

# KOMBINASI CAESAR CIPHER DAN REVERSE CIPHER BERDASARKAN CIPHER BLOCK CHAINING

*(Combination of Caesar Cipher and Reverse Cipher Based on Cipher Block Chaining)*

**Maulidyah Lailatun Najah, Kiswara Agung Santoso**

Jurusan Matematika, Fakultas MIPA, Universitas Jember

Jl. Kalimantan 37, Jember 68121

Email : [maulidyahlailatun01@gmail.com](mailto:maulidyahlailatun01@gmail.com), [kiswaras@gmail.com](mailto:kiswaras@gmail.com)

**Abstract.** Communication in the current era of globalization is very developed. Many applications that can be used to facilitate communication. However, because of this convenience, the security of the information contained in it will be more easily hacked by irresponsible people. Cryptography is the science or art for security message. In cryptography there are two important processes, namely encryption and decryption. The sender's job is to encrypt the message and the receiver's job is to decrypt the message. The key used for this cryptographic process is the Cipher Block Chaining (CBC) operation mode. CBC mode is a very simple operation mode, so additional techniques are needed to make it more secure. The plaintext will be replaced with new plaintext resulting from a combination of Caesar Cipher and Reverse Cipher techniques. The results obtained indicate that the application of plaintext modifications to CBC can improve message security because the keys used are increasingly complex.

**Keywords:** Caesar Cipher, Cipher Block Chaining, Modern Cryptography, Reverse Cipher

**MSC2020 :** 68P25

## A. Pendahuluan

Perkembangan teknologi saat ini membuat komunikasi semakin mudah. Kemudahan komunikasi untuk bertukar pesan dapat berisiko dalam keamanannya. Seseorang dapat mencuri atau memodifikasi pesan dalam proses komunikasi tersebut. Salah satu teknik yang dapat digunakan untuk keamanan pesan adalah kriptografi. Kriptografi dapat mengkodekan suatu pesan, sehingga pesan tersebut tidak bisa dipahami oleh orang yang tidak mengetahui kuncinya.

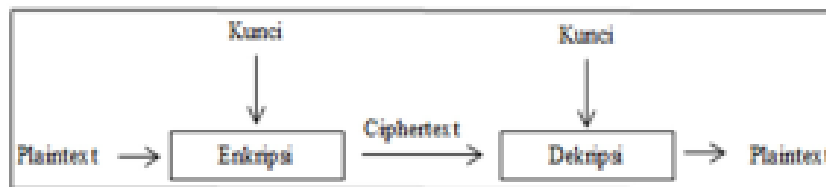
Kriptografi diklasifikasikan menjadi 2 macam, yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik merupakan kriptografi berbasis karakter dengan huruf abjad A-Z. Kriptografi ini memungkinkan pesan diretas lebih mudah karena banyak karakter hanya ada 26. Sehingga, kurang efisien digunakan untuk keamanan pesan. Sedangkan kriptografi modern merupakan kriptografi berbasis kode bit biner (0 dan 1) yang membuat pesan lebih aman dan sulit untuk diretas. Oleh karena itu, kedua

kriptografi tersebut akan dikombinasikan menjadi suatu algoritma yang tingkat keamanannya lebih tinggi.

Algoritma yang diusulkan dalam penelitian ini adalah modifikasi plainteks pada Cipher Block Chaining (CBC). CBC merupakan mode operasi kriptografi modern berbasis blok. Hasil enkripsi blok saat ini dijadikan umpan balik untuk enkripsi blok selanjutnya. Kemudian, blok plaintext dan blok ciphertext hasil enkripsi dioperasikan dengan XOR. Sehingga, setiap block ciphertext pada CBC bergantung pada blok plaintextnya dan seluruh blok plaintext sebelumnya. Agar lebih aman, plainteks akan di proses terlebih dahulu dengan menggunakan teknik Caesar Cipher dan Reverse Cipher. Kedua teknik ini merupakan teknik dasar dalam kriptografi klasik. Dengan mengkombinasikan kedua algoritma tersebut diharapkan dapat meningkatkan keamanan mode operasi CBC.

## B. Metode Penelitian

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan dengan cara mengubahnya ke dalam bentuk yang sulit dipahami [1]. Pesan asli sebelum dikodekan disebut plainteks dan pesan sesudah dikodekan disebut cipherteks. Proses mengubah plainteks menjadi cipherteks disebut enkripsi, dan sebaliknya cipherteks ke plainteks disebut dekripsi. Proses enkripsi dan dekripsi dapat dilihat seperti Gambar 1.



**Gambar 1.** Proses enkripsi dan dekripsi

Kriptografi diklasifikasikan menjadi 2 macam, yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik menggunakan mode berbasis karakter, sedangkan kriptografi modern menggunakan mode berbasis bit biner [6]. Kriptografi modern mempunyai tingkat kesulitan yang lebih kompleks, sehingga menyebabkan kriptanalisis sulit memecahkan cipherteks tanpa mengetahui kuncinya. Adapun jenis kunci dalam kriptografi ada 2, yaitu kunci simetris dan kunci asimetris. Kunci simetris disebut juga privat key, dimana dalam proses enkripsi dan dekripsinya menggunakan kunci yang sama. Sedangkan kunci asimetris disebut juga dengan public key, dimana proses enkripsi dan dekripsinya menggunakan kunci yang berbeda [3].

Algoritma yang diusulkan dalam penelitian adalah modifikasi plainteks pada mode operasi Cipher Block Chaining (CBC). CBC merupakan mode operasi kriptografi modern berbasis blok. Proses mode CBC diawali dengan menetapkan nilai awal *IV* dengan panjang *n* [4]. Kemudian, tetapkan  $c_0 = IV$ . Secara matematis, proses

enkripsi blok untuk  $c_i$  dan dekripsi blok untuk  $p_i$  didefinisikan oleh Persamaan (1) dan Persamaan (2).

$$c_i = E_k(c_{i-1} \oplus p_i) \text{ untuk } 1 \leq i \leq l \quad (1)$$

$$p_i = D_k(c_i) \oplus c_{i-1} \text{ untuk } 1 \leq i \leq l \quad (2)$$

Dalam CBC, setiap blok cipherteks tergantung pada plainteksnya dan juga semua blok cipherteks sebelumnya [2]. Karena kunci enkripsi dan dekripsinya sangat sederhana, maka perlu teknik tambahan untuk meningkatkan keamanan pesan.

Teknik yang akan digunakan adalah Caesar Cipher dan Reverse Cipher. Kedua teknik tersebut merupakan teknik dasar dalam kriptografi klasik. Caesar cipher biasa disebut dengan Shift Cipher, karena tekniknya hanya dengan menggeser karakter sebesar kunci yang dipilih [6]. Misalkan diketahui plainteks 'MATEMATIKA' dengan kunci=3. Artinya, setiap karakter akan digeser sebanyak 3 kali sesuai urutan huruf alphabet.

#### **Proses Enkripsi**

Plainteks : MATEMATIKA  
Cipherteks : PDWHPDWLND

#### **Proses Dekripsi**

Cipherteks : PDWHPDWLND  
Plainteks : MATEMATIKA

Sedangkan Reverse Cipher merupakan teknik yang sangat sederhana, karena hanya mengubah plainteks dengan menuliskan setiap karakter dengan cara terbalik [5]. Kedua teknik di atas akan digunakan untuk mengacak bit dalam plainteks. Setelah plainteks baru terbetuk, maka mode operasi CBC dapat dilakukan.

Berikut adalah algoritma modifikasi CBC :

#### **Proses Enkripsi**

1. Bagi plainteks menjadi blok-blok berukuran 4 bit, atau dalam notasi heksadesimal (HEX).
2. Membentuk plainteks baru. Untuk setiap blok :
  - Terapkan pola Reverse Cipher, yaitu dengan membaca bit secara terbalik.
  - Terapkan pola Caesar Cipher, yaitu dengan menggeser bit sebanyak dua kali.
3. Mode operasi CBC dengan kunci.

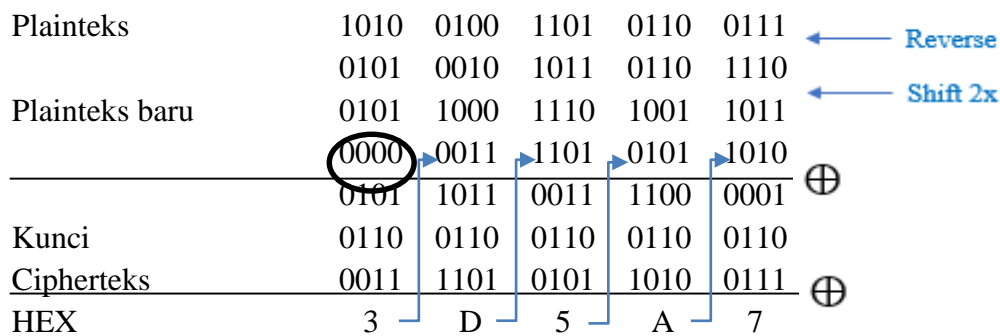
**Proses Dekripsi**

1. Bagi cipherteks mejadi blok-blok berukuran 4 bit, atau dalam notasi heksadesimal (HEX).
2. Mode operasi CBC dengan kunci.
3. Membentuk plainteks baru. Untuk setiap blok :
  - Terapkan pola Caesar Cipher, yaitu dengan menggeser bit sebanyak dua kali
  - Terapkan pola Reverse Cipher, yaitu dengan membaca bit secara terbalik

**C. Pembahasan**

Algoritma yang diusulkan akan diterapkan pada plainteks dengan perhitungan manual. Misalkan plainteksnya adalah : 10100100110101100111. Setelah itu bagi plainteks menjadi blok-blok berukuran 4 bit. Dalam HEX plainteks dibaca A4D67. Untuk membangun plainteks baru, setiap blok dalam plainteks akan dimodifikasi dengan teknik Caesar Cipher Dan Reverse Cipher. Pola pertama yaitu dengan membaca setiap bit dalam blok secara terbalik. Misalkan 1010 menjadi 0101, 0100 menjadi 0010, dan seterusnya. Kemudian, hasil-hsil tersebut dioperasikan dengan pola kedua yaitu menggeser bit sebanyak dua kali dalam setiap blok. Karena plainteks baru sudah terbentuk, maka mode operasi Cipher Block Chaining (CBC) dapat dilakukan. Tetapkan  $IV = 0000$  untuk enkripsi blok pertama dan kunci 0110. Proses enkripsi dirangkum secara sistematis di bawah ini agar lebih mudah dipahami.

**Proses Enkripsi**



Sedangkan untuk proses dekripsi diawali dengan pembagian cipherteks menjadi blok-blok berukuran 4 atau dalam notasi HEX adalah 3D5A7. Kemudian, cipherteks dioperasikan dengan mode CBC. Setelah itu, hasil-hasil bit dalam setiap blok di geser dua kali dan di reverse. Untuk mempermudah perhitungan, dapat dilihat proses dekripsi di bawah ini.

### Proses Dekripsi

|            |       |      |      |      |      |            |
|------------|-------|------|------|------|------|------------|
| Cipherteks | 0011  | 1101 | 0101 | 1010 | 0111 |            |
| Kunci      | 0110  | 0110 | 0110 | 0110 | 0110 |            |
|            | <hr/> |      |      |      |      | ⊕          |
|            | 0101  | 1011 | 0011 | 1100 | 0001 |            |
|            | <hr/> |      |      |      |      | ⊕          |
|            | 0000  | 0011 | 1101 | 0101 | 1010 |            |
|            | <hr/> |      |      |      |      | ⊕          |
|            | 0101  | 1000 | 1110 | 1001 | 1011 |            |
|            | <hr/> |      |      |      |      | ← Shift 2x |
|            | 0101  | 0010 | 1011 | 0110 | 1110 |            |
| Plainteks  | 1010  | 0100 | 1101 | 0110 | 0111 | ← Reverse  |
| HEX        | A     | 4    | D    | 6    | 7    |            |

## D. Kesimpulan

Berdasarkan hasil di atas dapat disimpulkan bahwa modifikasi plainteks dengan teknik Caesar Cipher Dan Reverse Cipher dapat digunakan untuk mode operasi Cipher Block Chaining (CBC). Plainteks A4D67 dimodifikasi dan enkripsi menghasilkan cipherteks 3D5A7. Sebaliknya, proses dekripsi 3D5A7 menghasilkan A4D67. Dengan adanya modifikasi ini, membuat kriptanalisis semakin kesulitan untuk memecahkan kuncinya. Sehingga, dapat meningkatkan keamanan pesan.

## Daftar Pustaka

- [1] Katz.J, Lindell.Y, (2015), *Introduction to Modern Cryptography (Second Edition)*, New York: CRC Press.
- [2] Knudsen.L,R, Robshaw.M,J,B, (2011), *The Block Cipher Companion*, New York: Springer.
- [3] Munir.R, (2006), *Kriptografi*, Bandung: Departemen Informatika ITB.
- [4] Kumar.N, Poovarasana, Harish.S, Jagadish, (2017), A comparative analysis of symmetric and asymmetric key cryptography, *IRJET*, Vol.4, PP: 287-290.
- [5] Santoso.A.R, Riski.A, Kamsyakawuni.A, (2018), Implementasi algoritma reversed vigenere encryption pada pengamanan citra. *Berkala Sainstek*, Vol.7(2), ISSN: 2339-0069, PP: 61-66.
- [6] Sumandri, (2017), Studi model algoritma kriptografi klasik dan modern. *Seminar Matematika dan Pendidikan Matematika UNY*, PP: 265-272.

