Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 2, Februari 2020, Page 76-82
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

Modifikasi Platform Kunci Algoritma Playfair Untuk Meningkatkan Nilai Confusion Pada Ciphertext

Rivalri Kristianto Hondro

Prodi Teknik Informatika, STMIK Budi Darma, Medan, Indonesia
E-Mail: rivalryhondro@gmail.com

Abstrak−Kriptografi adalah ilmu mengenai teknik penyandian "naskah asli" atau disebut degan istilah plaintext, yang susunannya diacak dengan menggunakan kunci sehingga menjadi "naskah acak yang sulit dibaca" atau disebut dengan istilah ciphertext. Dengan dilakukan proses ini maka seseorang yang tidak memiliki kunci dekripsi tidak bisa membaca data asli. Teknik penerapan kriptografi sering juga disebut Algoritma atau Cipher, salah satu algoritma kriptografi yang dibahas dalam artikel ini adalah Algoritma Playfair. Modifikasi dilakukan terhadap tabel kunci yang dimiliki Algoritma Playfair sehingga ada penambahan karakter selain huruf, ada angka dan simbol. Hasil yang ingin dicapai adalah dari modifikasi algoritma playfair dapat diterapkan pada prose enkripsi sehingga menghasilkan ciphertext yang memiliki nilai confusion. selain itu juga dapat diterapkan pada proses dekripsi sehingga menghasilkan plaintext yang dapat dimengerti.

Kata Kunci: Modifikasi, Algoritma, Playfair, Confusion, Enkripsi, Dekripsi

Abstract−Cryptography is the science of "original manuscript" encoding techniques, called plaintext terms, the arrangement of which is encrypted using a key so that it becomes "random text that is difficult to read" or referred to as ciphertext. By doing this process, someone who does not have a decryption key cannot read the original data. The cryptographic application technique is often also called the Algorithm or Cipher, one of the cryptographic algorithms discussed in this article is the Playfair Algorithm. Modifications are made to the key table that is owned by the Playfair Algorithm so that there are additional characters besides letters, there are numbers and symbols. The result to be achieved is from the modification of the Playfair algorithm that can be applied to the encryption process so as to produce a ciphertext that has a confusion value. but it can also be applied to the decryption process so as to produce an understandable plaintext.

Keywords: Modification, Algorithm, Playfair, Confusion, Encryption, Decryption

1. PENDAHULUAN

Kriptografi adalah ilmu dan seni yang mempelajari tentang bagaimana mengamankan pesan atau data agar tidak dapat diketahui informasi nya oleh orang yang tidak berkepentingan. Mendukung kinerja penerapan kriptografi dibutuhkan algoritma enkripsi dan dekripsi yang dapat memberikan nilai kebinguan *(confusion)* terhadap pesan atau data yang dirahasiakan[1]. Pemilihan dan modifikasi algoritma enkripsi dan dekripsi hal ini perlu dilakukan karena begitu banyak nya jenis serangan terhadap sejumlah data dan informasi yang diamankan dengan menggunakan teknik kriptografi khususnya kriptografi klasik. Salah satu algoritma kriptografi klasik yang akan dibahas dalam penelitian ini adalah algoritma playfair.

Algoritma playfair adalah algoritma kriptografi klasik yang menerapkan teknik enkripsi dan dekripsi pesan dan informasi yang hanya mengandung huruf, sementara bentuk karakter seperti angka dan simbol tidak dapat di enkripsi dengan menggunakan algoritma ini[2]. Selain itu juga jumlah huruf yang ditampilkan tidak lebih dari 25 huruf artinya pembentukan kunci dapat ditebak berformat matriks 5x5, sehingga memungkinkan algoritma ini dapat diserang dengan mudah menggunakan teknik serangan yang dikenal dengan istilah *Dual frequency distribution technique*.

Modifikasi platform kunci algoritma playfair yang diuraikan dalam penelitian ini adalah menambahkan sejumlah karakter lain seperti angka dan simbol pada platform kunci algoritma playfair sehingga membentuk bujursangkar dengan format matriks 8x8. Kemudian menghilangkan ketentuan pergantian huruf "I" menjadi huruf "J" atau sebaliknya, sehingga ciphertext yang dihasilkan dapat memberi nilai *confusion* yang tidak dapat mudah ditebak. Hasil modifikasi terhadap algoritma ini disebut dengan istilah Playfair+ (plus). Susunan urutan angka dan simbol yang ditambahkan dapat dilihat pada tabel 1.

2. METODE PENELITIAN

2.1 Kriptografi

Kriptografi merupakan ilmu yang menerapkan teknik keamanan mengenai penyandian (enkripsi) dimana naskah/pesan asli yang disebut *plaintext* diacak dengan menggunakan kunci yang telah ditentukan sehingga menghasilkan naskah/pesan yang acak dan tidak dapat dipahami makna/artinya objek pesan/naskah ini disebut dengan istilah *ciphertext*.

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 2, Februari 2020, Page 76-82
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

Kriptografi adalah salah satu teknik yang dapat digunakan untuk menjaga dan mengamankan data atau informasi pada saat dilakukan proses distribusi dari suatu tempat ke tempat lainnya[3].

Teknik kriptografi pada proses penerapannya memberikan 5 aspek penting sehingga data atau informasi dapat dikatakan aman, antara lain adalah kerahasiaan, integritas, autentikasi, nir-penyangkalan (). Teknik kriptografi memiliki banyak algoritma untuk menjamin 5 aspek diatas diantaranya adalah Caesar Cipher, Affine Cipher, Hill Cipher, Vegenere Cipher, Triangle Chain Cipher, GOST, DES, AES dan lainnya.

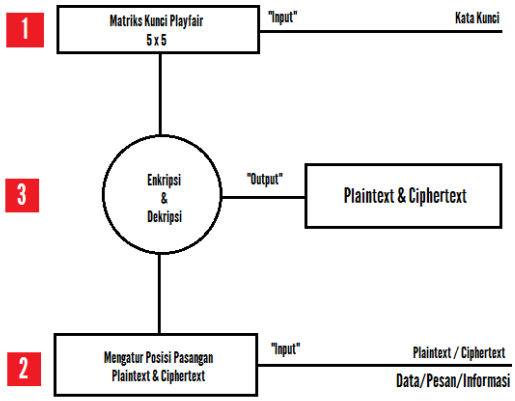
2.2 Nilai Confusion

Nilai confusioan adalah salah satu aspek yang diharapkan dari penerapan model kunci pada saat menerapkan algoritma kriptografi. *Confusion* adalah kata dalam bahas inggris yang berarti dalam bahasa indonesia adalah pembinggungan. Tujuan pembinggungan pada hasil penerapan teknik kriptografi agar pihak yang tidak berkepentingan terhadap pesan/data/informasi yang diamankan tidak dapat memahami arti dari pada pesan/data/informasi tersebut, jika tanpa melalui proses dekripsi[4].

2.3 Algoritma Playfair

Algoritma Playfair atau Cipher Playfair atau Playfair square atau Wheatstone-Playfair cipher adalah teknik enkripsi simetris manual dan merupakan cipher substitusi digram literal pertama. Skema ini ditemukan pada tahun 1854 oleh Charles Wheatstone, namun dipromosikan oleh Baron Lyon Playfair (1819 - 1898) pada tahun 1854. Sandi Playfair pertama kali digunakan untuk tujuan-tujuan taktis oleh pasukan Inggris dalam Perang Boer II dan Perang Dunia I.

Algoritma Playfair bekerja dengan tiga tahap utama yaitu membuat bujursangkar/matriks kunci, proses mengatur pesan, proses enkripsi/dekripsi[5] lebih jelas dapat dilihat model gambar dan urain penjelasannya:



Gambar 1. Skema Kerja Algoritma Playfair

Penjelasan gambar di atas:

1. Membuat Bujursangkar Kunci
   Membuat bujur sangkar kunci playfair cipher dengan matriks 5x5, dengan ketentuan sebagai berikut:
   a. Memilih kunci dari sebuah kata atau kalimat yang mudah diingat
   b. Membuang huruf yang berulang dan huruf J jika ada pada kata kunci
   c. Menambahkan huruf-huruf yang belum ada (kecuali J) disusun berurutan sesuai huruf abjad.
   d. Memasukkan kunci tersebut ke dalam bujur sangkar.
   e. Pseudocode membuat bujur sangkar matriks kunci 5x5, menggunakan bahasa python

```
key=input("Enter key ")
key=key.replace(" ", "")
key=key.upper()
def matrix(x,y,initial):
    return [[initial for i in range(x)] for j in range(y)]

result=list()

for c in key: #storing key
    if c not in result:
        if c=='J':
            result.append('I')
        else:
            result.append(c)
```

```
flag=0

for i in range(65,91): #storing other character
   if chr(i) not in result:
      if i==73 and chr(74) not in result:
         result.append("I")
         flag=1
      elif flag==0 and i==73 or i==74:
         pass
      else:
         result.append(chr(i))
k=0
my_matrix=matrix(5,5,0) #initialize matrix
for i in range(0,5): #making matrix
   for j in range(0,5):
      my_matrix[i][j]=result[k]
      k+=1
```

2. Mengatur Pesan (Plaintext/Ciphertext)
   a. Mengganti huruf J (bila ada) dengan huruf I.
   b. Menulis pesan dalam pasangan huruf.
   c. Jika terdapat pasangan huruf yang sama, maka harus disisipkan huruf Z di tengahnya.
   d. Jika jumlah huruf ganjil, maka harus ditambahkan huruf Z di akhir kunci.
   e. Pseudocode mengatur pesan menggunakan bahasa python

```
def locindex(c): #get location of each character
   loc=list()
   if c=='J':
      c='I'
   for i ,j in enumerate(my_matrix):
      for k,l in enumerate(j):
         if c==l:
            loc.append(i)
            loc.append(k)
            return loc
```

3. Melakukan Proses Enkripsi atau Dekripsi
   a. Algoritma Enkripsi Playfair
      1) Jika terdapat dua huruf pada baris kunci yang sama maka masing-masing huruf
      2) diganti dengan huruf di kanannya (pada kunci yang sudah diperluas).
      3) Jika terdapat dua huruf pada kolom kunci yang sama maka masing-masing huruf
      4) diganti dengan huruf di bawahnya (pada kunci yang sudah diperluas).
      5) Jika dua huruf tidak terdapat pada baris atau kolom yang sama, maka huruf pertama diganti dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari 3 huruf (huruf yang digunakan untuk mencarai huruf ganti huruf pertama) yang digunakan.
   b. Algoritma Dekripsi Playfair
      1) Jika terdapat dua huruf pada baris kunci yang sama maka masing-masing huruf
      2) diganti dengan huruf di kirinya (pada kunci yang sudah diperluas).
      3) Jika terdapat dua huruf pada kolom kunci yang sama maka masing-masing huruf
      4) diganti dengan huruf di atasnya (pada kunci yang sudah diperluas).
      5) Jika dua huruf tidak terdapat pada baris atau kolom yang sama, maka huruf pertama diganti dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari 3 huruf (huruf yang digunakan untuk mencarai huruf ganti huruf pertama) yang digunakan.
   c. Pseudocode Proses Enkripsi dan Dekripsi Playfair

```
def encrypt():  #Encryption
   msg=str(input("ENTER MSG:"))
   msg=msg.upper()
   msg=msg.replace(" ", "")
   i=0
   for s in range(0,len(msg)+1,2):
      if s<len(msg)-1:
```

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 2, Februari 2020, Page 76-82
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

```
            if msg[s]==msg[s+1]:
                msg=msg[:s+1]+'X'+msg[s+1:]
        if len(msg)%2!=0:
            msg=msg[:]+'X'
        print("CIPHER TEXT:",end=' ')
        while i<len(msg):
            loc=list()
            loc=locindex(msg[i])
            loc1=list()
            loc1=locindex(msg[i+1])
            if loc[1]==loc1[1]:
                print("{}{}".format(my_matrix[(loc[0]+1)%5][loc[1]],my_matrix[(loc1[0]+1)%5][loc1[1]]),end=' ')
            elif loc[0]==loc1[0]:
                print("{}{}".format(my_matrix[loc[0]][(loc[1]+1)%5],my_matrix[loc1[0]][(loc1[1]+1)%5]),end=' ')
            else:
                print("{}{}".format(my_matrix[loc[0]][loc1[1]],my_matrix[loc1[0]][loc[1]]),end=' ')
            i=i+2

    def decrypt():  #decryption
        msg=str(input("ENTER CIPHER TEXT:"))
        msg=msg.upper()
        msg=msg.replace(" ", "")
        print("PLAIN TEXT:",end=' ')
        i=0
        while i<len(msg):
            loc=list()
            loc=locindex(msg[i])
            loc1=list()
            loc1=locindex(msg[i+1])
            if loc[1]==loc1[1]:
                print("{}{}".format(my_matrix[(loc[0]-1)%5][loc[1]],my_matrix[(loc1[0]-1)%5][loc1[1]]),end=' ')
            elif loc[0]==loc1[0]:
                print("{}{}".format(my_matrix[loc[0]][(loc[1]-1)%5],my_matrix[loc1[0]][(loc1[1]-1)%5]),end=' ')
            else:
                print("{}{}".format(my_matrix[loc[0]][loc1[1]],my_matrix[loc1[0]][loc[1]]),end=' ')
            i=i+2
```

3. HASIL DAN PEMBAHASAN

Berdasarkan prosedur penerapan proses enkripsi dan dekripsi algoritma playfair seperti yang sudah dijelaskan di atas, maka diketahui format matriks kunci yang digunakan adalah 5x5. Karakter yang disusun dalam tabel kunci tersebut terdiri dari huruf abjad yang dimulai dari huruf "a" sampai dengan huruf "z" dan huruf "j" tidak digunakan. Hasil dari penerapan algoritma ini akan menghasilkan ciphertext yang isiannya hanya terdiri dari huruf saja. Sehingga dapat mudah ditebak kunci yang digunakan jika sesorang memiliki bocoran sebagian huruf dari plaintext. Jenis serangan yang digunakan sering disebut dengan istilah *Dual frequency distribution technique*[6]. *Dual frequency distribution technique* yaitu teknik dengan menghitung frekuensi kemunculan pasangan dua huruf sandi yang kemudian dibandingkan dengan frekuensi pasangan dua huruf pada suatu pesan yang telah dienkripsi.

Modifikasi pada algoritma ini terletak pada proses pembentukan matriks kunci dan proses pengaturan pesan[7]. Pembentukan matriks kunci dibentuk dengan ordo 8x8 dimana penambahan karakter angka dan simbol dilakukan setelah huruf "z", lebih jelasnya dapat dilihat tabel 1 dan 2.

Tabel 1. Urutan Susunan Angka dan Simbol yang ditambahkan

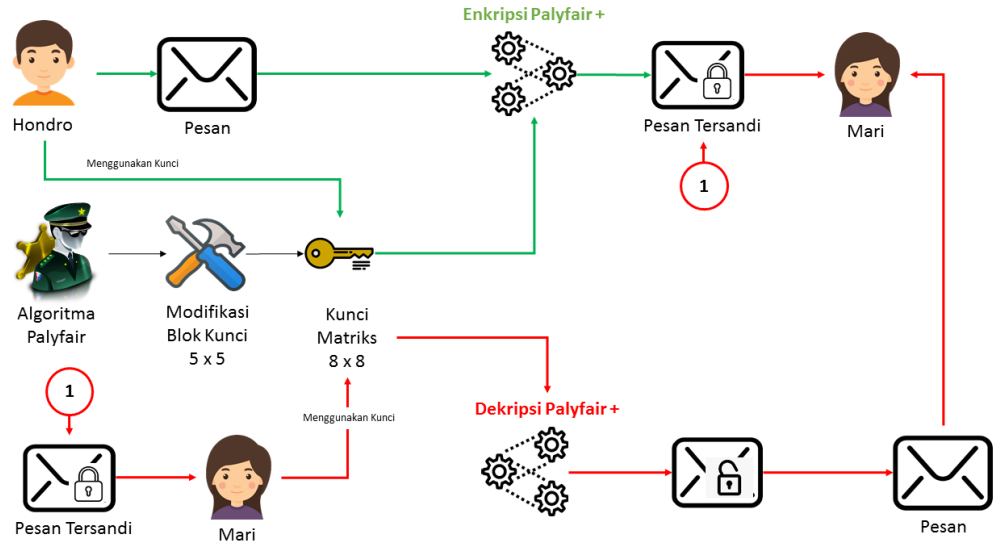
0	1	2	3	4	5	6	7
8	9	!	@	#	$	%	^
&	*	(	)	-	+	=	{
}	[	]	|	\	:	;	"
,	<	>	.	/	?		

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 2, Februari 2020, Page 76-82
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

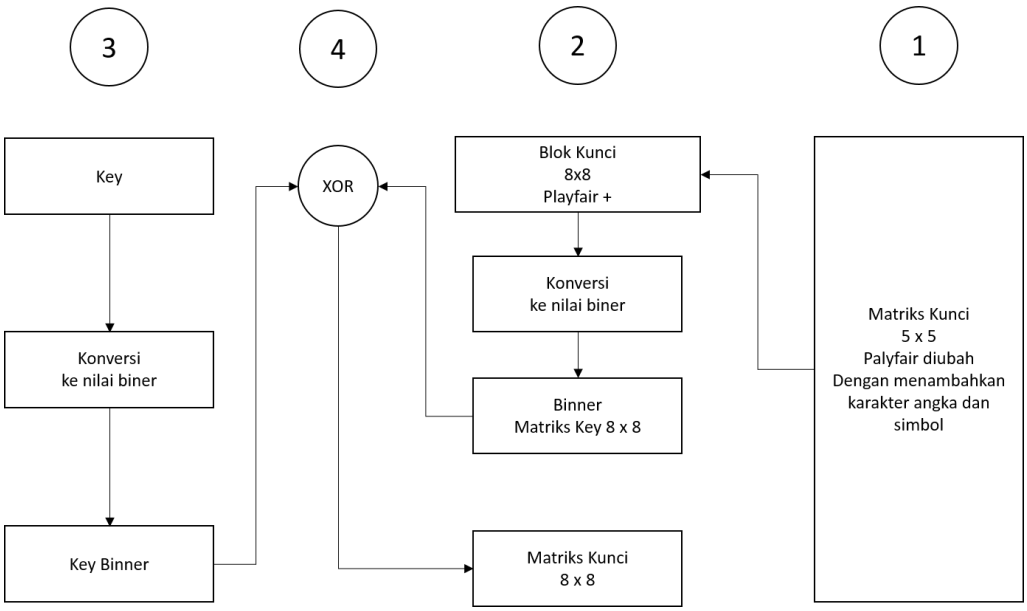
Tabel 2. Isi Matriks Kunci Ordo 8x8

A	B	C	D	E	F	G	H
I	J	K	L	M	N	O	P
Q	R	S	T	U	V	W	X
Y	Z	0	1	2	3	4	5
6	7	8	9	!	@	#	$
%	^	&	*	(	)	-	+
=	{	}	[	]	|	\	:
;	“	,	<	>	.	/	?

Skema proses penerapan Playfair yang telah dimodifikasi ditunjukan pada gambar dua dan tiga.



Gambar 2. Skema Penerapan Algoritma Playfair +



Gambar 3. Skema pembentukan Kunci Playfair +

3.1 Proses Enkripsi

Diketahui *plaintext* dan *key* yang akan digunakan pada pembahasan kali ini, sebagai berikut
Plaintext = RIVALRI
Kunci = HONDRO

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 2, Februari 2020, Page 76-82
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

Berikut proses pembentukan kunci Playfair +,

Tabel 3. Bentuk tabel kunci Playfair +, dengan matriks kunci 8 x 8

index	1	2	3	4	5	6	7	8
1	A	B	C	D	E	F	G	H
2	I	J	K	L	M	N	O	P
3	Q	R	S	T	U	V	W	X
4	Y	Z	0	1	2	3	4	5
5	6	7	8	9	!	@	#	$
6	%	^	&	*	(	)	-	+
7	=	{	}	[	]	|	\	:
8	;	“	,	<	>	.	/	?

Bentuk tabel kunci Playfair +, dengan matriks kunci 8 x 8 setelah di masukkan dengan Kunci “HONDRO”

Tabel 4. Kunci Playfair + “HONDRO”

index	1	2	3	4	5	6	7	8
1	**H**	**O**	**N**	**D**	**R**	A	B	C
2	E	F	G	I	J	K	L	M
3	P	Q	S	T	U	V	W	X
4	Y	Z	0	1	2	3	4	5
5	6	7	8	9	!	@	#	$
6	%	^	&	*	(	)	-	+
7	=	{	}	[	]	|	\	:
8	;	“	,	<	>	.	/	?

Selanjutnya pengelompokan plaintext “RIVALRY” menjadi “RI”, “VA”, “LR”, “Y”, setelah di kelompokan karena huruf “Y” ganjil, ditambahkan karakter “+” maka nilai nya menjadi **RI VA LR Y+**. Selanjutnya lakukan proses enkripsi dengan mengikuti ketentuan Playfair +

Tabel 5. Hasil enkripsi playfair +

Plaintext	**Keterangan**	**Ciphertext**
RI	Berada pada baris dan kolom yang berbeda	**DJ**
VA	Berada pada kolom yang sama	**3K**
LR	Berada pada baris dan kolom yang berbeda	**JB**
Y+	Berada pada baris dan kolom yang berbeda	**5%**

Maka *ciphertext* yang dihasilkan dari proses enkripsi Playfair^{+} adalah **DJ3KJB5%**

3.2 Proses Dekripsi

Proses dekripsi tentunya masih menggunakan platform kunci yang sama yaitu matriks kunci pada tabel 2. Berikut proses dekripsi playfair^{+} :
Ciphertext = **DJ3KJB5%**
Kelompokan, selanjutnya lakukan proses dekrispi sesuai ketentuan pada teori

Tabel 6. Hasil enkripsi playfair^{+}

Plaintext	**Keterangan**	**Ciphertext**
DJ	Berada pada baris dan kolom yang berbeda	**RI**
3K	Berada pada kolom yang sama	**VA**
JB	Berada pada baris dan kolom yang berbeda	**LR**
5%	Berada pada baris dan kolom yang berbeda	**Y+**

Maka ciphertext yang dihasilkan dari proses enkripsi Playfair^{+} adalah **RIVALRY+**

4. KESIMPULAN

Berdasarkan pembahasan di atas, maka dapat disimpulkan bahwa :

1. Penambahan karakter pada matriks kunci playfair^{+} dapat diimplementasikan pada proses enkripsi dan proses dekripsi.
2. Adanya penambahan blok matriks kunci playfair^{+} menjadi 8 x 8, dapat menghasilkan *ciphertext* yang bentuknya berfariasi.
3. Modifikasi kunci playfair menjadi model playfair+ sangat efektif untuk mempersulit pihak penyerang yang menggunakan teknik *Dual frequency distribution technique*.

REFERENCES

[1] R. K. Hondro and G. W. Nurcahyo, "ANALISIS DAN PERANCANGAN SISTEM YANG MENERAPKAN ALGORITMA TRIANGLE CHAIN CIPHER (TCC) UNTUK ENKRIPSI RECORD TABEL DATABASE," *J. Teknol. Inf. dan Komput.*, vol. 3, no. 2, pp. 118–127, 2014.
[2] J. A. BUCHMANN, *Introduction to Cryptography*, 2nd ed. Springer, 2001.
[3] D. Ariyus, *Pengantar Ilmu Kriptografi*. Yogyakarta: Andi, 2008.
[4] W. STALLINGS, *Network and Internetwork Security*, Prentice H. US: Springer, 1995.
[5] E. SETIANINGSIH, *Kriptografi dan Implementasi Menggunakan Matlab*. Yogyakarta: Andi, 2015.
[6] R. K. Hondro, "Aplikasi Enkripsi Dan Dekripsi SMS Dengan Algoritma Zig Zag Cipher Pada Mobile Phone Berbasis Android," *Pelita Inform. Budi Darma*, vol. 3, no. 10, pp. 122–127, 2015.
[7] M. P. and S. G, "Modified Version of Playfair Cipher using Linear Feedback Shift Register," *Int. Conf. Inf. Manag. Eng.*, vol. 09, pp. 488–490, 2009.
[8] M. Syahrizal, Murdani, S. D. Nasution, Mesran, R. Rahim, and A. P. U. Siahaan, "Modified Playfair Cipher Using Random Key Linear Congruent Method," *J. Online Jar. COT POLIPD*, vol. 8, no. 1, pp. 45–49, 2017.
[9] I. Solihin, Mesran, and A. P. U. Siahaan, "IMPLEMENTASI ALGORITMA SUPER PLAYFAIR CHIPHER DAN TWO SQUARE CIPHER DALAM PENGAMANAN PESAN TEKS," *KOMIK (Konferensi Nas. Teknol. Inf. dan Komputer)*, vol. 1, no. 1, pp. 195–201, 2017.
[10] A. Putera, U. Siahaan, M. Mesran, and I. Solihin, "Implementation of Super Playfair in Messaging," in *ICASI 2018*, 2018, pp. 109–118.