangan Sistem Kriptanalisis RSA dengan menggunakan Jaringan Syaraf Tiruan Back Propagation

Edi Krisnayana dan Darmaji
Jurusan Matematika
Fakultas Matematika dan Ilmu Pengetahuan Alam
Institut Teknologi Sepuluh Nopember (ITS)
Jl. Arief Rahman Hakim, Surabaya 60111 Indonesia
e-mail: darmaji@matematika.its.ac.id

***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.**

I. PENDAHULUAN

Kriptografi secara cepat telah menjadi sebuah bagian yang sangat krusial dalam pengamanan data. Sebelum tahun 1980-an, kriptografi digunakan utamanya untuk bidang militer dan komunikasi diplomatik, perbankan, perdagangan, dan hampir dalam konteks-konteks yang dibatasi. Dalam dunia belakangan ini, komunikasi berkembang dengan sangat cepat dengan adanya teknologi internet, akibatnya seorang hacker dengan siap sedia bisa mengintip transmisi data komputer untuk informasi yang berharga. Karena itu dibutuhkannya cara untuk melindungi ke komputer (melalui sandi lewat (*password*) dan akses jarak jauh yang terenkripsi), transaksi komersial (nomor-nomor kartu kredit dan data bank), dan informasi-informasi lainnya.

RSA adalah algoritma kriptografi kunci publik paling populer yang digunakan saat ini. Algoritma ini diciptakan pada tahun 1976 oleh Rivest, Shamir, dan Adleman. Popularitas dari algoritma ini bersumber pada tingkat keamanannya yang sangat baik, yang dipengaruhi oleh sulitnya pemfaktoran terhadap sebuah bilangan integer besar sebagai kuncinya menjadi bilangan prima.

Jaringan syaraf tiruan, seperti manusia, belajar dari suatu contoh karena mempunyai karakteristik yang adaptif, yaitu dapat belajar dari data-data sebelumnya dan mengenal pola data yang selalu berubah. Selain itu, jaringan saraf tiruan merupakan sistem yang tak terprogram, artinya semua keluaran atau kesimpulan yang ditarik oleh jaringan didasarkan pada pengalamanya selama mengikuti proses pembelajaran/ pelatihan.

Hal yang ingin dicapai dengan melatih jaringan saraf tiruan adalah untuk mencapai keseimbangan antara kemampuan memorisasi dan generalisasi. Yang dimaksud kemampuan memorisasi adalah kemampuan jaringan saraf tiruan untuk mengambil kembali secara sempurna sebuah pola yang telah dipelajari. Kemampuan *generalisasi* adalah kemampuan jaringan saraf tiruan untuk menghasilkan respons yang bisa diterima terhadap pola-pola input yang serupa (namun tidak identik) dengan pola-pola yang sebelumnya telah dipelajari. Hal ini sangat bermanfaat bila pada suatu saat ke dalam jaringan saraf tiruan diinputkan informasi baru yang belum pernah dipelajari, maka jaringan saraf tiruan masih akan tetap dapat memberikan tanggapan yang baik, memberikan keluaran yang paling mendekati pola yang telah dipelajari[6].

Kriptanalisis adalah ilmu yang mempelajari cara membaca pesan terenkripsi tanpa mengetahui metode atau kunci yang digunakan untuk menenkripsi pesan tersebut. Kriptanalisis diperlukan sampai saat ini. Kriptanalisis diperlukan di berbagai bidang. Dan yang terpenting kriptanalisis diperlukan untuk mengukur sejauh mana kekuatan dari metode yang digunakan untuk menenkripsi satu pesan. Berbagai pendekatan telah diusulkan sebagai metode kriptanalisis terhadap RSA. Beberapa macam serangan terhadap RSA antara lain Serangan GCD (Greatest Common Divisor), Serangan Common Modulus, Serangan Faktorisasi, Serangan Brute-Force dan Timming, Implementation Attack. Namun dari pendekatan-pendekatan tersebut masih membutuhkan waktu yang cukup lama. Tujuan dari penelitian ini yaitu mendapatkan proses pembelajaran cipherteks RSA dengan Jaringan Syaraf Tiruan yang tepat sehingga cipherteks tersebut dapat kembali ke plainteks awalnya. Kemudian membuktikan apakah jaringan syaraf tiruan mampu untuk melakukan kriptamalisis RSA.

II. PROSES PEMBELAJARAN BACK PROPAGATION

Dalam proses pembelajaran nilai bobot diinisialisasi lebih dahulu dengan metode nguyen-widrow:

1. Inisialisasi bobot v_{ji} dengan bilangan random [-0.5,0.5]

2. Hitung $\|v_j\| = \sqrt{{v_{j1}}^2 + {v_{j2}}^2 + \cdots + {v_{jn}}^2}$
3. Bobot yang dipakai sebagai inisialisasi $v_{ij} = \frac{\beta v_{ji(lama)}}{\|v_j\|}$
4. Bias yang dipakai sebagai inisialisasi v_{j0} adalah bilangan acak antara $-\beta$ dan β

Keterangan:

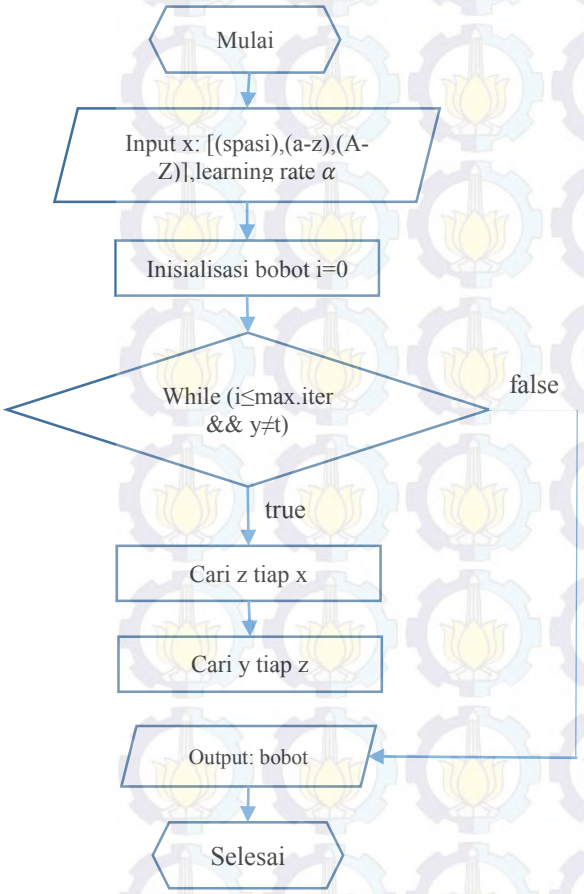
$\beta = 0.7\sqrt[n]{p}$

n = jumlah unit masukan

p = jumlah unit tersembunyi

sedangkan untuk bobot unit tersembunyi w_{ij} diinisialisasi dengan bilangan random [-1,1]

setelah semua nilai bobot diinisialisasi, proses pembelajaran diterapkan dengan data *input* berupa kumpulan setiap huruf yang sudah diinisialisasi pada proses sebelumnya. Tujuan dari proses pembelajaran ini untuk mendapatkan nilai bobot akhir yang sesuai dengan target pembelajaran, bobot akhir yang didapatkan setelah proses pembelajaran digunakan dalam proses pengenalan teks. *Flowchart* proses pembelajaran cipherteks dengan Perceptron dapat dilihat pada Gambar



Gambar 2.1 Diagram alir proses pembelajaran

Pelatihan dimulai dengan menggunakan 95 karakter keyboard. Karakter tersebut dienkripsi menggunakan RSA untuk mendapatkan bilangan hasil enkripsinya. Kemudian diolah melalui pra-proses untuk mendapatkan matriks *input*. Setelah matriks *input* diinisialisasi, plainteks awal diinisialisasi melalui pra-proses sebelum menjadi target pelatihan jaringan syaraf tiruan.

Proses ini merupakan tahap pembelajaran data (*training)*, dimana pada proses ini akan mengeluarkan hasil pembelajaran berupa matriks bobot terpelajar, matriks bias dan banyaknya iterasi pembelajaran. Proses pembelajaran mengikuti langkah-langkah algoritma pembelajaran Back Propagation. Step awal yaitu nyatakan setiap pola masukan dan target sebagai vektor biner yang elemenya sudah diinisialisasi pada pra-proses. Untuk setiap pasang data x: i=1,2,3,...,n yang sudah diinisialisasi, hitung respon:

Untuk setiap unit tersembunyi z: j=1,2,3,...,p dengan menggunakan rumus:

$$z\_net_j = v_{j0} + \sum_{i=1}^{n} x_i v_{ji}$$

$$z_j = f(z\_net_j) = \frac{1}{1 + e^{-z\_net_j}}$$

Untuk setiap unit keluaran y: k=1,2,3,...,m dengan menggunakan rumus:

$$y\_net_k = w_{k0} + \sum_{j=1}^{p} z_j w_{kj}$$

$$y_k = f(y\_net_k) = \frac{1}{1 + e^{-y\_net_k}}$$

Hitung faktor δ unit keluaran y_k

$$\delta_k = (t_k - y_k) y_k (1 - y_k)$$

Hitung suku perubahan bobot $\Delta w_{kj} = \alpha \delta_k z_j$

Hitung faktor δ unit tersembunyi z_j

$$\delta\_net_j = \sum_{k=1}^{m} \delta_k w_{kj}$$

$$\delta_j = \delta_{net_j} z_j (1 - z_j)$$

Hitung suku perubahan bobot $\Delta v_{ji} = \alpha \delta_j x_i$

Hitung semua perubahan bobot:

$$w_{kj}(baru) = w_{kj}(lama) + \Delta w_{kj}$$

$$v_{ji}(baru) = v_{ji}(lama) + \Delta v_{ji}$$

Setelah bobot-bobotnya diperbarui, lakukan perhitungan seperti diatas untuk setiap pasang *input* dan target berikutnya dengan menggunakan bobot baru dan bias baru. Lakukan terus untuk semua pasangan *input* X dan target sampai tidak ada perubahan bobot lagi, jika sampai epoch maksimum bobot tetap mengalami perubahan, maka pelatihan dihentikan dan bobot dipakai apa adanya. Bobot-bobot inilah yang nanti akan digunakan untuk kriptanalisis cipherteks.

III. DEKRIPSI DENGAN BACK PROPAGATION

Setelah dilakukan proses training, maka proses selanjutnya adalah proses testing. Proses ini dilakukan pada saat proses training berakhir dan data dari proses training akan diuji dan diterapkan. Proses ini berfungsi untuk melihat hasil pembelajaran cipherteks yang sudah di training dengan jaringan syaraf tiruan back propagation. Pada tahap ini dengan menggunakan bobot terpelajar dan nilai bias hasil pembelajaran, dihitung apakah hasil yang didapatkan sesuai dengan target pembelajarannya.

Pengenalan huruf dimulai dengan menggunakan cipherteks hasil enkripsi RSA. Cipherteks tersebut kemudian dikonversi menjadi urutan bilangan hasil enkripsinya dan diinisialisasi bersama dengan kunci publiknya. Proses tersebut merupakan pra-proses inisialisasi data input pengenalan cipherteks dengan jaringan syaraf tiruan back propagation. Algoritma back propagation yang dipakai untuk pengujian sama seperti algoritma perceptron pada proses pembelajaran, namun disini yang digunakan hanya step awal saja. Jadi tanpa pengujian nilai target dan perubahan bobot. Penggunaan step awal tersebut untuk mendapatkan nilai keluaran pada setiap neuron yang akan diuji.

Proses ini akan mengambil nilai bobot dan bias hasil training, kemudian digunakan untuk mencari nilai keluaran dari setiap neuron. Hasil keluaran dari setiap neuron kemudian di cek dengan nilai target data setiap plainteks pada proses training. Proses ini akan mengeluarkan karakter hasil klasifikasi jaringan syaraf tiruan.

Langkah pertama untuk mendekripsikan sebuah cipherteks yaitu menginisialisasi dahulu cipherteks melalui pra-proses. Setelah semua data diinisialisasi dan diimplementasikan ke dalam matriks-matriks yang siap untuk dicari vektor keluaranya. Untuk setiap vektor x dalam matriks, Set nilai aktivasi dari unit masukan dengan cara menghitung total masukan ke unit keluaran menggunakan rumus :

$$z\_net_j = v_{j0} + \sum_{i=1}^{n} x_i v_{ji}$$

$$z_j = f(z\_net_j) = \frac{1}{1 + e^{-z\_net_j}}$$

$$y\_net_k = w_{k0} + \sum_{j=1}^{p} z_j w_{kj}$$

$$y_k = f(y\_net_k) = \frac{1}{1 + e^{-y\_net_k}}$$

Setelah setiap unit masukkan didapatkan, jika $y_k = 1$ berarti pola yang dimasukkan merupakan huruf ke-k. Jika tidak ada satupun $y_k = 1$ maka pola di*input*kan tidak bisa diklasifikasikan.

IV. HASIL PEMBELAJARAN (TRAINING)

Hasil pembelajaran untuk mendekripsikan cipherteks yang memiliki public key (e,N) = (634515158563,7867358004155 6098559) ditunjukkan pada Tabel 3.1. Proses pembelajaran ini menggunakan data karakter[(spasi), A-Z, a-z].

Tabel 3.1 hasil pembelajaran

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

Berdasarkan hasil uji coba diatas tampak bahwa pada proses pembelajaran learning rate 1 menghasilkan terasi yang lebih sedikit dan membutuhkan waktu yang lebih singkat, sedangkan jika learning rate diperkecil maka proses pembelajaran membutuhkan waktu yang lebih lama dan terasi yang lebih banyak.

V. HASIL PENGENALAN

Pengujian proses pembelajaran dilakukan dalam bentuk simulasi. Sistem diuji dengan menggunakan jenis plainteks yang sudah dienkripsi dengan kunci yang berbeda serta dilakukan juga pengujian dengan data yang sama dengan data yang sudah ditraining untuk mendapatkan tingkat kesalahan.

Sample cipherteks ini diambil dari sebuah kalimat yang sudah dienkripsi dahulu dengan kunci RSA. Kunci RSA yang dipakai pada pengujian ini meliputi kunci yang sama dengan data yang ditraining dan dengan *sample* kunci yang baru yang tidak diikutsertakan dalam proses training. Jadi, untuk mendekripsikan data yang pertama diperlukan kunci publik(E,N) yang dimiliki oleh cipherteks yang pertama. Kunci publik ini digunakan untuk menginisialisasi huruf sebelum di pelajari oleh algoritma perceptron untuk mendapatkan nilai beban akhirnya. Selanjutnya untuk mendekripsikan data yang ke dua langsung menggunakan beban akhir hasil dari pembelajaran inisialisasi data yang pertama. Berikut *sample* data plainteks dan cipherteks RSA yang digunakan pada proses pengujian:

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 dipatenkannya."
P=8930447971 Q=8809589429 Public Key (e,N)= (634515158563,7867358004155 6098559) Private Key (d,M)= (10362619973609444467,78673580023816061160)
Cipherteks:

þ%x=Ò¼e————————————————————ü³Ý¼† ¢\

Pengujian hasil Pembelajaran:
Hasil pendekripsian dengan JST mendapatkan 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. "

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

VI. KESIMPULAN/RINGKASAN

Dari hasil yang didapatkan, proses pendekripsian cipherteks menggunakan jaringan syaraf tiruan dengan mempelajari public keynya terlebih dahulu sudah berhasil. Konsep ini bisa digunakan karena pada kriptanalisis data RSA sudah tidak membutuhkan kunci privatenya lagi meskipun membutuhkun kunci publiknya untuk menginisialisasi data awal pada proses pembelajaran setiap karakter jaringan syaraf tiruan back propagation.

Berdasarkan analisis terhadap hasil pengujian sistem kriptanalisis RSA dengan menggunakan jaringan syaraf tiruan back propagation, maka dapat diambil beberapa kesimpulan sebagai berikut:

1. Learning rate berpengaruh terhadap lama waktu dan jumlah epoch yang dibutuhkan untuk proses training. Semakin besar learning rate, semakin cepat waktu yang dibutuhkan dan semakin sedikit epoch yang dibutuhkan untuk proses training. Dari penelitian yang dilakukan, didapatkan bahwa learning rate α=1 adalah yang paling efisien.
2. Meskipun membutuhkan epoch yang cukup banyak dan waktu yang cukup lama untuk proses training, namun back propagation memiliki tingkat keberhasilan training mencapai 99%.
3. Waktu yang dibutuhkan jaringan syaraf tiruan back propagation untuk mendekripsi cipherteks hampir sama dengan waktu mendekripsi dengan menggunakan algoritma RSA itu sendiri.

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.