INDEXIA: Informatic and Computational Intelligent Journal
Vol.07, No.02, November 2025, hlm. 130-141
P-ISSN: 2657-0424
E-ISSN: 2657-0432

PENGAMANAN TEKS MENGGUNAKAN KOMBINASI *BLOCK CIPHER ELECTRONIC CODE* (ECB) DAN CAESAR CIPHER BERDASARKAN *SEVEN SEGMENT DISPLAY*

Firdani Dwi Ismawati[1*], Kiswara Agung Santoso[2]
[1,2] Jurusan Matematika, Fakultas MIPA, Universitas Jember
Jalan Kalimantan No.37, Kampus Bumi Tegalboto,Sumbersari,Jember,Jawa Timur,68121,Indonesia

e-mail: firdadwiismawati@gmail.com[1)], kiswara.fmipa@unej.ac.id[2)]

(Naskah masuk : 28 Juni 2025 Diterima untuk diterbitkan : 28 Agustus 2025)

ABSTRAK

Keamanan komunikasi dalam lingkungan internal, khususnya dalam peliputan kasus sensitif menjadi aspek krusial untuk mencegah kebocoran informasi yang dapat berdampak negatif terhadap individu maupun institusi. Penelitian ini bertujuan untuk mengembangkan sistem pengamanan pada aplikasi chat internal dengan menerapkan algoritma kriptografi berbasis *block cipher* mode *Electronic Code Book* (ECB) yang dikombinasikan dengan metode representasi kunci menggunakan *Seven Segment Display*. Representasi kunci melalui pola biner seven segment digunakan untuk menambah kompleksitas proses enkripsi sehingga lebih tahan terhadap serangan kriptanalisis sederhana. Proses enkripsi dilakukan dengan mengubah karakter menjadi biner 7 – bit ASCII, kemudian dilakukan operasi XOR dengan kunci biner seven segment dan diikuti pergeseran bit serta konversi ke karakter ASCII menggunakan algoritma *Caesar Cipher* untuk menghasilkan cipherteks akhir. Hasil pengujian menunjukkan bahwa kombinasi metode *Electronic Code Book* (ECB) dan *Seven Segment Display* mampu menyamarkan pola plainteks dengan baik, serta memberikan tingkat keamanan yang layak untuk kebutuhan komunikasi terbatas dalam lingkungan internal. Dengan pendekatan ini, sistem pengamanan pesan internal menjadi lebih kuat, sederhana, dan tetap efisien untuk diterapkan dalam skala institusi.
***Kata Kunci**: Kriptografi, Electronic Code Book, Keamanan,Caesar Cipher*

ABSTRACT

Communication security within internal environments, particularly when covering sensitive cases, is a crucial aspect in preventing information leaks that could have negative impacts on individuals and institutions. This study aims to develop a security system for internal chat applications by implementing a cryptographic algorithm based on the Electronic Code Book (ECB) block cipher mode combined with a key representation method using a Seven Segment Display. Key representation through seven-segment binary patterns is used to increase the complexity of the encryption process, making it more resistant to simple cryptanalysis attacks. The encryption process involves converting characters into 7 – bit ASCII binary, followed by an XOR operation with the seven-segment binary key, bit shifting, and conversion back to ASCII characters using the Caesar Cipher algorithm to produce the final ciphertext. Test results indicate that the combination of the ECB method and seven-segment display effectively obscures plaintext patterns and provides adequate security for limited communication needs within an internal environment. With this approach, the internal message security system becomes stronger, simpler, and remains efficient for implementation at an institutional scale
***Keywords**: Cryptography, Electronic Code Book, Security, Caesar Cipher*

I. PENDAHULUAN

Globalisasi telah mengubah dunia dari batas - batas wilayah yang tertutup menjadi lebih fleksibel kemajuan pesat dalam bidang transportasi dan perkembangan komunikasi dan teknologi yang semakin meluas seluruh dunia. Salah satu ciri dari globalisasi adalah globalisasi digital, teknologi digital yang semakin berkembang memiliki tantangan [1]. Penggunaan teknologi digital seperti penggunaan smartphone di Indonesia telah menjadi bagian dari gaya hidup modern yang tidak terpisahkan. Jumlah penduduk mencapai sekitar 274,9 juta jiwa pada tahun 2021, penggunaan perangkat ini mengalami pertumbuhan yang signifikan [2]. Kemajuan teknologi informasi telah menciptakan sebuah pola baru yang mengubah cara masyarakat beraktivitas dan berinteraksi [3]. Media sosial sangat populer karena

memungkinakan orang membuat dan mendistribusikan informasi dengan mudah dan cepat. Kemajuan teknologi informasi saat ini menawarkan banyak manfaat, bukan hanya kemampuan untuk berbalas pesan dan bertukar informasi melalui layanan media sosial seperti Facebook, Instagram, Whatsapp dan lain sebagainya. Media sosial sangat umum digunakan sebagai salah satu cara untuk menyebarkan informasi rahasia [4] [5]. Media sosial menjadi sangat populer karena kemungkinan banyak orang yang membuat dan menyebarkan informasi dengan cepat dan mudah [6]. Teknologi tidak hanya memudahkan komunikasi tetapi membawa resiko terkait keamanan data dan privasi [7].

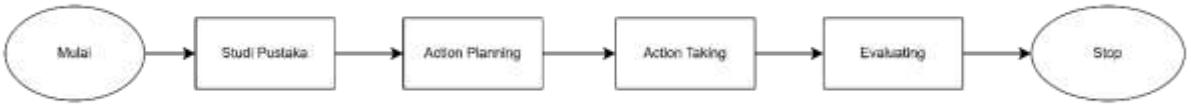
Aplikasi untuk berkomunikasi biasanya disebut dengan chat, chat merupakan bentuk komunikasi berbasis teks yang hidup [8]. Fitur *real-time* pada chat membuat komunikasi menjadi cepat, efisien dan terasa seperti percakapan langsung [9]. Teknologi komunikasi digital telah memunculkan berbagai aplikasi pesan instan atau *chat* yang mendukung komunikasi *real-time*, namun tidak semua aplikasi memberikan jaminan keamanan data yang memadai, khususnya dalam perlindungan privasi pengguna [10]. Keamanan komunikasi menjadi aspek yang sangat penting, terutama dalam konteks peliputan kasus-kasus yang bersifat sensitif dan membutuhkan kerahasiaan tingkat tinggi [11]. Salah satu contoh nyata adalah proses investigasi yang dilakukan oleh tim jurnalis atau penyidik yang sedang menyelidiki kasus seperti korupsi, kejahatan terorganisir, atau penyalahgunaan kekuasaan [12]. Namun, chat internal yang tidak dilengkapi dengan sistem keamanan memadai sangat rentan terhadap penyadapan atau serangan siber yang dapat menyebabkan bocornya informasi penting [13]. Upaya melindungi data dari akses tidak sah enkripsi digunakan sebagai perlindungan keamanan.

Enkripsi adalah teknik yang digunakan untuk mengubah data asli menjadi bentuk yang disamarkan atau tidak dikenali dengan tujuan menjaga keamanan informasi dari seseorang yang bertindak jahat atau akses yang tidak sah [11]. Data yang telah dienkripsi hanya dapat dibaca kembali setelah melalui porses dekripsi menggunakan kunci tertentu [14]. Sistem keamanan diperlukan untuk menjaga informasi yang bersifat pribadi. Salah satu sistem keamanan yang sering digunakan adalah kriptografi. Kriptografi dari bahasa Yunani yang terdiri dari dua kata yaitu kripto yang berarti menyembunyikan dan graphia yang berarti tulisan [15]. Secara umum, kriptografi merupakan cabang ilmu matematika yang digunakan untuk menjaga keamanan informasi. Kriptografi bertujuan untuk menjaga keamanan, salah satu metode kriptografi klasik adalah *Caesar Cipher. Caesar cipher* merupakan salah satu algoritma tertua yang menyusun huruf dalam plainteks yang digeser dan diganti huruf beberapa posisi tetap dibawah alfabet [16]. *Caesar cipher* juga didefiniskan suatu algoritma cipher substitution yang memanfaatkan perubahan huruf dengan modulo 26 [17]. *Seven segment Display* merupakan salah satu komponen digital yang umum digunakan dalam berbagai perangkat elektronik untuk menampilkan visualisasi berupa angka namun, juga dapat digunakan untuk merepresentasikan beberapa huruf dalam alfabet meskipun tidak sekompleks layar karakter lainnya [3]

Kriptografi memiliki algortima *block cipher* untuk membuat chat internal dalam mendalami kasus sensitif tidak menyebar dan bersifat privasi, *block cipher* menggunakan kumpulan bit dengan panjang tetap untuk mengenkripsi pesan. *Block cipher* memiliki lima mode yaitu *Electronic code book* (ECB), *Cipher Block Chaining* (CBC), *Cipher Feedback* (CFB), *Output Feedback* (OFB) dan *Counter* (CTR). Penelitian ini menggunakan *Block Cipher Electronic Code Book* (ECB) sebagai solusi untuk mengamankan chat internal dalam peliputan kasus sensitif [18]. Penelitian ini menggunakan metode *Electronic Code Book* (ECB) yang dikombinasikan dengan *Caesar Cipher* dan *Seven Segment Display* yang bertujuan untuk menjaga keamanan chat internal yang membahas kasus sensitif. Pada penelitian [19] menyatakan kombinasi metode *Electronic Code Book* (ECB) dan kode *Seven Segment Display* dapat digunakan untuk mengamankan data teks dengan baik. Data tersebut dapat diubah cipherteks melalu tahap enkripsi. Cipherteks yang dihasilkan berupa karakter printable pada ASCII. Penelitian lainnya [20] menyatakan bahwa mode *Electronic Code Book* (ECB) setiap bloknya bekerja secara mandiri dan lebih rentan terhadap pola dalam data. Mode ECB menghasilkan perubahan besar pada ciphertext dan menunjukkan pola perubahan bit yang terfragmentasi. Karakteristik *Electronic Code Book* (ECB) setiap blok dienkripsi secara independen dan kelebihannya adalah cepat dan sederhana sedangkan kelemahannya tidak aman untuk data berulang [21]. Tujuan dari penelitian ini adalah merancang dan mengimplementasikan sistem enkripsi dan dekripsi yang mampu menjaga kerahasiaan komunikasi dalam aplikasi chat internal dengan memanfaatkan kombinasi algoritma *Electronic Code Book* (ECB), *Caesar Cipher* dan *Seven Segment Display.*

INDEXIA: Informatic and Computational Intelligent Journal
Vol.07, No.02, November 2025, hlm. 130-141
P-ISSN: 2657-0424
E-ISSN: 2657-0432

II. METODE PENELITIAN



Gambar 1. Flowchart Metode Penelitian

Metode yang digunakan pada penelitian ini adalah

a. Studi Pustaka

Penelitian ini menggunakan metode studi pustaka yaitu tinjauan literatur untuk mendapatkan referensi mengenai kriptografi, metode *Caesar Cipher*, metode *Blok Cipher Electronic Code Book* (ECB) dan *Seven Segment Display*.

b. Action Planning

Action planning adalah kegiatan yang menentukan metode yang akan diambil dalam proses enkripsi kriptografi. Pada penelitian ini menggunakan metode *Electronic Code Book* dengan kombinasi *Caesar Cipher* dan *Seven Segment Display*. *Electronic Code Book* (ECB) merupakan salah satu algoritma dari blok cipher yang memiliki karakteristik setiap blok dienkripsi secara independen dengan memiliki kelebihan cepat dan sederhana. Rumus *Electronic Code Book* (ECB) pada tahap enkripsi plainteks sederhana dinotasikan sebagai berikut:

$$E_k(P) = (P \oplus K) \ll 1 \quad (1)$$

dengan:
$\oplus$ = operasi logika XOR
$\ll$ = pergeseran bit ke kiri
P = Plainteks
K = Kunci

Tahapan dekripsi merupakan kebalikan dari tahapan enkripsi, tahapan dekripsi dinotasikan sebagai berikut :

$$D_k(C) = (C \ll 1) \oplus K \quad (2)$$

dengan:
$\oplus$ = operasi logika XOR
$\gg$ = pergeseran bit ke kanan
C = Cipherteks
K = Kunci
D_k = Fungsi Dekripsi

Perangkat yang biasanya menampilkan angka 0 sampai dengan 9 dan beberapa huruf alphabet adalah *Sevent Segment Display*. Penelitian ini menggunakan *Seven Segment Display* untuk menampilkan angka 0 sampai dengan 9 sebagai representasi visual biner. Setiap angka atau karakter direpresentasikan dalam bentuk tujuh segmen yang bisa dinyalakan atau dimatikan sesuai dengan pola binernya.

Caesar cipher merupakan algoritma yang termasuk kriptografi klasik yang memiliki kunci simetris atau hanya satu kunci yang mana biasa digunakan dalam mengenkripsi atau dekripsi data dan informasi. *Caesar cipher* adalah kriptografi klasik maka proses enkripsi dan dekripsinya dilakukan dengan cara subtitusi. *Caesar cipher* pada penelitian ini menggunakan aturan ASCII untuk menemukan enkripsi dan dekripsinya, aturan yang digunakan adalah ASCII dimana tabel ASCII dapat dilihat pada google, kemudian kunci yang digunakan adalah 9 untuk menggeser bit. Rumus enkripsi *Caesar Cipher* pada printable ASCII 32 – 126 adalah sebagai berikut :

$$C = ((P - 32) + K) \; mod \; 95 + 32 \quad (3)$$

dengan:
P = Plainteks
K = Kunci
C = Cipherteks

Rumus dekripsi *Caesar Cipher* pada printable ASCII 32 – 126 adalah sebagai berikut:

$$C = \big((P - 32) - K\big)\ mod\ 95 + 32 \quad (4)$$

dengan :
P = Plainteks
K = Kunci
C = Cipherteks

c. Action Taking

Action taking merupakan tahapan implementasi berdasarkan penelitian yang telah dibuat yaitu program kriptografi. Tahap ini menerapkan solusi yang diterapkan untuk mengatasi permasalahan yang telah di teliti.

Tabel 1. Kode untuk menampilkan angka 5 pada *Seven Segment Display*

	Tampilan Segmen							Angka yang Tampil
	a	b	c	d	e	f	g	
Tingkat Tegangan (V)	5	0	5	5	0	5	5	5
Nilai Biner	1	0	1	1	0	1	1	

Tabel 2. Kode Menampilkan Angka pada *Seven Segment Display*

Tampilan Segmen							Angka yang Tampil
a	b	c	d	e	f	g	
1	1	1	1	1	1	0	0
0	1	1	0	0	0	0	1
1	1	0	1	1	0	1	2
1	1	1	1	0	0	1	3
0	1	1	0	0	1	1	4
1	0	1	1	0	1	1	5
1	0	1	1	1	1	1	6
1	1	1	0	0	0	0	7
1	1	1	1	1	1	1	8
1	1	1	0	0	1	1	9

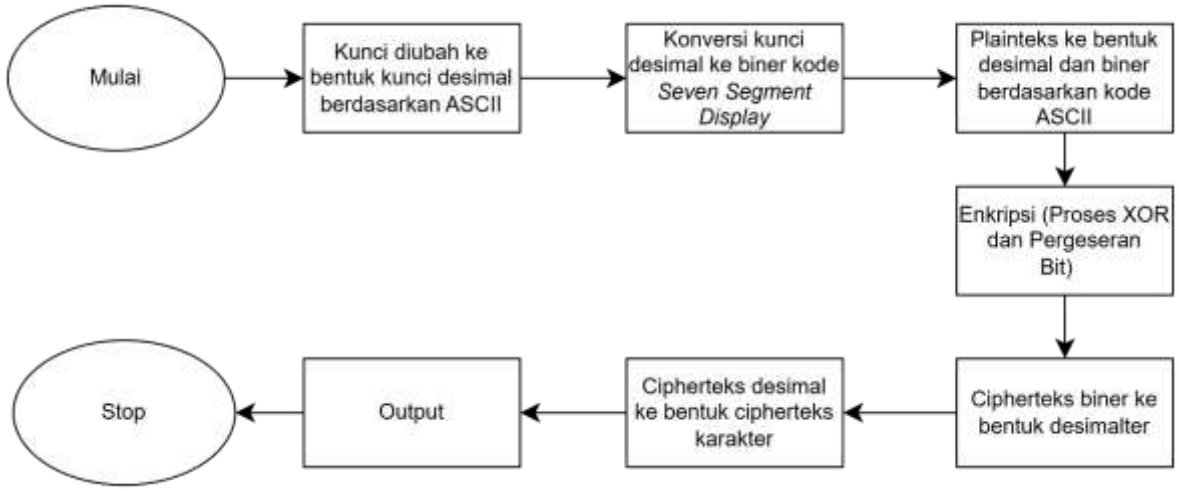
d. Evaluating

Evaluasi adalah proses penyimpulan terhadap penelitian yang dilakukan. Evaluasi dilakukan menggunakan analisis dengan tujuan membuktikan hasil akhir yang diperoleh antara enkripsi dan dekripsi telah sesuai dengan konsep yang dirancang. Hasil analisis ditentukan melalaui proses pengamanan teks menggunakan proses yang telah dirancang yaitu enkripsi dan dekripsi. Penelitian dikatakan berhasil jika menggunakan metode enkripsi dari plainteks dapat diubah menjadi cipherteks. Metode dekripsi adalah mengembalikan cipherteks ke plainteks.

INDEXIA: Informatic and Computational Intelligent Journal
Vol.07, No.02, November 2025, hlm. 130-141
P-ISSN: 2657-0424
E-ISSN: 2657-0432

III. HASIL DAN PEMBAHASAN

3.1 Tahap Enkripsi



Gambar 2. Flowchart Tahap Enkripsi

Tahap yang mengubah plainteks dan kunci sehingga menghasilkan cipherteks, kemudian cipherteks akan digunakan sebagai input bersamaan dengan kunci ketika proses dekripsi untuk dikembalikan ke plainteks. Plainteks yang digunakan adalah sebagai berikut :
Plainteks : KASUS SENSITIF
Kunci : F
Langkah – langkah yang dilakukan pada tahap enskripsi adalah sebagai berikut :

1. Konversi kunci ke bentuk kunci desimal berdasarkan kode ASCII
   Kunci yang digunakan adalah F diubah menjadi kunci desimal berdasarkan kode ASCII, sehingga diperoleh :
   Kunci Desimal : {70}
2. Konversi kunci desimal ke bentuk kunci biner berdasarkan kode *Seven Segment Display*
   Kunci desimal yang diperoleh dipisahkan tiap digitnya sehingga diperoleh sebagai berikut :
   Kunci Desimal : {7,0}
   Kemudian kunci desimal diubah ke bentuk kunci biner, kunci desimal 7 dan 0 dikonversi kunci biner yang dapat dilihat pada tabel 2 sehingga diperoleh :

Tabel 3. Kunci Desimal dan Biner

Kunci Desimal	Kunci Biner
7	1110000
0	1111110

3. Konversi plainteks ke bentuk plainteks desimal, kemudian diubah ke bentuk plainteks biner berdasarkan kode ASCII
   Plainteks yang digunakan adalah KASUS SENSITIF, tiap karakter dikonversi ke bentuk desimal dan bentuk biner dimulai dari karakter ke – 1 yaitu K berdasarkan kode ASCII.

4. Proses enkripsi metode ECB
   Plainteks biner dan kunci biner kemudian diproses pada inti metode *Electronic Code Book* (ECB).
   a. Proses XOR

$$CB_i = PB_i \oplus KB_{(i-1 \bmod m)+1}$$

Keterangan :
CB = Cipherteks Biner
PB = Plainteks Biner
KB = Kunci Biner
Dengan i menyatakan indeks pada PB yang bergerak dari 1 hingga sepanjang PB, dan m menyatakan panjang kunci. Berikut adalah perhitungan cipherteks biner mulai dari CB_i berdasarkan persamaan :

$$CB_i = PB_1 \oplus KB_{(1-1 \bmod 2)+1}$$
$$CB_1 = 1001011 \oplus 1110000$$
$$CB_i = 0111011$$

Perhitungan diatas berlaku juga untuk menghitung CB_2 hingga CB_{14}, sehingga keseluruhan dihasilkan cipherteks biner sebagai berikut :

$$CB = \{0111011,0111111,0100011,0101011,0100011,1011110,$$
$$0100011,0110000,0111110,0101101,0111001,0101010,0111001,0111000\}$$

b. Pergeseran Bit

Pergeseran bit dilakukan di tiap blok biner pada cipherteks biner dengan menggeser bit sejauh 1 bit ke kiri bit paling kiri akan terlempar ke posisi bit paling kanan mulai dari blok cipherteks biner pertama hingga terakhir sehingga diperoleh :

$$CB = \{1110110,1111110,1000110,1010110,1000110,0111101,1000110,$$
$$1100000,1111100,1011010,1110010,1010100,1110010,1110000\}$$

Tabel 4. Kode ASCII dari Plainteks KASUS SENSITIF

Plainteks	Plainteks Desimal	Plainteks Biner
K	75	1001011
A	65	1000001
S	83	1010011
U	85	1010101
S	83	1010011
Spasi	32	0100000
S	83	1010011
E	69	1000101
N	78	1001110
S	83	1010011
I	73	1001001
T	84	1010100
I	73	1001001
F	70	1000110

INDEXIA: Informatic and Computational Intelligent Journal
Vol.07, No.02, November 2025, hlm. 130-141
P-ISSN: 2657-0424
E-ISSN: 2657-0432

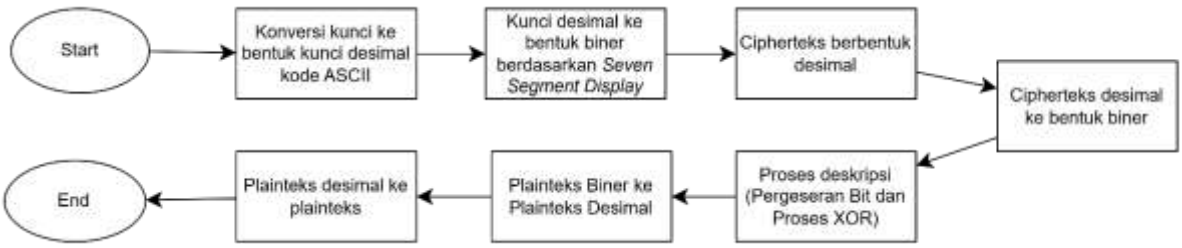
5. Konversi cipherteks biner ke bentuk ciphertext desimal sesuai dengan aturan ASCII
   Cipherteks biner diubah ke bentuk desimal, mulai dari CB pertama hingga CB ke 14 diperoleh sebagai berikut :
   Cipherteks Desimal = {118,126,70,86,70,61,70,96,124,90,114,84,114,112}
6. Konversi cipherteks desimal ke bentuk cipherteks karakter
   Hasil akhir dari enkripsi plainteks **KASUS SENSITIF** adalah **v~FVF=F'|ZrTrp**
7. Hasil tersebut akan diproses kembali ke dalam enkripsi menggunakan algoritma *Caesar Cipher* dengan kunci yaitu 9, perhitungan *Caesar Cipher* ini akan menghasilkan nilai seperti pada tabel 3 sehingga diperoleh sebagai berikut:

Tabel 5. Perhitungan *Caesar Cipher* pada Cipherteks sementara

Cipherteks sementara	$((C-32)+K)\ mod\ 95+32$	Cipherteks
v	32	(Spasi)
~	40	(
F	79	O
V	95	-
F	79	O
=	70	F
F	79	O
‘	105	i
|	38	&
Z	99	c
r	123	{
T	93	]
r	123	{
p	121	y

Hasil akhir cipherteks = **(Spasi) (O-OFOi&c{]{y**

3.2 Tahap Deskrispsi



Gambar 3. Flowchart Tahap Deskripsi

Tahap dekripsi berbeda dengan fase enkripsi yaitu tahap ini merubah cipherteks menjadi plainteks yang mudah dibaca atau dimengerti. Langkah – langkah yang dilakukan pada tahap dekripsi adalah :

1. Konversi kunci ke bentuk kunci desimal berdasarkan kode ASCII
   Kunci yang digunakan adalah F diubah menjadi kunci desimal berdasarkan kode ASCII, sehingga diperoleh :
   Kunci Desimal : {70}
2. Konversi kunci desimal ke bentuk kunci biner berdasarkan kode *Seven Segment Display*
   Kunci desimal yang diperoleh dipisahkan tiap digitnya sehingga diperoleh sebagai berikut :
   Kunci Desimal : {7,0}
   Kemudian kunci desimal diubah ke bentuk kunci biner, kunci desimal 7 dan 0 dikonversi kunci biner yang dapat dilihat pada tabel sehingga diperoleh:

Tabel 6. Kunci Desimal dan Kunci Biner dari kunci F

Kunci Desimal	Kunci Biner
7	1110000
0	1111110

3. Konversi cipherteks ke bentuk cipherteks desimal berdasarkan Kode ASCII, berikut chipeterks yang dihasilkan sebelumnya :
   $$C = (\text{Spasi})\ (\text{O} - \text{OFOi\&c\{]\{y}$$
   Cipherteks tersebut terdiri dari 14 karakter, tiap karakter dikonversi ke bentuk desimal dimulai dari karakter pertama. Sehingga keseluruhan cipherteks desimal adalah sebagai berikut :
   $$CD = \{32,40,79,95,79,70,79,105,38,99,123,93,123,121\}$$
   Cipherteks desimal kemudian ditranformasi dengan ketentuan *Caesar Cipher* dengan kunci yang digunakan adalah 9 sehingga diperoleh sebagai berikut :

   Hasil Cipherteks Desimal setelah ditransformasi sama seperti hasil tahap enkripsi
   $$CD = \{118,126,70,86,70,61,70,96,124,90,114,84,114,112\}$$
4. Konversi Cipherteks desimal ke bentuk cipherteks biner
   Cipherteks desimal kemudian diubah ke bentuk cipherteks biner dengan panjang 7 bit, sehingga keseluruhan cipherteks biner adalah sebagai berikut :
   $$CB = \{1110110,1111110,1000110,1010110,1000110,0111101,1000110,$$
   $$1100000,1111100,1011010,1110010,1010100,1110010,1110000\}$$
5. Proses Dekripsi Metode ECB
   a. Pergeseran Bit
      Pergeseran bit dengan menggeser sejauh 1 bit ke kanan dan bit yang paling kanan akan terlempar ke posisi paling kiri, dilakukan mulai cipherteks biner pertama hingga akhir. Hasil dari pergeseran bit adalah sebagai berikut :
      $$CB = \{0111011,0111111,0100011,0101011,0100011,1011110,$$
      $$0100011,0110000,0111110,0101101,0111001,0101010,0111001,0111000\}$$
   b. Proses XOR
      Proses XOR antara biner dengan kunci biner menghasilkan plainteks biner.
      $$CB_i = PB_i \oplus KB_{(i-1\ mod\ m)+1}$$

      Keterangan :
      CB = Cipherteks Biner
      PB = Plainteks Biner
      KB = Kunci Biner

INDEXIA: Informatic and Computational Intelligent Journal
Vol.07, No.02, November 2025, hlm. 130-141
P-ISSN: 2657-0424
E-ISSN: 2657-0432

Berikut adalah perhitungan untuk mencari plainteks biner mulai dari plainteks biner pertama hingga plainteks biner terakhir sehingga diperoleh plainteks biner sebagai berikut :

$$PB = \{1001011,1000001,1010011,1010101,1010011,0100000,1010011,1000101,1001110,1010011,1001001,1010100,1001001,1000110\}$$

Tabel 7. Perhitungan Caesar Cipher dari Cipherteks Karakter

Cipherteks Karakter	$((C-32)-k) \bmod 95 + 32$	Cipherteks Karakter (Hasil transformasi)
(spasi)	118	v
(	126	~
O	70	F
-	86	V
O	70	F
F	61	=
O	70	F
i	96	‘
&	124	|
c	90	Z
{	114	r
]	84	T
{	114	r
y	112	p

6. Konversi Plainteks Biner ke bentuk Plainteks Desimal
   Plainteks biner yang telah diperoleh sebelumnya diubah menjadi plainteks desimal, mulai dari PB pertama hingga PB ke 14, sehingga diperoleh keseluruhan plainteks desimal sebagai berikut :
   $$PD = \{75,65,83,32,83,69,78,83,73,84,73,70\}$$
7. Konversi plainteks desimal ke bentuk plainteks
   Plainteks desimal menjadi bentuk karakter dimulai dari plainteks desimal pertama hingga plainteks desimal terakhir dengan aturan ASCII, sehingga kita dapat memperoleh hasil plainteks sebagai berikut :
   Plainteks = **KASUS SENSITIF**

3.3 Pembuatan Program

Proses enkripsi dan dekripsi dalam penelitian ini disajikan dalam bentuk pseudocode agar lebih mudah dipahami. Pseudocode enkripsi dan deskripsi adalah sebagai berikut :

A. Pseudocode Enkripsi ECB + Caesar Cipher

Input:
Plaintext = KASUS SENSITIF
key_char = F
caesar_key = 9

Langkah – langkah:

1. Ubah key_char menjadi biner seven segment (7 – bit per digit) dengan inisial nama key_bin
2. Ubah setiap karakter plaintext ke biner 7 – bit dengan inisial plaintext_bin_list
3. Untuk setiap biner p dalam plaintext_bin_list :
   a. Ambil 7 – bit key_segment dari key_bin secara melingkar
   b. Jika panjang key_segment < 7 :
      Tambahkan bit dari awal key_bin hingga panjangnya 7
   c. XOR p dengan key_segment dengan inisial hasil_xor
   d. Simpan hasil_xor ke list cipher_bin
4. Lakukan pergeseran kiri pada setiap bit string dalam cipher_bin → shifted_bin
5. Ubah setiap elemen shifted_bin ke desimal → chiper_desimal
6. Tambahkan caesar shift sebanyak +9 pada setiap nilai desimal (module 127) → caesar_result
7. Ubah setiap angka pada caesar_result ke karakter ASCII → cipher_text

Output:
cipher_text

B. Pseudocode Dekripsi ECB + Caesar cipher

Input:
Cipher_text (hasil dari proses enkripsi)
Key_char ← F
Caesar_key ← 9
Langkah – langkah :

1. Ubah setiap karakter dalam chipher_text ke ASCII, lalu kurangi 9 (modulo 127) → decrypted_decimal
2. Ubah setiap angka pada decrypted_decimal ke biner 7 – bit → decrypted_bin_list
3. Lakukan pergeseran kanan pada setiap string biner dalam decrypted_bin_list → shifted_back_bin
4. Untuk setiap biner c dalam shifted_back_bin:
   a. Ambil 7 – bit key_segment dari key_bin secara melingkar
   b. Jika panjang key_segment < 7:
      Tambahkan bit dari awal key_bin hingga panjangnya 7
   c. XOR c dengan key_segment → hasil_xor
   d. Simpan hasil_xor ke list recovered_bin
5. Ubah setiap elemen recovered_bin ke karakter ASCII → recovered_text

Output:
Recovered_text (hasil deksripsi berupa plaintext asli)

Program enkripsidan dekripsi pada penelitian ini di implementasikan menggunakan Google Colab dengan bahasa pemrograman Python. Proses enkripsi dilakukan terhadap pesan berupa teks dengan menerapkan algoritma block cipher mode *Electronic Code Book* (ECB) yang dikombinasikan dengan representasi kunci berbasis *Seven segment Display*. Setelah itu dikombinasikan kembali dengan algoritma *Caesar Cipher* untuk memperkuat penyamaran karakter dan membuat semakin privat. Proses dekripsi membalikkan cipherteks menjadi plainteks semula untuk membuktikan bahwa enkripsi dan dekripsi mempertahankan keutuhan pesan.

IV. KESIMPULAN

Berdasarkan implementasi yang telah dilakukan, pengamanan komunikasi intelektual khususnya dalam peliputan kasus yang sensitif sangat penting untuk mencegah kebocoran informasi. Upaya melindungi data dari akses tidak sah adalah dengan enkripsi digunakan sebagai perlindungan keamanan. Penggabungan algoritma kriptografi *Electronic Code Book* (ECB), Caesar Cipher dan representasi kunci menggunakan *Seven Segment Display*, sistem enkripsi yang dibangun mampu menyamarkan data teks secara efektif. Penggunaan kriptografi dalam bentuk block cipher *Electronic Code Book* (ECB) memungkinkan setiap blok data dalam chat internal untuk dienkripsi secara sistematis. Namun,

kelemahan *Electronic Code Book* (ECB) yang cenderung menghasilkan pola berulang diatasi dengan *Caesar cipher* dan *Seven Segment Display*. Hasil implementasi Google Colab menunjukkan bahwa metode ini bekerja secara akurat dan efisien, serta mampu meningkatkan kerahasiaan data dalam aplikasi chat internal. Kombinasi ketiga metode menghasilkan sistem pengamanan untuk menjaga komunikasi dan informasi yang tertutup dan sensitif.

DAFTAR PUSTAKA

[1] C. I. Tobing *et al.*, "Globalisasi Digital Dan Cybercrime: Tantangan Hukum Dalam Menghadapi Kejahatan Siber Lintas Batas," *Jurnal Hukum Sasana*, vol. 10, no. 2, pp. 105–123, Dec. 2024, doi: 10.31599/sasana.v10i2.3170.

[2] G. Fanani, I. Riadi, and A. Yudhana, "Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics Research Workshop," *Jurnal Media Informatika Budidarma*, vol. 6, no. 2, pp. 1263–1271, Apr. 2022, doi: 10.30865/mib.v6i2.3946.

[3] K. A. Santoso, A. Pradjaningsih, and E. Delenia, "Pengaman Teks dengan Kombinasi Metode *Electronic Code Book* (ECB) dan Kode *Seven Segment Display*," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 11, no. 1, pp. 85–94, Feb. 2024, doi: 10.25126/jtiik.20241117448.

[4] M. Betty Yel and M. K. M Nasution, "Keamanan Informasi Data Pribadi Pada Media Sosial," *Jurnal Informatika Kaputama*, vol. 6, no. 1, pp. 92–101, Jan. 2022.

[5] M. R. Ardiansyah and R. Ardiana, "Kewajiban Dan Tanggung Jawab Hukum Perdata Dalam Perlindungan Privasi Data Pasien Dalam Layanan Kesehatan Digital," *Jurnal Ilmu Hukum dan Sosial*, vol. 1, no. 4, pp. 276–287, 2023, doi: 10.51903/hakim.v1i4.1470.

[6] T. Khairani, K. A. Santoso, and A. Kamsyakawuni, "Pengkodean Monoalphabetic Menggunakan Affine Cipher dengan Kunci Diffie-Hellman," *Pengkodean Monoalphabetic Menggunakan Affine Cipher dengan Kunci Diffie-Hellman*, vol. 4, no. 221, pp. 553–559, Apr. 2021, Accessed: Feb. 25, 2025. [Online]. Available: https://journal.unnes.ac.id/sju/prisma/article/view/45027

[7] P. Giri Pamungkas, M. Algoritma Kriptografi Caesar, and A. Hendi Muhammad, "Modifikasi Algoritma Kriptografi Caesar Cipher pada Deretan Simbol dan Huruf di Smarphone dan Laptop," *Jurnal of Information Technology*, vol. 2, no. 1, pp. 1–5, Mar. 2022.

[8] K. A. Santoso, R. A. Sukmawati, and A. Pradjaningsih, "Image security development using 3D playfair cipher combination and bit shift," in *AIP Conference Proceeding*, Djogyakarta: AIP Conference Proceedings , Mar. 2022, p. 020013. doi: 10.1063/5.0079220.

[9] Ariska and Wahyuddin, "Penerapan Kriptografi Menggunakan Algoritma DES (Data Encryption Standard)," *Jurnal Sintaks Logika*, vol. 2, no. 2, pp. 9–19, May 2022, [Online]. Available: https://jurnal.umpar.ac.id/index.php/syloghttps://jurnal.umpar.ac.id/index.php/sylog

[10] K. Andrea, A. Wardana, B. S. Wanandi, and A. Ikhwan, "Penerapan Kriptografi Caesar Cipher Pada Fitur Aplikasi Chatting Whatsapp," *Jurnal Hasi Penelitian Dan Pengkajian Ilmiah Eksakta*, vol. 2, no. 1, pp. 6–11, Jan. 2023, doi: 10.47233/jppie.v2i1.660.

[11] R. A. Putri, K. A. Santoso, and A. Kamsyakawuni, "Pengkodean Polyalphabetic dengan Modifikasi Algoritma ElGamal-Caesar Cipher," *PRISMA*, vol. 4, no. 1, pp. 540–547, Feb. 2021, Accessed: Feb. 25, 2025. [Online]. Available: https://journal.unnes.ac.id/sju/prisma/article/view/45022

[12] A. S. Farid and M. Ardiansyah, "Peran Jurnalis Investigatif dalam Mengungkap Kasus Narkoba: Analisis Tantangan dan Hambatan Investigasi Jurnalisme," *Jurnal Ilmu Komunikasi*, vol. 2, no. 3, pp. 186–195, Aug. 2023, doi: 10.54259/mukasi.v2i3.1787.

[13] G. Yafi, D. Hariyadi, T. Febrianto, A. Yani Yogyakarta, and P. Widya Adijaya Nusantara, "Analisis Lalu Lintas Jaringan Terenkripsi dari Secure Instant Messaging Application :Studi Kasus pada Aplikasi Pesan Instan Synology Chat," *Jurnal CyberSecurity dan Forensik Digital*, vol. 5, no. 2, pp. 71–76, Nov. 2022.

[14] B. B. P. Fransiska, K. Chrisntsia, A.Riza, C. Marcellino M, F. Fernandino, and Manikin, "Pemodelan dan Simulasi Algoritma DES (Data Encryption Standard) untuk Enkripsi dan Dekripsi Pesan Teks Menggunakan Cryptool2," *Jurnal Device*, vol. 15, no. 1, pp. 156–162, May 2025.

[15] M. A. Rohim, K. A. Santoso, and A. F. Hadi, "Primary Key Encryption Using Hill Cipher Chain (Case Study: STIE Mandala PMB Site)," in *Advances in Computer Science Research*, 2022. doi: 10.2991/acsr.k.220202.041.

[16] M. Hidayat, M. Tahir, A. Sukriyadi, A. Sulton, C. Ajeng, and S. Abduh, "Penerapan Kriptografi Caesar Cipher Dalam Pengamanan Data," *Jurnal Ilmiah Multidisiplin*, vol. 2, no. 3, pp. 35–41, May 2023, doi: 10.56127/jukim.v2i0.

[17] M. Harun Alfirdaus *et al.*, “Perancangan Aplikasi Enkripsi Dekripsi Mengunakan Metode Caesar Cipher Berbasis Web,” *Jurnal Teknik Mesin, Industri, Eletro dan Informatika*, vol. 2, no. 2, pp. 64–76, Jun. 2023.

[18] H. Nasution, M. Azhar Irwansyah, J. Informatika, F. Teknik, and U. H. Tanjungpura Jalan Hadari Nawawi, “Perancangan Teknik Kriptografi Block Cipher Berbasis Pola Peta Administrasi Kalimantan Barat Menggunakan Key - Dependent S-Box,” *Jurnal Informatika Polinema*, vol. 10, no. 3, pp. 323–332, May 2024.

[19] D. R. K. Gusti, K. A. Santoso, and A. Kamsyakawuni, “VIGENERE CIPHER DENGAN MODIFIKASI PLAINTEXT,” *Majalah Ilmiah Matematika dan Statistika*, vol. 20, no. 1, p. 15, Mar. 2020, doi: 10.19184/mims.v20i1.17219.

[20] K. A. Santoso, S. Hidayatulloh, and A. Kamsyakawuni, “Image Security System Using Playfair Cipher and Modification of Electronic Code Book (ECB) Algorithm,” *EFILKOM : Journal of Technology and Information Systems*, vol. 1, no. 1, pp. 12–20, Jun. 2023, Accessed: Feb. 25, 2025. [Online]. Available: https://ejournal.katersipublisher.com/index.php/REFILKOM/article/view/11

[21] W. Prabowo and A. Nizirwan, “Pengujian Model Simulasi Efek Avalanche Kriptografi Simetris Algoritma AES 128-bit, Mode ECB dan CBC,” *Jurnal ikraith-infromatika*, vol. 1, no. 9, pp. 178–186, Mar. 2025, doi: 10.37817/ikraith-informatika.v9i1.