PERANCANGAN ALGORITMA KRIPTOGRAFI KUNCI SIMETRI DENGAN MENGGUNAKAN JARINGAN SARAF TIRUAN

Ibrahim Arief – NIM : 13503038

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if13038@students.if.itb.ac.id

Abstrak

Komputasi algoritma kriptografi kunci simetri memiliki beberapa kesamaan dengan komputasi jaringan saraf tiruan dalam hal menghasilkan data keluaran yang berdasarkan operasi terhadap data masukan dan saling memiliki keterkaitan. Kesamaan ini dapat dilihat pada salah satu penggunaan jaringan saraf tiruan, yaitu untuk keperluan kompresi data yang menghasilkan data keluaran dengan pola yang berkaitan dengan data masukan. Cipherteks dapat dianggap sebagai representasi plainteks dengan pola yang berbeda namun masih memiliki keterkaitan antara data masukan dengan data keluaran.

Makalah ini membahas tentang upaya perancangan algoritma kriptografi kunci simetri dengan menggunakan jaringan saraf tiruan. Kunci simetri yang digunakan dalam kriptografi kunci simetri dalam rancangan algoritma ini dimanfaatkan sebagai bobot antar unit-unit dalam jaringan saraf tiruan yang digunakan dalam proses enkripsi. Kemudian dengan melakukan pembelajaran mesin dan data simulasi enkripsi dari jaringan saraf tiruan enkripsi, maka dapat dibangun jaringan saraf tiruan untuk mencari pola keterkaitan antara plainteks dengan cipherteks agar dapat digunakan dalam proses dekripsi.

***Kata kunci**: perancangan algoritma kriptografi, kunci simetri, jaringan saraf tiruan, cipherteks, plainteks, enkripsi, dekripsi*.

1. Pendahuluan

Sebuah pesan yang dikirimkan dari pengirim ke penerima melalui suatu media transmisi pesan memiliki resiko untuk disadap oleh pihak yang tidak berkepentingan.

Untuk menjaga kerahasiaan pesan, terdapat dua macam pendekatan yang umum digunakan, yaitu dengan menggunakan jalur komunikasi yang terjamin keamanannya, atau dengan menyandikan pesan dalam bentuk yang hanya dapat dibaca oleh pihak yang berkepentingan.

Pendekatan yang banyak digunakan adalah pendekatan kedua, hal ini dikarenakan menjaga keamanan jalur komunikasi membutuhkan usaha yang cukup besar jika dibandingkan dengan menjaga kerahasiaan pesan dengan penyandian.

Untuk mencapai tujuan menjaga kerahasiaan dari pesan, algoritma penyandian menggunakan kunci rahasia dalam proses enkripsi dan dekripsi dari pesan. Kunci rahasia tersebut dioperasikan dengan pesan dan menghasilkan pesan yang telah dirahasiakan. Pesan yang telah dirahasiakan tersebut dapat dikirimkan melalui media transmisi yang tidak terjamin keamanannya karena tidak dapat dibaca oleh pihak yang tidak berkepentingan selama pihak tersebut tidak memiliki kunci rahasia untuk membaca pesan yang telah menjalani proses enkripsi.

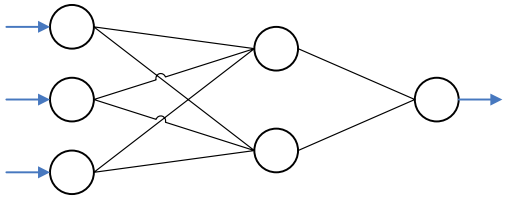
Terdapat dua jenis sistem kriptografi, yaitu sistem kriptografi kunci simetri dan sistem kriptografi kunci publik. Perbedaan antara kedua sistem kriptografi tersebut adalah pemanfaatan kunci yang digunakan dalam proses enkripsi dan dekripsi. Pada kriptografi kunci simetri, kunci yang digunakan untuk proses pengenkripsian adalah sama dengan kunci yang digunakan untuk proses pendekripsian. Hal ini menyebabkan kerahasiaan kunci yang digunakan dalam kriptografi kunci simetri menjadi sangat penting untuk dijaga. Sedangkan pada kriptografi kunci publik, kunci yang digunakan untuk proses pendekripsian berbeda dengan kunci yang digunakan untuk proses pengenkripsian. Hal ini menyebabkan kunci pengenkripsi tidak harus dijaga kerahasiaannya dan dapat dipublikasikan dengan bebas.

Sistem kriptografi kunci simetri dapat digabungkan dengan arsitektur jaringan saraf tiruan untuk menghasilkan sebuah algoritma kriptografi yang dapat memanfaatkan karakteristik dari jaringan saraf tiruan dalam proses enkripsi dan dekripsinya. Algoritma kriptografi ini termasuk ke dalam kategori cipher blok dan merupakan algoritma kriptografi yang *robust* karena memiliki efek *avalanche*.yang dihasilkan dari sifat keterhubungan antar node-node dalam jaringan saraf tiruan. Sifat ini dapat menyebabkan pengkodean setiap blok bit berkaitan dengan seluruh blok bit dalam pesan dan pengubahan satu bit dalam plainteks akan mempengaruhi seluruh cipherteks. Penggunaan kunci simetri dalam arsitektur ini adalah untuk menentuan bobot-bobot antar node masukan dan node keluaran.

2. Jaringan Saraf Tiruan

2.1 Definisi Jaringan Saraf Tiruan

Jaringan saraf tiruan merupakan suatu paradigma pemrosesan informasi yang meniru cara kerja sistem saraf biologis. Jaringan saraf tiruan terdiri dari sekumpulan unit pemrosesan yang dikenal sebagai unit neuron. Kumpulan unit neuron tersebut saling terhubung dan saling berkerja sama dalam mencari solusi dari sebuah permasalahan.



Gambar 1. Arsitektur jaringan saraf tiruan

Permasalahan yang cocok untuk ditangani oleh jaringan saraf tiruan terbagi menjadi tiga kelompok [1], yaitu:

1. Permasalahan klasifikasi
   Permasalahan penentuan kelas yang cocok untuk sebuah masukan dengan pola tertentu.

2. Prediksi pola
   Permasalahan pembuatan suatu pola secara lengkap dari sebagian masukan pola dan memprediksi kecenderungan yang mungkin muncul dari data masukan tersebut.

3. Kompresi data
   Permasalahan pengurangan jumlah bit dari suatu blok data untuk disimpan atau dikirim dalam batas-batas kesalahan yang diperkenankan. Sebuah pola tertentu dapat dikenali dari data masukan dan dijadikan basis penmbangkitan data keluaran dengan ukuran lebih kecil. Namun penggunaan jaringan saraf tiruan untuk permasalahan ini memiliki resiko karena pembacaan pola keluaran untuk menghasilkan kembali data masukan rentan akan kesalahan pengklasifikasian data.

2.2 Neuron

Neuron merupakan unit pemroses pada jaringan saraf tiruan. Pada jaringan saraf tiruan, neuron memiliki empat komponen utama, yaitu:

1. Koneksi masukan
   Sumber masukan neuron yang menerima masukan dari neuron-neuron lainnya atau dari luar jaringan. Setiap masukan memiliki bobot yang bersesuaian dengan setiap koneksi antar neuron. Umumnya masukan pada setiap neuron bernilai kontinu dengan rentang nilai antara [0, 1] atau [-1, -1].

2. Fungsi penjumlah
   Fungsi ini menjumlahkan masukan-masukan yang diterima berdasarkan bobot dari masukan tersebut. Masukan yang diterima dikalikan dengan bobotnya lalu hasil seluruh perkalian tersebut dijumlahkan. Fungsi penjumlah dapat didefinisikan melalui persamaan berikut:

$$net = \sum_{i=0}^{n} w_i x_i \qquad (2.1)$$

   yang dalam hal ini net adalah hasil keluaran dari fungsi penjumlahan, w_i menyatakan bobot koneksi masukan ke-i, dan x_i menyatakan masukan dari bobot tersebut.

3. Fungsi aktivasi
   Fungsi aktivasi adalah fungsi yang menentukan keluaran sebuah neuron dari hasil penjumlahan yang didapat melalui persamaan (2.1). Fungsi aktivasi ini dilambangkan dengan notasi

σ. Terdapat beberapa jenis fungsi aktivasi, yaitu:

a. Fungsi linier
Nilai keluaran neuron sama dengan hasil penjumlahan yang didapat melalui persamaan (2.1), yaitu:

$$\sigma(net) = net \qquad (2.2)$$

yang dalam hal ini net menyatakan nilai hasil penjumlahan yang didapat melalui persamaan (2.1).

b. Fungsi ambang (threshold)
Nilai keluaran neuron dikeluarkan secara diskrit jika nilai hasil penjumlahan dari persamaan (2.1) melebihi nilai ambang tertentu. Dalam penggunaan fungsi ambang, biasanya batasan nilai tersebut adalah nol karena nilai batasan telah ikut diperhitungkan dari adanya bobot bias yang dimiliki unit neuron. Fungsi ambang dapat didefinisikan sebagai berikut:

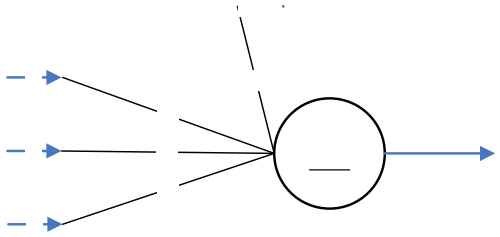
$$\sigma(net) = \begin{cases} 1 \text{ untuk } net > 0 \\ 0 \text{ untuk } net \leq 0 \end{cases} \qquad (2.3)$$

c. Fungsi sigmoid
Nilai keluaran dipetakan dari rentang $(-\infty,+\infty)$ menjadi bilangan riil dengan rentang antara [0, 1]. Fungsi ini dipilih agar pembelajaran yang menggunakan turunan dari fungsi aktivasi dapat menggunakan fungsi yang kontinu. Fungsi ini dapat didefinisikan sebagai berikut:

$$\sigma(net) = \frac{1}{1 + e^{-net}}. \qquad (2.4)$$

4. Koneksi keluaran
Koneksi keluaran mengirimkan keluaran neuron ke neuron-neuron lainnya atau sebagai keluaran dari jaringan saraf tiruan.

Ilustrasi dari neuron pada jaringan saraf tiruan dapat dilihat pada Gambar 2.



Gambar 2. Unit neuron pada jaringan saraf tiruan

2.3 Arsitektur Jaringan Saraf Tiruan

Jaringan saraf tiruan dapat terdiri dari beberapa lapisan neuron yang semua neuron dalam satu lapisan saling terhubung dengan lapisan tetangganya. Lapisan neuron terbagi menjadi tiga jenis menurut lokasinya dalam jaringan saraf tiruan [2], yaitu:

1. Lapisan masukan
2. Lapisan tersembunyi
3. Lapisan keluaran

Pada jaringan saraf tiruan hanya terdapat satu lapisan lapisan masukan dan satu lapisan keluaran. Sedangkan untuk lapisan tersembunyi jumlahnya bervariasi sesuai dengan permasalahan yang dihadapi jaringan saraf tiruan. Namun umumnya jumlah lapisan tersembunyi adalah antara nol sampai dengan tiga lapisan. Hal ini dikarenakan jaringan saraf tiruan dengan tiga lapisan tersembunyi sudah mencukupi untuk menyelesaikan berbagai permasalahan yang mungkin dihadapi.

Jumlah unit neuron pada lapisan masukan bersesuaian dengan jumlah data masukan diskrit dari permasalahan yang dihadapi. Sedangkan jumlah unit neuron pada lapisan keluaran bersesuaian dengan jumlah yang dibutuhkan untuk memodelkan solusi dari permasalahan. Untuk lapisan tersembunyi, jumlah yang diperlukan sangat bervariasi dan biasanya dibutuhkan analisa *heuristik* untuk menentukan jumlah unit yang optimal untuk permasalahan yang dihadapi jaringan saraf tiruan.

Fungsi aktivasi yang digunakan adalah fungsi aktivasi sigmoid.

2.4 Pembelajaran Jaringan Saraf Tiruan

Jaringan saraf tiruan cocok untuk digunakan dalam permasalahan pengolahan data yang memiliki pola. Dalam menghadapi permasalahan tersebut, jaringan saraf tiruan memiliki kemampuan pembelajaran untuk mengenali dan memprediksi pola data masukan.

Pembelajaran dalam jaringan saraf tiruan dilakukan dengan mengubah bobot-bobot yang dimiliki setiap koneksi antar unit pemroses. Algoritma yang umum digunakan dalam pembelajaran jaringan saraf tiruan adalah algoritma propagasi balik.

Algoritma propagasi balik dapat digunakan untuk menentukan bobot dalam koneksi antar neuron-neuron dalam jaringan saraf tiruan. Algoritma ini secara garis besar memiliki empat tahapan:

1. Pengkalkulasian nilai keluaran dari data masukan.
2. Perbandingkan nilai keluaran yang didapat dengan nilai keluaran yang diharapkan untuk menentukan tingkat kesalahan.
3. Propagasi balik tingkat kesalahan yang didapat dari lapisan neuron keluaran menuju lapisan neuron masukan.
4. Pengubahan bobot koneksi yang dimiliki setiap neuron sesuai dengan tingkat kesalahan masing-masing neuron tersebut.

Algoritma propagasi balik memiliki beberapa parameter yang dapat menentukan tingkat efektivitas pembelajaran jaringan saraf tiruan. Parameter-parameter tersebut adalah:

1. *Maximum epoch*
   Menentukan berapa iterasi pembelajaran yang akan dilakukan pada jaringan saraf tiruan. Semakin besar *maximum epoch* maka tingkat kesalahan jaringan saraf tiruan akan semakin menurun. Namun, penentuan *maximum epoch* yang terlalu besar akan menyebabkan jaringan saraf tiruan terlalu mengikuti pola data pelatihan dan meningkatkan kesalahan yang mungkin terjadi ketika jaringan saraf tiruan diberikan data masukan dari permasalahan sebenarnya. Hal ini dikenal dengan *overfitting*.

2. Laju pembelajaran
   Laju pembelajaran menunjukan seberapa cepat jaringan saraf tiruan akan menyesuaikan diri dengan data pelatihan yang diterimanya.

3. Momentum
   Momentum menunjukan seberapa besar pelatihan pada iterasi pelatihan saat itu hendak dipengaruhi oleh iterasi pelatihan sebelumnya.

3. Sistem Kriptografi Kunci Simetri

Kriptografi kunci simetri adalah sistem kriptografi yang menggunakan kunci yang sama dalam proses enkripsi dan dekripsi. Kriptografi kunci simetri ini dapat dikelompokan menjadi dua kategori [3], yaitu:

1. Cipher aliran (*stream cipher*)
   Algoritma kriptografi beroperasi pada plainteks/cipherteks dalam bentuk bit tunggal, yang dalam hal ini rangkaian bit dienkripsikan/didekripsikan bit per bit.

2. Cipher blok (*block cipher*)
   Algoritma kriptografi beroperasi pada plainteks/cipherteks dalam bentuk blok bit, yang dalam hal ini rangkaian but dibagi menjadi blok-blok bit yang panjangnya sudah ditentukan sebelumnya. Misalnya panjang blok adalah 64 bit, maka itu berarti algoritma enkripsi memperlakukan 8 karakter setiap kali penyandian (1 karakter = 8 bit dalam pengkodean ASCII).

Makalah ini hanya akan membahas kategori kriptografi kunci simetri yang digunakan dalam perancangan algoritma kriptografi dengan menggunakan jaringan saraf tiruan. Kategori tersebut adalah kategori cipher blok.

3.1 Cipher Blok

Pada cipher blok, rangkaian bit-bit plainteks dibagi menjadi blok-blok bit dengan panjang sama. Enkripsi dilakukan terhadap blok bit plainteks dengan menggunakan bit-bit kunci yang memiliki ukuran yang sama dengan ukuran blok plainteks. Algoritma enkripsi menghasilkan blok cipherteks yang berukuran sama dengan blok plainteks. Dekripsi dilakukan dengan cara yang sama dengan enkripsi.

Sebagai ilustrasi, misalkan blok plainteks yang berukuran tertentu dapat dinyatakan sebagai vektor berikut:

$$P = (p_1, p_2, ..., p_m)$$

yang dalam hal ini P menyatakan blok plainteks, m menyatakan jumlah bit dalam blok tersebut, dan p_i adalah nilai biner 0 atau 1 untuk i = 1, 2, ..., m

Dan blok cipherteks dinyatakan sebagai vektor berikut:

$$C = (c_1, c_2, ..., c_m)$$

yang dalam hal ini C menyatakan blok cipherteks, m menyatakan jumlah bit dalam blok tersebut, dan c_i adalah nilai biner 0 atau 1 untuk i = 1, 2, ..., m.

Bila plainteks dibagi menjadi n buah blok, barisan blok-blok plainteks dinyatakan sebagai berikut:

$$(P_1, P_2, ..., P_n)$$

Untuk masing-masing blok plainteks, bit-bit penyusunnya dapat dinyatakan sebagai vektor berikut:

$$P_i = (p_{i1}, p_{i2}, ..., p_{im})$$

yang dalam hal ini P_i menyatakan blok plainteks ke-i.

Kemudian, untuk enkripsi dan dekripsi dengan menggunakan kunci simetri, dapat dinyatakan dengan persamaan:

$$E_K(P) = C$$

untuk fungsi enkripsi, dan

$$D_K(C) = P$$

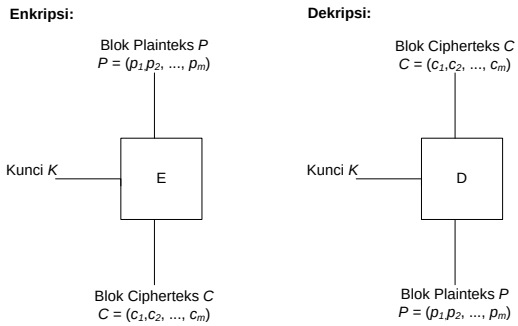
yang dalam hal ini K menyatakan kunci simetri, E_K menyatakan fungsi enkripsi, D_K menyatakan fungsi dekripsi, P menyatakan plainteks, dan C menyatakan cipherteks.

Fungsi E haruslah fungsi yang berkoresponden satu-ke-satu, sehingga:

$$E^{-1} = D$$

yang dalam hal ini E^{-1} menyatakan fungsi invers dari E.

Skema enkripsi dan dekripsi dengan cipher blok digambarkan pada Gambar 3. Fungsi E dan D dispesifikasikan oleh kriptografer.



Gambar 3. Skema Enkripsi dan Dekripsi dengan Cipher Blok

4. Perancangan Algoritma Kriptografi Kunci Simetri Menggunakan Jaringan Saraf Tiruan

Beberapa kriteria digunakan sebagai panduan dalam perancangan algoritma kriptografi kunci simetri dengan menggunakan jaringan saraf tiruan. Kriteria-kriteria tersebut adalah:

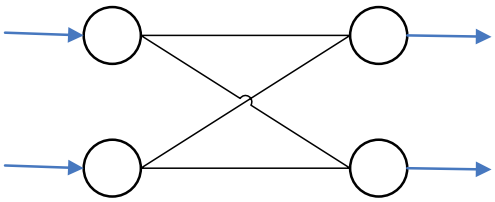
1. Untuk mencapai efek avalanche dalam proses pengenkripsian, setiap bit masukan harus mempengaruhi bit keluaran sedemikian rupa sehingga pengubahan satu bit masukan akan dapat mempengaruhi seluruh keluaran dari hasil enkripsi.

2. Untuk mencapai efek avalanche dalam proses pengenkripsian, setiap bit dalam kunci harus mempengaruhi bit keluaran sedemikian rupa sehingga pengubahan satu bit kunci akan dapat mempengaruhi seluruh keluaran dari hasil enkripsi.

3. Dalam proses pendekripsian, algoritma yang dihasilkan harus melakukan proses dekripsi dengan tingkat kesalahan serendah mungkin untuk menghindari kesalahan pendekripsian.

4.1 Arsitektur Jaringan Saraf Tiruan

Dari kriteria-kriteria yang telah disebutkan di atas, maka rancangan arsitektur jaringan saraf tiruan adalah sebagai berikut:



Gambar 4. Arsitektur Jaringan Saraf Tiruan untuk Kriptografi Kunci Simetri

Arsitektur jaringan saraf tiruan adalah satu lapisan masukan dan satu lapisan keluaran yang semua node dalam masing-masing lapisan terhubung dengan semua node dalam lapisan tetangganya. Jumlah node masukan dan node keluaran dalam jaringan saraf tiruan adalah sama dan sebesar jumlah blok yang dimiliki oleh sistem.

Pemilihan arsitektur jaringan saraf tiruan yang tidak menggunakan lapisan tersembunyi adalah untuk menekan tingkat kesalahan yang mungkin terjadi pada saat proses pendekripsian. Hal ini didapat setelah dilakukan pengujian antara bermacam-macam arsitektur jaringan saraf tiruan untuk menemukan arsitektur yang optimal bagi jaringan saraf tiruan untuk kriptografi kunci simetri. Hasil pengujian menemukan bahwa untuk jaringan saraf tiruan yang menggunakan lapisan tersembunyi dengan jumlah node yang sama dengan jumlah node masukan dan keluaran, tingkat akurasi pada saat pendekripsian adalah sekitar 60%, sedangkan penggunaan jaringan saraf tiruan yang tidak memiliki lapisan tersembunyi bisa meningkatkan tingkat akurasi hingga 98%.

Untuk jumlah node masukan dan node keluaran, dilakukan pengujian untuk menentukan jumlah yang optimal. Pengujian dilakukan dengan menggunakan parameter *maximum epoch*=1000, laju pembelajaran = 0.5, dan momentum = 0.3. Dari data pelatihan yang berjumlah 50 buah. Pengujian dilakukan untuk jumlah node antara dua node dan enam node. Hasil pengujian terdapat pada tabel berikut:

Tabel 1. Tingkat Kesalahan Dekripsi Terhadap Jumlah Node

Jumlah Node	Kesalahan Dekripsi (%)
2	13.80634
3	14.80912
4	20.13559
5	17.37220
6	18.20474

Dari pengujian, dapat disimpulkan bahwa jumlah node yang paling optimal dalam jaringan saraf tiruan untuk kriptografi kunci simetri adalah dua node masukan dan dua node keluaran. Dengan demikian, besar blok menjadi bersesuaian dengan dua masukan jaringan saraf tiruan.

Kemudian untuk parameter laju pembelajaran dan momentum, dilakukan pengujian untuk menemukan parameter yang paling optimal. Pengujian dilakukan dengan menggunakan parameter *maximum epoch*=5000. Sedangkan untuk parameter α dan η, dilakukan pengujian dengan nilai {0,2 <= α <= 0.8} dan {0,2 <= η <= 0.8} untuk melihat parameter yang optimal untuk jaringan saraf tiruan dekripsi.

Tabel 2. Tabel Kesalahan Jaringan Saraf Tiruan (Dalam %) Terhadap Momentum Dan Laju Pembelajaran.

	0,2	0,3	0,4	0,5	0,6	0,7	0,8 (α)
0,2	10.779	10.015	9.140	8.098	6.884	5.458	3.935
0,3	8.475	7.722	6.876	5.954	4.955	3.947	3.110
0,4	6.876	6.195	5.463	4.701	3.953	3.291	2.873
0,5	5.754	5.159	4.552	3.953	3.414	3.004	2.805
0,6	4.952	4.447	3.953	3.496	3.123	2.878	2.787
0,7	4.370	3.946	3.557	3.218	2.966	2.823	2.784
0,8 (η)	3.944	3.602	3.295	3.049	2.881	2.800	2.788

Dari hasil pengujian ditemukan bahwa parameter optimal bagi jaringan saraf tiruan dekripsi adalah 0.7 untuk parameter laju pembelajaran dan 0.8 untuk parameter momentum.

Dari hasil pengujian, ditemukan bahwa tingkat kesalahan jaringan saraf tiruan dapat ditekan hingga sekitar 2,7%. Karena dalam pemrosesan nilai masukan jaringan saraf tiruan dibutuhkan pemetaan nilai ke rentang nilai [0, 1], maka akan terdapat kesalahan dalam pembulatan nilai pada saat proses enkripsi dan dekripsi. Tingkat kesalahan tersebut dapat dihitung dengan membagi besar rentang dengan pengkodean karakter yang dimungkinkan, yaitu sebesar:

$$(1 - 0) / 25 = 0.04$$
$$= 4\%$$

Karena tingkat kesalahan jaringan saraf tiruan dapat ditekan hingga sekitar 2,7%, maka kesalahan pengkodean dapat turut ditekan.

4.2 Penggunaan Kunci Simetri

Dalam algoritma kunci simetri dengan menggunakan jaringan saraf tiruan, kunci simetri dimanfaatkan untuk menentukan nilai bobot hubungan antar node-node masukan dengan node keluaran.

Karena nilai bobot untuk kunci memiliki rentang [0, 1], maka kunci menjalani pemetaan menjadi nilai pecahan yang berada diantara rentang tersebut. Setelah kunci menjalani pembacaan dan pengkonversian menjadi nilai karakter yang bersesuaian dengan urutan karakter, kunci kemudian dipetakan menjadi nilai pecahan antara 0 dan 1. Untuk pemetaan nilai karakter digunakan persamaan sebagai berikut:

$$P_k = b / 25 \qquad (1)$$

yang dalam hal ini P_k menyatakan nilai pecahan kunci yang dihasilkan dan b menyatakan nilai karakter.

Kemudian nilai-nilai pecahan yang dihasilkan dari pengkonversian nilai karakter kunci dengan persamaan (1) digunakan untuk menginisialisasi bobot-bobot yang terdapat pada jaringan saraf tiruan.

Untuk langkah inisialisasi, pertama-tama dibangun terlebih dahulu sebuah tabel yang menunjukan hubungan jaringan antara seluruh node masukan dengan seluruh node keluaran.

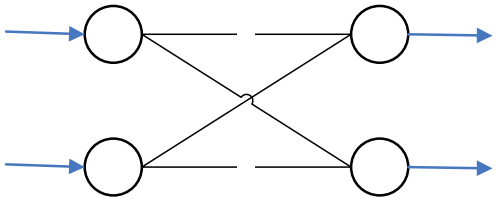
Kemudian, nilai-nilai pecahan dimasukan ke dalam tabel secara terurut dari pojok kiri atas sampai pojok kanan bawah. Jika nilai-nilai pecahan tidak mencukupi untuk mengisi seluruh tabel, maka pengisian tabel kembali menggunakan nilai pecahan yang telah digunakan sebelumnya secara terurut. Ilustrasi tabel tersebut adalah sebagai berikut:

Tabel 3. Tabel hubungan bobot antar node jaringan

	O_1	O_2
I_1	K_1	K_2
I_2	K_3	K_1

yang dalam hal ini I_1 menyatakan node masukan pertama, I_2 menyatakan node masukan kedua, O_1 menyatakan node keluaran pertama, O_2 menyatakan node keluaran kedua, K_1 menyatakan nilai pecahan pertama yang didapat melalui persamaan (1), K_2 menyatakan nilai pecahan kedua, dan K_3 menyatakan nilai pecahan kedua. Dalam ilustrasi ini kunci yang digunakan dimisalkan memiliki tiga nilai pecahan setelah mengalami proses pemetaan.

Selanjutnya data bobot dari tabel tersebut dimasukan ke dalam bobot hubungan jaringan antar node masukan dan node keluaran yang sesuai dengan urutan tabel.



Gambar 5. Jaringan Saraf Tiruan Setelah Mengalami Pembobotan

4.3 Langkah-langkah Enkripsi Algoritma

Langkah-langkah enkripsi dari algoritma kriptografi dengan menggunakan jaringan saraf tiruan adalah sebagai berikut:

1. Pembacaan plainteks
   Pada langkah ini, plainteks dibaca per karakter. Kemudian, tiap karakter yang dibaca dikonversikan menjadi nilai karakter yang bersesuaian dengan urutan karakter. Nilai karakter ini kemudian dipetakan menjadi nilai pecahan dengan rentang nilai antara 0 dan 1.

   Untuk pemetaan nilai karakter menjadi nilai pecahan, digunakan persamaan sebagai berikut:

   $$P_p = b / 25 \qquad (2)$$

   yang dalam hal ini P_p menyatakan nilai pecahan plainteks yang dihasilkan, b menyatakan nilai karakter.

   Kemudian, nilai pecahan dari plainteks dikelompokan menjadi blok-blok. Ukuran masing-masing blok akan menentukan akurasi proses dekripsi dengan menggunakan jaringan saraf tiruan.

2. Pembacaan kunci
   Pada langkah ini, kunci menjalani pembacaan dan pengkonversian menjadi nilai karakter yang bersesuaian dengan urutan huruf. Kunci kemudian dipetakan menjadi nilai pecahan antara 0 dan 1. Perbedaannya dengan langkah sebelumnya adalah persamaan yang digunakan dalam pemetaan nilai karakter menjadi nilai pecahan. Untuk pemetaan nilai karakter, digunakan persamaan (1).

3. Inisialisasi arsitektur jaringan saraf tiruan
   Pada langkah ini, jaringan saraf tiruan dibangun dan diinisialisasikan. Arsitektur jaringan saraf tiruan adalah satu lapisan masukan dan satu lapisan keluaran yang semua node dalam masing-masing lapisan terhubung dengan semua node dalam lapisan tetangganya. Jumlah node masukan dan node keluaran dalam jaringan saraf tiruan adalah sama dan sebesar jumlah blok.

4. Inisialisasi bobot-bobot yang digunakan dalam jaringan saraf tiruan
   Dalam langkah ini, nilai-nilai pecahan yang dihasilkan dari pengkonversian nilai byte dari kunci pada langkah 2 digunakan untuk menginisialisasi bobot-bobot yang terdapat pada jaringan sara tiruan.

   Untuk langkah inisialisasi, pertama-tama dibangun terlebih dahulu sebuah tabel yang menunjukan hubungan jaringan antara seluruh node masukan dengan seluruh node keluaran.

   Kemudian, nilai-nilai pecahan dimasukan ke dalam tabel secara terurut dari pojok kiri atas sampai pojok kanan bawah. Jika nilai-nilai pecahan tidak mencukupi untuk mengisi seluruh tabel, maka pengisian tabel kembali menggunakan nilai pecahan yang telah digunakan sebelumnya secara terurut.

   Selanjutnya data bobot dari tabel tersebut dimasukan ke dalam bobot hubungan jaringan antar node masukan dan node keluaran yang sesuai dengan urutan tabel.

5. Pengenkripsian menggunakan jaringan saraf tiruan
   Pada langkah ini, nilai pecahan plainteks yang telah didapat pada tahap sebelumnya dimasukan ke dalam jaringan saraf tiruan. Kemudian dari nilai masukan tersebut dikalkulasikan oleh jaringan saraf tiruan untuk menghasilkan kelompok nilai pecahan cipherteks.

   Langkah ini kemudian diulang kembali sampai seluruh kelompok nilai pecahan plainteks telah diproses menjadi nilai pecahan cipherteks.

6. Pengubahan nilai pecahan cipherteks menjadi blok karakter
   Pada langkah ini, nilai pecahan dari cipherteks dipetakan kembali menjadi nilai byte untuk disimpan dalam berkas dengan menggunakan pengkodean ASCII.

   Untuk pemetaan nilai pecahan menjadi nilai byte, digunakan persamaan sebagai berikut:

   $$B_c = [P_c * 255] \qquad (3)$$

   yang dalam ini B_c adalah karakter cipherteks, dan P_c adalah nilai pecahan cipherteks.

7. Pengumpulan blok-blok yang dienkripsi secara terpisah menjadi satu kumpulan cipherteks.
   Pada langkah ini, kumpulan byte-byte cipherteks dikumpulkan dan diubah menjadi cipherteks.

4.4 Langkah-langkah Dekripsi Algoritma

Untuk langkah-langkah dekripsi dari algoritma kriptografi dengan menggunakan jaringan saraf tiruan, secara garis besar terdiri dari langkah pembangkitan data pelatihan untuk jaringan saraf tiruan dekripsi, langkah berikutnya adalah pelatihan jaringan saraf tiruan dekripsi dengan data pelatihan tersebut. Secara mendetail, untuk mencapai hasil dekripsi dibutuhkan langkah-langkah sebagai berikut:

1. Pembacaan kunci
   Pada langkah ini, kunci menjalani pembacaan dan pengkonversian menjadi nilai karakter yang bersesuaian dengan urutan karakter. Kunci kemudian dipetakan menjadi nilai pecahan antara 0 dan 1.
   Untuk pemetaan nilai karakter kunci, persamaan yang digunakan adalah persamaan (1).

2. Pembacaan cipherteks
   Pada langkah ini, cipherteks dibaca per karakter. Kemudian, tiap karakter yang dibaca dikonversikan menjadi nilai byte yang bersesuaian dengan menggunakan

pengkodean ASCII. Nilai byte ini kemudian dikelompokan setiap dua byte dan dipetakan menjadi nilai pecahan dengan rentang nilai antara 0 dan 1.

Untuk pemetaan nilai byte menjadi nilai pecahan, digunakan persamaan sebagai berikut:

$$P_c = b / 255 \qquad (4)$$

yang dalam hal ini P_c menyatakan nilai pecahan cipherteks yang dihasilkan, b_1 menyatakan nilai byte dari karakter.

Kemudian, nilai pecahan dari cipherteks dikelompokan menjadi blok-blok. Ukuran masing-masing blok akan menentukan akurasi proses dekripsi dengan menggunakan jaringan saraf tiruan.

3. Inisialisasi arsitektur jaringan saraf tiruan pelatihan
   Pada langkah ini, sebuah jaringan saraf tiruan untuk tujuan pelatihan jaringan saraf tiruan dekripsi dibangun dan diinisialisasikan. Arsitektur jaringan saraf tiruan adalah satu lapisan masukan dan satu lapisan keluaran yang semua node dalam masing-masing lapisan terhubung dengan semua node dalam lapisan tetangganya.

   Jumlah node masukan dan node keluaran dalam jaringan saraf tiruan adalah sama dan sejumlah besar blok yang digunakan dalam algoritma.

4. Inisialisasi bobot-bobot yang digunakan dalam jaringan saraf tiruan
   Dalam langkah ini, nilai-nilai pecahan yang dihasilkan dari pengkonversian nilai byte dari kunci pada langkah 1 digunakan untuk menginisialisasi bobot-bobot yang terdapat pada jaringan saraf tiruan.

   Untuk langkah inisialisasi, pertama-tama dibangun terlebih dahulu sebuah tabel yang menunjukan hubungan jaringan antara seluruh node masukan dengan seluruh node keluaran.

   Kemudian, nilai-nilai pecahan dimasukan ke dalam tabel secara terurut dari pojok kiri atas sampai pojok kanan bawah. Jika nilai-nilai pecahan tidak mencukupi untuk mengisi seluruh tabel, maka pengisian tabel kembali menggunakan nilai pecahan yang telah digunakan sebelumnya secara terurut.

   Selanjutnya data bobot dari tabel tersebut dimasukan ke dalam bobot hubungan jaringan antar node masukan dan node keluaran yang sesuai dengan urutan tabel.

5. Pembangkitan nilai pelatihan jaringan saraf tiruan dekripsi
   Langkah ini bertujuan untuk membangkitkan data pelatihan untuk jaringan saraf tiruan dekripsi dengan menggunakan jaringan saraf tiruan pelatihan yang telah dibangun pada langkah sebelumnya.

   Data pelatihan memiliki format sebagai berikut:

   $$\langle \vec{X}, \vec{T} \rangle$$

   yang dalam hal ini $\vec{X}$ adalah vektor data-data masukan dan $\vec{T}$ adalah vektor data-data keluaran yang diharapkan.

   Pembangkitan data pelatihan masukan dilakukan secara acak. Setiap data pelatihan yang dibangkitkan memiliki ukuran yang sama dengan cipherteks. Data pelatihan masukan ini kemudian dimasukan ke dalam jaringan saraf tiruan pelatihan dan dikalkulasi keluarannya. Hasil keluaran jaringan saraf tiruan pelatihan untuk data masukan tersebut dipasangkan dengan data masukan sebagai keluaran yang diharapkan.

   Pembangkitan ini dilakukan secara berulang-ulang hingga tercipta sejumlah data pelatihan yang memadai untuk pelatihan jaringan saraf tiruan. Dari pengujian langsung ditemukan bahwa data pelatihan dengan jumlah lebih besar atau sama dengan 50 buah data saja sudah dapat memberikan tingkat akurasi jaringan saraf tiruan dekripsi yang mencapai 98% terhadap data pengujian. Namun karena data pelatihan dibangkitkan secara otomatis dari

masukan data yang acak, maka data pelatihan dapat terus dibangkitkan sesuai dengan kebutuhan peningkatan akurasi jaringan saraf tiruan dekripsi.

6. Inisialisasi arsitektur jaringan saraf tiruan dekripsi
   Pada langkah ini, jaringan saraf tiruan dekripsi dibangun dan diinisialisasikan. Arsitektur jaringan saraf tiruan adalah satu lapisan masukan dan satu lapisan keluaran yang semua node dalam masing-masing lapisan terhubung dengan semua node dalam lapisan tetangganya.

7. Pelatihan jaringan saraf tiruan dekripsi
   Langkah ini memanfaatkan data pelatihan yang telah dibangkitkan pada langkah sebelumnya dan bertujuan untuk melatih jaringan saraf tiruan dekripsi dalam melakukan proses dekripsi dari data yang terenkripsi.

   Dalam proses pelatihan jaringan saraf tiruan, terdapat beberapa parameter yang dapat disesuaikan dengan kebutuhan jaringan, yaitu:

   E = Epoch
   α = Momentum
   η = Laju pembelajaran

   Epoch menunjukan seberapa banyak pelatihan instans data yang diinginkan. Momentum menunjukan seberapa besar pelatihan pada instans sekarang hendak dipengaruhi oleh instans sebelumnya. Sedangkan laju pembelajaran menunjukan seberapa cepat jaringan saraf tiruan akan menyesuaikan diri dengan data pelatihan yang diterimanya.

   Pengujian dilakukan dengan menggunakan parameter E = 5000.

8. Pendekripsian pesan terenkripsi menggunakan jaringan saraf tiruan
   Pada langkah ini, jaringan saraf tiruan dekripsi yang telah dilatih digunakan untuk melakukan proses dekripsi dari pesan yang terenkripsi. Langkah ini memanfaatkan data pelatihan yang telah dibangkitkan pada langkah sebelumnya dan bertujuan untuk melatih jaringan saraf tiruan dekripsi dalam melakukan proses dekripsi dari pesan yang terenkripsi.

   Hasil dari langkah ini adalah nilai pecahan yang merupakan keluaran dari jaringan saraf tiruan. Nilai pecahan ini masih harus diproses lebih lanjut untuk menghasilkan plainteks semula.

9. Pengubahan nilai pecahan plainteks menjadi blok karakter
   Pada langkah ini, nilai pecahan dari plainteks yang dihasilkan dipetakan kembali menjadi nilai byte untuk disimpan dalam berkas atau ditampilkan dengan menggunakan pengkodean ASCII.

   Untuk pemetaan nilai pecahan menjadi nilai byte, digunakan persamaan sebagai berikut:

   $$B_p = [P_p * 25] \quad (5)$$

   yang dalam ini B_p adalah karakter plainteks hasil dekripsi dan P_p adalah nilai pecahan plainteks hasil dekripsi.

10. Pengumpulan blok-blok
    Blok-blok yang didekripsi secara terpisah dikumpulkan menjadi satu kumpulan plainteks hasil dekripsi.

5. Pengujian Algoritma

Untuk melihat proses enkripsi dan dekrripsi dari algoritma kriptografi dengan menggunakan jaringan saraf tiruan, maka dibutuhkan pengujian dalam bentuk langkah-langkah percobaan enkripsi dan dekripsi dengan menggunakan kasus uji tertentu.

5.1 Perancangan Kasus Uji

Dalam pengujian, digunakan kasus uji dengan plainteks dan kunci berupa kumpulan karakter untuk melihat cara kerja pengenkripsian dan pendekripsian algoritma kriptografi dengan menggunakan jaringan saraf tiruan ini. Kunci yang digunakan adalah “KEY”, sedangkan plainteks yang digunakan adalah “ATTACKUK”.

5.2 Langkah-langkah Enkripsi Pengujian

Langkah-langkah enkripsi pengujian dari sistem kriptografi jaringan saraf tiruan ini adalah sebagai berikut:

1. Pembacaan plainteks

Plainteks yang hendak dienkripsi adalah "ATTACKUK". Untuk setiap karakter, nilai pecahan dihitung dengan menggunakan persamaan (2). Misalnya, untuk karakter pertama:

b = 0
Pp = 0 / 25
= 0.0

Untuk pengkodean nilai pecahan seluruh plainteks dapat dilihat pada tabel berikut:

Tabel 4. Pengkodean nilai pecahan plainteks "ATTACKATDAWN"

Kelompok Karakter	Nilai Pecahan
A	0.00
T	0.76
T	0.76
A	0.00
C	0.08
K	0.40
U	0.80
K	0.40

2. Pembacaan kunci
Kunci yang hendak digunakan dalam proses enkripsi adalah "KEY". Untuk setiap karakter, nilai pecahan dihitung dengan menggunakan persamaan (1). Misalnya, untuk karakter pertama:

b = 10
Pp = 10 / 25
= 0.40

Untuk pengkodean nilai pecahan seluruh kunci dapat dilihat pada tabel berikut:

Tabel 5. Pengkodean nilai pecahan kunci "KEY"

Kelompok Karakter	Nilai Pecahan
K	0.40
E	0.16
Y	0.96

3. Inisialisasi arsitektur jaringan saraf tiruan.

Pada langkah ini, jaringan saraf tiruan dibangun dan diinisialisasikan. Arsitektur jaringan saraf tiruan adalah satu lapisan masukan dan satu lapisan keluaran yang semua node dalam masing-masing lapisan terhubung dengan semua node dalam lapisan tetangganya.

Jumlah node masukan dan node keluaran dalam jaringan saraf tiruan adalah sama dan sebesar jumlah blok yang dimiliki oleh sistem.

4. Inisialisasi bobot-bobot yang digunakan dalam jaringan saraf tiruan
Dalam langkah ini, nilai-nilai pecahan yang dihasilkan dari pengkonversian nilai byte dari kunci pada langkah 2 digunakan untuk menginisialisasi bobot-bobot yang terdapat pada jaringan sara tiruan.

Untuk langkah inisialisasi, pertama-tama dibangun terlebih dahulu sebuah tabel yang menunjukan hubungan jaringan antara seluruh node masukan dengan seluruh node keluaran.

Kemudian, nilai-nilai pecahan dimasukan ke dalam tabel secara terurut dari pojok kiri atas sampai pojok kanan bawah. Jika nilai-nilai pecahan tidak mencukupi untuk mengisi seluruh tabel, maka pengisian tabel kembali menggunakan nilai pecahan yang telah digunakan sebelumnya secara terurut.

Tabel 6. Tabel hubungan bobot antar node jaringan

	Node Keluaran 1	Node Keluaran 2
Node Masukan 1	0.40	0.16
Node Masukan 2	0.96	0.40

Selanjutnya data bobot dari tabel tersebut dimasukan ke dalam bobot hubungan jaringan antar node masukan dan node keluaran yang sesuai dengan urutan tabel.

5. Pengenkripsian menggunakan jaringan saraf tiruan

Pada langkah ini, nilai pecahan plainteks yang telah didapat pada tahap sebelumnya dimasukan ke dalam jaringan saraf tiruan. Kemudian dari nilai masukan tersebut dikalkulasikan oleh jaringan saraf tiruan untuk menghasilkan kelompok nilai pecahan cipherteks.

Langkah ini kemudian diulang kembali sampai seluruh kelompok nilai pecahan plainteks telah diproses menjadi nilai pecahan cipherteks. Hasil pemrosesan nilai pecahan plainteks "ATTACKUK" dapat dilihat pada Tabel 7.

Tabel 7. Tabel hasil kalkulasi nilai pecahan cipherteks

Nilai Pecahan Plainteks	Nilai Pecahan Cipherteks
0.00	0.674717
0.76	0.575420
0.76	0.575420
0.00	0.530363
0.08	0.602526
0.40	0.543093
0.80	0.669074
0.40	0.571506

6. Pengubahan nilai pecahan cipherteks menjadi karakter.
   Pada langkah ini, nilai pecahan dari cipherteks dipetakan kembali menjadi nilai byte untuk disimpan dalam berkas dengan menggunakan pengkodean ASCII. Untuk pemetaan nilai byte menjadi nilai pecahan, digunakan persamaan (3).

Tabel 8. Tabel hasil kalkulasi nilai byte cipherteks

Nilai Pecahan Cipherteks	Kode Byte Karakter Cipherteks	Karakter Cipherteks
0.674717	173	-
0.575420	147	"
0.575420	147	"
0.530363	136	ˆ
0.602526	154	š
0.543093	139	‹
0.669074	171	«
0.571506	146	'

7. Pengumpulan blok-blok yang dienkripsi secara terpisah menjadi satu kumpulan cipherteks.
   Pada langkah ini, kumpulan byte-byte cipherteks dikumpulkan dan diubah menjadi cipherteks. Hasil dari pengumpulan cipherteks tersebut dan perbandingannya dengan plainteks dapat dilihat pada tabel berikut:

Tabel 9. Tabel perbandingan plainteks dengan cipherteks

Plainteks	Cipherteks
ATTACKUK	-""ˆš‹'"

5.3 Langkah-langkah Dekripsi Pengujian

Untuk dekripsi, digunakan cipherteks yang didapat dari pengujian enkripsi sebelumnya. Langkah-langkah pengujian dekripsi dari sistem kriptografi jaringan saraf tiruan ini adalah sebagai berikut:

1. Pembacaan kunci
   Kunci yang hendak digunakan dalam proses enkripsi adalah "KEY". Untuk setiap karakter, nilai pecahan dihitung dengan menggunakan persamaan (1). Misalnya, untuk karakter pertama:

   b = 10
   Pp = 10 / 25
   = 0.40

   Untuk pengkodean nilai pecahan seluruh kunci dapat dilihat pada tabel berikut:

Tabel 10. Pengkodean nilai pecahan kunci "KEY"

Kelompok Karakter	Nilai Pecahan
K	0.40
E	0.16
Y	0.96

2. Pembacaan cipherteks
   Cipherteks yang hendak didekripsi adalah "-""ˆš‹'"". Untuk setiap karakter, nilai pecahan dihitung dengan menggunakan persamaan (2). Misalnya, untuk karakter pertama:

   b = 173

$$P_p = 173 / 256$$
$$= 0.67578125$$

Untuk pengkodean nilai pecahan seluruh plainteks dapat dilihat pada tabel berikut:

Tabel 11. Pengkodean nilai pecahan cipherteks "-""^š‹"'"

Kelompok Karakter	Nilai Pecahan
-	0.678431
"	0.576471
"	0.576471
^	0.533333
š	0.603922
‹	0.545098
«	0.670588
'	0.572549

3. Inisialisasi arsitektur jaringan saraf tiruan pelatihan
   Pada langkah ini, sebuah jaringan saraf tiruan untuk tujuan pelatihan jaringan saraf tiruan dekripsi dibangun dan diinisialisasikan. Arsitektur jaringan saraf tiruan adalah satu lapisan masukan dan satu lapisan keluaran yang semua node dalam masing-masing lapisan terhubung dengan semua node dalam lapisan tetangganya. Jumlah node masukan dan node keluaran dalam jaringan saraf tiruan adalah sama dan sebesar jumlah blok yang digunakan dalam algoritma.

4. Inisialisasi bobot arsitektur jaringan saraf tiruan pelatihan
   Dalam langkah ini, nilai-nilai pecahan yang dihasilkan dari pengkonversian nilai byte dari kunci pada langkah 2 digunakan untuk menginisialisasi bobot-bobot yang terdapat pada jaringan saraf tiruan. Inisialisasi bobot sesuai dengan Tabel 6.

5. Pembangkitan nilai pelatihan jaringan saraf tiruan dekripsi
   Langkah ini bertujuan untuk membangkitkan data pelatihan untuk jaringan saraf tiruan dekripsi dengan menggunakan jaringan saraf tiruan pelatihan yang telah dibangun pada langkah sebelumnya.

   Pembangkitan data pelatihan masukan dilakukan secara acak. Setiap data pelatihan yang dibangkitkan memiliki ukuran yang sama dengan cipherteks. Data pelatihan masukan ini kemudian dimasukan ke dalam jaringan saraf tiruan pelatihan dan dikalkulasi keluarannya. Hasil keluaran jaringan saraf tiruan pelatihan untuk data masukan tersebut dipasangkan dengan data masukan sebagai keluaran yang diharapkan.

   Pembangkitan ini dilakukan secara berulang-ulang hingga tercipta sejumlah data pelatihan yang memadai untuk pelatihan jaringan saraf tiruan. Dari pengujian langsung ditemukan bahwa data pelatihan dengan jumlah lebih besar atau sama dengan 50 buah data saja sudah dapat memberikan tingkat akurasi jaringan saraf tiruan dekripsi yang mencapai 98% terhadap data pengujian. Namun karena data pelatihan dibangkitkan secara otomatis dari masukan data yang acak, maka data pelatihan dapat terus dibangkitkan sesuai dengan kebutuhan peningkatan akurasi jaringan saraf tiruan dekripsi.

6. Inisialisasi arsitektur jaringan saraf tiruan dekripsi
   Pada langkah ini, jaringan saraf tiruan dekripsi dibangun dan diinisialisasikan. Arsitektur jaringan saraf tiruan adalah satu lapisan masukan dan satu lapisan keluaran yang semua node dalam masing-masing lapisan terhubung dengan semua node dalam lapisan tetangganya.

7. Pelatihan jaringan saraf tiruan dekripsi
   Langkah ini memanfaatkan data pelatihan yang telah dibangkitkan pada langkah sebelumnya dan bertujuan untuk melatih jaringan saraf tiruan dekripsi dalam melakukan proses dekripsi dari data yang terenkripsi.

   Dalam proses pelatihan jaringan saraf tiruan, terdapat beberapa parameter yang dapat disesuaikan dengan kebutuhan jaringan, yaitu:

   E = Epoch

α = Momentum
η = Laju pembelajaran

Pengujian dilakukan dengan menggunakan parameter E = 5000, α = 0.8, dan η = 0.7. Nilai parameter α dan η didapat dari pengujian nilai parameter optimal.

Setelah pelatihan jaringan saraf tiruan dekripsi sebanyak 5000 kali, dihasilkan jaringan saraf tiruan dengan tingkat akurasi mencapai 98%.

8. Pendekripsian pesan terenkripsi menggunakan jaringan saraf tiruan
Hasil dari langkah ini adalah nilai pecahan yang merupakan keluaran dari jaringan saraf tiruan. Nilai pecahan ini masih harus diproses lebih lanjut untuk menghasilkan plainteks semula.

Hasil pemrosesan nilai pecahan cipherteks dapat dilihat pada Tabel 12.

Tabel 12. Tabel hasil kalkulasi nilai pecahan plainteks

Nilai Pecahan Cipherteks	Nilai Pecahan Plainteks
0.678431	0.076076
0.576471	0.777351
0.576471	0.589260
0.533333	0.534617
0.603922	0.621045
0.545098	0.548566
0.670588	0.693587
0.572549	0.580807

9. Pengubahan nilai pecahan plainteks menjadi blok karakter
Pada langkah ini, nilai pecahan dari cipherteks dipetakan kembali menjadi nilai karakter sesuai dengan dengan urutan dari karakter. Untuk pemetaan nilai pecahan menjadi nilai karakter, digunakan persamaan (5).

Tabel 13. Tabel hasil kalkulasi nilai byte cipherteks

Nilai Pecahan Cipherteks	Nilai Karakter Cipherteks	Karakter Cipherteks
0.076076	2	C
0.777351	19	T
0.589260	15	P
0.534617	13	N
0.621045	16	Q
0.548566	14	O
0.536429	17	R
0.532896	15	P

10. Pengumpulan blok-blok
Pada langkah ini, kumpulan karakter plainteks yang dihasilkan dikumpulkan dan diubah menjadi plainteks hasil dekripsi. Hasil dari pengumpulan plainteks yang dihasilkan tersebut dan perbandingannya dengan plainteks awal dapat dilihat pada tabel berikut:

Tabel 14. Tabel perbandingan plainteks dengan cipherteks

Plainteks	Plainteks yang Didekripsi
ATTACKUK	CTPNQORP

5.5 Analisis Hasil

Hasil pengujian menunjukan bahwa akurasi jaringan saraf tiruan masih rendah. Dari delapan karakter yang dienkripsi, hanya satu karakter yang berhasil didekripsi tanpa adanya kesalahan.

Tingkat kesalahan dekripsi dihitung dengan menggunakan rumus sebagai berikut:

$$E = | P–C | / 25 \quad (6)$$

yang dalam hal ini E menyatakan tingkat kesalahan, P menyatakan kode urutan karakter plainteks, dan C menyatakan kode urutan karakter cipherteks yang didekripsi. Kesalahan dekripsi dapat dilihat pada tabel berikut:

Tabel 15. Tabel perbandingan plainteks dengan hasil dekripsi cipherteks

Karakter Plainteks	Karakter Hasil Dekripsi	Tingkat Kesalahan
A	C	8%
T	T	0%
T	P	16%
A	N	52%
C	Q	56%
K	O	16%
U	R	12%
K	P	2%

Tingkat kesalahan rata-rata dari pengujian jaringan saraf tiruan adalah sebesar 22.5%. Meskipun demikian, jaringan saraf tiruan sudah dapat mengenali pola hubungan enkripsi antara plainteks dan cipherteks. Hal ini dikarenakan jaringan saraf tiruan menghasilkan tingkat kesalahan yang lebih kecil dibandingkan pengkodean secara acak yang menghasilkan tingkat kesalahan sebesar 96%.

Kesalahan pendekripsian diperkirakan karena proses enkripsi dari nilai pecahan plainteks menjadi nilai pecahan cipherteks yang menghasilkan nilai pecahan cipherteks yang memiliki rentang yang rendah. Hal ini menyebabkan jaringan saraf tiruan kesulitan untuk membedakan antara satu nilai pecahan dengan nilai yang lainnya.

Rendahnya rentang nilai pecahan cipherteks ini dikarenakan penggunaan fungsi aktivasi sigmoid pada jaringan saraf tiruan. Fungsi aktivasi ini memetakan rentang nilai $(-\infty, +\infty)$ menjadi [0, 1], sementara nilai masukan hanya memiliki rentang [0, 25].

Pembulatan hasil pengkodean cipherteks tidak begitu mempengaruhi hasil enkripsi. Hal ini dikarenakan pengkodean dilakukan dari nilai plainteks yang berkisar antara [0, 25] menjadi nilai pengkodean ASCII yang berkisar antara [0, 255], sehingga akurasi saat pembulatan cipherteks lebih tinggi daripada akurasi saat pembulatan plainteks.

Selain itu, diduga training data yang hanya berjumlah sebanyak 50 buah menyebabkan terjadinya overfitting pada jaringan saraf tiruan dekripsi yang dihasilkan.

Kemudian, setelah melakukan analisa pada arsitektur jaringan saraf tiruan, ditemukan bahwa terdapat kemiripan antara kalkulasi jaringan saraf tiruan dengan sistem persamaan linier polinomial. Hal ini memberikan alternatif dekripsi jaringan saraf tiruan dengan mengkalkulasi langsung bobot-bobot pada jaringan saraf tiruan yang dibutuhkan untuk proses dekripsi dan tidak melalui proses pembelajaran seperti yang dipaparkan dalam makalah ini.

6. Kesimpulan

Kesimpulan yang dapat diambil dari perancangan algoritma kriptografi kunci simetri dengan menggunakan jaringan saraf tiruan adalah sebagai berikut:

1. Akurasi jaringan saraf tiruan yang dihasilkan masih rendah namun tetap lebih tinggi daripada pengkodean secara acak
2. Kesalahan pendekripsian disebabkan oleh pemetaan nilai pecahan cipherteks menjadi nilai pecahan plainteks yang memiliki rentang yang sedikit
3. Penggunaan fungsi aktivasi yang memetakan rentang nilai yang lebih sempit daripada fungsi aktivasi sigmoid diperkirakan dapat meningkatkan akurasi dekripsi jaringan saraf tiruan.
4. Penggunaan training data dengan jumlah yang lebih banyak diperkirakan dapat meningkatkan akurasi dekripsi jaringan saraf tiruan.
5. Penggunaan teorema sistem persamaan linier dapat menjadi alternatif dekripsi dari hasil enkripsi jaringan saraf tiruan.

DAFTAR PUSTAKA

[1] Laksmi, Agrita. (2002). Penyusunan Melodi pada Berkas MIDI dengan Jaringan Syaraf Tiruan. Departemen Teknik Informatika, Fakultas Teknologi Industri, Institut Teknologi Bandung.

[2] Mitchell M., Tom. (1997). Machine Learning. The McGraw-Hill Companies, Inc.

[3] Munir, Rinaldi. (2006). Bahan Kuliah IF5054 Kriptografi. Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung.