BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 2, No 2, April 2022
DOI 10.47065/bulletincsr.v2i2.155 | Hal 47−52
https://hostjournals.com/bulletincsr

Kombinasi Algoritma Cipher Block Chaining dan Triangle Chain Cipher dalam Penyandian File Text

Nurul Hapifah Purba

Fakultas Ilmu Komputer dan Teknologi Informasi, Prodi Teknik Informatika, Universitas Budi Darma, Medan, Indonesia
Email:nurulhapifahpurba@gmail.com,

Abstrak−Saat ini penggunaan teknologi informasi sebagai media pertukaran informasi berkembang sangat luas. Berbagai jenis informasi seperti teks, gambar, suara dan video dapat dikonversikan menjadi media digital yang memungkinkan untuk diperbanyak maupun dikirimkan melalui berbagai media. Salah satunya adalah internet, melalui internet kita dapat dengan mudah untuk saling bertukar informasi dengan orang lain di berbagai tempat. Namun Ada saatnya informasi/pesan bersifat rahasia, dimana tidak boleh ada pihak lain yang mengetahui isi dari informasi ini selain pihak pengirim dan penerima. Maka diperlukan sebuah keamanan terhadap pesan tersebut. Krptografi adalah teknik dan seni untuk menyandikan pesan atau informasi dalam suatu media, seperti teks, gambar, audio ataupun video yang bertujuan untuk menghindari kecurigaan dari orang yang tidak berhak. Untuk itu diperlukan sebuah perangkat lunak yang dapat menyandikan informasi yang bersifat rahasia pada sebuah file teks. Namun dalam melakukannya penyembunyian pesan pada file teks dengan menggunakan kriptografi saja belum tentu aman maka dibutuhkan algoritma yang berguna untuk meningkatkan keamanan oleh sebab itu dibutuhkan algortma Chiper Block Chaining dan Triangle Chain Cipher. Tujuan penelitian yakni untuk menerapkan algortma Chiper Block Chaining dan Triangle Chain Cipher untuk aplikasi penyandian file teks. Hal ini diperlukan karena sering terjadi bahwa pesan teks yang dikirim merupakan suatu pesan rahasia yang tidak boleh diketahui sembarang orang. Chiper Block Chaining dan Triangle Chain Cipher merupakan algoritma yang berguna untuk memberikan keuntungan dalam hal peningkatan keamanan dalam file teks.

Kata Kunci: Kriptografi; Keamanan; File Teks; Cipher Block Chaining; Triangle Block Cipher

Abstract−Currently the use of information technology as a medium of information exchange is growing very widely. Various types of information such as text, images, sound and video can be converted into digital media that allows it to be reproduced or transmitted through various media. One of them is the internet, through the internet we can easily exchange information with other people in various places. However, there are times when information/messages are confidential, where no other party may know the contents of this information other than the sender and recipient. So we need a security against the message. Cryptography is a technique and art to encode messages or information in a medium, such as text, images, audio or video which aims to avoid suspicion from unauthorized people. For that we need a software that can encode confidential information in a text file. However, in hiding messages in text files using cryptography alone is not necessarily safe, so a useful algorithm is needed to improve security, therefore Cipher Block Chaining and Triangle Chain Cipher algorithms are needed. The research objective is to apply the Cipher Block Chaining and Triangle Chain Cipher algorithms for text file encoding applications. This is necessary because it often happens that the text message sent is a secret message that should not be known to just anyone. Block Chaining Ciphers and Triangle Chain Ciphers are useful algorithms to provide an advantage in terms of increased security in text files.

Keywords: Cryptography; Security; Text Files; Cipher Block Chaining; Triangle Block Cipher

1. PENDAHULUAN

Kriptografi merupakan ilmu untuk menjaga kerahasian pesan dengan cara menyandikan kebentuk yang tidak dimengerti. Keunggulan dari kriptografi adalah kemampuan penyandian pesan sehingga pesan terlihat seperti diacak. Kriptografi tidak sekedar berupa kerahasian data (*privacy*) saja, tapi juga bertujuan untuk menjaga integritas data (*data integrity*), keaslian data (*authentication*) dan anti penyangkalan (*nonrepudation*)[1], [2].

File text merupakan *file* yang berisi informasi-informasi dalam bentuk teks. Data yang berasal dari dokumen pengolah kata, angka yang digunakan dalam perhitungan, nama dan alamat dalam basis data merupakan contoh masukan data teks yang terdiri dari karakter, angka dan tanda baca. *File* teks merupakan *file* komputer yang tersusun atas rangkaian baris teks. Jenis–jenis *file* teks yang termasuk dalam kategori umumnya berisi rangkaian karakter tanpa informasi format visual. Konten *file* kategori ini biasanya merupakan catatan atau daftar personal, artikel, buku, dan lain sebagainya. *File* teks mirip dengan *file* yang dihasilkan oleh program pengolahan kata yang konten utamanya bersifat tekstual masukan dan keluaran data teks direpresentasikan[3], [4].

Pada penelitian sebelumnya yang telah dilakukan oleh beberapa penemu yaitu Holder Simorangkir dengan judul penelitian "Perancanan Aplikasi Penyandia, File Tesk Dengan Metode Multiple XOR" menyimpulkan bahwa untuk pengenkripsian data , bila input data di mana *character* ber beda dengan key maka pengenkripsian data dapat dilakukan langsung. Bila input data di mana *character* inputannya ada yang sama dengan key maka hasil XOR-nya adalah nol maka hasil *cipertext* nya di tempatkan pada ASCII(180) agar menghasilkan *characters* yang tidak berbeda , maka harus dibalik charactersny. Hasil *Plaeintext* ke *chipertext* dan *chipertext* ke *plaintext* harus sama supaya informasi yang dikirim sama dengan yang diterima [5].

Penelitian lainnya juga dilakkan oleh Septi Maryanti dengan judul penelitian "Perancangan Aplikasi Kerahasiaan Pesan Dengan Algortma *Hill Cipher*" menyimpulkan bahwa proses enkripsi dan dekripsi dengan menggunakan algoritma kriptografi *hill cipher* ini memiliki kelebihan dalam data enkripsi seperti resitansi terhadap analisis frekuensi. Persamaan aljabar linearnya adalah C = K x P (mod m). *Hill Cipher* termasuk kepada algoritma kriptografi klasikyang sangat sulit dipecahkan oleh kriptanalis apabila dilakukan hanya dengan mengetahui berkas *ciphertext* saja. Namun, teknik ini dapat dipecahkan dengan cukup mudah apabila kriptanalis memiliki berkas *ciphertext* dan potongan berkas *plaintext* [6].

BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 2, No 2, April 2022
DOI 10.47065/bulletincsr.v2i2.155 | Hal 47−52
https://hostjournals.com/bulletincsr

Masalah penyandian data teks merupakan salah satu aspek paling pentig dalam dunia teknologi informasi. Setiap orang memerlukan suatu aplikasi yang dapat mengamankan suatu teks rahasia dan penting agar teks tersebut hanya dapat dilihat dan dibaca oleh orang tertentu saja. Beberapa cara telah dikembangkan untuk menangaini masalah ini, Salah satu cara untuk mengamankan data teks adalah menggunakan sistem kriptografi yaitu dengan penyandian isi informasi (*plaintext*) tersebut menjadi isi yang tidak dipahami melalui proses enkripsi dan untuk memperoleh kembali informasi yang asli, dilakukan proses dekripsi disertai dengan menggunakan kunci yang benar. Keamanan dilakukan nya penyandian *file* teks.

Untuk mengatasi permasalahan yang ada data yang sangat penting maka digunakanlah metode kriptografi yang akan mengenkripsi dan deskripsikan data. Salah satu metode yang akan digunakan dalam pembuatan perangkat aplikasi ini adalah algoritma *Cipher Block Chaining* dan *Triangle Chain Cipher,* Sehingga perlindungan terhadap kerahasiaan data meningkat, salah satu cara adalah penyandian *file* teks atau enkripsi. salah satunya adalah dengan cara merubah data tersebut ke dalam bentuk data yang lain yang tidak dapat dimengerti dalam bentuk penyandian dan kerahasiaan data dengan teknik kriptografi.

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Algoritma kriptografi atau sering disebut dengan *cipher* adalah suatu fungsi matematis yang digunakan untuk melakukan enkripsi dan dekripsi. Defenisi terminologinya adalah urutan langkah-langkah logis untuk penyelesaian masalah yang disusun secara sistimatis.Algoritma kriptografi merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut [1], [7].

2.1 Algortima Cipher Block Chaining (CBC)

Mode operasi *Cipher Block Chaining* (CBC) melakukan proses enkripsi dan dekripsi berdasarkan operasi XOR antara *blok plain* dengan *cipher* sebelumnya. Salah satu ciri utama dari CBC adalah setiap *blokcipher* selalu bergantung pada *blok-blok* sebelumnya. Proses enkripsi yang pertama memerlukan *cipher* awal yang diwakili oleh sebuah *blok biner* yang ditentukan sendiri dan disebut dengan istilah *Initialization Vector*(IV) atau sering disebut *cipher* awal (C_0) dimana Jumlah bit C_0 harus sama dengan jumlah bit kunci. *Biner cipher* yang dihasilkan dari setiap blok dipindahkan (*shift*) sebesar *n-bit* ke kanan atau kiri. Kesalahan satu bit pada sebuah blok *plaintext* akan merambat pada blok *ciphertext* yang *berkoresponden* dan semua blok *ciphertex*t berikutnya dan inilah yang menjadi kelemahan mode operasi ini. Mode operasi CBC juga memiliki kelebihan dimana blok-blok *plaintext* yang sama tidak menghasilkan blok-blok *ciphertext* yang sama, sehingga kriptanalisis menjadi lebih sulit. Mode operasi *cipher block chaining* melakukan proses enkripsi pada setiap blok n-bit *plaintext* yang di-XOR-kan dengan blok n- bit *ciphertext* sebelumnya, kecuali blok *plaintext* pertama di-XOR kan dengan *cipher* awal atau *Initialization Vector*(IV), sebesar n-bit, Secara matematis, enkripsi dan dekripsi berdasarkan mode operasi CBC adalah sebagai berikut :

$Ci = EK(Pi \oplus (Ci-1 \oplus K))$ ..... (1)
$Pi = DK(Ci \oplus (Ci-1 \oplus K))$ ..... (2)

Blok *plaintext* pertama menggunakan C_0 sebagai *cipher* awal dalam hal ini diwakili oleh blok*Initialization Vector* (IV) [8].

2.2 Algoritma Triangle Chain Cipher (TCC)

Triangle Chain Cipher (TCC) merupakan pengembangan dari algoritma kriptografi abjad tunggal khususnya algoritma substitusi abjad tunggal yang sangat mudah diserang dengan teknik analisis *frekuensi*. Kunci yang digunakan pada proses enkripsi dan dekripsi yaitu nilai integer yang menunjukkan pergeseran karakter-karakter sesuai dengan operasi pada *caesar cipher*. Hal inilah yang menjadi kekuatan utama dari algoritma ini. Barisan bilangan-bilangan yang berfungsi sebagai pengali dengan kunci yang berupa bilangan tertentu seperti deret bilangan ganjil, deret bilangan genap, deret fibonaci, deret bilangan prima, serta deret bilangan yang dapat dibuat sendiri menjadi kekuatan keduanya.

Algoritma ini melakukan proses enkripsi dan dekripsi secara ganda yang membentuk pola matriks segitiga pertama dan segitiga kedua. Proses enkripsi dilakukan dua kali dalam pola matriks segitiga pertama dan segitiga kedua.

1. Matriks Enkripsi Segitiga Pertama Baris Ke-1:
   $M[1\ j] = P[j] + (K * R[1]) \bmod 256$… ..... (3)
   Baris ke-2 dan seterusnya untuk nilai $j \geq i$:
   $M[i\ j] = M[i-1], j + (K * R[i]) \bmod 256$… ..... (4)
   Sehingga nilai *ciphertext* yang diperoleh dengan M [i j] pada nilai j = (N+i) – N
2. Matriks Enkripsi Segitiga Kedua untuk Baris Ke-1
   $M[1j] = P[j] + (K * R[1]) \bmod 256$. ..... (5)
   untuk baris ke-2 dan seterusnya untuk nilai$j \leq (N+1)-i$:
   $M[i\ j] = M[i-1], j + (K * R[i]) \bmod 256$ ..... (6)
   Sehingga nilai *ciphertext*yang diperoleh dengan M [i j] = [(N+1) –i, j].

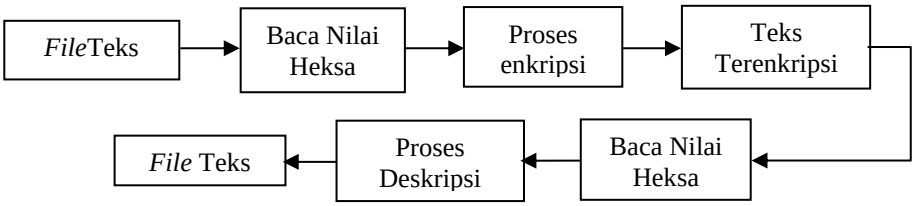
BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 2, No 2, April 2022
DOI 10.47065/bulletincsr.v2i2.155 | Hal 47−52
https://hostjournals.com/bulletincsr

2.3 File Text

File text merupakan *file* yang berisi informasi-informasi dalam bentuk teks. Data yang berasal dari dokumen pengolah kata, angka yang digunakan dalam perhitungan, nama dan alamat dalam basis data merupakan contoh masukan data teks yang terdiri dari karakter, angka dan tanda baca. *File* teks merupakan *file* komputer yang tersusun atas rangkaian baris teks. Jenis–jenis *file* teks yang termasuk dalam kategori umumnya berisi rangkaian karakter tanpa informasi format visual. Konten *file* kategori ini biasanya merupakan catatan atau daftar personal, artikel, buku, dan lain sebagainya. *File* teks mirip dengan *file* yang dihasilkan oleh program pengolahan kata yang konten utamanya bersifat tekstual masukan dan keluaran data teks direpresentasikan [9].

3. HASIL DAN PEMBAHASAN

Algoritma ini merupakan salah satu teknik kompresi simetris yang dapat mennkripsi suatu data berdasarkan dengan frekuensi karakter pada objek yang akan dilakukan prosesenkripsi. Penggunaan algoritma *ini* akan dilakukan berdasarkan karakter yang sering muncul dan akan memiliki jumlah bit terkecil berdasarkan kode, sedangkan karakter yang paling sedikit muncul akan memiliki jumlah bit terpanjang.



Gambar 1. Prosedur Enkripsi Deskripsi *File* Teks.

3.1 Penerapan Algoritma Triangle Chain Cipher

Pada tahapan ini, akan membahas 2 proses utama yaitu proses enkripsi dan proses deskripsi, penulis akan melakukan proses enkripsi pada file teks dengan menggunakan algoritma *Triangle Chain Cipher* (TCC) merupakan salah satu algoritma yang termasuk di dalam metode *simetris. File* yang akan di ekripsi terlebih dahulu dilakukan pembacaan biner yang terdapat pada *file* teks untuk mendapatkan data berupa data biner. Membaca biner yang terdapat pada *file* teks menggunakan aplikasi *Binery Viewer* untuk mencari nilai biner pada file teks.

Tabel 1. Konversi Teks ke Decimal Dan Biner

Plainteks	Decimal	Biner
N	78	01001110
U	85	01010101
R	82	01010010
U	85	01010101
L	76	01001100
SP	32	00100000
H	72	01001000
A	65	01000001
P	80	01010000
I	73	01001001
F	70	01000110
A	65	01000001
H	72	01001000
X	88	01011000

Berikutnya Kunci terelebih dahulu di rubah ke dalam bilangan decimal lalu ubah kembali ke bilangan biner (Kunci : XY = 16Bit)

Tabel 2. Kunci Setelah Drubah ke dalam bilangan biner

IV/C0	Decimal	Biner
U R	85 82	01010101 01010010

Setelah kode berhasil di *encode* berdasarkan perhitungan algoritma *Star-Step-Stop Code*, setelah itu adalah mengurutkan kembali nilai biner yang telah dihasilkan dari proses kompresi sesuai dengan posisi karakter pada nilai heksadesimal.

Adapun sususan dari algoritma Triangle Chain Cipher (TCC) dalam proses enkripsi adalah sebagai berikut :

1. Proses Enkripsi
   NILAI DESIMAL → 53 228 254 131 175 174 251 107 55 191 154 114 167 56

ISSN 2774-3659 (Media Online)
Vol 2, No 2, April 2022
DOI 10.47065/bulletincsr.v2i2.155 | Hal 47−52
https://hostjournals.com/bulletincsr

Langkah selanjutnya melakukan proses enkripsi segitiga pertama: K =4
N = 14
R = 1,2,3,4,5,6,7,8,9,10,11,12,13,14.

2. Rumus baris pertama (i = 1) :
   *M [1 j] = P[j] + (K * R[1]) Mod 256*
   Maka penyelesaian proses enkripsi baris perama : M11 = (P[1]+ (4 * R[1])) Mod 256
   = (+ (4 *(1))) Mod 256
   = (53 + 4) Mod 256
   = 57 (huruf 9 dalam karakter ASCII) M12 =(P[2] + (4 * R[1])) Mod 256
   = (+ (4 *(1))) Mod 256
   = (228 + 4) Mod 256
   = 232 (huruf Φ dalam karakter ASCII)
   M13 = (P[3] + (4 * R[1])) Mod 256
   = (+ (4 *(1))) Mod 256
   = (254 + 4) Mod 256
   = 2 (huruf STX dalam karakter ASCII) M14 = (P[4] + (4 * R[1])) Mod 256
   = (+ (4 *(1))) Mod 256
   = (131 + 4) Mod 256
   = 135 (huruf ç dalam karakter ASCII) M15 = (P[5] + (4 * R[1])) Mod 256
   = (+ (4 *(1))) Mod 256
   = (175 + 4) Mod 256
   = 179 (huruf │ dalam karakter ASCII) M16 = (P[6] + (4 * R[1])) Mod 256
   = (+ (4 *(1))) Mod 256
   = (174 + 4) Mod 256
   = 178 (huruf ▒ dalam karakter ASCII) M17 = (P[7] + (4 * R[1])) Mod 256
   = (+ (4 *(1))) Mod 256
   = (251 + 4) Mod 256
   = 255 (huruf dalam karakter ASCII) M18= (P[8] + (4 * R[1])) Mod 256
   = (+ (4 *(1))) Mod 256
   = (107 + 4) Mod 256
   = 111 (huruf o dalam karakter ASCII) M19 = (P[9] + (4 * R[1])) Mod 256
   = (+ (4 *(1))) Mod 256
   = (55 + 4) Mod 256
   = 59 (huruf ; dalam karakter ASCII) M20 = (P[10] + (4 * R[1])) Mod 256
   = (+ (4 *(1))) Mod 256
   = (191 + 4) Mod 256

Tabel 3. Tabel Enkripsi

Cipertext													
61	244	26	175	239	6	111	255	239	159	166	174	23	**204**
69	252	34	183	247	14	119	7	247	167	174	182	**31**	
81	8	46	195	3	26	131	19	3	179	186	**194**		
97	24	62	211	19	42	147	35	19	195	**202**			
117	44	82	231	39	62	167	55	39	**215**				
141	68	106	255	63	86	167	79	**63**					
169	96	134	27	91	114	195	**107**						
201	127	166	59	123	146	**227**							
237	163	202	95	159	**182**								
21	203	242	135	**199**									
65	247	30	**179**										
113	39	**78**											
165	**91**												
225													

Adapun sususan dari algoritma Triangle Chain Cipher (TCC) dalam proses dekripsi adalah sebagai berikut :

1. Proses Dekripsi Algoritma Triangle Chain Cipher (TCC)
2. Proses Dekripsi Algoritma Triangle Chain Cipher Segitiga Pertama.
3. *M [1 j] = C[j] - (K * R[1]) Mod 256*
   Maka penyelesaian proses Dekripsi baris perama : M11= (C[1]- (4 * R[1])) Mod 256

ISSN 2774-3659 (Media Online)
Vol 2, No 2, April 2022
DOI 10.47065/bulletincsr.v2i2.155 | Hal 47−52
https://hostjournals.com/bulletincsr

= (- (4 *(1))) Mod 256
= (225 - 4) Mod 256
= 221 (huruf h dalam karakter ASCII) M12=(C[2] (4 * R[1])) Mod 256
= (- (4 *(1))) Mod 256
= (91 - 4) Mod 256
=87(huruf 0 dalam karakter ASCII) M13 = (C[3] - (4 * R[1])) Mod 256
= (- (4 *(1))) Mod 256
= (78 - 4) Mod 256
= 74 (huruf dalam karakter ASCII) M14 = (C[4] - (4 * R[1])) Mod 256
= (- (4 *(1))) Mod 256
= (179 - 4) Mod 256
= 175 (huruf ╠ dalam karakter ASCII) M15= (C[5] + (4 * R[1])) Mod 256
= (- (4 *(1))) Mod 256
= (199 - 4) Mod 256
= 195 (huruf á dalam karakter ASCII) M16= (C[6] - (4 *
R[1])) Mod 256
= (- (4 *(1))) Mod 256
= (182 - 4) Mod 256
= 178 (huruf x dalam karakter ASCII) M17= (C[7] - (4 * R[1])) Mod 256
= (- (4 *(1))) Mod 256
= (227 - 4) Mod 256
= 223 (huruf T dalam karakter ASCII) M18= (C[8] - (4 * R[1])) Mod 256

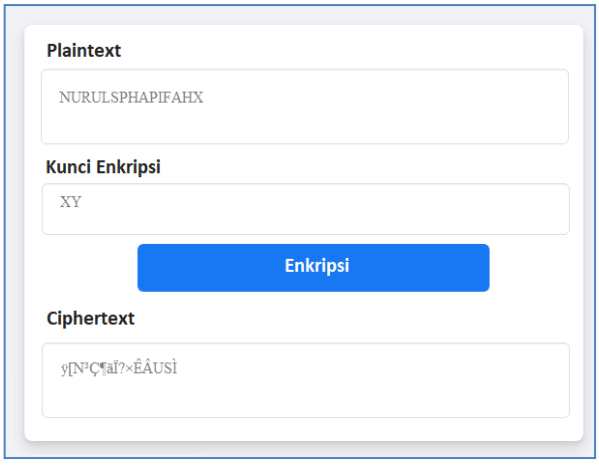
Tabel 4. Tabel Deskripsi

Binner	Decimal
0011 0101	53
1100 0100	196
1111 1100	252
1000 0011	131
0001 1011	27
1101 0010	210
0101 1101	93
1100 0010	194
1101 1101	221
0100 0011	67
1011 1101	189
1100 0010	194
0101 1100	92
0101 0010	82

3.2 Pengujian Sistem

1. Pengujian Proses Enkripsi

Proses enkripsi pada peujian akan dimulai dengan mencari *file* teks berformat docx yang akan di enkripsi, kemudian klik tombol enkrispis untuk memulai proses enkripsi, selanjutnya akan muncul hasil enkripsio dari *file* teks.

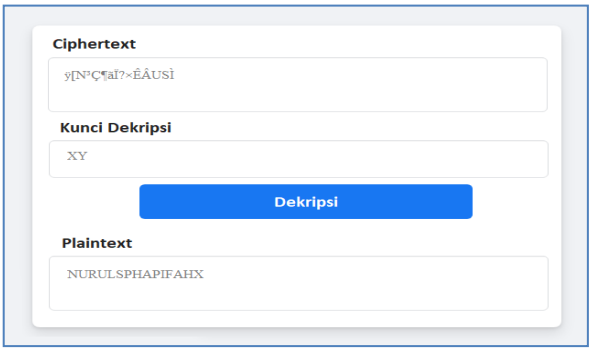


Gambar 2. Hasil Pengujian Kompresi

ISSN 2774-3659 (Media Online)
Vol 2, No 2, April 2022
DOI 10.47065/bulletincsr.v2i2.155 | Hal 47−52
https://hostjournals.com/bulletincsr

2. Pengujian Proses Deskripsi

Proses Deskripsi disini akan berfungsi untuk mengolah kembali *file* yang sudah dienkripsi agar kembali menjadi ukuran dan format *file* diawal. Berikut adalah tampilan *form* Deskripsi.



Gambar 3. Hasil Pengujian Dekompresi

Hasil pengujian pada dapat terlihat seperti pada tabel 5, dengan menggunakan beberapa bentuk karakter *plaintext* dan kunci yang berbeda-beda, sebagai berikut:

No	Plaintext	Kunci	Ciphertext	Keterangan
1	NURULSPHAPIFAHX	XY	ÿ[N³Ç¶ãÏ?×ÊÂUSÌ	Berhasil

4. KESIMPULAN

Hasil penelitian disimpulkan bahwa proses peningkatan keamanan pesan berdasarkan teknik kriptografi yaitu dengan tahapan penyandian pesan atau file teks yang bertujuan untuk menyembunyikan data agar tidak terlihat oleh orang yang tidak berhak melihatnya. Penerapan algoritma chiper block chaining dan triangle chain cipher dalam penyandian file teks dengan menggunakan algoritma skriptografi yang paling sederhana dan mudah diimplementasikan.

REFERENCES

[1] D. Salomon, *Data Compression The Complete Reference FourthEdition*, vol. 53, no. 9. 2007.
[2] E. Setyaningsih, *Kriptografi & Implementasinya Menggunakan Matlab*. Yogyakarta: CV.ANDI OFFSET, 2015.
[3] I. Kurniawan, "Implementasi dan Studi Perbandingan Steganografi pada File Audio WAVE Menggunakan Teknik Low-Bit Encoding dengan Teknik End Of File," *J. Informatics Technol.*, vol. 2, no. 3, pp. 0–11, 2013.
[4] F. C. Venna, "Implementasi steganografi audio pada file wav dengan metode redundant pattern encoding (rpe) berbasis android," 2019.
[5] U. S. Utara, U. S. Utara, and U. S. Utara, "Analisis Perbandingan Kinerja Algoritma Start-Step-Stop Code dan Gopala-Hemachandra Code 2 (GH-2 (n)) pada Kompresi File Teks," vol. 2, 2019.
[6] J. N. Denenberg, E. D. Weinberger, and M. L. Gordon, "DATA COMPRESSION METHOD FOR USE IN A COMPUTERIZED INFORMATIONAL AND TRANSACTIONAL NETWORK," vol. 32, N, 1996.
[7] O. K. Sulaiman, M. Ihwani, and S. F. Rizki, "MODEL KEAMANAN INFORMASI BERBASIS TANDA TANGAN DIGITAL DENGAN DATA ENCRYPTION STANDARD (DES) ALGORITHM," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 1, no. 1, pp. 14–19, Sep. 2016.
[8] M. I. Dzulhaq and A. A. Andayani, "Aplikasi Kompresi File Dengan metode Lempel-Ziv-Welchof," *J. Sisfotek Glob.*, vol. 4, no. 1, pp. 1–4, 2014.
[9] C. D. A. N. Root, "Analisa implementasi aplikasi keamanan file audio wav dengan menerapkan algoritma beaufort cipher dan root 13," vol. 18, pp. 372–379, 2019.