HASIL CEK_60020397_Point-C64-IRD-850GB-Kombinasi Sinkronisasi Jaringan Syaraf Tiruan dan Vigenere Cipher untuk Optimasi Keamanan Informasi

by Imam Riadi 60020397

Submission date: 11-Dec-2020 10:55AM (UTC+0700)
Submission ID: 1471707259
File name: Tiruan_dan_Vigenere_Cipher_untuk_Optimasi_Keamanan_Informasi.pdf (638.81K)
Word count: 4889
Character count: 29293

Kombinasi Sinkronisasi Jaringan Syaraf Tiruan dan Vigenere Cipher untuk Optimasi Keamanan Informasi

Abdul Fadlil[1], Imam Riadi[2], Achmad Nugrahantoro[3]
[1]Program Studi Teknik Elektro, Universitas Ahmad Dahlan,
[2]Program Studi Sistem Informasi, Universitas Ahmad Dahlan,
[3]Program Studi Teknik Informatika, Universitas Ahmad Dahlan,
[1,2,3]Jl. Prof. Dr. Soepomo, S.H, Janturan, Warungboto, Umbulharjo, Yogyakarta
e-mail: [1]fadlil@mti.uad.ac.id, [2]imam.riadi@is.uad.ac.id,
[3]achmad1907048001@webmail.uad.ac.id

Abstrak

Kriptografi pengubahan pesan asli menjadi disamarkan berguna menjaga kerahasiaan, integritas, keaslian, autentikasi pesan ketika proses komunikasi. Kriptografi klasik dengan subtitusi polialfabetik Vigenere memiliki tabel alphabet 26 baris yang relatif sederhana menjamin kerahasiaan. Kini pendekatan pembelajaran mesin Jaringan Syaraf Tiruan (JST) menjadi solusi layak untuk kriptografi dengan membentuk kunci rahasia dalam bobot jaringan sulit terpecahkan. Kunci dihasilkan dari bidirectional learning, dua pohon paritas saling tersinkronisasi dengan paramater hidden neuron, input neuron dan bobot. Sinkronisasi pada saluran publik dengan mengadopsi cara kerja Tree Parity Machine (TPM) dengan tipe feed forward. Pendekatan Kriptografi JST bermanfaat sebagai perlindungan dan serangan kriptografi. Penelitian ini memanfaatkan kombinasi sinkronisasi JST dan Vigenere dalam bentuk generator untuk optimasi pesan. Hasil pengujian kombinasi metode tidak berpengaruh dengan jumlah tampungan karakter pesan dan nilai parameter. Keunggulan kunci yang dihasilkan tidak bisa digunakan secara berulang meski nilai parameter sama, namun panjang karakter kunci berjumlah sama. Sisi fungsionalitas menghasilkan nilai 100%.

Kata kunci: Kriptografi, Jaringan Syaraf Tiruan (JST), *Tree Parity Machine* (TPM), Vigenere Cipher

Abstract

Cryptography changes the original message to be disguised useful to maintain the security message. Vigenere polyalphabetic substitution relatively simple 26-row alphabetical table guaranteeing confidentiality. Machine learning approach Artificial Neural Network (ANN) becomes feasible solution for cryptography by forming secret key in the weight of the network that's difficult to solve. The key's generated from bidirectional learning, two parity trees synchronized with hidden neurons, input neurons, and weights. Synchronize public channels by adopting the work of Tree Parity Machine (TPM) with feedforward type. This research utilizes the combination of synchronization ANN and Vigenere from generators. The result of testing the combination of methods doesn't affect the number of message character and parameter values. The advantages of the resulting key cannot be used repeatedly even though the parameter values are the same, but the key length is the same number of characters. The functionality produces 100% value.

Keywords: *Cryptography, Artificial Neural Networks (ANN), Tree Parity Machine (TPM), Vigenere Cipher*

1. Pendahuluan

Kriptografi merupakan teknik yang biasa digunakan untuk menjaga kerahasiaan data atau informasi menjadi bentuk yang tidak dimengerti dengan cara disamarkan [1][2][3]. Penyamaran kriptografi diubah menjadi sandi yang sengaja dibuat untuk membatasi hak akses kepada pihak yang dikehendaki [4][5][6]. Pada kehidupan sehari-hari teknik ini sudah banyak digunakan, misalkan penggunaan kartu cerdas yang sudah tersimpan sertifikat digital dan informasi personal pemilik yang tersimpan dalam bentuk *PIN (Personal Identification Number)*. Salah satunya ATM (Anjungan Tunai Mandiri) yang digunakan transaksi perbankan berbasis sertifikat digital yang divalidasi oleh CA *(Card Issuer)* memiliki PIN yang hanya diperbolehkan *entry* maksimum 3 kali dalam satu waktu, maka jika salah kartu ATM akan terblokir. Masalah tersebut membuktikan jika masalah kriptografi memegang peranan penting dalam menjaga autentikasi dalam hal kepemilikan.

Secara garis besar penerapan kriptografi diharapkan mampu melindungi layanan keamanan dengan menjaga kerahasiaan, integritas data untuk menjaga keaslian informasi [7][8], autentikasi dengan memastikan kebenaran pihak komunikasi dan pembuktian dengan membenarkan pihak yang terkait baik penerima [9] dan pemberi informasi atau disebut *non repudiation* [10]. Hal tersebut menjadi aspek penting untuk dijaga agar tidak dibajak ketika proses komunikasi [11].

Kini pembelajaran mesin sudah digunakan pada beberapa penelitian, pendekatan berbasis Jaringan Saraf Tiruan (JST) memberi solusi yang layak untuk kriptografi. Cara kerja JST mampu membentuk kunci enkripsi dan dekripsi terbentuk dalam bobot jaringan yang sulit dipecahkan. Proses sinkronisasi antara ke dua jaringan sangat cepat sehingga penyerang kesulitan menemukan celah [12]. Penelitian yang dilakukan oleh [13] sepakat jika JST tidak hanya bermanfaat sebagai perlindungan, namun bermanfaat juga untuk menahan serangan kriptografi. Kriptografi dengan pendekatan JST mampu menghasilkan kunci rahasia yang dihasilkan dari dua jaringan saluran publik, yang diimplementasikan menggunakan *Tree Parity Machine* (TPM) dengan tipe *feed fordward* [14]. Penelitian oleh [15] mengungkapkan jika JST menjadi keamanan model yang berbeda dari teknik kriptografi pada biasanya yang didasarkan pada teori fungsi angka, melainkan parameter berdasarkan desimal. Namun JST belum mampu melakukan proses enkripsi dan dekripsi yang dilakukan secara bersamaan.

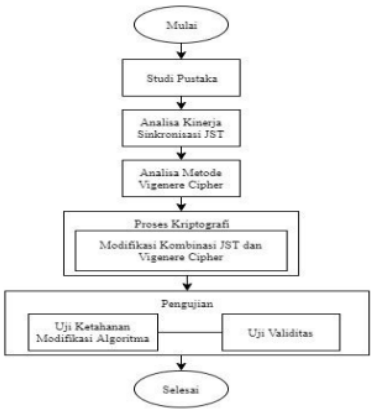
Mengacu pada penelitian terdahulu konsep sinkronisasi dengan jaringan syaraf sudah dimanfaatkan pada beberapa penelitian, yakni oleh [15] membuktikan jika pemodelan ini aman dari serangan *brute force* namun belum mampu menemukan enkripsi dalam bentuk asimetris kunci. Penelitian dari [16] kompleksitas linier skala protokol untuk sinkronisasi pembangkitan kunci dipengaruhi oleh ukuran pada *hidden layer* dan *input layer* dari struktur *Tree Parity Machine* (TPM) dengan hasil maksimal dengan serial varian kunci 132 bit cocok di implementasikan sebagai generator membantu komunikasi kabel atau nirkabel. Protokol pertukaran kunci pada Jaringan Syaraf Tiruan (JST) bergantung pada sinkronisasi jaringan pada dua pohon, konsep tersebut membuktikan jika sinkronisasi membuat untuk saling belajar [17]. Algoritma JST memungkinkan untuk dikombinasi dengan algoritma lain. Penelitian [13] bahkan menganggap metode JST cocok digunakan kriptanalisis karena cukup efektif dalam analisis lalu lintas metadata. Selain itu, penemuan bidang kriptografi dengan JST menjadi penemuan dengan pemanfaatan arsitektur pada jaringan dengan kecepatan sinkronisasi yang sangat tinggi, sehingga mencegah penyerangan selama proses pembelajaran bersama [14]. Penelitian JST kombinasi metode lain juga dilakukan oleh [18] dengan hasil yang dapat dioptimalkan dan diharapkan dapat diterapkan pada sistem berbasis nirkabel. Nilai-nilai parameter pada JST termasuk nilai *hidden neuron, input neuron* dan nilai bobot *(weight)* diproses pada saluran yang bersifat publik, karena setiap bobot vektor akan dipilih secara acak. Nilai vektor *input* dan

vektot *output* yang tetap ditransmisikan pada saluran publik, sehingga seringkali kunci yang dihasilkan akan berbeda-beda [17].

Metode yang umum digunakan untuk kriptografi salah satunya adalah Vigenere cipher. Cara kerja Vigenere termasuk dalam kriptografi klasik dengan pendekatan subtitusi majemuk pada abjad [11]. Kunci yang digunakan pada Vigenere akan diulangi sehingga mencapai panjang plainteks, sehingga meminimalkan terpecahnya cipherteks [19]. Namun pemecahan dengan metode kasiski analisis frekuensi mampu memecahkan cipherteks dan ketahanan algoritma pada penggunaan Vigenere cipher [20]. Penelitian yang mengkombinasikan metode Vigenere dilakukan oleh [21], mengungkapkan jika semakin besar file untuk di enkripsi maka waktu proses semakin lama. Vigenere cipher adalah salah satu metode kriptografi klasik. Kunci pada Vigenere cipher menyesuaikan dari panjangnya informasi dimana proses enkripsi dan dekripsi bekerja membaca kata sesuai per karakte. Penelitian dengan pemanfaatan Vigenere *cipher* belum bisa diketahui *testing* aplikasi [19], maka dalam usulan penelitan ini akan dikombinasikan JST untuk diketahui kecepatan waktu proses dan validasi algoritma. Vigenere dapat diterapkan dalam *platform* apa saja termasuk implementasi dengan *Personal Home Page* (PHP), seperti dalam penelitian yang dilakukan oleh [11] namun pada penelitian tersebut belum dilakukan *testing*. Metode Vigenere sudah dikombinasikan dengan metode lain, dimana jika dilihat dari sisi efektifitas dari segi ukuran *file* ketika proses enkripsi dan dekripsi paling kecil dibanding transposisi [21]. Dari penelitian sebelumnya, penggunaan JST hanya digunakan sebagai kunci publik. Namun untuk menambah ketahanan algoritma tersebut, peneliti mengkombinasikan dengan cara kerja Vigenere *chiper* sehingga mampu digunakan sebagai kunci rahasia. Selain itu, penelitian ini akan mengukur kinerja parameter-parameter yang digunakan pada kriptografi JST dengan kombinasi Vigenere *chiper* dalam menganalisa pola panjangnya kunci rahasia yang dihasilkan, dimana pada penelitian terdahulu belum dilakukan.

Berangkat dari latar belakang, maka akan dilakukan penelitian yang memanfaatkan pembelajaran mesin untuk pertukaran kunci secara acak menggunakan arsitektur Tree Parity Machine (TPM) pada Jaringan Syaraf Tiruan (JST) untuk proses enkripsi dan dekripsi kriptografi yang dikombinasikan dengan Vigenere cipher. Pemodelan akan diimplementasi sebagai generator sebagai optimasi mengamankan pesan dengan mengukur tingkat kecepatan pada waktu komputasi ketika iterasi dalam menghasilkan kunci dan pengaruh daya tampung karakter proses kriptografi. Sehingga mampu dimanfaatkan untuk pertukaran informasi secara rahasia yang hanya digunakan sekali atau tidak berulang dan pembangkitan kunci secara acak dengan kombinasi huruf.

2. Metode Penelitian



Gambar 1. Alir Diagram Kriptografi JST kombinasi Vigenere Cipher

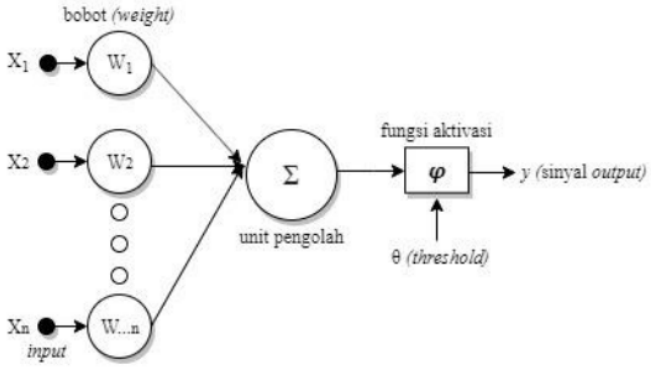
2.1. Studi Pustaka

Kegiatan ini menghimpun beberapa informasi yang dibutuhkan mengenai obyek yang akan diteliti, yakni referensi dari topik dan masalah dari buku, jurnal, karya ilmiah dan sumber pendukung lainnya terutama pada bidang keamanan informasi. Upaya kriptografi dengan pendekatan Jaringan Syaraf Tiruan (JST) dan Vigenere cipher untuk mengetahui cara kerjanya.

2.2. Analisa Kinerja Sinkronisasi Jaringan Syaraf Tiruan (JST)

Kinerja dari sinkronisasi Jaringan Syaraf Tiruan (JST) menggunakan *Tree Parity Machine* (TPM) untuk pembangkitan kunci publik, guna proses Vigenere cipher. Proses sinkronisasi dilakukan dengan melibatkan bobot, *hidden neurons* dan *input neurons* sehingga dilakukan pembelajaran mesin sampai proses berhenti [22].

Jaringan Syaraf Tiruan (JST) merupakan paradigma yang memproses informasi yang diilhami oleh struktur dan aspek fungsional pada jaringan syaraf biologis, yang menyerupai otak dalam memproses informasi [18]. JST merupakan cabang kecerdasan buatan yang memodelkan sistem komputasi pada informasi yang terdiri dari elemen-elemen pemrosesan saling berhubungan yang disebut neuron atau *artificial neurons*[23]. Elemen JST terdiri dari 3 (tiga) bagian utama : bobot, *threshold* dan fungsi aktivasi. Pemodelan sederhana dari JST terdapat pada Gambar 2.



Gambar 2 Model Struktur *Single* Neuron Jaringan Syaraf Tiruan (JST)

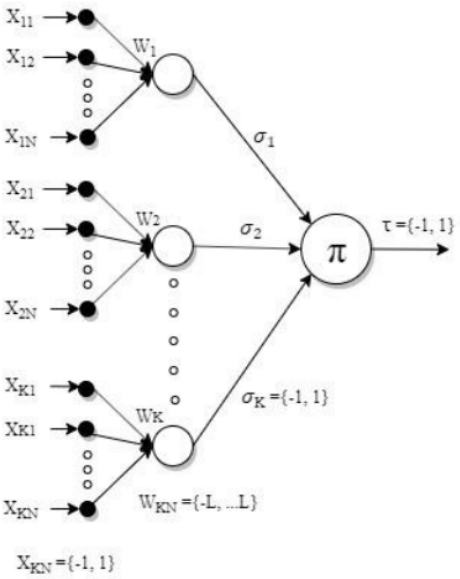
Mengacu pada Gambar 2, dijelaskan jika *input* (X_1, X_2, ... X_n) menjadi sinyal yang akan masuk ke sel syaraf. Nilai W_1, W_2, ...$W_{...n}$ adalah faktor bobot yang menghubungkan dengan masing-masing node, dimana setiap *input* akan dikalikan tiap bobot yang terhubung menyesuaikan fungsi aktivasi. Kemudian, menghasilkan *threshold* menjadi nilai amban internal yang berpengaruh pada besarnya nilai *offset* aktivasi node *output y*, dengan persamaan nilai (1)

$$y = \sum_{i=1}^{n} Xi\ Wi - \theta \qquad (1)$$

Fungsi aktivasi menjadi operasi fungsi matematik yang digunakan menghasilkan *y* sinyal *output*.

a. Tree Parity Machine (TPM)

Tree Parity Machine adalah JST dengan tipe dari *multi layer feed forward* yang terdiri dari *hidden neuron*, *input neuron* dan bobot [18][24].



Gambar 3. Arsitektur Tree Parity Machine

Lihat pada Gambar 3. arsitektur TPM terdiri dari nilai 1 *output* neuron, dengan nilai *K* sebagai *hidden neuron* dan *N* sebagai *input neuron*. Fungsi *input* ke jaringan dalam bentuk biner dengan fungsi (2)

$$Xij \in \{-1, +1\} \quad (2)$$

Weight adalah nilai bobot dari *input* dan *hidden neuron* yang didapatkan dari persamaan (3)

$$Wij \in \{-L, \dots, 0, \dots, +L\} \quad (3)$$

Sehingga nilai *output* dari setiap *hidden neuron* dikalkulasikan dari perhitungan jumlah dari semua *input neuron* dan nilai L sebagai bobot. Fungsi persamaan tersebut adalah (4).

$$\sigma_i = sgn\left(\sum_{j=1}^{N} w_{ij}\ x_{ij}\right) \quad (4)$$

Nilai pada sgn atau signum menjadi hitungan penyederhanaan mengembalikan nilai -1, 0 atau 1, yakni dengan ketentuan jika $sgn\ (x)$ -1 jika nilai $x < 0$; bernilai 0 jika $x = 0$; dan berinilai 1 jika $x < 0$. *Output* dari JST merupakan hasil dari nilai pada *hidden neuron*. Mengacu pada Gambar 1 *output* dari TPM dalam bentuk biner yang dihasilkan dari persamaan (5).

$$\tau = \prod_{i=1}^{K} sgn\left(\sum_{j=1}^{N} w_{ij}\ x_{ij}\right) \quad (5)$$

Keterangan, jika K sebagai *hidden neuron*, N sebagai *input neuron* dan nilai $_{ij}$.

b. Sinkronisasi JST TPM untuk Kriptografi

Nilai kunci yang dihasilkan dari kinerja TPM dihasilkan dari 2 (dua) jaringan pohon paritas yang disinkronisasi dalam saluran publik, sinkronisasi bobot yang bergantung pada waktu agar ke 2 (dua) paritas memiliki nilai yang sama. Proses sinkronisasi akan berlangsung cepat karena kedua paritas akan saling belajar sehingga menghasilkan kunci yang berguna untuk proses kriptografi.

Ketika proses sinkronisasi tercapai, yakni nilai bobot pada w_{ij} bernilai sama yang berasal dari kedua pohon paritas. Pendekatan ini menjadi proses dua arah mesin yang saling belajar. Namun, jika nilai bobot belum tercapai atau bernilai sama maka bobot TPM akan terus diperbarui. Beberapa persamaan yang digunakan ketika proses sinkronisasi sebagai berikut (6) (7) (8)

Hebbian learning rule:

$$w_{X^+j} = g\{w_i + \sigma_i x_i \ominus (\sigma_i \tau) \ominus (\tau^A \tau^B)\} \quad (6)$$

Anti-hebian learning rule :

$$w_{X^+j} = g\{w_i + \sigma_i x_i \ominus (\sigma_i \tau) \ominus (\tau^A \tau^B)\} \quad (7)$$

Random walk :

$$w_{X^+j} = g\{w_i + \sigma_i x_i \ominus (\sigma_i \tau) \ominus (\tau^A \tau^B)\} \quad (8)$$

Keterangan persamaan (6) (7) (8)
g menjaga rentang nilai pada bobot {-L, + L}
x vektor *input*
w vektor *weight*
Nilai masukan yang bernilai positif akan menghasilkan keluaran nilai 1 dan negatif bernilai 0.

2.3. Analisa Kinerja Vigenere Cipher

Hasil kunci publik dari hasil sinkronisasi Jaringan Syaraf Tiruan (JST) akan digunakan untuk proses Kriptografi enkripsi dan dekripsi pesan. Cara kerja Vigenere adalah deretan alfabet yang disandikan berdasarkan pendekatan Caesar berdasarkan huruf pada kunci [19]. Alfabet yang digunakan yaitu A, B, C, D, … sampai Z dalam prosesnya dikonversikan kedalam angka 0,1,2,3, ... sampai 25 [25]. Vigenere merupakan bentuk dari sandi subtitusi polialfabetik. Jika dibandingkan dengan Caesar, pendekatan ini tidak cukup rentan jika di retas dengan analisis frekuensi. Fungsi matematis Vigenere cipher untuk enkripsi (9) (10)

$$Ci = (Pi + Ki) \ mod \ 26 \quad (9)$$

Atau

$$Ci = (Pi + Ki) \quad (10)$$

jika jumlah Pi dan Ki dibawah 26 dan -26 jika hasil jumlah diatas 26

Fungsi untuk dekripsi Vigenere cipher (11) (12)

$$Pi = (Ci - Ki) \ mod \ 26 \quad (11)$$

Atau

$$Pi = (Ci - Ki) \quad (12)$$

jika hasil pengurangan dari Ci dengan Ki positif dan +26 jika *minus*

Keterangan fungsi matematis (1) (2) (3) (4)

$Ci = nilai\ ASCII\ dari\ karater\ cipherteks\ ke - i$
$Pi = nilai\ ASCII\ dari\ karater\ plainteks\ ke - i$
$Ki = nilai\ ASCII\ dari\ karater\ ke - i$
Nilai penyesuaian desimal A=0, B=1, C=2, ... Z=25

2.4. Usulan Penelitian Kombinasi Metode JST dan Vigenere

Usulan metode kriptografi melalui pendekatan Jaringan Syaraf Tiruan (JST) yang di kombinasikan dengan Vigenere cipher. Sinkronisasi JST menggukan konsep kinerja dari *Tree Parity Machine* (TPM), diharapkan dari 2 (dua) jaringan paritas yang memiliki parameter *input* layer, *hidden* layer dan bobot di sinkronisasi menghasilkan kunci rahasia sehingga akan dilanjutkan dengan perhitungan menggunakan Vigenere.

2.5. Pengujian

a. Uji Ketahanan Algoritma

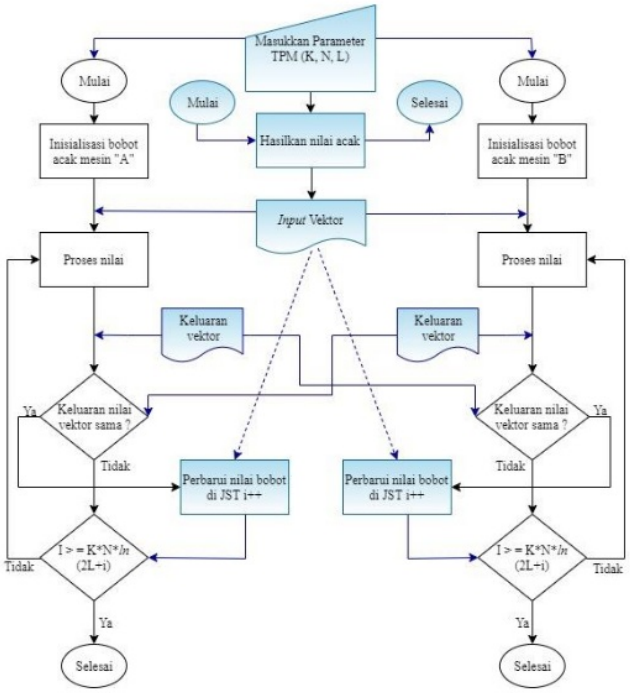
Pengujian ketahanan algoritma yakni pengujian yang dilakukan untuk mengetahui nilai efektivitas dari kecepatan dan daya tampung karakter ketika proses enkripsi dan dekripsi.

b. Uji Validitas

Uji fungsionalitas diperlukan dengan menyusun skenario proses enkripsi dan dekripsi ketika menggunakan kunci yang benar dan salah, untuk mengetahui jika metode kombinasi dapat digunakan.

3. Hasil dan Pembahasan

3.1. Kriptografi Sinkronisasi Jaringan Syaraf Tiruan (JST) dengan Tree Parity Machine (TPM)



Gambar 4. Alir Diagram Kriptografi Jaringan Syaraf Tiruan (JST)

Keterangan :

K merupakan parameter nilai *hidden neurons*
N merupakan parameter nilai *input neurons*
L merupakan parameter nilai bobot
A merupakan jaringan pohon paritas pihak pertama
B merupakan jaringan pohon paritas pihak kedua

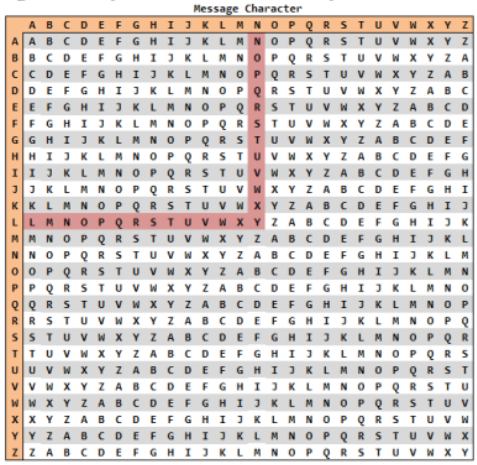
Mengacu pada Gambar 4 yang diambil dari referensi oleh [18], jika sinkronisasi terdapat dari kinerja 2 (dua) jaringan yang disebut dengan "A" dan "B" atau sebagai masing-masing pohon paritas. Kedua jaringan tersebut memiliki langkah kerja dan capaian yang sama, yakni sebagai berikut :

a. Perhitungan pada
b. Inisialisasi nilai bobot acak
c. Proses nilai : sinkronisasi hingga nilai tercapai dan sama sesuai dengan parameter yang dimasukkan, langkah proses tersebut :
   1) Menghasilkan nilai vektor acak, apakah keluaran vektor sudah sesuai *input* parameter, jika sudah maka memperbarui nilai bobot, jika sudah maka akan ke proses perhitungan berikutnya.
   2) Melakukan perhitungan antar nilai-nilai yang disembunyikan antar *neurons*
   3) Menghitung nilai keluaran vektor pada *neurons*, untuk kemudian dibandingkan dengan ketentuan : jika hasilnya berbeda maka akan kembali ke proses b dan jika sudah mencapai hasil yang sama sesuai ketetapan proses akan berhenti.

Metode *bidirectional learning* adalah ketika dua pohon paritas saling tersinkronisasi hingga menghasilkan kunci [18]. Jika nilai bobot keduanya seperti Gambar 6 belum saling terpenuhi maka akan perbarui nilai bobot sesuai dengan perhitungan nilai bobot pada Jaringan Syaraf Tiruan (JST).

3.2. Kriptografi dengan Vigenere Cipher

Pendekatan dengan metode ini sejenis dengen subtitusi *polyalphabetic* dalam proses mengenkripsi teks alfabet. Vigenere Cipher memiliki tabel seperti Gambar 5.



Gambar 5. Tabel Vigenere Cipher [26]

Informasi pada plainteks tedapat pada *"message character"* yang akan dilakukan titik temu dengan kunci yang dipakai, sehingga titik temu keduanya akan mengasilkan cipherteks. Namun proses akan semakin cepat menggunakan rumus module. Simulasi pengerjaan Vigenere cipher, misal diketahui :

Plainteks (P) : TEKNIK INFORMATIKA
Kunci (K) : MTIUAD

Maka proses enkripsi bisa disesuaikan dengan Gambar 5. atau bisa menggunakan dengan persamaan (9) dan (10), penyelesaiannya :

Tabel 1. Proses Enkripsi Vigenere Cipher

Proses Enkripsi (Pengubahan Plainteks ke Cipherteks)																	
P:	**T**	**E**	**K**	**N**	**I**	**K**	**I**	**N**	**F**	**O**	**R**	**M**	**A**	**T**	**I**	**K**	**A**
P(i)	19	4	10	13	8	10	8	13	5	14	17	12	0	19	8	10	0
K:	**M**	**T**	**I**	**U**	**A**	**D**	**M**	**T**	**I**	**U**	**A**	**D**	**M**	**T**	**I**	**U**	**A**
K(i)	12	19	8	20	0	3	12	19	8	20	0	3	12	19	8	20	0

$$(T) : Ci = (Pi + Ki)\ mod\ 26 = (19 + 12)\ mod\ 26 = 5\ atau\ (F) \quad (13)$$
$$(E) : Ci = (Pi + Ki) = (4 + 19) = 23\ atau\ (X) \quad (14)$$
$$(K) : Ci = (Pi + Ki) = (10 + 8) = 18\ atau\ (S) \quad (15)$$
$$(N) : Ci = (Pi + Ki)\ mod\ 26 = (13 + 20)\ mod\ 26 = 7\ atau\ (H) \quad (16)$$
$$(I) : Ci = (Pi + Ki) = (8 + 0) = 8\ atau\ (I) \quad (17)$$
$$(K) : Ci = (Pi + Ki) = (10 + 3) = 13\ atau\ (N) \quad (18)$$

...
Dst..

Sehingga dihasilkan cipherteks "FXSHIN UGNIRPMMQEA". Pencarian cipherteks juga bisa dilakukan dengan pencocokan antara "*message character*" dan *key character* sesuai Gambar 7. Kemudian untuk proses dekripsi atau pengembalian pesan kesemula yaitu :
Fungsi untuk dekripsi Vigenere *cipher* (11) (12)

Tabel 2. Proses Dekripsi Vigenere Cipher

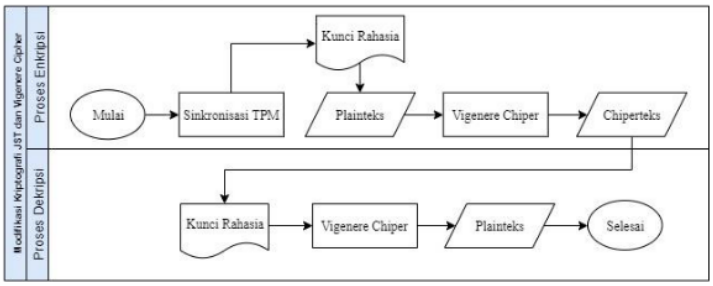
Proses Dekripsi (Pengubahan Cipherteks ke Plainteks)																	
C:	**F**	**X**	**S**	**H**	**I**	**N**	**U**	**G**	**N**	**I**	**R**	**P**	**M**	**M**	**Q**	**E**	**A**
C(i)	5	23	18	7	8	13	20	6	13	8	17	15	12	12	16	4	0
K:	**M**	**T**	**I**	**U**	**A**	**D**	**M**	**T**	**I**	**U**	**A**	**D**	**M**	**T**	**I**	**U**	**A**
K(i)	12	19	8	20	0	3	12	19	8	20	0	3	12	19	8	20	0

$$(F) : Pi = (Ci - Ki) + 26 = (5 - 12) + 26 = 19\ atau\ (T) \quad (19)$$
$$(X) : Pi = (Ci - Ki) = (23 - 19) = 4\ atau\ (E) \quad (20)$$
$$(S) : Pi = (Ci - Ki) = (18 - 8) = 10\ atau\ (K) \quad (21)$$
$$(H) : Pi = (Ci - Ki) + 26 = (7 - 20) + 26 = 13\ atau\ (N) \quad (22)$$
$$(I) : Pi = (Ci - Ki) = (8 - 0) = 8\ atau\ (I) \quad (23)$$
$$(N) : Pi = (Ci - Ki)\ mod\ 26 = (13 - 3) = 10\ atau\ (K) \quad (24)$$

...
Dst..

Maka dekripsi akan mengembalikan pesan semula cipherteks menjadi plainteks.

3.3. Modifikasi Jaringan Syaraf Tiruan (JST) kombinasi Vigenere Cipher



Gambar 6. Alur Kerja Kriptografi Kombinasi JST dan Vigenere Cipher

Alur kerja modifikasi kombinasi JST dan Vigenere cipher dijelaskan pada Gambar 6, yaitu sinkronisasi TPM dengan menginisiasi nilai dari K, N, L dari proses tersebut akan menghasilkan kunci rahasia yang berguna untuk proses dengan Vigenere cipher. Proses tersebut akan menghasilkan pesan rahasia. Kemudian, dilakukan proses dekripsi yaitu pesan tersandi atau cipherteks dibuka menjadi plainteks dengan pendekatan Vigenere.

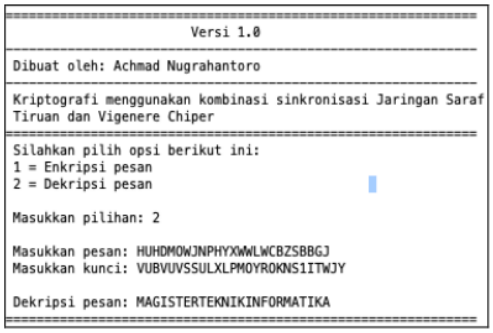
Implementasi Kriptografi modifikasi JST kombinasi Vigenere cipher digunakan untuk generator dengan antar muka pada Gambar 7 dan Gambar 8. Generator pada sistem ini terdiri dari masukan parameter TPM, yaitu *hidden neurons*, *input neurons* dan *weight* untuk menghasilkan kunci kemudian masukan plainteks hingga menampilkan hasil enkripsi. Pengembalian pesan dapat dilakukan dengan memasukkan chiperteks dan kunci maka pesan tersebut dapat kembali seperti semula.

```
============================================================
                        Versi 1.0
------------------------------------------------------------
Dibuat oleh: Achmad Nugrahantoro
------------------------------------------------------------
Kriptografi menggunakan kombinasi sinkronisasi Jaringan Saraf
Tiruan dan Vigenere Chiper
============================================================
Silahkan pilih opsi berikut ini:
1 = Enkripsi pesan
2 = Dekripsi pesan

Masukkan pilihan: 1

Parameter:
(K: hidden neurons, N: input neurons, L: bobot)

Masukkan K = 9
Masukkan N = 12
Masukkan L = 4

Iterasi Maksimal: 27648

Menyinkronkan Jaringan TPM ...

Status: BERHASIL!

Iterasi: 916
Data Diubah: 100 KiB
Panjang Kunci: 27
Kunci: VUBVUVSSULXLPMOYROKNS1ITWJY

Masukkan pesan: MAGISTERTEKNIKINFORMATIKA

Enkripsi pesan: HUHDMOWJNPHYXWWLWCBZSBBGJ
============================================================
```

Gambar 7. Antar Muka Enkripsi Generator JST dan Vigenere Cipher

Mengacu pada Gambar 7. terdapat tampilan antar muka ketika proses enkripsi, pada proses tersebut *user* diharapkan memasukkan nilai pada parameter K, N dan L untuk

sinkronisasi dengan pendekatan Jaringan Syaraf Tiruan (JST) sehingga menghasilkan kunci yang baru. Proses enkripsi menampilkan jumlah iterasi yang terjadi yakni proses sinkronisasi untuk mendapatkan bobot yang sama pada kedua pohon paritas A dan B (lihat Gambar 4) dan menghitung panjang kunci yang terbentuk.



Gambar 8. Antar Muka Enkripsi Generator JST dan Vigenere Cipher

Proses dekripsi pada Gambar 8., karena enkripsi tergolong dalam simetri maka menggunakan kunci rahasia yang sama pada kedua proses. Kelebihan dari metode ini adalah walaupun berkali-kali menggunakan nilai-nilai parameter yang sama, namun akan sedikit kemungkinan jika akan menghasilkan kunci yang serupa

3.4. Skenario Pengujian

a. Pengujian Ketahanan Algoritma

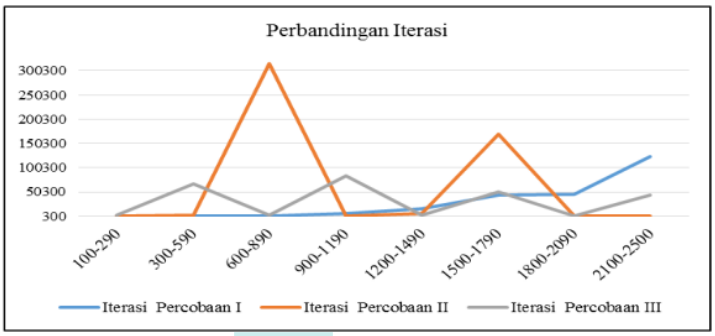
Pengujian ini perlu dilakukan untuk mengetahui efektivitas dari kecepatan dan daya tampung karakter ketika proses enkripsi dan dekripsi. Tabel 3 disajikan hasil pengujian ketahanan algoritma.

Tabel 3. Hasil Pengujian Ketahanan Algoritma

Karakter	Percobaan I			Panjang Kunci	Percobaan II			Panjang Kunci	Percobaan III			Panjang Kunci	Status*
	K	N	L		K	N	L		K	N	L		Berhasil
100-290	4	4	4	4	3	3	3	1	5	5	5	8	Berhasil
300-590	5	5	5	8	6	6	6	18	10	10	10	100	Berhasil
600-890	6	6	6	18	9	9	9	81	5	5	5	8	Berhasil
900-1190	7	7	7	24	3	3	3	1	10	10	10	100	Berhasil
1200-1490	8	8	8	32	6	6	6	18	5	5	5	8	Berhasil
1500-1790	9	9	9	81	11	11	11	121	10	10	10	100	Berhasil
1800-2090	10	10	10	100	3	3	3	1	5	5	5	8	Berhasil
2100-2500	11	11	11	121	6	6	6	18	10	10	10	100	Berhasil

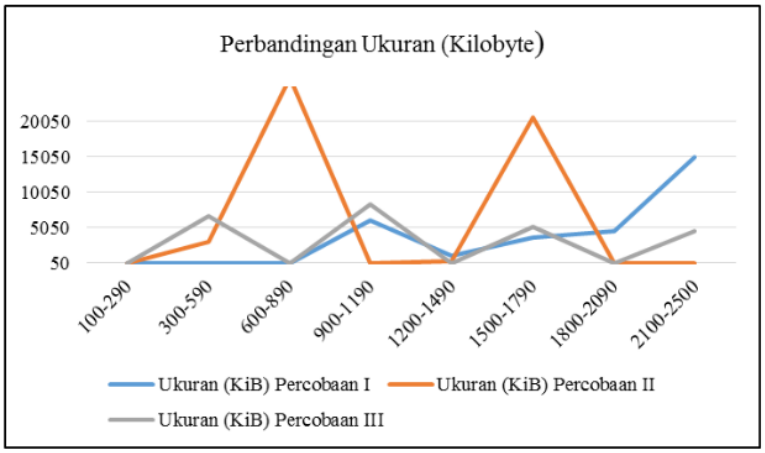
*status keberhasilan proses enkripsi dan dekripsi

Berdasarkan pada Tabel 3. akan menguji perbandingan iterasi, perubahan nilai bobot pada kunci dan panjang kunci yang dihasilkan dengan skenario nilai parameter K,N,L.



Gambar 9. Perbandingan Iterasi

Pada Gambar 9. dijelaskan jika grafik untuk nilai iterasi tertinggi dalam membentuk kunci yang mencocokan antara 2 pohon paritas, terjadi ketika tampungan karakter sebanyak 600-890, yakni dengan nilai K, N, L masing-masing adalah 9. Padahal ada karakter dengan daya tampung lebih banyak dan penggunaan parameter K, N, L lebih tinggi. Hal ini membuktikan jika penggunaan pendekatan dengan JST mampu memanipulasi dan tidak mudah ditebak dalam hal iterasi sinkronisasi 2 pohon paritas, karena tidak terlalu berpengaruh dengan banyaknya tampungan karakter dan nilai-nilai pada parameter.



Gambar 10. Perbandingan Ukuran (Kilobyte)

Mengacu pada Gambar 10. terjadi perubahan bobot sesuai dengan alur sinkronisasi TPM (Gambar 4), jika kedua paritas saling sinkronisasi jika belum menemukan kecocokan untuk menghasilkan kunci maka akan memperbarui nilai bobotnya. Terlihat pada Gambar 12 jika tampungan karakter 600-890 paling tertinggi, pembuktian jika semakin tinggi nilai iterasi maka perubahan nilai bobot JST akan semakin banyak.

Kinerja dari kombinasi JST dan Vigenere ini cenderung akan menghasilkan panjang kunci yang sama, jika menggunakan nilai K, N, L yang sama terus-menerus. Sehingga pola tersebut memungkinkan terbaca dan diketahui berapa banyak karakter kunci yang dihasilkan, hal ini bisa menjadi perhatian untuk penelitian kedepannya. Terlihat pada Tabel 3. jika menggunakan nilai K,N,L bernilai 5 maka akan konsisten panjang kuncinya adalah 8.

a. Pengujian Validitas

Pengujian ini perlu dilakukan untuk mengetahui jika kinerja modifikasi algoritma Kriptografi ini bisa bekerja dengan benar pada sistem. Skenario uji pada sistem ini menggunakan fungsionalitas ketika proses *generate* kunci kemudian proses pengubahan plainteks ke chiperteks (enkripsi) dan proses sebaliknya yaitu proses pengubahan chiperteks ke plainteks (dekripsi). Tabel 4. disajikan hasil pengujian dengan beberapa macam skenario proses enkripsi dan dekripsi ketika menggunakan kunci yang benar dan sengaja disalahkan.

Tabel 4. Hasil Pengujian Validitas

No.	Skenario Input	Hasil Output	Hasil
1.	Masukkan parameter TPM valid	Menampilkan hasil *generate* kunci berhasil	Valid
	Masukkan plainteks	Menampilkan hasil enkripsi	Valid
	Masukkan chiperteks benar dan kunci benar	Menampilkan hasil dekripsi benar	Valid
2.	Masukkan parameter TPM valid	Menampilkan hasil *generate* kunci berhasil	Valid
	Masukkan plainteks	Menampilkan hasil enkripsi	Valid
	Masukkan chiperteks benar dan kunci salah	Menampilkan hasil dekripsi salah	Valid
3.	Masukkan parameter TPM valid	Menampilkan hasil *generate* kunci berhasil	Valid
	Masukkan plainteks	Menampilkan hasil enkripsi	Valid
	Masukkan chiperteks salah dan kunci salah	Menampilkan hasil dekripsi salah	Valid
4.	Masukkan parameter TPM valid	Menampilkan hasil *generate* kunci berhasil	Valid
	Masukkan plainteks	Menampilkan hasil enkripsi	Valid
	Masukkan chiperteks benar dan kunci benar	Menampilkan hasil dekripsi salah	Valid
5.	Masukkan parameter TPM invalid	Menampilkan hasil *generate* kunci gagal	Valid

Pengujian validitas pada Tabel 4. menunjukkan bahwa kinerja modifikasi algoritma Kriptografi ini bekerja dengan benar pada sistem, hal ini dibuktikan pada keberhasilan saat proses *generate* kunci kemudian proses enkripsi atau sebaliknya yaitu proses dekripsi dari beberapa skenario uji pada sistem mengasilkan nilai 100% dengan *output* sesuai dengan yang diharapkan.

4. Kesimpulan

. Dari pengujian validitas menghasilkan nilai 100% dimana pengujian fungsionalitas tersebut menunjukkan hasil yang valid. Nilai iterasi ketika akan menghasilkan kunci rahasia, tidak terlalu berpengaruh dengan daya tampung karakter meski nilai pembaruan bobot akan semakin tinggi mengikuti banyaknya iterasi. Pola kunci panjang kunci yang dihasilkan jika mengunakan parameter *hidden layer*, *input layer* dan bobot yang sama pada tiap proses enkripsi cenderung memiliki jumlah karakter yang sama. Penelitian ini masih dalam bentuk generator, namun untuk kedepannya pendekatan akan berguna dalam kehidupan sehari-hari. Penerapan

algoritma kriptografi modifikasi dibutuhkan untuk dimanfaatkan dalam mengamankan data dan informasi pada sistem web maupun *mobile*. Pada sisi web pengamanan bisa diterapkan dalam pembuatan token bisa juga diterapkan dalam pembuatan *Application Programming Interface* (API), sedangkan untuk *mobile* bisa diterapkan untuk pengamanan alamat web Selain itu, algoritma ini diharapkan bisa dimanfaatkan juga untuk proses mengamankan file dokumen penting, sehingga keabsahan informasi tetap terjaga dan tidak bisa disalahgunakan oleh pihak tidak berwenang.

Daftar Pustaka

[1] D. Ariyus, "Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi," l. Yogyakarta: Penerbit Andi, 2008.

[2] S. D. Putra, M. Yudhiprawira, S. Sutikno, Y. Kurniawan, and A. S. Ahmad, "Power Analysis Attack Against Encryption Devices: a Comprehensive Analysis of AES, DES, and BC3," *TELKOMNIKA (Telecommunication Comput. Electron. Control.*, vol. 17, no. 3, p. 1282, 2019.

[3] P. S. Nugroho and E. Aribowo, "Pengembangan Modul Enkripsi dan Dekripsi pada Php dengan Modifikasi Metode Kriptografi Vigenere Cipher dan Cipher Block Chaining (Studi Kasus pada Geekybyte. com)," *J. Sarj. Tek. Inform.*, vol. 2, no. 1, pp. 333–341, 2014.

[4] R. Munir, "Pengantar Kriptografi," *ITB, Bandung*, 2006.

[5] A. G. Konheim, "Computer Security and Cryptography," John Wiley & Sons, 2007.

[6] V. Wati, H. Sa'diyah, and D. Ariyus, "Pendekatan Stego-Kripto Mode Cipher Block Chaining Untuk Pengamanan Informasi Pada Citra Digital," *JITK (Jurnal Ilmu Pengetah. dan Teknol. Komputer)*, vol. 5, no. 2, pp. 197–204, 2020.

[7] Y. Arta, "Implementasi Intrusion Detection System Pada Rule Based System Menggunakan Sniffer Mode Pada Jaringan Lokal," *IT J. Res. Dev.*, vol. 2, no. 1, p. 43, Nov. 2017.

[8] P. Irfan, Y. Prayudi, and I. Riadi, "Image Encryption using Combination of Chaotic System and Rivers Shamir Adleman (RSA)," *Int. J. Comput. Appl.*, vol. 123, no. 6, pp. 11–16, 2015.

[9] N. Laila and A. S. R. Sinaga, "Implementasi Steganografi LSB Dengan Enkripsi Vigenere Cipher Pada Citra," *Sci. Comput. Sci. Informatics J.*, vol. 1, no. 2, p. 47, 2019.

[10] A. Sofwan, A. B. P, and T. Susanto, "Aplikasi Kriptografi dengan Algoritma Message Digest 5 (Md5)," *Transmisi*, vol. 8, no. 1, pp. 22–27, 2006.

[11] M. D. Irawan, "Implementasi Kriptografi Vigenere Cipher dengan Php," *J. Teknol. Inf.*, vol. 1, no. 1, p. 11, 2017.

[12] P. P. Hadke and S. G. Kale, "Use of Neural Networks in Cryptography: A Review," *IEEE WCTFTR 2016 - Proc. 2016 World Conf. Futur. Trends Res. Innov. Soc. Welf.*, pp. 1–4, 2016.

[13] M. Abadi and D. G. Andersen, "Learning to Protect Communications with Adversarial Neural Cryptography," *arXiv Prepr. arXiv1610.06918*, pp. 1–15, 2016.

[14] P. P. Hadke and P. M. R. Dubey, "Neural Cryptography for Secret Key Exchange," *Int. J. Mod. Trends Sci. Technol.*, vol. 03, no. March, pp. 15–18, 2017.

[15] S. Pattanayak and S. A. Ludwig, "Encryption Based on Neural Cryptography," *Adv.*

Intell. Syst. Comput., vol. 734, pp. 321–330, 2018.

[16] S. Wallner, "Designing low-cost cryptographic hardware for wired- or wireless point-to-point connections," *Commun. Comput. Inf. Sci.*, vol. 36, pp. 1–10, 2009.

[17] A. Singh and N. Aarti, "Neural Cryptography for Secret Key Exchange and Encryption with AES," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 3, no. 5, pp. 376–381, 2013.

[18] S. Man and S. Shrestha, "C ++ Implementation of Neural Cryptography for Public Key Exchange and Secure Message Encryption with Rijndael Cipher," *Academia.Edu*, pp. 1–8, 2013.

[19] A. Amrulloh and E. I. H. Ujianto, "Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher," *J. CoreIT*, vol. 5, no. 2, pp. 71–77, 2019.

[20] H. Sadiyah, V. Wati, and D. Ariyus, "Telematika Implementasi Keamanan Pesan pada Citra Steganografi Menggunakan Modifikasi Cipher Block Chaining (CBC) Vigenere," *Telematika*, vol. 13, no. 1, pp. 44–55, 2020.

[21] M. A. Maricar and N. P. Sastra, "Efektivitas Pesan Teks Dengan Cipher Substitusi, Vigenere Cipher, dan Cipher Transposisi," *Maj. Ilm. Teknol. Elektro*, vol. 17, no. 1, p. 59, 2018.

[22] B. C. Hrishikesh, D. Queenie, A. Krati, and K. Lavanya, "Vectorized Neural Key Exchange using Tree Parity Machine," *An Int. J. Adv. Comput. Technol.*, vol. 8, no. 5, 2019.

[23] I. Riadi, A. Wirawan, and S. -, "Network Packet Classification using Neural Network based on Training Function and Hidden Layer Neuron Number Variation," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 6, 2017.

[24] A. Ruttor, "Neural Synchronization and Cryptography," 2007.

[25] E. H. A. Mendrofa, E. Y. Purba, B. Y. Siahaan, and R. W. Sembiring, "Collaborative Encryption Algorithm Between Vigenere Cipher, Rotation of Matrix (ROM), and One Time Pad (OTP) Algoritma," *Adv. Sci. Technol. Eng. Syst. J.*, vol. 2, no. 5, pp. 13–21, 2017.

[26] Wikibooks, "Visual Basic for Applications," 2020. .

HASIL CEK_60020397_Point-C64-IRD-850GB-Kombinasi Sinkronisasi Jaringan Syaraf Tiruan dan Vigenere Cipher untuk Optimasi Keamanan Informasi

ORIGINALITY REPORT

8%	5%	4%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to UIN Sultan Syarif Kasim Riau Student Paper	3%
2	journal.unilak.ac.id Internet Source	2%
3	media.neliti.com Internet Source	1%
4	pdfs.semanticscholar.org Internet Source	1%

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		