JTIM : Jurnal Teknologi Informasi dan Multimedia
Vol. 3 No. 1, Mei 2021, hlm. 8-13

p-ISSN : 2715-2529
e-ISSN : 2684-9151

Implementasi Kombinasi *Caesar Cipher* dan *Hill Cipher* Menggunakan Modifikasi Sandi Morse Untuk Pengamanan Pesan Berbasis Teks

(*Implementation of the Combination of Caesar Cipherand Hill Cipher Using Modified Morse Code forText-Based Message Security***)**

Muhammad Azmi[1]*, Zulkarnaen[2]

[1]Sistem Informasi, STMIK Syaikh Zainuddin NW Anjani
[2]Teknik Informatika, STMIK Syaikh Zainuddin NW Anjani
E-mail:muhammad4zmi@gmail.com, zolcakep@gmail.com

KEYWORDS:
Message Security, Combination of Caesar Cipher and Hill Cipher, Morse Code, Steganography

ABSTRACT
The security and confidentiality of a message or document sent to other people must be guaranteed its confidentiality and security, so that the message or document is not misused by parties who do not have an interest in the message. Security and confidentiality of messages or documents can be kept confidential and secure by using cryptography. data security and confidentiality issues are very important from an information. Because of the importance of this information, the person concerned will question whether the authenticity of the information is still maintained or whether the information has been hijacked. So in the process of securing data and information with cryptography, of course it requires a qualified algorithm to maintain the confidentiality of the information, so that the purpose of this research is how to maintain the confidentiality of information by converting information into codes known only to the sender and receiver by using cryptographic techniques and steganography. Then the process of securing the data or information the researcher uses a combination of Caesar Chiper and Hill Chiper which is modified into Morse code then the resulting CipherText results will be saved into a JPEG file using the LSB (Least Significant Bit) Steganography method. The process of storing messages or ciphertext into image files will make it difficult for irresponsible people or cryptoanalysts to solve messages sent in the form of images.

KATA KUNCI:
Keamanan Pesan, Kombinasi Caesar Cipher dan Hill Cipher, Sandi Morse, Steganografi

ABSTRAK
Keamanan dan kerahasian sebuah pesan atau dokumen yang dikirim kepada orang lain haruslah dijamin kerahasiaan dan keamanannya, sehingga pesan atau dokumen tersebut tidak disalah gunakan oleh pihak-pihak yang tidak memilki kepentingan terhadap pesan tesebut. Keamanan dan kerahasiaan pesan atau dokumen dapat dijaga kerahasiaan dan keamanannya dengan menggunakan Kriptografi. masalah keamanan dan kerahasiaan data merupakan sesuatu yang sangat penting dari sebuah informasi. Karena pentingnya sebuah informasi tersebut maka terkait akan mempertanyakan apakah informasi tersebut masih terjaga keasliannya ataukah informasi tersebut sudah terbajak. Maka dalam proses pengamanan data dan informasi dengan kriptografi tentu membutuhkan algoritma yang mumpuni untuk menjaga kerahasiaan informasi tersebut, Sehingga tujuan dari penelitian ini adalah bagaimana menjaga kerahasiaan sebuah informasi dengan mengubah informasi menjadi kode- kode yang hanya diketahui oleh pengirim dan penerima dengan menggunakan teknik kriptografi dan steganografi. Kemudian proses pengamanan data atau informasi tersebut peneliti menggunakan kombinasi antara Caesar Chiper dan Hill Chiper yang di modifikasi menjadi sandi morse kemudian hasil CipherText yang dihasilkan akan disimpan kedalam File JPEG dengan metode Steganografi LSB (Least Significant Bit). Proses penyimpanan pesan atau ciphertext kedalam file gambar akan menyulitkan orang-orang yang tidak bertanggung jawab atau criptoanalys untuk memecahkan pesan yang dikirim dalam bentuk gambar.

*Penulis Korespondensi (Muhammad Azmi)
Email : *muhammad4zmi@gmail.com*

I. PENDAHULUAN

Kriptografi merupakan disiplin ilmu yang di dalamnya mempelajari keamanan sebuah pesan dan kerahasiaannya. Di dalam kriptografi sendiri ada 2 (dua) proses utama yaitu proses enkripsi dan proses deskripsi. Enkripsi sendiri merupakan proses penyandian atau penyandian pesan asli yang disebut dengan *plaintext ke ciphertext*, sedangkan deskripsi merupakan kebalikan dari enkripsi[1].

Kriptografi muncul yang sebabkan karena adanya proses komunikasi yang mengalami perkembangan, di mana dalam proses komunikasi kita bisa dengan mudah berkomunikasi dan melakukan pertukaran data atau informasi dengan sangat mudah serta tidak berpengaruh terhadap jarak. Oleh sebab itu seiring dengan perkembangan pola atau model komunikasi tersebut maka tuntutan akan keamanan sebuah data atau informasi semakin meningkat, di mana setiap individu, organisasi, pemerintah atau perusahaan harus menjaga kerahasiaan data atau informasi sehingga data atau informasi tersebut tidak diketahui oleh orang yang tidak bertanggung jawab. Sebab itulah muncul cabang atau disiplin ilmu baru yang mempelajari cara- cara pengamanan terhadap data dan informasi yang dikenal dengan nama disiplin ilmu kriptografi[2].

Kriptografi berasal dari bahasa Yunani yaitu *kryptos* yang berarti tersembunyi dan graphein yang bermakna tulisan. Kriptografi adalah ilmu menulis pesan rahasia yang mana bertujuan untuk menyembunyikan makna sesungguhnya dari pesan tersebut. Tetapi seiring perkembangan zaman hingga saat ini pengertian kriptografi berkembang menjadi ilmu tentang teknik matematis yang digunakan untuk menyelesaikan persoalan keamanan berupa privasi dan otentikasi[3].

Dalam proses pengamanan data dan informasi dengan kriptografi tentu membutuhkan algoritma yang mumpuni, *caesar cipher* dan *hill cipher* merupakan 2 (dua) algoritma klasik yang sudah banyak digunakan. *Caesar cipher* merupakan algoritma yang sudah ada sejak mulai zaman Kerajaan Romawi pada masa pemerintahan Julius Caesar tahun 50 SM, di mana Caesar mengkodekan informasi dengan melakukan perubahan setiap huruf dalam informasi menjadi tiga huruf setelah informasi asli dalam urutan alpabet. Algoritma yang dipakai dalam *caesar cipher* sangat sederhana dan terlalu mudah untuk dipecahkan[4].

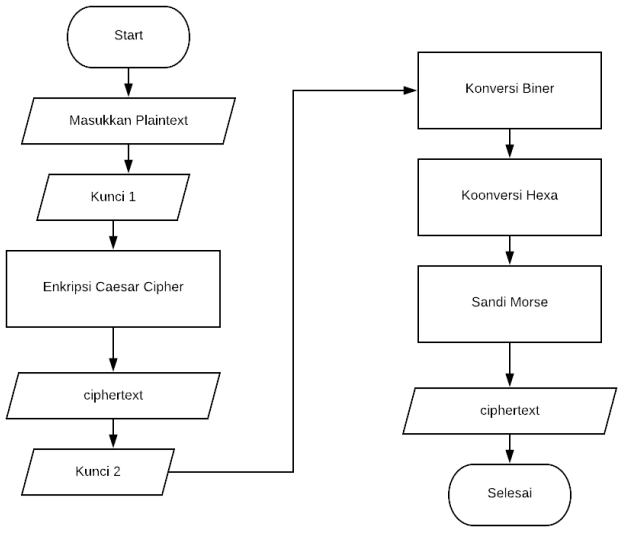
Pada saat ini masalah keamanan dan kerahasiaan data merupakan sesuatu yang sangat penting dari sebuah informasi. Karena pentingnya sebuah informasi tersebut maka terkait akan mempertanyakan apakah informasi tersebut masih terjaga keasliannya ataukah informasi tersebut sudah terbajak. Karena sebuah informasi akan menjadi tidak berguna jika sudah diakses dan dibajak oleh pihak yang tidak memiliki kepentingan terhadap informasi tersebut.

Sehingga tujuan dari penelitian ini adalah bagaimana menjaga kerahasiaan sebuah informasi dengan mengubah informasi menjadi kode- kode yang hanya diketahui oleh pengirim dan penerima dengan menggunakan teknik kriptografi dan steganografi.

Berdasarkan uraian diatas penulis akan mencoba melakukan kombinasi terhadap algoritma *caesar cipher dengan hill cipher* yang akan dimodifikasi menjadi bentuk *hexadecimal* dan kemudian hasil dari *ciphertext* tersebut akan di ubah dalam sandi Morse yang akan disisipkan kedalam gambar dengan teknik Steganografi.

II. METODOLOGI

Penelitian ini dilakukan dengan beberapa tahap sesuai dengan yang dijelaskan pada gambar 1 dibawah ini :



Gbr. 1 Proses Enkripsi Text dengan Modifikasi Morse

Berdasarkan Gbr.1 diagram alur diatas, maka terdapat beberapa tahap proses enkripsi pesan dengan kombinasi *Caesar Cipher* dan *Hill Cipher*. Berikut tahapannya :

A. Proses Enkripsi dengan Caesar Cipher

Langkah- langkah proses enkripsi dengan *caesar cipher* yang akan dimodifikasi dengan sandi morse sebagai berikut:

a. Dalam proses enkripsi pertama- tama yang akan dilakukan adalah melakukan proses enkripsi caesar cipher terlebih dahulu.
b. Pesan Teks diubah dalam menggunakan algoritma *caisar chiper*, dimana kunci yang digunakan menggunakan angka.
   Contoh : plainteks = **"SEGERA WISUDA".**
   Key = 4.

Susunan Semula

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Key a=4, menjadi **"SEGERA WISUDA"**

E	F	G	H	I	J	K	L	M	N	O	P	Q
4	5	6	7	8	9	10	11	12	13	14	15	16
R	S	T	U	V	W	X	Y	Z	A	B	C	D
17	18	19	20	21	22	23	24	25	0	1	2	3

c. Maka, berdasarkan ketentuan kunci di atas *ciphertex*t hasil dari enkripsi caesar chiper seperti berikut:

"WIKIVEAMWYHE"

B. Proses Enkripsi dengan Hill Cipher

Langkah- langkah proses enkripsi dengan *Hill cipher* yang akan dimodifikasi dengan sandi morse sebagai berikut:

a. Setelah mendapatkan *ciphertext* hasil enkripsi dari *caesar cipher*, selanjutnya akan dilakukan enkripsi kembali dengan *hill cipher* menggunakan indeks masing-masing karakter ke dalam numerik seperti A=0 sampai Z=25 dan menggunakan kunci matriks ordo 2x2.

Misalnya menggunakan kunci =$\begin{bmatrix}9 & 3\\7 & 6\end{bmatrix}$

TABEL I
INDEKS KARAKTER

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

b. Mengubah karakter menjadi nilai numerik berdasarkan tabel indeks karakter:

$$\begin{matrix}W\\I\end{matrix} = \begin{bmatrix}22\\8\end{bmatrix} \quad \begin{matrix}V\\E\end{matrix} = \begin{bmatrix}21\\4\end{bmatrix} \quad \begin{matrix}W\\Y\end{matrix} = \begin{bmatrix}22\\24\end{bmatrix}$$
$$\begin{matrix}I\\K\end{matrix} = \begin{bmatrix}10\\8\end{bmatrix} \quad \begin{matrix}A\\M\end{matrix} = \begin{bmatrix}0\\12\end{bmatrix} \quad \begin{matrix}H\\E\end{matrix} = \begin{bmatrix}7\\4\end{bmatrix}$$

c. Pengerjaan selanjutnya dengan menggunakan rumus hill cipher, C = K.P mod 26 maka,

$$\begin{bmatrix}9 & 3\\7 & 6\end{bmatrix}\begin{bmatrix}22\\8\end{bmatrix} = \begin{bmatrix}9.22 + & 3.8\\7.22 & 6.8\end{bmatrix} = \begin{bmatrix}222\\202\end{bmatrix} mod26 = \begin{bmatrix}O\\U\end{bmatrix}$$
$$\begin{bmatrix}9 & 3\\7 & 6\end{bmatrix}\begin{bmatrix}10\\8\end{bmatrix} = \begin{bmatrix}9.10 & 3.8\\7.10 + & 6.8\end{bmatrix} = \begin{bmatrix}114\\118\end{bmatrix} mod26 = \begin{bmatrix}K\\O\end{bmatrix}$$
$$\begin{bmatrix}9 & 3\\7 & 6\end{bmatrix}\begin{bmatrix}21\\4\end{bmatrix} = \begin{bmatrix}9.21 & 3.4\\7.21 + & 6.4\end{bmatrix} = \begin{bmatrix}201\\171\end{bmatrix} mod26 = \begin{bmatrix}T\\P\end{bmatrix}$$
$$\begin{bmatrix}9 & 3\\7 & 6\end{bmatrix}\begin{bmatrix}0\\12\end{bmatrix} = \begin{bmatrix}9.0 & 3.12\\7.0 + & 6.12\end{bmatrix} = \begin{bmatrix}36\\72\end{bmatrix} mod26 = \begin{bmatrix}K\\U\end{bmatrix}$$
$$\begin{bmatrix}9 & 3\\7 & 6\end{bmatrix}\begin{bmatrix}22\\24\end{bmatrix} = \begin{bmatrix}9.22 & 3.24\\7.22 + & 6.24\end{bmatrix} = \begin{bmatrix}270\\298\end{bmatrix} mod26 = \begin{bmatrix}K\\M\end{bmatrix}$$
$$\begin{bmatrix}9 & 3\\7 & 6\end{bmatrix}\begin{bmatrix}7\\4\end{bmatrix} = \begin{bmatrix}9.7 & 3.4\\7.7 + & 6.4\end{bmatrix} = \begin{bmatrix}75\\73\end{bmatrix} mod26 = \begin{bmatrix}X\\V\end{bmatrix}$$

Berdasarkan hasil matriks tersebut maka didapatkan *ciphertext* sebagai berikut :**"OUKOTPKUKMXV"**

C. Konversi Ciphertext kedalam Bilangan Biner, Hexadecimal dan Modifikasi Sandi Morse

Sandi morse merupakan sistem representatif huruf, angka dan tanda baca dengan menggunakan sinyal kode. *Samuel FinleyBreese Morse* adalah penemu sandi Morse yang berasal dari Amerika Serikat[9].

a) Pada tahap berikutnya akan dilakukan konversi ke dalam bilangan biner berdasarkan hasil ciphertext dari kombinasi *Caesar Cipher* dan *Hill Cipher* :

O= 0110111	K= 01001011
U= 0101011	U= 0101011
K= 01001011	K= 01001011
O= 0110111	M= 01001101
T= 01010100	X= 01011000
P= 01010000	V= 01010110

b) Tahap berikutnya adalah mengubah hasil biner menjadi *hexadecimal*:

0110111 = 37	01001011 = 4B
0101011 = 2B	0101011 = 2B
01001011 = 4B	01001011 = 4B
0110111 = 37	01001101 = 4D
01010100 = 54	01011000 = 58
01010000 = 50	01010110 = 56

Tahap berikutnya adalah mengubah hasil konversi hexadecimal menjadi sandi morse dengan membalik hasil konversinya di mana huruf akhir menjadi awal.

Plaintext : **372B4B3754504B2B4B4D5856**

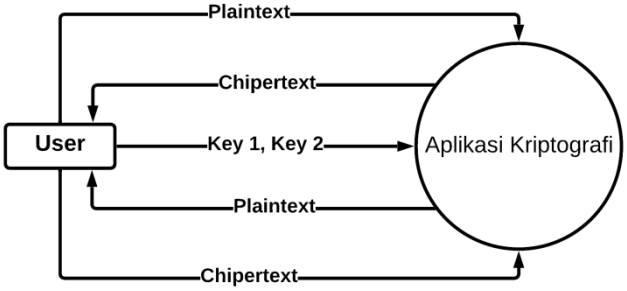
Ciphertext dalam sandi morse : "**….-,…..,---..,…..,-..,….-,-…,….-,-…,..---,-…,….-,-----,…..,….-,…..,--…,…--,-…,….-,..---,--…,…--**"

III. HASIL DAN PEMBAHASAN

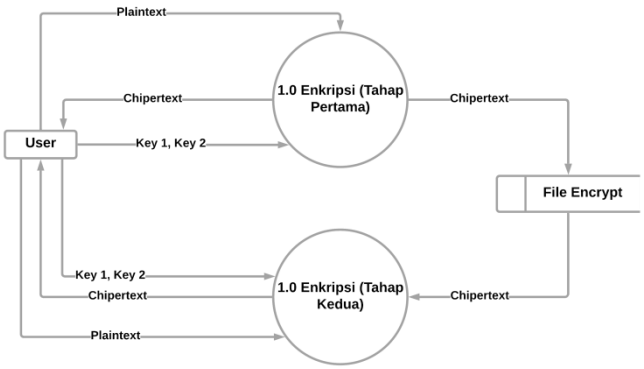
A. Perancangan Sistem

Perancangan sistem merupakan tahapan yang dilakukan sebelum melakukan pengkodean sistem. Perancangan sistem yang dibuat dalam penelitian ini berupa *Data Flow Diagram (DFD). Data Flow Diagram (DFD)* adalah diagram yang digunakan untuk menggambarkan aliran sistem data dalam suatu proses atau sistem. DFD sendiri juga memberikan informasi mengenai input, proses dan output pada sistem[10].

Berikut rancangan *Data Flow Diagram* Aplikasi Kriptografi, seperti pada Gbr 2.



Gbr. 2 DFD Konteks (Level 0)

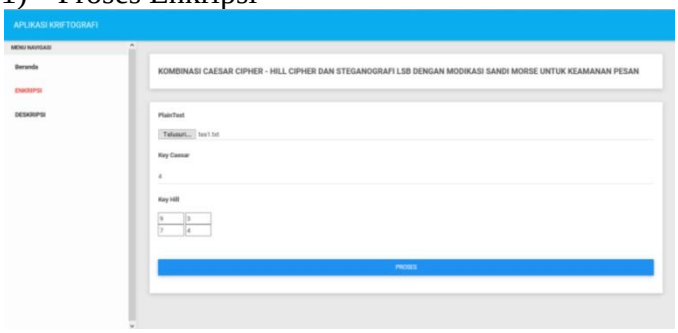


Gbr. 3 DFD Level 1

B. Implementasi Sistem

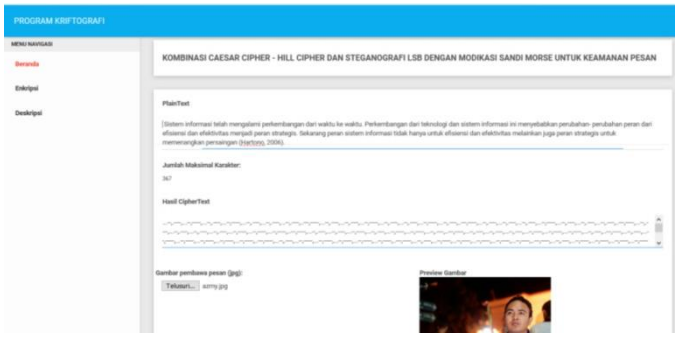
Implementasi sistem merupakan tahapan menterjemahkan rancangan (DFD) kedalam aplikasi (perangkat lunak). Hal ini bertujuan untuk pada saat pengkodean tidak melenceng dari hasil analisis.

1) Proses Enkripsi



Gbr.4 Proses Enkripsi

Dalam proses yang ditunjukkan Gbr. 4 tersebut sebuah dokumen *Plaintext* dengan ekstensi . TXT dimasukkan kedalam aplikasi, kemudian memasukkan *Key 1 Caesar Cipher* dan *Key 2 Hill Cipher* dalam bentuk Matriks ordo 2x2.



Gbr. 5 Hasil Enkripsi dalam bentuk Sandi Morse

Setelah dilakukan enkripsi seperti pada Gbr.5 maka aplikasi akan mengubah *Plaintext* yang telah

dimasukkan menjadi sandi Morse, kemudian hasil *CipherText* yang dihasilkan akan disimpan kedalam File JPEG dengan metode Steganografi LSB (*Least Significant Bit***)**.

C. Pengujian Sistem

Tahapan pengujian pada proses pembuatan aplikasi bertujuan untuk memastikan dan menguji bahwa semua fungsi dan proses berjalan sesuai dengan rancangan pada desain sistem. Berikut hasil pengujian aplikasi kriptografi untuk pengamanan pesan teks menggunakan kombinasi *Caesar Cipher* dan *Hill Cipher* dengan modifikasi sandi Morse serta steganografi dengan LSB.

TABEL II
PENGUJIAN PROSES ENKRIPSI

File	Karakter	Ukuran Awal Image	Size Hasil	TimeExce	Keterangan
TXT,JPG	1155	1536 KB	9,5 MB	1.0005 s	Berhasil
TXT,JPG	578	59 KB	723 KB	0.6839 s	Berhasil
TXT, PNG	327	148 KB	-	0.2881 s	Gagal
TXT, JPG	167	205 KB	795 KB	0.1576 s	Berhasil

IV. KESIMPULAN

Kesimpulan

Berdasarkan penelitian dan uji coba yang telah dilakukan, maka didapatkan kesimpulan sebagai berikut:

1. Dari hasil penelitian ini dilakukan proses menkombinasikan Algoritma *Caesar Cipher* dan *Hill Cipher* yang kemudian dimodifikasi menjadi sandi Morse, dimana hasil enkripsi ini akan sulit di pecahkan oleh pihak- pihak yang tidak bertanggung jawab.
2. Proses penyimpanan pesan atau ciphertext kedalam file gambar akan menyulitkan orang-orang yang tidak bertanggung jawab atau criptoanalys untuk memecahkan pesan yang dikirim dalam bentuk gambar.
3. Waktu eksekusi pada proses enkripsi tergantung pada jumlah karakter yang di enkripsi.
4. Ukuran image yang sudah di proses dengan steganografi LSB menjadi semakin besar disebabkan banyaknya karakter hasil enkripsi yang di simpan.
5. Image atau gambar yang dapat digunakan untuk menyimpan hasil penyandian (ciphertext) hanya gambar yang berekstensi JPEG/JPG.

Saran

Dari kesimpulan yang telah dijelaskan diatas, maka penulis menyarakan sebagai berikut:

1. Untuk pengembangan aplikasi pengamanan data selanjutnya, dapat menggunakan algortima kriptografi lainnya sehingga dapat dilakukan perbandingan tingkat keamanan.
2. Disarankan juga proses pengamanan data atau informasi yang dimasukkan kedalam image tidak hanya terbatas pada ekstensi image tertentu.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada pihak STMIK Syaikh Zainuddin NW Anjani Lombok Timur yang telah memfasilitasi penelitian ini dan juga penulis ucapkan terima kasih kepada tim redaksi Jurnal JTIM yang telah memberikan kesempatan untuk mempublikasikan hasil penelitian ini.

REFERENSI

[1] R. Sulaiman and B. Isnanto, "'Peningkatan Keamanan Pesan Dengan Kriptografi RC4 dan Steganografi LSB Pada File JPEG,'" *Konf. Nas. Sist. Inf. 2018*, pp. 8–9, 2018.

[2] Deliana Br Tarigan, "IMPLEMENTASI ALGORITMA KRIPTOGRAFI HILL CIPHER DALAM PENYANDIAN DATA GAMBAR," *Pelita Inform. Budi Darma*, vol. Volume : V, 2014.

[3] C. A. Sari and E. H. Rachmawanto, "Gabungan Algoritma Vernam Chiper dan End of File untuk Keamanan Data," *Techno.COM*, vol. 13, no. 3, pp. 150–157, 2014.

[4] I. Darmayanti, D. N. Astrida, and D. Arius, "Penerapan Keamanan Pesan Teks Menggunakan Modifikasi Algoritma Caisar Chiper Kedalam Bentuk Sandi Morse," *J. IT CIDA*, vol. 4, no. 1, pp. 39–47, 2018.

[5] A. H. Hasugian, "Implementasi Algoritma Hill Cipher," no. August 2013, pp. 115–122, 2017.

[6] F. Piper, S. Murphy, F. Piper, and S. Murphy, *2. Understanding cryptography*. 2013.

[7] Rifki Sadikin, *Kriptografi untuk keamanan jaringan*, I. Yogyakarta: Penerbit Andi.

[8] Rinaldi Munir, *Kriptografi*. Bandung: Informatika, 2006.

[9] A. Juliatmojo, T., Eko, *Pembelajaran Sandi Morse*

dan Sandi Semaphore dalam bentuk Simulasi berbasis Mutimedia. 2013.

[10] A. W. Fuadz Hasyim, "Peningkatan mutu akreditasi perguruan tinggi menggunakan sistem manajemen dokumen elektronik (electronic document management system)," *NJCA (Nusantara J. Comput. Its Appl.*, vol. Volume 4, pp. 1–6, 2019.