

# Penerapan Metode Cipher Block Chaining (CBC) Untuk Keamanan E-Document Pada Kantor Kepala Desa Bulu Cina

*Implementation of the Cipher Block Chaining (CBC) Method for E-Document Security at the Bulu Cina Village Head's Office*

**Maulidya Aryuni Syaputri<sup>a,1</sup>, Rahmad Doni<sup>b,2</sup>**

<sup>a,b</sup>Informatika, Universitas Potensi Utama, Medan 20241, Sumatera Utara, Indonesia  
Email: maulidyaaryuni@gmail.com<sup>1</sup>, rahmaddoni113@gmail.com<sup>2</sup>

---

## ABSTRAK

Keamanan dokumen elektronik (*e-document*) menjadi salah satu tantangan utama dalam era digital, terutama bagi lembaga pemerintahan seperti Kantor Kepala Desa Bulu Cina. Sebagai pusat administrasi desa, kantor ini mengelola berbagai dokumen penting yang rentan terhadap ancaman kebocoran, manipulasi, dan perusakan data. Sistem keamanan yang ada belum mampu memberikan perlindungan optimal, sehingga diperlukan solusi yang efektif untuk mengatasi masalah tersebut. Penelitian ini bertujuan untuk mengembangkan sistem keamanan *e-document* dengan menggunakan metode Cipher Block Chaining (CBC). Metode CBC merupakan salah satu teknik enkripsi yang bekerja dengan memecah data menjadi blok-blok yang saling bergantung, sehingga perubahan pada satu blok akan memengaruhi keseluruhan blok lainnya. Hal ini membuat metode ini sangat efektif dalam memastikan kerahasiaan dan integritas data. Penerapan metode CBC pada *e-document* di Kantor Kepala Desa Bulu Cina dilakukan melalui beberapa tahap, mulai dari analisis kebutuhan, desain sistem, hingga implementasi dan pengujian. Hasil penelitian menunjukkan bahwa metode CBC mampu meningkatkan keamanan dokumen elektronik secara signifikan, baik dalam hal pencegahan akses tidak sah maupun perlindungan terhadap manipulasi data.

*Kata Kunci : Enkripsi, Deskripsi, Keamanan, Dokumen Elektronik, Metode Cipher Block Chaining.*

## ABSTRACT

Security of electronic documents (*e-documents*) is one of the main challenges in the digital era, especially for government institutions such as the Office of the Bulu Cina Village Head. As the village administration center, this office manages various important documents that are vulnerable to threats of data leakage, manipulation and destruction. The existing security system is not able to provide optimal protection, so an effective solution is needed to overcome this problem. This research aims to develop an *e-document* security system using the Cipher Block Chaining (CBC) method. The CBC method is an encryption technique that works by breaking data into interdependent blocks, so that changes to one block will affect all the other blocks. This makes this method very effective in ensuring data confidentiality and integrity. The application of the CBC method to *e-documents* at the Bulu Cina Village Head's Office was carried out through several stages, starting from needs analysis, system design, to implementation and testing. The research results show that the CBC method is able to significantly increase the security of electronic documents, both in terms of preventing unauthorized access and protecting against data manipulation.

*Keywords : Encryption, Description, Security, Electronic Documents, Cipher Block Chaining Method.*

---

Disubmit:

Info Artikel :

Direview:

Diterima :

---

Copyright © 2025 – senadimu. All rights reserved.

---

## 1. PENDAHULUAN

Perkembangan teknologi yang sangat pesat di era globalisasi saat ini telah memberikan banyak manfaat dalam kemajuan diberbagai aspek social [1]. Kemajuan teknologi dan digitalisasi telah membawa perubahan yang signifikan dalam cara masyarakat memperoleh informasi [2]. Dengan adanya kemajuan teknologibesarmemungkinkankitauntuk mengetahuiinformasi tidak hanya melalui media buku saja, melainkan dimanapun dan kapanpun kita bisamencari informasi dengan mudah [3].

Kantor Kepala Desa Bulu Cina merupakan salah satu lembaga pemerintahan di tingkat desa yang memiliki peran penting dalam memberikan pelayanan kepada masyarakat. Berbagai kegiatan administrasi, mulai dari pembuatan surat menyurat, pengelolaan data penduduk, hingga dokumentasi aktivitas desa, menjadi bagian dari tanggung jawab utama kantor ini. Dalam era digital, kantor desa Bulu Cina telah mulai mengadopsi teknologi informasi untuk mendukung proses administrasi yang lebih efisien dan cepat. Namun, seiring dengan digitalisasi, muncul pula tantangan dalam hal keamanan data.

Salah satu permasalahan utama yang dihadapi adalah keamanan e-document yang digunakan untuk pengelolaan data administrasi. E-Document adalah sebuah konten elektronik berupa program atau file komputer yang dapat ditampilkan atau dilihat menggunakan media elektronik. Penyimpanan dokumen secara elektronik akan lebih efisien jika dibandingkan dengan penyimpanan secara manual karena lebih hemat tempat atau ruangan [4]. Dokumen-dokumen elektronik, seperti surat keputusan, data penduduk, dan dokumen penting lainnya, rentan terhadap ancaman kebocoran, perusakan, atau manipulasi oleh pihak-pihak yang tidak bertanggung jawab. Sistem keamanan yang ada saat ini belum mampu memberikan perlindungan optimal terhadap ancaman tersebut. Akibatnya, terdapat risiko hilangnya kepercayaan masyarakat terhadap integritas dan kerahasiaan data yang dikelola oleh kantor desa.

Untuk mengatasi permasalahan tersebut, diperlukan sebuah solusi yang dapat menjamin keamanan dokumen elektronik secara menyeluruh. Secara umum, enkripsi merupakan proses mengubah data atau informasi asli (plaintext) menjadi bentuk yang tidak dapat dibaca (ciphertext) menggunakan algoritma tertentu, dengan tujuan menjaga kerahasiaan dan keamanan informasi dari pihak yang tidak berwenang [5]. Dalam konteks keamanan data digital, enkripsi berfungsi untuk melindungi integritas dan privasi data selama proses penyimpanan maupun transmisi, sehingga hanya pihak yang memiliki kunci dekripsi yang sah dapat mengakses informasi aslinya [6]. Secara umum, deskripsi merupakan suatu bentuk penggambaran atau pemaparan yang bertujuan untuk menjelaskan suatu objek, peristiwa, atau konsep secara terperinci agar pembaca atau pendengar dapat memahami dengan jelas apa yang dimaksud [7]. Deskripsi digunakan untuk menyajikan informasi secara sistematis dan faktual mengenai karakteristik, sifat, atau kondisi suatu objek penelitian sehingga memberikan gambaran yang nyata dan informatif kepada pembaca [8].

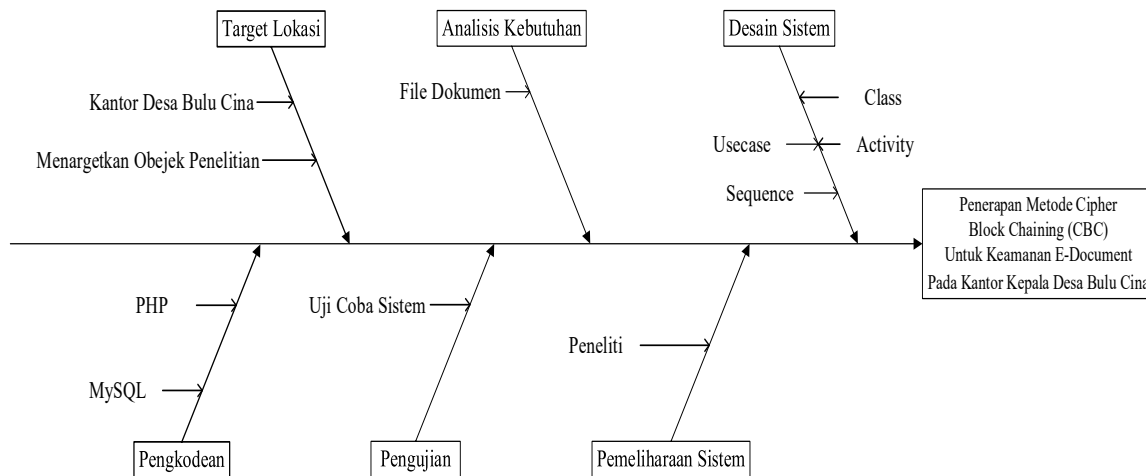
Metode Cipher Block Chaining (CBC) merupakan salah satu teknik enkripsi yang sangat efektif untuk mengamankan data elektronik. Cipher Block Chaining (CBC) merupakan salah satu mode operasi dalam algoritma kriptografi blok yang berfungsi untuk meningkatkan keamanan proses enkripsi dengan cara mengaitkan setiap blok ciphertext dengan blok plaintext sebelumnya menggunakan operasi exclusive OR (XOR) [9]. Pada metode ini, proses enkripsi tidak hanya bergantung pada kunci enkripsi, tetapi juga pada hasil enkripsi dari blok sebelumnya [10]. CBC menggunakan Initialization Vector (IV) sebagai nilai awal yang diacak untuk mengenkripsi blok pertama, guna memastikan bahwa hasil enkripsi berbeda setiap kali proses dilakukan, meskipun data dan kuncinya sama [11].

Penelitian “Implementasi Mode Operasi Kombinasi Cipher Block Chaining dan Metode LSB-1 Pada Pengamanan Data text”. Proses hasil dari uji coba yang kami lakukan adalah Tahapan penelitian, Diagram Proses Kombinasi CBC dengan LSB-1 [12]. Penelitian “Kombinasi Algoritma Cipher Block Chaining dan Triangle Chain Cipher dalam Penyandian File Text”. Cipher Block Chaining dan Triangle Chain Cipher merupakan algoritma yang berguna untuk memberikan keuntungan dalam hal peningkatan keamanan dalam file teks [13]. Penelitian “Text Encoding Using Cipher Block Chaining Algorithm”. Penulis mencoba untuk ikut menciptakan penyandian teks untuk mengamankan data dengan metode kriptografi Cipher Block Chaining (CBC) [14]. Penelitian “Design and Build Zakat Website Application

Based on QR Code Using Cipher Block Chaining Algorithm”. Dalam proses transaksi zakat, Kode QR digunakan dengan menerapkan algoritma Cipher Block Chaining. Hasil penelitian ini Adalah aplikasi situs web untuk zakat [15].

## 2. METODE

Pengembangan sistem dapat berupa menyusun suatu sistem yang baru dan menggantikan sistem yang lama secara keseluruhan atau memperbaiki sistem yang telah ada. Setiap tahap harus di selesaikan terlebih dahulu kemudian diteruskan ke tahap berikutnya untuk menghindari terjadinya pengulangan tahap. Metodologi pengembangan sistem *Fishbone* dapat dilihat pada Gambar I.1 berikut :



Gambar 1. Diagram Fishbone

### 1. Target Lokasi

Target lokasi penelitian ini adalah Kantor Kepala Desa Bulu Cina, yang terletak di Kabupaten Deli Serdang, Provinsi Sumatera Utara. Kantor desa ini merupakan lembaga pemerintahan tingkat desa yang memiliki tugas administratif, pelayanan masyarakat, serta pengelolaan data dan dokumen penting secara elektronik. Objek penelitian yang menjadi fokus utama adalah sistem keamanan terhadap dokumen elektronik (*e-document*) yang digunakan dalam kegiatan administrasi kantor desa. Keamanan dokumen menjadi hal yang krusial mengingat banyaknya informasi bersifat rahasia yang dikelola secara digital.

### 2. Analisis Kebutuhan

Pada tahap ini dilakukan identifikasi dan analisis terhadap kebutuhan sistem, khususnya kebutuhan akan perlindungan data digital yang berupa *file* dokumen elektronik. Jenis dokumen yang dimaksud mencakup surat keputusan, laporan kegiatan, data penduduk, serta dokumen lain yang bersifat rahasia atau administratif. Analisis dilakukan untuk mengetahui bagaimana dokumen dikelola, disimpan, dibagikan, dan sejauh mana sistem saat ini mampu melindungi dokumen dari akses ilegal atau manipulasi data.

### 3. Desain Sistem

Desain sistem keamanan *e-document* dilakukan dengan pendekatan *Unified Modeling Language* (UML). Beberapa diagram yang digunakan dalam desain sistem antara lain:

- Use Case Diagram* untuk menggambarkan hubungan antara pengguna (aktor) dan fungsi sistem.
- Class Diagram* untuk menunjukkan struktur kelas dan relasi antar objek dalam sistem.

- c. *Activity Diagram* untuk memvisualisasikan alur proses atau aktivitas dalam pengelolaan *e-document*.
- d. *Sequence Diagram* untuk menjelaskan interaksi antar objek secara berurutan dalam proses enkripsi dan dekripsi dokumen.
4. Pengkodean (Implementasi Program)  
Tahap pengkodean dilakukan dengan menggunakan bahasa pemrograman PHP untuk membangun logika sistem, sedangkan MySQL digunakan untuk manajemen basis data dokumen. Proses implementasi meliputi pembuatan modul enkripsi dan dekripsi dengan metode *Cipher Block Chaining* (CBC), serta integrasi sistem dengan antarmuka pengguna untuk pengelolaan dokumen.
5. Pengujian (Testing)  
Untuk memastikan sistem bekerja sesuai dengan yang dirancang, dilakukan pengujian menggunakan metode *Black Box Testing*. Pengujian ini fokus pada pengujian fungsionalitas sistem dari sisi pengguna, tanpa memeriksa kode program secara langsung. Tujuan utamanya adalah memastikan bahwa semua fitur seperti unggah dokumen, enkripsi, dekripsi, dan akses pengguna dapat berjalan dengan baik sesuai kebutuhan.
6. Pemeliharaan Sistem  
Tahap ini dilakukan oleh peneliti selaku pengembang sistem. Pemeliharaan meliputi perbaikan bug, penyesuaian fungsionalitas berdasarkan masukan pengguna, serta pembaruan sistem untuk menjaga keamanannya seiring waktu. Sistem juga dapat dikembangkan lebih lanjut agar mendukung fitur tambahan seperti pencatatan log aktivitas pengguna dan notifikasi keamanan.

### 3. HASIL DAN PEMBAHASAN

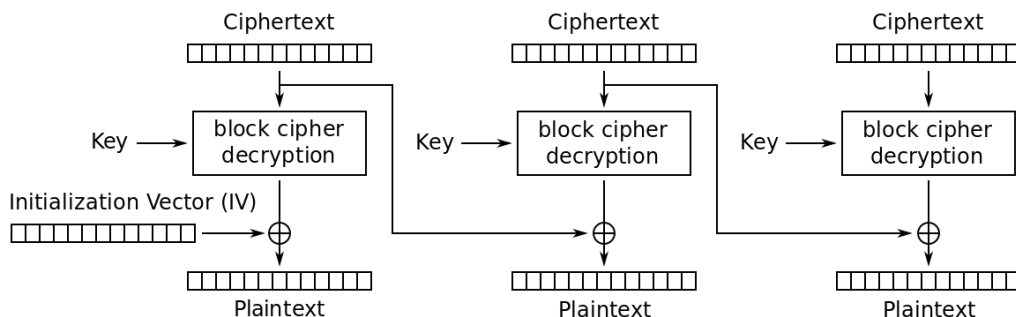
*Cipher Block Chaining* (CBC) adalah mode operasi yang menerapkan umpan-balik (*feedback*) pada sebuah blok, tiap blok dari *plaintext* dilakukan XOR dengan hasil *ciphertext* dari blok sebelumnya yang kemudian dilakukan enkripsi. Pada mode CBC *ciphertext* dari masing-masing blok akan tergantung pada seluruh hasil *ciphertext* dari blok-blok sebelumnya. Pada proses awal enkripsi blok data akan di XOR dengan IV (*Initialization Vector*) untuk membuat tiap *plaintext* menjadi unik[16]. Rumus matematis untuk enkripsi pada mode CBC adalah:

$$C_i = E_k(P_i \oplus C_{i-1}), C_0 = IV \dots \dots \dots (1)$$

Sedangkan rumus matematis untuk dekripsi pada mode CBC adalah:

$$P_i = D_k(C_i) \oplus C_{i-1,0} = IV \dots \dots \dots (2)$$

Blok *plaintext* pertama menggunakan  $C_0$  sebagai *initialization vector* atau IV yang diberikan secara acak dan digunakan menggantikan blok *ciphertext* sebelumnya. Adapun tampilan proses metode CBC dapat dilihat pada gambar berikut :



Gambar 2. *Cipher Block Chaining* (CBC)

#### 3.1 Proses Cipher Block Chaining (CBC)

Adapun Langkah-langkah metode *Cipher Block Chaining* (CBC) dapat dijelaskan sebagai berikut :

## 1. Enkripsi

Tahap awal melakukan persiapan data, sebagai contoh data yang digunakan dapat dijelaskan sebagai berikut :

|           |   |   |   |   |   |   |   |   |   |  |   |   |   |   |
|-----------|---|---|---|---|---|---|---|---|---|--|---|---|---|---|
| Plaintext | D | E | S | A |   | B | U | L | U |  | C | I | N | A |
| Key       | P | E | R | A | K |   |   |   |   |  |   |   |   |   |
| IV        | 2 | 0 | 3 | 7 | 4 |   |   |   |   |  |   |   |   |   |

Setelah itu lakukan konversi *plaintext*, *key*, dan *Initialization Vector* (IV) ke nilai ASCII, yang dapat dijelaskan sebagai berikut :

Tabel 1. Nilai ASCII

| Plaintext | ASCII | Key | ASCII | IV | ASCII |
|-----------|-------|-----|-------|----|-------|
| D         | 68    | P   | 80    | 2  | 50    |
| E         | 69    | E   | 69    | 0  | 48    |
| S         | 83    | R   | 82    | 3  | 51    |
| A         | 65    | A   | 65    | 7  | 55    |
|           | 32    | K   | 75    | 4  | 52    |
| B         | 66    |     |       |    |       |
| U         | 85    |     |       |    |       |
| L         | 76    |     |       |    |       |
| U         | 85    |     |       |    |       |
|           | 32    |     |       |    |       |
| C         | 67    |     |       |    |       |
| I         | 73    |     |       |    |       |
| N         | 78    |     |       |    |       |
| A         | 65    |     |       |    |       |

Karena CBC bekerja dalam blok, maka perlu menambahkan *padding* jika panjang plaintext tidak kelipatan blok. Misalkan menggunakan blok 5 *byte* (sesuai panjang IV):

*Plaintext* :

68 69 83 65 32 66 85 76 85 32 67 73 78 65

Panjang *plaintext*: 14 byte.

*Padding* diperlukan: 1 *byte* (karena  $14 + 1 = 15$ , yang merupakan kelipatan 5).

*Padding* : 0x01 (sesuai PKCS7).

*Plaintext* dengan *padding*:

68 69 83 65 32 66 85 76 85 32 67 73 78 65 01

### a. Blok 1

Gunakan XOR antara *plaintext* dan kunci. Jika panjang kunci lebih pendek dari blok, kunci diulang.

1) Plaintext: 68 69 83 65 32

2) IV: 50 48 51 55 52

3) XOR *Plaintext* dengan IV:

Tabel 2. XOR Plaintext Blok 1

| Plaintext | IV | XOR |
|-----------|----|-----|
| 68        | 50 | 118 |
| 69        | 48 | 117 |
| 83        | 51 | 96  |
| 65        | 55 | 118 |
| 32        | 52 | 20  |

4) Enkripsi dengan Kunci:

Kunci: 80 69 82 65 75

XOR hasil XOR dengan kunci:

Tabel 3. Enkripsi Blok 1

| Hasil XOR | Kunci | XOR |
|-----------|-------|-----|
| 118       | 80    | 38  |
| 117       | 69    | 48  |
| 96        | 82    | 50  |
| 118       | 65    | 55  |
| 20        | 75    | 95  |

Sehingga hasil enkripsi pada blok 1 menghasilkan deretan karakter acak yang dapat dijelaskan sebagai berikut :

38 48 50 55 95

b. Blok 2

Gunakan XOR antara *plaintext* dan kunci. Jika panjang kunci lebih pendek dari blok, kunci diulang.

1) Plaintext: 66 85 76 85 32

2) IV: 50 48 51 55 52

3) XOR *Plaintext* dengan IV:

Tabel 4. XOR Plaintext Blok 2

| Plaintext | IV | XOR |
|-----------|----|-----|
| 66        | 50 | 112 |
| 85        | 48 | 101 |
| 76        | 51 | 127 |
| 85        | 55 | 98  |
| 32        | 52 | 20  |

4) Enkripsi dengan Kunci:

Kunci: 80 69 82 65 75

XOR hasil XOR dengan kunci:

Tabel 5. Enkripsi Blok 2

| Hasil XOR | Kunci | XOR |
|-----------|-------|-----|
| 112       | 80    | 32  |
| 101       | 69    | 32  |
| 127       | 82    | 45  |
| 98        | 65    | 35  |
| 20        | 75    | 95  |

Sehingga hasil enkripsi pada blok 2 menghasilkan deretan karakter acak yang dapat dijelaskan sebagai berikut :

32 32 45 35 95

c. Blok 3

Gunakan XOR antara *plaintext* dan kunci. Jika panjang kunci lebih pendek dari blok, kunci diulang.

1) Plaintext: 67 73 78 65 01

2) IV: 50 48 51 55 52

3) XOR *Plaintext* dengan IV:

Tabel 6. XOR Plaintext Blok 3

| Plaintext | IV | XOR |
|-----------|----|-----|
| 67        | 50 | 113 |
| 73        | 48 | 121 |
| 78        | 51 | 125 |

|    |    |     |
|----|----|-----|
| 65 | 55 | 118 |
| 01 | 52 | 01  |

- 4) Enkripsi dengan Kunci:  
Kunci: 80 69 82 65 75  
XOR hasil XOR dengan kunci:

Tabel 7. Enkripsi Blok 3

| Hasil XOR | Kunci | XOR |
|-----------|-------|-----|
| 113       | 80    | 33  |
| 121       | 69    | 60  |
| 125       | 82    | 47  |
| 118       | 65    | 55  |
| 01        | 75    | 01  |

Sehingga hasil enkripsi pada blok 3 menghasilkan deretan karakter acak yang dapat dijelaskan sebagai berikut :

33 60 47 55 01

Sehingga hasil enkripsi setiap blok ya dapat dijelaskan sebagai berikut :

|             |    |    |    |    |        |    |    |    |    |        |    |    |    |    |
|-------------|----|----|----|----|--------|----|----|----|----|--------|----|----|----|----|
| Blok 1      |    |    |    |    | Blok 2 |    |    |    |    | Blok 3 |    |    |    |    |
| 38          | 48 | 50 | 55 | 95 | 32     | 32 | 45 | 35 | 95 | 33     | 60 | 47 | 55 | 01 |
| Hexadesimal |    |    |    |    |        |    |    |    |    |        |    |    |    |    |
| 26          | 30 | 32 | 37 | 5F | 20     | 20 | 2D | 23 | 5F | 21     | 3C | 2F | 37 | 01 |

## 2. Deskripsi

Proses deskripsi adalah proses kebalikan dari proses enkripsi, Adapun Langkah-langkahnya dapat dijelaskan sebagai berikut :

*Ciphertext* (Hasil Enkripsi):

|             |    |    |    |    |    |
|-------------|----|----|----|----|----|
| Blok 1      | 38 | 48 | 50 | 55 | 95 |
| Blok 2      | 32 | 32 | 45 | 35 | 95 |
| Blok 3      | 33 | 60 | 47 | 55 | 01 |
| Kunci ascii | 80 | 69 | 82 | 65 | 75 |
| IV ascii    | 50 | 48 | 51 | 55 | 52 |

### a. Blok 1

1) Ciphertex Blok 1: 38 48 50 55 95

2) Kunci: 80 69 82 65 75

3) XOR dengan IV:

IV : 50 48 51 55 52

XOR hasil deskripsi dengan IV :

Tabel 8. XOR Ciphertext Blok 1

| Ciphertext | IV | XOR |
|------------|----|-----|
| 38         | 50 | 20  |
| 48         | 48 | 0   |
| 50         | 51 | 1   |
| 55         | 55 | 0   |
| 95         | 52 | 107 |

4) XOR *ciphertext* dengan kunci:

Tabel 9. Deskripsi Blok 1

| Hasil XOR | Kunci | XOR | ASCII |
|-----------|-------|-----|-------|
| 20        | 80    | 68  | D     |
| 0         | 69    | 69  | E     |

|     |    |    |   |
|-----|----|----|---|
| 1   | 82 | 83 | S |
| 0   | 65 | 65 | A |
| 107 | 75 | 32 |   |

## b. Blok 2

- 1) Ciphertex Blok 2: 32 32 45 35 95
- 2) Kunci: 80 69 82 65 75
- 3) XOR dengan IV:  
IV : 50 48 51 55 52  
XOR hasil deskripsi dengan IV :

Tabel 10. XOR Ciphertext Blok 2

| Ciphertext | IV | XOR |
|------------|----|-----|
| 32         | 50 | 18  |
| 32         | 48 | 16  |
| 45         | 51 | 30  |
| 35         | 55 | 20  |
| 95         | 52 | 107 |

- 4) XOR *ciphertext* dengan kunci:

Tabel 11. Deskripsi Blok 2

| Hasil XOR | Kunci | XOR | ASCII |
|-----------|-------|-----|-------|
| 18        | 80    | 66  | B     |
| 16        | 69    | 85  | U     |
| 30        | 82    | 76  | L     |
| 20        | 65    | 85  | U     |
| 107       | 75    | 32  |       |

## c. Blok 3

- 1) Ciphertex Blok 33 60 47 55 01
- 2) Kunci: 80 69 82 65 75
- 3) XOR dengan IV:  
IV : 50 48 51 55 52  
XOR hasil deskripsi dengan IV :

Tabel 12. XOR Ciphertext Blok 3

| Ciphertext | IV | XOR |
|------------|----|-----|
| 33         | 50 | 19  |
| 60         | 48 | 12  |
| 47         | 51 | 28  |
| 55         | 55 | 0   |
| 01         | 52 | 1   |

- 4) XOR *ciphertext* dengan kunci:

Tabel 13. Deskripsi Blok 3

| Hasil XOR | Kunci | XOR | ASCII |
|-----------|-------|-----|-------|
| 19        | 80    | 67  | C     |
| 12        | 69    | 73  | I     |
| 28        | 82    | 78  | N     |
| 0         | 65    | 65  | A     |
| 1         | 75    | 01  |       |

Sehingga hasil deskripsi setiap blok ya dapat dijelaskan sebagai berikut :

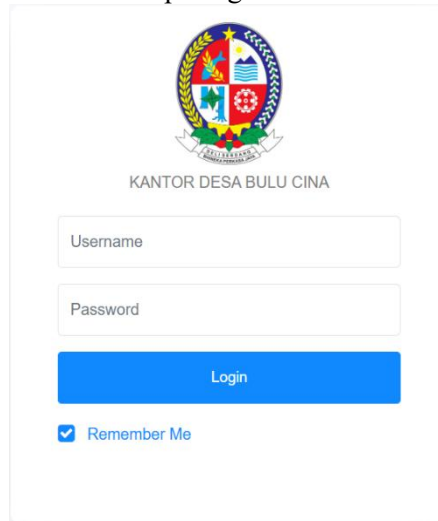
| Blok 1 |    |    |    |    | Blok 2 |    |    |    |    | Blok 3 |    |    |    |   |
|--------|----|----|----|----|--------|----|----|----|----|--------|----|----|----|---|
| 68     | 69 | 83 | 65 | 32 | 66     | 85 | 76 | 85 | 32 | 67     | 73 | 78 | 65 | 1 |
| ASCII  |    |    |    |    |        |    |    |    |    |        |    |    |    |   |
| D      | E  | S  | A  | -  | B      | U  | L  | U  | -  | C      | I  | N  | A  | - |

### 3.2 Tampilan Hasil

Berikut ini dijelaskan tentang tampilan hasil dari perancangan sistem yang dibangun dapat dilihat sebagai berikut :

#### 1. Tampilan Menu *Login*

Tampilan menu *login* pada sistem terlihat pada gambar berikut :

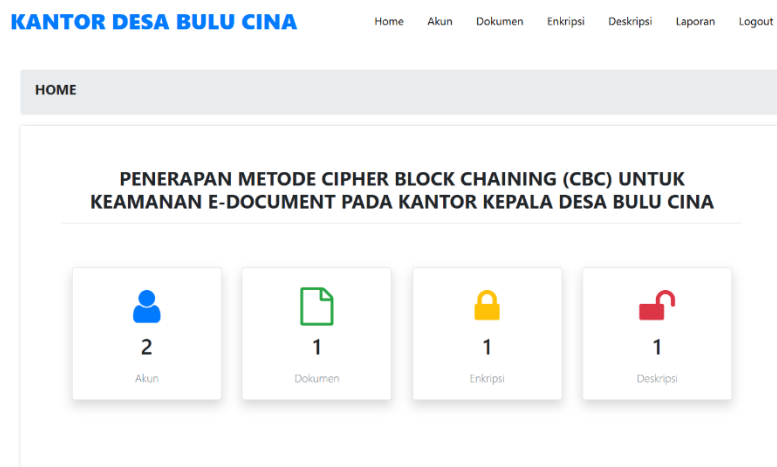


Gambar 3. Tampilan Menu *Login*

Menu *Login* merupakan tampilan awal yang dapat diakses oleh dua jenis pengguna, yaitu Admin dan Kepala Desa (Kades), untuk masuk ke dalam sistem. Pengguna diminta untuk memasukkan *username* dan *password* melalui dua kolom *input* teks yang disediakan. Kolom pertama berlabel "*Username*" digunakan untuk memasukkan nama pengguna, sedangkan kolom kedua berlabel "*Password*" berfungsi untuk mengisi kata sandi yang bersifat rahasia. Setelah mengisi kedua kolom tersebut, pengguna dapat menekan tombol *Login* untuk memverifikasi data dan mengautentikasi masuk ke sistem. Jika *login* berhasil, pengguna akan diarahkan ke halaman sesuai dengan hak akses mereka, sedangkan jika gagal, biasanya akan muncul pesan *error* yang meminta pengguna memeriksa kembali *username* atau *password* yang dimasukkan.

#### 2. Tampilan Menu Home

Tampilan menu home pada sistem terlihat pada gambar berikut :



Gambar 4. Tampilan Menu Home

Tampilan Menu *Home* merupakan halaman utama yang hanya dapat diakses oleh Admin dan Kepala Desa (Kades) setelah berhasil *login*. Halaman ini berfungsi sebagai pusat navigasi yang menyediakan berbagai menu penting untuk mengelola sistem. Di dalamnya terdapat beberapa opsi, yaitu Menu Akun (untuk mengelola data pengguna), Menu Dokumen (untuk mengunggah, melihat, atau mengatur dokumen), Menu Enkripsi (untuk mengenkripsi dokumen penting agar aman dari pihak yang tidak berwenang), Menu Deskripsi (untuk membuka kembali dokumen yang telah dienkripsi), Menu Laporan (untuk melihat atau mencetak laporan kegiatan), dan Menu *Logout* (untuk keluar dari sistem dan mengakhiri sesi).

### 3. Tampilan Akun

Tampilan akun pada sistem terlihat pada gambar berikut :



Gambar 5. Tampilan Akun

Tampilan Menu Akun merupakan bagian yang hanya dapat diakses oleh Admin dan Kepala Desa (Kades) untuk mengubah informasi *login*. Pada menu ini, terdapat beberapa kolom input teks yang memungkinkan pengguna memperbarui data pribadi, yaitu Nama Lengkap, *Username*, dan *Password*. Kolom Nama Lengkap digunakan untuk memasukkan atau memperbarui nama pengguna, sementara kolom *Username* berfungsi untuk mengubah identitas *login* jika diperlukan. Adapun

kolom *Password* memungkinkan pengguna mengganti kata sandi lama dengan yang baru untuk menjaga keamanan akun. Menu ini sangat penting untuk memastikan data *login* tetap mutakhir dan aman.

#### 4. Tampilan Dokumen

Tampilan data dokumen pada sistem terlihat pada gambar berikut :

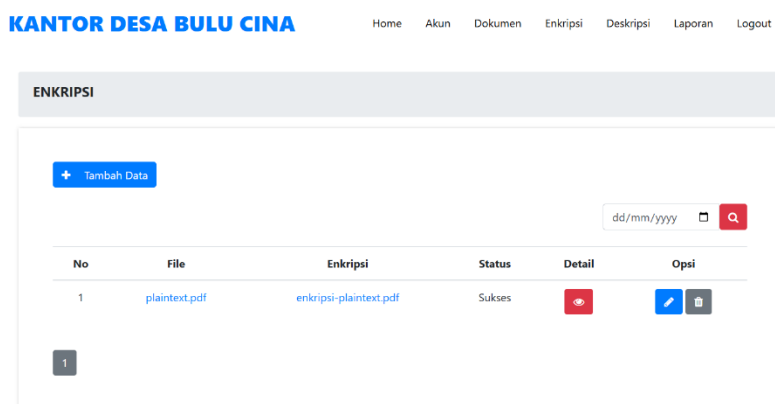


Gambar 6. Tampilan Dokumen

Tampilan Menu Dokumen merupakan fitur eksklusif yang hanya dapat diakses oleh Admin untuk mengelola berbagai dokumen dalam format PDF. Menu ini berfungsi sebagai repositori digital yang memungkinkan Admin menyimpan, mengatur, dan memelihara dokumen-dokumen penting secara terpusat. Dalam menu ini, terdapat beberapa fitur utama, yaitu Tambah Data (untuk mengunggah dokumen baru ke sistem), Ubah (untuk memperbarui atau mengedit informasi dokumen yang sudah tersimpan), dan Hapus (untuk menghapus dokumen yang tidak diperlukan lagi). Setiap dokumen yang diunggah dapat dikategorikan atau diberi label untuk memudahkan pencarian dan pengelolaan.

#### 5. Tampilan Enkripsi

Tampilan proses enkripsi pada sistem terlihat pada gambar berikut :

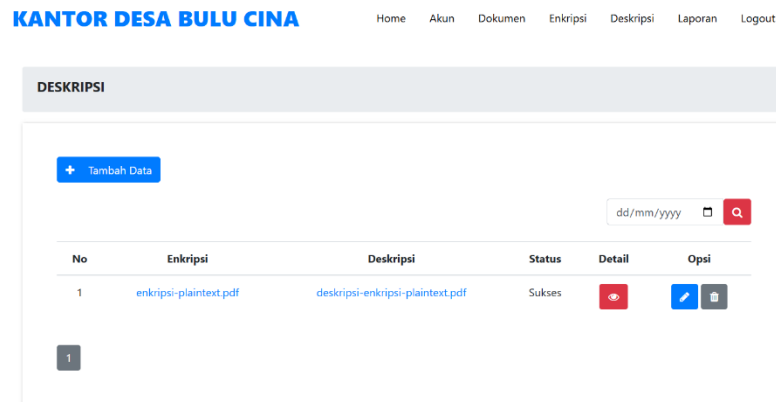


Gambar 7. Tampilan Enkripsi

Tampilan Menu Enkripsi merupakan fitur khusus yang hanya dapat diakses oleh Admin untuk melakukan proses pengamanan dokumen melalui teknik enkripsi. Menu ini berfungsi untuk mengubah dokumen atau data penting menjadi bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang, sehingga kerahasiaan informasi tetap terjaga. Dalam menu ini, Admin dapat menggunakan beberapa opsi utama, yaitu Tambah Data (untuk memilih dokumen yang akan dienkripsi), Ubah (untuk memodifikasi pengaturan enkripsi atau dokumen yang sudah diproses), dan Hapus (untuk menghapus data enkripsi yang sudah tidak diperlukan). Proses enkripsi biasanya melibatkan algoritma keamanan CBC, yang memastikan bahwa hanya pihak yang memiliki kunci dekripsi yang dapat mengakses dokumen asli.

#### 6. Tampilan Deskripsi

Tampilan proses deskripsi pada sistem terlihat pada gambar berikut :



Gambar 8. Tampilan Deskripsi

Tampilan Menu Deskripsi merupakan fitur khusus yang hanya dapat diakses oleh Admin untuk melakukan proses dekripsi dokumen yang sebelumnya telah dienkripsi. Menu ini berfungsi untuk mengembalikan dokumen terenkripsi ke bentuk aslinya yang dapat dibaca, menggunakan kunci dekripsi yang sesuai. Dalam menu ini, Admin dapat menemukan beberapa opsi utama, yaitu Tambah Data (untuk memilih dokumen terenkripsi yang akan dideskripsi), Ubah (untuk memperbarui pengaturan dekripsi atau dokumen yang telah diproses), dan Hapus (untuk menghapus hasil dekripsi yang sudah tidak diperlukan). Proses dekripsi ini sangat penting untuk mengamankan akses informasi, memastikan bahwa hanya Admin yang berwenang dapat membuka dan melihat isi dokumen asli.

#### 7. Tampilan Laporan

Tampilan laporan pada sistem terlihat pada gambar berikut :

**KANTOR DESA BULU CINA** Home Akun Dokumen Enkripsi Deskripsi Laporan Logout

**LAPORAN**

dd/mm/yyyy s/d dd/mm/yyyy 🔍

| No | Tanggal    | File                          | Enkripsi                               | Deskripsi                                        | Ukuran   | Keterangan       | Status |
|----|------------|-------------------------------|----------------------------------------|--------------------------------------------------|----------|------------------|--------|
| 1  | 2025-06-21 | <a href="#">plaintext.pdf</a> | <a href="#">enkripsi-plaintext.pdf</a> | <a href="#">deskripsi-enkripsi-plaintext.pdf</a> | 46.64 KB | sampel plaintext | Sukses |

1

Gambar 9. Tampilan Laporan

Tampilan Menu Laporan merupakan fitur yang dapat diakses secara eksklusif oleh Admin dan Pimpinan untuk mengelola serta mencetak dokumen laporan secara sistematis. Menu ini menyediakan fungsi untuk menampilkan berbagai laporan kegiatan atau dokumen penting yang dapat difilter berdasarkan periode waktu tertentu.

#### 4. KESIMPULAN

1. Metode Cipher Block Chaining (CBC) mampu meningkatkan keamanan e-document dengan cara mengacak isi dokumen sehingga tidak dapat dibaca langsung oleh pihak yang tidak berwenang.
2. Hanya pihak yang memiliki kunci enkripsi dan Initialization Vector (IV) yang sah yang dapat membuka dan membaca isi dokumen, hal ini sangat membantu mencegah kebocoran data di lingkungan Kantor Kepala Desa Bulu Cina, karena IV berperan penting dalam membedakan hasil enkripsi meskipun isi dokumen sama.
3. Sistem yang dirancang menggunakan PHP dan MySQL cukup ringan dan praktis, serta dapat diintegrasikan ke dalam sistem manajemen dokumen yang sudah ada atau dikembangkan.

#### UCAPAN TERIMA KASIH

Sebagai penutup, penulis mengucapkan terima kasih kepada Universitas Potensi Utama yang telah memberikan kesempatan dan dukungan dalam penyelesaian Karya Tulis Ilmiah (KTI) ini.

#### REFERENSI

- [1] Putri, A. C., & Doni, R. (2024). Sistem Informasi Pencarian Lokasi Jasa Grooming Kucing Peliharaan Berbasis Android. *Jurnal Info Digit (JID)*, 2(1), 130-142.
- [2] Rahmad, I. F., h Ekadiansya, E., Doni, R., & Akbar, M. R. (2023). PKM MEMBUAT JAM DIGITAL DAN PESAN BERJALAN DENGAN LED DOT MATRIX DI SEKOLAH PAB 8 SAMPALI. *UNES Journal of Community Service*, 8(2), 058-066.

- [3] Wahyuni, S., & Doni, R. (2024). Penerapan Augmented Reality Sebagai Metode Jenis-Jenis Gunung Di Sumatera Utara Menggunakan Metode Marker Based Tracking Berbasis Android. *Jurnal Info Digit (JID)*, 2(2), 472-484.
- [4] Edi Kalsid, & Henri Septanto. (2023). RANCANG BANGUN APLIKASI E-DOCUMENT SEBAGAI MEDIA PENDISTRIBUSIAN PURCHASE ORDER DAN BERBASIS WEB PADA PT. IRC INOAC PENYIMPANAN DATA DIGITAL. *Jurnal Informatika Dan Teknologi Komputer (JITEK)*, 3(2), 146–154. <https://doi.org/10.55606/jitek.v3i2.1844>.
- [5] Situmorang, Y. B., & Tanti, L. (2023). Aplikasi Keamanan Group Chat Menggunakan Kombinasi Metode RSA dan ELGAMAL. *Jurnal Info Digit (JID)*, 1(2), 450-460.
- [6] Agustawan, T., & Nasution, M. I. A. (2025). Penerapan Algoritma Vigenere Cipher Dan Aes Untuk Keamanan Biodata Siswa Baru Di SMK Tarbiyah Islamiyah. *Jurnal Info Digit (JID)*, 3(2), 682-694.
- [7] Hadi, S., & Alfina, O. (2025). Rancang Bangun Aplikasi Keamanan Data File Inventaris Dengan Menggunakan Cloud Storage Dan Algoritma Camellia (Studi Kasus: Divisi Kesehatan Lingkungan Rsu Imelda Pekerja Indonesia). *Jurnal Info Digit (JID)*, 3(2), 750-765.
- [8] Guloa, T., & Rustam, M. T. (2024). Implementasi Keamanan Data Dana Desa Dengan Metode Railfence Cipher Dan Beaufort Cipher (Studi Kasus Kantor Desa Atauluo). *Jurnal Info Digit (JID)*, 2(1), 75-88.
- [9] Afsari, M., Mulyana, D. I., Damaiyanti, A., & Sa'adah, N. (2022). Implementasi Mode Operasi Kombinasi Cipher Block Chaining dan Metode LSB-1 Pada Pengamanan Data text. *J. Pendidik. Sains dan Komput*, 2(01), 70-82.
- [10] Lubis, A. F. L. F. (2024). Modifikasi Metode Cipher Block Chaining (CBC) Dengan Pembangkit Kunci Mid Square. *Jurnal Ilmu Komputer, Teknologi Dan Informasi*, 2(1), 32-38.
- [11] Siregar, S. (2023). Implementasi Mode Operasi Cipher Block Chaining (CBC) Untuk Mengoptimalkan Algoritma Affine Cipher Dalam Pengamanan Data. *Bulletin of Information System Research*, 1(3), 99-109.
- [12] Afsari, M., Mulyana, D. I., Damaiyanti, A., & Sa'adah, N. (2022). Implementasi Mode Operasi Kombinasi Cipher Block Chaining dan Metode LSB-1 Pada Pengamanan Data text. *J. Pendidik. Sains dan Komput*, 2(01), 70-82.
- [13] Purba, N. H. (2022). Kombinasi Algoritma Cipher Block Chaining dan Triangle Chain Cipher dalam Penyandian File Text. *Bulletin of Computer Science Research*, 2(2), 47-52.
- [14] Sinurat, S., & Pasaribu, M. (2021). Text Encoding Using Cipher Block Chaining Algorithm. *Jurnal Info Sains: Informatika dan Sains*, 11(2), 13-17.
- [15] Somantri, A. A., & Maulana, N. (2022, August). Design and Build Zakat Website Application Based on QR Code Using Cipher Block Chaining Algorithm. In *UNISSET 2021: Proceedings of the 2nd Universitas Kuningan International Conference on System, Engineering, and Technology, UNISSET 2021, 2 December 2021, Kuningan, West Java, Indonesia* (p. 354). European Alliance for Innovation.

- [16] Manullang, S. (2023). Implementasi Kriptografi Pengamanan Data File Dokumen Menggunakan Algoritma Advanced Encryption Standard Mode Chiper Block Chaining. *Jurnal Nasional Teknologi Komputer*, 3(2), 87-95.