Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 2, April 2026: halaman 102-111

P-ISSN: 2746-5985
e-ISSN: 2797-0930

DOI: https://doi.org/10.52362/jmijayakarta.v6i2.2239

IMPLEMENTASI KRIPTANALIS BERBASIS NEURAL NETWORK FEEDFORWARD BACKPROPAGATION MULTI LAPIS TERHADAP KRIPTOGRAFI S-DES

[1]Fritz Gamaliel*, [2] P. Yudi Dwi Arliyanto

[1]Program Studi Teknologi Rekayasa Perangkat Lunak, Politeknik META Industri Cikarang
[2]Program Studi Teknik Industri, Politeknik META Industri Cikarang
Jln. Inti Blok C1 No7 Lippo Cikarang

*e-mail: fritzgamaliel@gmail.com

Abstrak

Kriptografi digunakan untuk menjamin keamanan informasi rahasia antara pengirim informasi dan penerima informasi. Pengirim melaksanakan enkripsi terhadap informasi yang dirahasiakan tersebut sebelum informasi rahasia tersebut dikirim ke penerima informasi. Setelah informasi rahasia yang telah dienkripsi tersebut diterima di sisi penerima informasi rahasia kemudian penerima melaksanakan dekripsi terhadap informasi rahasia yang terenkripsi tersebut. Dalam praktiknya terdapat pihak ketiga yang berupaya melaksanakan berbagai cara untuk mencari tau apa isi informasi rahasia tersebut. Pada penelitian ini, peneliti melaksanakan kriptanalis terhadap kriptografi. Peneliti menggunakan metode kriptografi S-DES dan kriptanalis berbasis neural network backpropagation multi lapis. Baik dalam proses training maupun testingnya menggunakan seluruh kemungkinan kombinasi plaintext, kunci, dan ciphertext yang terdapat pada kriptografi S-DES. Pengujian akurasi terhadap model hasil training dilaksanakan dengan cara menghitung persentase ciphertext model yang sama dengan ciphertext S-DES. Hasil penelitian menunjukkan bahwa kriptanalis berbasis neural network yang digunakan dalam penelitian kurang begitu akurat dalam melaksanakan kriptanalis terhadap kriptografi S-DES. Hal tersebut dapat dilihat dari hasil pengujian tingkat keakuratannya yang berada di bawah 1%.

Kata kunci: Kriptografi, S-DES, Kriptanalis, Neural Network.

Abstract

Cryptography is used to ensure the confidential information between the sender and the recipient. The sender encrypts the confidential information before it is transmitted to the recipient. After the encrypted confidential information is received by the recipient, the recipient then performs decryption on the encrypted confidential information. In practice, there are third parties who attempt to use various methods to find out the contents of the confidential information. In this study, the researchers perform cryptanalysis on the cryptographic system. The researchers use the S-DES cryptographic method and the neural network multilayer backpropagation cryptanalysis method. Both the training and testing processes use all possible combinations of plaintexts, keys, and ciphertexts in the S-DES cryptographic system. The accuracy of the trained model is evaluated by calculating the match percentage between ciphertext that produced by the model and ciphertext that produced by S-DES. The results show the neural network–based cryptanalysis that used in this research is not sufficiently accurate in performing cryptanalysis on the S-DES cryptographic system. This can be seen from the accuracy test results, which are below 1%.

Keywords: *Cryptography, S-DES, Cryptanalyst, Neural Network*

Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 2, April 2026: halaman 102-111
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v6i2.2239

1 Pendahuluan

Dalam kehidupan sehari-hari manusia melaksanakan komunikasinya baik dengan cara verbal maupun dengan cara non-verbal. Dalam komunikasi tersebut, salah satunya terdapat informasi yang disampaikan oleh pemberi informasi dan penerima informasi. Ketika informasi yang disampaikan bersifat rahasia, pastinya diharapkan informasi rahasia tersebut hanya dapat diketahui oleh pemberi informasi dan penerima informasi. Sejauh ini terdapat berbagai cara yang telah dilaksanakan untuk memenuhi harapan tersebut, baik cara-cara yang bersifat teknis maupun cara-cara yang bersifat sosial. Cara-cara yang bersifat teknis salah satunya dengan menggunakan kriptografi. Cara-cara yang bersifat sosial salah satunya dengan menggunakan peraturan-peraturan semisal Undang-Undang Perlindungan Data. Adapun pada penelitian ini peneliti menyempitkan ruang lingkup hanya kepada cara-cara yang bersifat teknis yaitu kriptografi S-DES.

Pada kriptografi, pengirim melaksanakan enkripsi terhadap informasi rahasia yang akan dikirimkan sehingga menjadi ciphertext. Selanjutnya ciphertext diterima oleh penerima untuk dilaksanakan dekripsi pada sisi penerima agar dapat diketahui apa isi asli ciphertext tersebut. Perkembangan kriptografi juga diikuti dengan perkembangan cara-cara untuk memecahkan sandi sandi kriptografi semisal kriptanalis berbasis kecerdasan buatan, kriptanalis aljabar, kriptanalis linear, kriptanalis berbasis *exhaustive search*. Adapun penelitian ini mengerucutkan kepada kriptanalis berbasis neural network terhadap kriptografi S-DES.

Terdapat penelitian-penelitian sebelumnya yang membahas tentang kriptanalis berbasis neural network terhadap kriptografi S-DES misalnya saja penelitian yang dilaksanakan oleh Khaled M. Alallayah dan kawan-kawan [1]. Penelitian-penelitian sebelumnya telah mengevaluasi kriptanalis berbasis neural network namun salah satunya belum terdapat evaluasi yang menghitung jumlah kesesuaian antara ciphertext S-DES dengan ciphertext model neural networknya yang merupakan hasil training menggunakan seluruh kemungkinan kombinasi plaintext, kunci, dan ciphertext yang terdapat pada kriptografi S-DES. Kontribusi dari penelitian ini adalah menyediakan evaluasi tersebut dan tidak bertujuan untuk membuktikan ulang ketidakamanan kriptografi S-DES.

2 Tinjauan Literatur

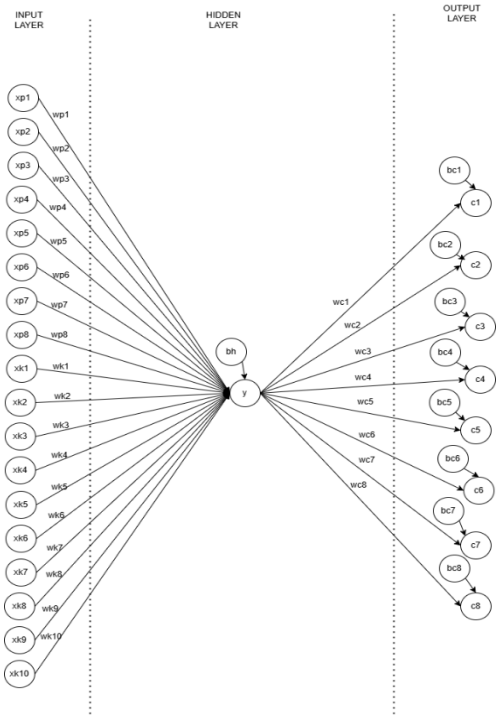
Peneliti menggunakan metode studi literatur dan eksperimen untuk dapat melaksanakan penelitian ini. Studi literatur dilaksanakan dengan mempelajari makalah-makalah terkait topik penelitian untuk mengetahui bagaimana kriptografi S-DES, dan bagaimana kriptanalisis berbasis neural network. Penelitian Khaled M. Alallayah dan kawan-kawan menganalisis kriptografi S-DES dengan menggunakan neural network feedforward multi lapis dengan target error_rate 0.00001, 1024 data training, dan 1640-7869 epoch [1]**.** Penelitian Mundi Wiwit Kurniaga dkk menganalisis kriptografi DES dengan menggunakan neural network feedforward 4 lapis dimana 64 neuron pada lapisan input, 100 neuron masing-masing pada lapisan tingkat menengah, dan 64 neuron pada lapisan output [2]. Penelitian Fadila Paradise dan Santi Indarjan menganalisis kriptografi S-DES dengan menggunakan kriptanalis aljabar [3]. Penelitian Yandi Anzari dan kawan-kawan dan menganalisis brute force terhadap kriptografi Caesar Cipher [4]**.** Penelitian Uci Julya Ningsih dan kawan-kawan menganalisis kriptanalis known plain attack, frequency analysis, dan brute force terhadap kriptografi Caesar Cipher [5]. Penelitian RizkyAlfiansyah dan kawan-kawan menganalisis kriptanalis brute force terhadap kriptografi MD5 [6]**.** Penelitian Farhan Amar Pramudya dan Suhardi salah satunya menggunakan kriptanalis berbasis brute force untuk menganalisis keamanan kriptografi Caesar Cipher dan DES [7]**.** Penelitian Bahubali Akiwate dan Veena Desa menganalisis kriptografi DES dengan menggunakan neural network feedforward 4 lapis dimana 64 neuron pada lapisan input, 100 neuron masing-masing pada lapisan tingkat menengah, dan 64 neuron pada lapisan output [8]**.** Penelitian Fadila Paradise dan Santi Indarjani menggunakan plaintext 01101101 dalam proses mendapatkan 8 persamaan aljabar S-DES [9]**.** Penelitian Stefan Andonov dan kawan-kawan menganalisis kriptografi DES menggunakan neural network yang lapisan hiddennya terdiri atas empat lapisan, di mana pengujian DES satu ronde dilakukan dengan 1.000 dataset pelatihan yang masing-masing terdiri atas 2^{19} pasangan ciphertext–plaintext, sedangkan pengujian DES 16 ronde menggunakan beberapa variasi

Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 2, April 2026: halaman 102-111
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v6i2.2239

susunan lapisan hiddennya yang dilakukan dengan 2^{17} pasangan ciphertext–plaintext [10]. Penelitian Sijie Fan and Yaqun Zhao menganalisis kriptografi DES dengan menggunakan neural network backpropagation yang telah dimodifikasi sedemikian yang dimana pada proses trainingnya sampai kedapatan error rate stagnan pada kisaran 10% [11]. Penelitian Ya Xiao menggunakan 3 macam arsitektur neural network (fat and shallow, deep and thin, dan cascade) dalam menganalisis kriptografi DES tereduksi, menggunakan 2 macam arsitektur neural network (fat and shallow, dan deep and thin) dalam menganalisis kriptografi Hitag2, dan masing-masingnya menggunakan 2^{16} sampai 2^{20} dataset training [12]. Penelitian Yulia Fatma dan kawan-kawan menganalisis kriptografi dengan menggunakan deep learning neural network feedforward backpropagation dengan jumlah lapisan hidden sebanyak 10 lapis dengan target error 0.01 atau target 200.000 epoch dan diujikan kepada dataset berukuran besar [13]**.** Penelitian Yusuf Ramadhan Nasution dan kawan-kawan mengamankan file PDF dengan menggunakan kriptografi Vernam [14]. Penelitian Bregas Arya Bagaskara dan kawan-kawan menguji keamanan website dinas sosial Surabaya [15]. Adapun yang menjadi pembeda antara penelitian ini dengan penelitian-penelitian tersebut adalah dalam penelitian ini menganalisis kriptografi S-DES dengan menggunakan neural network feedforward backpropagation multi lapis dengan menggunakan seluruh kemungkinan kombinasi plaintext, kunci, ciphertext yang ada pada kriptografi S-DES sebagai data trainingnya (ada 65536 data training) dan epoch 1000 sampai 10000.

3 Metode Penelitian (or Research Method)

Arsitektur Neural Network 1 Hidden Layer 1 Neuron yang digunakan dalam penelitian dapat dilihat seperti Gambar 1



Gambar 1 Arsitektur Yang Digunakan

Keterangan Gambar 1:

xp = bit plaintext. xp1 = bit ke-1 plaintext, xp2 = bit ke-2 plaintext, xp3 = bit ke-3 plaintext, xp4 = bit ke-4 plaintext, xp5 = bit ke-5 plaintext, xp6 = bit ke-6 plaintext, xp7 = bit ke-7 plaintext, xp8 = bit ke-8 plaintext

xk = bit kunci. xk1 = bit ke-1 kunci, xk2 = bit ke-2 kunci, xk3 = bit ke-3 kunci, xk4 = bit ke-4 kunci, xk5 = bit ke-5 kunci, xk6 = bit ke-6 kunci, xk7 = bit ke-7 kunci, xk8 = bit ke-8 kunci, xk9 = bit ke-9 kunci, xk10 = bit ke-10 kunci

Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 2, April 2026: halaman 102-111
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v6i2.2239

wp1, wp2, wp3, wp4, wp5, wp6, wp7, wp8, wk1, wk2, wk3, wk4, wk5, wk6, wk7, wk8, wk9, wk10, wc1, wc2, wc3, wc4, wc5, wc6, wc7, wc8 = Bobot. Bobot diinisialisasi dengan menggunakan metode He Uniform sehingga didapatkan range angka -0.577350269 s.d. +0.577350269. Misal ditetapkan wp1=0.000000001, wp2=0.000000005, wp3=0.000000010, wp4=0.000000015, wp5=0.000000020, wp6=0.000000025, wp7=0.000000030, wp8=0.000000035, wk1=0.000000040, wk2=0.000000045, wk3=0.000000050, wk4=0.000000055, wk5=0.000000060, wk6=0.000000065, wk7=0.000000070, wk8=0.000000075, wk9=0.000000080, wk10=0.000000085, wc1=0.000000090, wc2=0.000000095, wc3=0.000000100, wc4=0.000000105, wc5=0.000000110, wc6=0.000000115, wc7=0.000000120, wc8=0.000000125

bh, bc1, bc2, bc3, bc4, bc5, bc6, bc7, bc8= Bias. Bias diinisalisasi dengan angka 0. Jadi bh=0, bc1=0, bc2=0, bc3=0, bc4=0, bc5=0, bc6=0, bc7=0, bc8=0

c = bit ciphertext. c1=bit ke-1 ciphertext, c2=bit ke-2 ciphertext, c3=bit ke-3 ciphertext,c4=bit ke-4 ciphertext, c5=bit ke-5 ciphertext, c6=bit ke-6 ciphertext, c7=bit ke-7 ciphertext, c8=bit ke-8 ciphertext

Manual rumus feedforward dan backpropagation dari arsitektur Neural Network 1 Hidden Layer 1 Neuron yang digunakan dalam penelitian dapat dilihat seperti berikut

Feedforward

1. Menghitung y_out

[y_in]= [(bh + (xp1*wp1) + (xp2*wp2) + (xp3*wp3) + (xp4*wp4) + (xp5*wp5) + (xp6*wp6) + (xp7*wp7) + (xp8*wp8) + (xk1*wk1) + (xk2*wk2) + (xk3*wk3) + (xk4*wk4) + (xk5*wk5) + (xk6*wk6) + (xk7*wk7) + (xk8*wk8) + (xk9*wk9) + (xk10*wk10)]

$$[y\_out]=\left[\frac{1}{(1+e^{-1*y\_in})}\right]$$

2. Menghitung c_out

$$\begin{bmatrix} c1\_in \\ c2\_in \\ c3\_in \\ c4\_in \\ c5\_in \\ c6\_in \\ c7\_in \\ c8\_in \end{bmatrix} = \begin{bmatrix} bc1 + (y\_out * wc1) \\ bc2 + (y\_out * wc2) \\ bc3 + (y\_out * wc3) \\ bc4 + (y\_out * wc4) \\ bc5 + (y\_out * wc5) \\ bc6 + (y\_out * wc6) \\ bc7 + (y\_out * wc7) \\ bc8 + (y\_out * wc8) \end{bmatrix}$$

$$\begin{bmatrix} c1\_out \\ c2\_out \\ c3\_out \\ c4\_out \\ c5\_out \\ c6\_out \\ c7\_out \\ c8\_out \end{bmatrix} = \begin{bmatrix} \frac{1}{(1+e^{-1*c1\_in})} \\ \frac{1}{(1+e^{-1*c2\_in})} \\ \frac{1}{(1+e^{-1*c3\_in})} \\ \frac{1}{(1+e^{-1*c4\_in})} \\ \frac{1}{(1+e^{-1*c5\_in})} \\ \frac{1}{(1+e^{-1*c6\_in})} \\ \frac{1}{(1+e^{-1*c7\_in})} \\ \frac{1}{(1+e^{-1*c8\_in})} \end{bmatrix}$$

Backpropagation

1. Menghitung koreksi bobot dan bias

Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 2, April 2026: halaman 102-111
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v6i2.2239

$$\begin{bmatrix} error\_c1 \\ error\_c2 \\ error\_c3 \\ error\_c4 \\ error\_c5 \\ error\_c6 \\ error\_c7 \\ error\_c8 \end{bmatrix} = \begin{bmatrix} (target\_c1 - c1\_out) * (1 - c1\_out) * c1\_out \\ (target\_c2 - c2\_out) * (1 - c2\_out) * c2\_out \\ (target\_c3 - c3\_out) * (1 - c3\_out) * c3\_out \\ (target\_c4 - c4\_out) * (1 - c4\_out) * c4\_out \\ (target\_c5 - c5\_out) * (1 - c5\_out) * c5\_out \\ (target\_c6 - c6\_out) * (1 - c6\_out) * c6\_out \\ (target\_c7 - c7\_out) * (1 - c7\_out) * c7\_out \\ (target\_c8 - c8\_out) * (1 - c8\_out) * c8\_out \end{bmatrix}$$

[$error\_y$]=[y_out * (1-y_out) * ((error_c1*wc1) + (error_c2*wc2) + (error_c3*wc3) + (error_c4*wc4) + (error_c5*wc5) + (error_c6*wc6) + (error_c7*wc7) + (error_c8*wc8))]

$$\begin{bmatrix} \Delta wp1 \\ \Delta wp2 \\ \Delta wp3 \\ \Delta wp4 \\ \Delta wp5 \\ \Delta wp6 \\ \Delta wp7 \\ \Delta wp8 \\ \Delta wk1 \\ \Delta wk2 \\ \Delta wk3 \\ \Delta wk4 \\ \Delta wk5 \\ \Delta wk6 \\ \Delta wk7 \\ \Delta wk8 \\ \Delta wk9 \\ \Delta wk10 \\ \Delta bh \\ \Delta wc1 \\ \Delta wc2 \\ \Delta wc3 \\ \Delta wc4 \\ \Delta wc5 \\ \Delta wc6 \\ \Delta wc7 \\ \Delta wc8 \\ \Delta bc1 \\ \Delta bc2 \\ \Delta bc3 \\ \Delta bc4 \\ \Delta bc5 \\ \Delta bc6 \\ \Delta bc7 \\ \Delta bc8 \end{bmatrix} = \begin{bmatrix} Learning\ Rate * error\_y * xp1 \\ Learning\ Rate * error\_y * xp2 \\ Learning\ Rate * error\_y * xp3 \\ Learning\ Rate * error\_y * xp4 \\ Learning\ Rate * error\_y * xp5 \\ Learning\ Rate * error\_y * xp6 \\ Learning\ Rate * error\_y * xp7 \\ Learning\ Rate * error\_y * xp8 \\ Learning\ Rate * error\_y * xk1 \\ Learning\ Rate * error\_y * xk2 \\ Learning\ Rate * error\_y * xk3 \\ Learning\ Rate * error\_y * xk4 \\ Learning\ Rate * error\_y * xk5 \\ Learning\ Rate * error\_y * xk6 \\ Learning\ Rate * error\_y * xk7 \\ Learning\ Rate * error\_y * xk8 \\ Learning\ Rate * error\_y * xk9 \\ Learning\ Rate * error\_y * xk10 \\ Learning\ Rate * error\_y \\ Learning\ Rate * error\_c1 * y\_out \\ Learning\ Rate * error\_c2 * y\_out \\ Learning\ Rate * error\_c3 * y\_out \\ Learning\ Rate * error\_c4 * y\_out \\ Learning\ Rate * error\_c5 * y\_out \\ Learning\ Rate * error\_c6 * y\_out \\ Learning\ Rate * error\_c7 * y\_out \\ Learning\ Rate * error\_c8 * y\_out \\ Learning\ Rate * error\_c1 \\ Learning\ Rate * error\_c2 \\ Learning\ Rate * error\_c3 \\ Learning\ Rate * error\_c4 \\ Learning\ Rate * error\_c5 \\ Learning\ Rate * error\_c6 \\ Learning\ Rate * error\_c7 \\ Learning\ Rate * error\_c8 \end{bmatrix}$$

2. Mengupdate bobot dan bias

Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 2, April 2026: halaman 102-111
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v6i2.2239

$$\begin{bmatrix} wp1\_baru \\ wp2\_baru \\ wp3\_baru \\ wp4\_baru \\ wp5\_baru \\ wp6\_baru \\ wp7\_baru \\ wp8\_baru \\ wk1\_baru \\ wk2\_baru \\ wk3\_baru \\ wk4\_baru \\ wk5\_baru \\ wk6\_baru \\ wk7\_baru \\ wk8\_baru \\ wk9\_baru \\ wk10\_baru \\ bh\_baru \\ wc1\_baru \\ wc2\_baru \\ wc3\_baru \\ wc4\_baru \\ wc5\_baru \\ wc6\_baru \\ wc7\_baru \\ wc8\_baru \\ bc1\_baru \\ bc2\_baru \\ bc3\_baru \\ bc4\_baru \\ bc5\_baru \\ bc6\_baru \\ bc7\_baru \\ bc8\_baru \end{bmatrix} = \begin{bmatrix} wp1\_lama + \Delta wp1 \\ wp2\_lama + \Delta wp2 \\ wp3\_lama + \Delta wp3 \\ wp4\_lama + \Delta wp4 \\ wp5\_lama + \Delta wp5 \\ wp6\_lama + \Delta wp6 \\ wp7\_lama + \Delta wp7 \\ wp8\_lama + \Delta wp8 \\ wk1\_lama + \Delta wk1 \\ wk2\_lama + \Delta wk2 \\ wk3\_lama + \Delta wk3 \\ wk4\_lama + \Delta wk4 \\ wk5\_lama + \Delta wk5 \\ wk6\_lama + \Delta wk6 \\ wk7\_lama + \Delta wk7 \\ wk8\_lama + \Delta wk8 \\ wk9\_lama + \Delta wk9 \\ wk10\_lama + \Delta wk10 \\ bh\_lama + \Delta bh \\ wc1\_lama + \Delta wc1 \\ wc2\_lama + \Delta wc2 \\ wc3\_lama + \Delta wc3 \\ wc4\_lama + \Delta wc4 \\ wc5\_lama + \Delta wc5 \\ wc6\_lama + \Delta wc6 \\ wc7\_lama + \Delta wc7 \\ wc8\_lama + \Delta wc8 \\ bc1\_lama + \Delta bc1 \\ bc2\_lama + \Delta bc2 \\ bc3\_lama + \Delta bc3 \\ bc4\_lama + \Delta bc4 \\ bc5\_lama + \Delta bc5 \\ bc6\_lama + \Delta bc6 \\ bc7\_lama + \Delta bc7 \\ bc8\_lama + \Delta bc8 \end{bmatrix}$$

Dimisalkan terdapat inputan berikut:
Learning Rate = 0.1
Jumlah Maksimal Epoch = 1
Fungsi Aktivasi = Sigmoid

Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 2, April 2026: halaman 102-111
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v6i2.2239

Tabel 1 Contoh Data Learning

NOMOR	X1	X2	TARGET
DATA1	00000000	00000000	00000110
DATA2	00000001	00000000	11010011
DATA3	00000010	00000000	11001101

Tabel 2 Contoh Data Testing

NOMOR	X1	X2	TARGET
DATA4	00000011	00000000	10011101

Dari DATA1 Data Learning didapatkan xp1=0, xp2=0, xp3=0, xp4=0, xp5=0, xp6=0, xp7=0, xp8=0, xk1=0, xk2=0, xk3=0, xk4=0, xk5=0, xk6=0, xk7=0, xk8=0, xk9=0, xk10=0, target_c1=0, target_c2=0, target_c3=0, target_c4=0, target_c5=0, target_c6=1, target_c7=1, dan target_c8=0. Dari DATA2 Data Learning didapatkan xp1=0, xp2=0, xp3=0, xp4=0, xp5=0, xp6=0, xp7=0, xp8=1, xk1=0, xk2=0, xk3=0, xk4=0, xk5=0, xk6=0, xk7=0, xk8=0, xk9=0, xk10=0, target_c1=1, target_c2=1, target_c3=0, target_c4=1, target_c5=0, target_c6=0, target_c7=1, dan target_c8=1. Dari DATA3 Data Learning didapatkan xp1=0, xp2=0, xp3=0, xp4=0, xp5=0, xp6=0, xp7=1, xp8=0, xk1=0, xk2=0, xk3=0, xk4=0, xk5=0, xk6=0, xk7=0, xk8=0, xk9=0, xk10=0, target_c1=1, target_c2=1, target_c3=0, target_c4=0, target_c5=1, target_c6=1, target_c7=0, dan target_c8=1. Dari DATA4 Data Testing didapatkan xp1=0, xp2=0, xp3=0, xp4=0, xp5=0, xp6=0, xp7=1, xp8=1, xk1=0, xk2=0, xk3=0, xk4=0, xk5=0, xk6=0, xk7=0, xk8=0, xk9=0, xk10=0, target_c1=1, target_c2=0, target_c3=0, target_c4=1, target_c5=1, target_c6=1, target_c7=0, dan target_c8=1

Selanjutnya dilaksanakan proses training sehingga menghasilkan bobot dan bias

Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 2, April 2026: halaman 102-111
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v6i2.2239

$$\begin{bmatrix} wp1\_baru \\ wp2\_baru \\ wp3\_baru \\ wp4\_baru \\ wp5\_baru \\ wp6\_baru \\ wp7\_baru \\ wp8\_baru \\ wk1\_baru \\ wk2\_baru \\ wk3\_baru \\ wk4\_baru \\ wk5\_baru \\ wk6\_baru \\ wk7\_baru \\ wk8\_baru \\ wk9\_baru \\ wk10\_baru \\ bh\_baru \\ wc1\_baru \\ wc2\_baru \\ wc3\_baru \\ wc4\_baru \\ wc5\_baru \\ wc6\_baru \\ wc7\_baru \\ wc8\_baru \\ bc1\_baru \\ bc2\_baru \\ bc3\_baru \\ bc4\_baru \\ bc5\_baru \\ bc6\_baru \\ bc7\_baru \\ bc8\_baru \end{bmatrix} = \begin{bmatrix} 0.000000001 \\ 0.000000005 \\ 0.000000010 \\ 0.000000015 \\ 0.000000020 \\ 0.000000025 \\ 0{,}00011415368164437000000 \\ -0.0000402450531409603 \\ 0.000000040 \\ 0.000000045 \\ 0.000000050 \\ 0.000000055 \\ 0.000000060 \\ 0.000000065 \\ 0.000000070 \\ 0.000000075 \\ 0.000000080 \\ 0.000000085 \\ 0{,}00007384240975333670000 \\ -0{,}00620172025392133000000 \\ -0{,}00620171527705291000000 \\ -0{,}01860181750882420000000 \\ -0{,}00620170532331610000000 \\ -0{,}01860180755603340000000 \\ 0{,}00620192430552611000000 \\ 0{,}01860203647021850000000 \\ -0{,}00620168541584243000000 \\ -0{,}01240387230629920000000 \\ -0{,}01240387235256270000000 \\ -0{,}03720408240367280000000 \\ -0{,}01240387244508970000000 \\ -0{,}03720408249809210000000 \\ 0{,}01240387040949610000000 \\ 0{,}03720408032644750000000 \\ -0{,}01240387263014360000000 \end{bmatrix}$$

Selanjutnya dilaksanakan proses testing dengan menggunakan bobot dan bias dari hasil proses training sehingga menghasilkan c_out sebagai berikut

$$\begin{bmatrix} c1\_out \\ c2\_out \\ c3\_out \\ c4\_out \\ c5\_out \\ c6\_out \\ c7\_out \\ c8\_out \end{bmatrix} = \begin{bmatrix} 0{,}49612383727565900000000 \\ 0{,}49612383788621100000000 \\ 0{,}48837567542716000000000 \\ 0{,}49612383910731500000000 \\ 0{,}48837567664708600000000 \\ 0{,}50387618775697100000000 \\ 0{,}51162435141121600000000 \\ 0{,}49612384154952200000000 \end{bmatrix}$$

Dari hasil c_out tersebut dapat dilihat bahwa seharusnya c1_out=1, c2_out=0, c3_out=0, c4_out=1, c5_out=1, c6_out=1, c7_out=0, dan c8_out=1. tetapi hasil manual perhitungan neural

Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 2, April 2026: halaman 102-111
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v6i2.2239

networknya c1_out = 0.496123837275659 (pembulatan c1_out = 0), c2_out = 0,496123837886211 (pembulatan c2_out = 0), c3_out = 0,48837567542716 (pembulatan c3_out = 0), c4_out = 0,496123839107315 (pembulatan c4_out = 0), c5_out = 0,488375676647086 (pembulatan c5_out = 0), c6_out = 0,503876187756971 (pembulatan c6_out = 1), c7_out = 0,511624351411216 (pembulatan c7_out = 1), c8_out = 0,496123841549522 (pembulatan c8_out = 0)

4 Hasil dan Pembahasan (or Results and Analysis)

Berikut adalah hasil pengujian akurasi neural network backpropagation multilapis yang digunakan terhadap kriptografi S-DES. Adapun neural network backpropagationnya menggunakan metode He Uniform pada inisialisasi bobot, tidak menggunakan metode Normalisasi (juga tidak menggunakan metode deNormalisasi), menggunakan Sigmoid pada fungsi aktivasi, dan menggunakan konfigurasi 3 lapis yang mana 18 neuron di lapis input, 1 neuron di lapis hidden, 8 neuron di lapis output

Tabel 3 Hasil Percobaan

PERCOBAAN KE	LEARNING RATE	EPOCH	AKURASI
1	0.1	1000	0.439453125%
2	0.1	5000	0.439453125%
3	0.1	10000	0.439453125%

5 Kesimpulan (or Conclusion)

Berdasarkan penelitian yang telah dilaksanakan dapat ditarik kesimpulan berikut.

1. Telah dilaksanakan kriptanalisis berbasis neural network feedforward backpropagation multi lapis dengan konfigurasi 3 lapis yang mana 18 neuron di lapis input, 1 neuron di lapis hidden, 8 neuron yang dilatih dengan menggunakan seluruh kemungkinan kombinasi plaintext, kunci, dan ciphertext (ada jumlah total 65.536 kombinasi) dan yang kemudian diujikan dalam learning rate 0.1 dan dalam jumlah epoch 1000, 5000, dan 10.000
2. Dari pengujian yang telah dilaksanakan didapatkan bahwa pengujian dengan jumlah epoch 1000, 5000, dan 10.000 sama-sama menunjukkan jumlah akurasi yang sama yaitu 0.439453125%
3. Untuk penelitian selanjutnya menggunakan neural network feedforward backpropagation multi lapis dengan konfigurasi lainnya yang belum diujikan dalam penelitian ini.

Referensi (Reference)

[1] K. M. Alallayah, W. F. A. El-Wahed, M. Amin, and A. H. Alhamami, "Attack of Against Simplified Data Encryption Standard Cipher System Using Neural Networks," *J. Comput. Sci.*, vol. 6, no. 1, pp. 29–35, 2010.

[2] M. W. Kurniaga, A. Yulianto, and T. Setya Aji Kumoro, "Kriptanalisis DES menggunakan Jaringan Syaraf Tiruan," *Fidel. J. Tek. Elektro*, vol. 4, no. 2, pp. 40–44, 2022, doi: 10.52005/fidelity.v4i2.89.

[3] F. Paradise and S. Indarjani, "Pemulihan Kunci pada Simplified Data Encryption Standard (S-DES) Melalui Serangan Aljabar: Studi Kasus," *Info Kripto*, vol. 19, no. 1, pp. 13–27, 2025, doi: 10.56706/ik.v19i1.114.

[4] Y. Anzari, E. Sany, L. Simorangkir, M. Subhan, A. Rachmawati, and Suroto, "EVALUASI KINERJA KOMPUTASI DAN KRIPTANALISIS BRUTE FORCE PADA ALGORITMA CAESAR CIPHER BERBASIS PYTHON," *Djtechno J. Teknol. Inf.*, vol. 6, no. 3, pp. 1141–1154, 2025, doi: 10.46576/djtechno.

[5] U. J. Ningsih, S. Salsabila, I. Hutapea, D. Santika, and I. Gunawan, "Pendekripsian Caesar Chiper Dengan Menggunakan Teknik-Teknik Kriptanalisis," *J. Ilmu Komput. dan Multimed.*,

P-ISSN: 2746-5985
e-ISSN: 2797-0930

DOI: https://doi.org/10.52362/jmijayakarta.v6i2.2239

vol. 1, no. 1, pp. 11–15, 2024, doi: 10.46510/ilkomedia.v1i1.10.

[6] R. Alfiansyah, Fitriyani, and N. Ikhsan, "Kriptanalisis Md5 Dengan Menggunakan Pendekatan Komputasi," *e-Proceeding Eng.*, vol. 2, no. 2, pp. 6802–6806, 2015.

[7] F. A. Pramudya and Suhardi, "Analisis Keamanan Komparatif Caesar Cipher dan DES dalam Konteks Kebutuhan Keamanan Modern," *Cosm. J. Tek.*, vol. 2, no. 3, pp. 96–105, 2025.

[8] B. Akiwate and V. Desai, "Artificial Neural Networks for Cryptanalysis of," *Int. J. Innov. Eng. Technol.*, vol. 2, no. 4, pp. 11–17, 2013.

[9] F. Paradise and S. Indarjani, "ALGEBRAIC ATTACK PADA SIMPLIFIED DATA ENCRYPTION STANDARD (S-DES)," in *Seminar Nasional Matematika UI*, 2017, pp. 726–735.

[10] S. Andonov, J. Dobreva, L. Lumburovska, S. Pavlov, and A. Popovska-mitrovikj, "Application of Machine Learning in DES Cryptanalysis," *ICT-Innovations 2020*, pp. 124–134, 2020.

[11] S. Fan and Y. Zhao, "Analysis of des Plaintext Recovery Based on BP Neural Network," *Secur. Commun. Networks*, vol. 2019, doi: 10.1155/2019/9580862.

[12] Y. Xiao, Q. Hao, and D. D. Yao, "Neural Cryptanalysis: Metrics, Methodology, and Applications in CPS Ciphers," *2019 IEEE Conf. Dependable Secur. Comput. DSC 2019 - Proc.*, 2019, doi: 10.1109/DSC47296.2019.8937659.

[13] Y. Fatma, M. A. Remli, M. S. Mohamad, and J. Al Amien, "Deep learning-based cryptanalysis in recovering the secret key and plaintext on lightweight cryptography," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 38, no. 2, pp. 1115–1123, 2025, doi: 10.11591/ijeecs.v38.i2.pp1115-1123.

[14] Y. R. Nasution, H. Santoso, and S. W. Amalia, "Penerapan Algoritma Vernam dalam Mengamankan Dokumen PDF," *JIRE (Jurnal Inform. Rekayasa Elektron.*, vol. 6, no. 1, pp. 37–46, 2023.

[15] B. Arya Bagaskara, M. Idhom, and H. Endah Wahanani, "Pengujian Website Dinas Sosial Surabaya Menggunakan Metode Penetration Testing Dan Owasp Top 10," *J. Inform. Rekayasa Elektron.*, vol. 8, no. 1, pp. 40–50, 2025, [Online]. Available: http://e-journal.stmiklombok.ac.id/index.php/jireISSN.2620-6900.