**DOI: http://dx.doi.org/10.22441/fifo.2020.v12i1.002**

# Optimasi Keamanan Informasi Menggunakan Algoritma Advanced Encryption Standard (AES) Mode Chiper Block Chaining (CBC)

**Achmad Nugrahantoro[1], Abdul Fadlil[2], Imam Riadi[3]**
[1]*Program Studi Magister Teknik Informatika, Universitas Ahmad Dahlan*
[2]*Program Studi Teknik Elektro, Universitas Ahmad Dahlan*
[3]*Program Studi Sistem Informasi, Universitas Ahmad Dahlan*
Jl. Prof. Dr. Soepomo, S,H, Janturan, Warungboto, Umbulharjo, Yogyakarta
E-mail : [1]nugrahantoro0@gmail.com, [2]fadlil@mti.uad.ac.id, [3]imam.riadi@is.uad.ac.id

**Abstract**

*Information comes from a collection of data obtained from various sources that have been processed. An information can help in decision making, so it is considered to have a high effectiveness value for the recipient of the information. Information exchange that utilizes public media internet services is widely used, so the validity of information must be done security from unauthorized attacks. One of them uses cryptography. AES is a method used by the National Institute of Standards and Technology (NIST) as a standard for the United States Federal encryption algorithm. Creativity in cryptographic modification can increase the strength of an attack. This study uses AES 128, 192, and 256 bit CBC mode algorithms by conducting trials at the level of encryption, decryption and the appearance of character frequencies. Encryption test results obtained an average speed of 128 bit blocks, namely 14.2 ms, 256 bits 13.2 ms and 192 bits 11.5 ms. While the decryption test results obtained an average speed of 128 bit blocks, namely 13.2 ms, 192 bits 14 ms and 256 bits 16.5 ms. The pattern of occurrence of the average frequency generated by 9%, by accepting symbols and numbers using this algorithm has little to solve by reading the characters display. The validation test produces a value of 100% where the functionality testing shows the expected results.*
***Keyword**: Security Information, AES, CBC, AES Mode CBC*

**Abstrak**

*Informasi berasal dari sekumpulan data yang didapatkan dari berbagai sumber yang telah diolah. Sebuah informasi bisa membantu dalam pengambilan keputusan, sehingga dianggap memiliki nilai efektivitas tinggi bagi penerima informasi. Pertukaran informasi yang memanfaatkan layanan publik media internet marak digunakan, maka keabsahan informasi harus dilakukan keamanan dari serangan pihak tidak berwenang. Salah satunya menggunakan kriptografi. AES adalah metode yang dimanfaatkan National Institute of Standards and Technology (NIST) sebagai standar algoritma enkripsi Federal Amerika Serikat. Kreativitas dalam modifikasi kriptografi bisa meningkatkan kekuatan dari serangan. Penelitian ini menggunakan algoritma AES 128, 192, dan 256 bit mode CBC dengan melakukan uji coba pengujian pada tingkat kecepatan proses enkripsi, dekripsi dan kemunculan frekuensi karakter. Hasil uji coba pengujian enkripsi didapatkan tingkat kecepatan rata-rata blok 128 bit yaitu 14,2 ms, 256 bit 13,2 ms dan 192 bit 11,5 ms. Sedangkan hasil uji coba dekripsi didapatkan tingkat kecepatan rata-rata blok 128 bit yaitu 13,2 ms, 192 bit 14 ms dan 256 bit 16,5 ms. Pola kemunculan frekuensi rata-rata dihasilkan 9%, dengan menerima simbol dan angka menunjukan algoritma ini memiliki kemungkinan kecil dapat dipecahkan melalui pembacaan kemunculan karakternya. Pengujian validasi menghasilkan nilai 100% dimana pengujian fungsionalitas menunjukkan hasil yang sesuai diharapkan.*
**Kata Kunci:** *Keamanan Informasi, AES, CBC, AES Mode CBC*

**DOI: http://dx.doi.org/10.22441/fifo.2020.v12i1.002**

## I. PENDAHULUAN

Perkembangan web kini sudah dirasakan oleh semua kalangan, baik kalangan bisnis, pendidikan, peneliti hingga perorangan [1][2][3]. Kinerja dari web menjadi bagian dari layanan yang diakses melalui jaringan internet untuk memperoleh sekumpulan informasi [4]. Informasi merupakan sekumpulan data yang telah diolah dari satu atau beberapa sumber [5], sehingga dapat mendukung dalam pengambilan keputusan [6] dan berguna bagi penerimanya [7]. Nilai sebuah informasi pada sebuah web bisa memiliki nilai efektivitas tinggi [8], maka pertukaran informasi yang memanfaatkan internet yang bersifat publik perlu dilakukan upaya pengamanan dalam mempertahankan isi informasi [9]. Salah satunya pertukaran *Application Programming Interface* (API) dimana didalamnya tersimpan informasi. Transmisi isi informasi pada API ini biasanya bersifat rahasia sehingga harus selalu dalam keadaan aman.

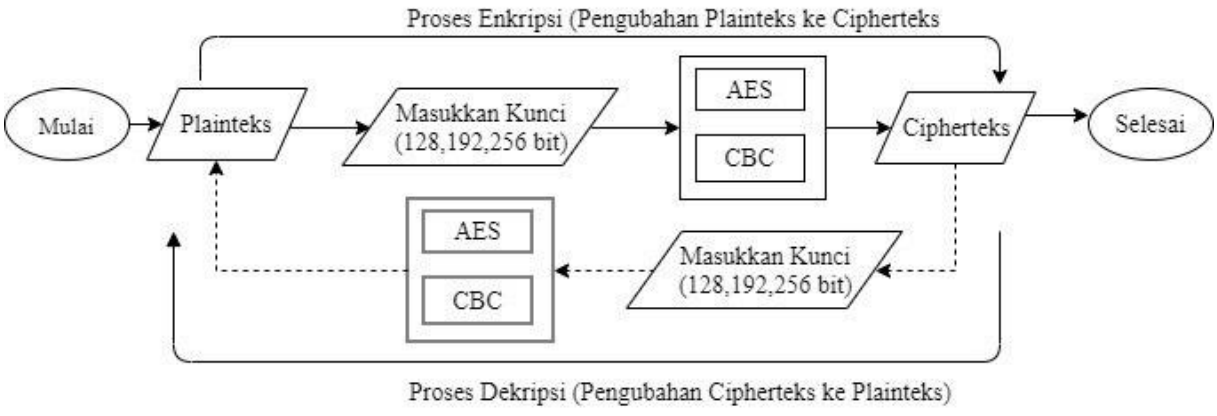
Keabsahan isi informasi perlu dilakukan pencegahan dari pengakses yang tidak berwenang [10]. Upaya tersebut untuk menjaga beberapa aspek keamanan informasi yang perlu dilindungi antara lain; *privacy* untuk menjaga keutuhan isi informasi [11], *confidentiality*, *availability* serta *access control* dengan menyediakan ketersediaan dengan memperhatikan penyadapan [12]. Aspek keamanan lain informasi perlu dijaga agar konsisten [13] dengan autentikasi pencocokan hak akses yang menandakan informasi diakses oleh pemilik [14][15]. Upaya perlindungan informasi pesan dari penyerang ketika terjadi interaksi pertukaran data bisa menerapkan kriptografi. Kriptografi adalah seni pengubahan isi informasi dari *plaintext* menjadi *ciphertext* yang bertujuan menjaga aspek-aspek keamanan pada pesan tersebut [16][17]. Pengamanan pada web tidak hanya pada kerahasiaan metodenya, namun kreativitas dalam modifikasi metode dalam meningkatkan kekuatan dari serangan [18][19].

Terdapat beberapa penelitian penggunaan kriptografi, penelitian yang dilakukan oleh [20] memanfaatkan kriptografi *Advanced Encryption Standard* (AES) dengan mode Cipher Blok Chaining (CBC) mampu meningkatkan penggunaannya dibandingkan metode tradisional dan metode tersebut pada penelitian [21] dapat mengamankan informasi. Namun penelitian [20][21] menggunakan kunci 128 bit. Penggunaan AES digunakan dalam penelitian [22] membuat sistem tahan dari *replay attack* namun perlu dikombinasikan dan penelitian serupa [23] masih menyimpan informasi hanya dalam bentuk *word*. Algoritma AES yang dikombinasi dengan Vigenere pernah dimanfaatkan dalam pengamanan database pada penelitian [24], namun proses belum mampu mendeteksi tabel terenkripsi dan dekripsi. Pengamanan pesan dengan CBC modifikasi terbukti mampu mengamankan pesan dalam bentuk *ciphertext* proses enkripsi dan mengembalikan pesan semula [9]

Maka penelitian ini akan digunakan dalam mengamankan informasi yang memanfaatkan algoritma AES 128 bit, 192 bit dan 256 bit mode *chaining* CBC sehingga penggunaan karakter pada penggunaan bit-bit blok tersebut membuat ketahanan algoritma lebih baik. Penggunaan bit pada AES dengan *Add Round Key* akan berpengaruh pada setiap putaran yang lebih banyak. Penyimpanan informasi akan diarahkan dalam bentuk data generator pengamanan informasi pesan, dimana isi informasi akan diterima dalam bentuk enkripsi bisa dibaca dengan kunci yang cocok.

## II. METODOLOGI PENELITIAN

Pada penelitian ini memanfaatkan modifikasi AES menggunakan rantai proses yang dipengaruhi tiap proses enkripsi maupun dekripsi sebelumnya. Penggambaran alur kerja penelitian tertera pada Gambar 1.




Gambar 1. Alur Kerja Enkripsi dan Dekripsi AES CBC

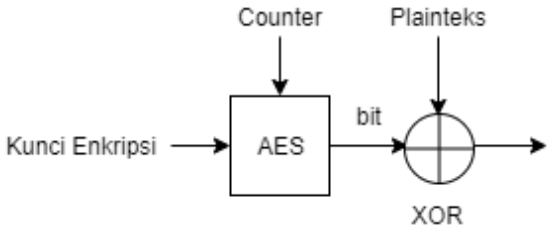
Pada Gambar 1. proses enkripsi dilakukan dengan memasukkan *plaintext* kemudian penggunaan kunci dengan penyesuaian bit. Proses pengamanan informasi menggunakan AES dan CBC kemudian jika sudah diproses akan muncul *ciphertext*. Sedangkan proses dekripsi maka akan mengembalikan pesan *ciphertext* ke dalam bentuk pesan informasi semula.

**Algoritma Advance Encryption Standard (AES)**

Kinerja dari Algoritma AES sudah banyak digunakan oleh *National Institute of Standards and Technology* (NIST) sebagai standar algoritma enkripsi Federal Amerika Serikat [25][26][27]. AES merupakan pengganti dari kriptografi algoritma *Data Encryption Standard* (DES), karena algoritma ini memakai blok 56 bit yang dianggap sudah tidak aman [22][28]. Algoritma AES termasuk pada algoritma kriptografi kunci simetri dengan *single key* yang menggunakan kunci yang sama ketika proses enkripsi dan dekripsi [29]. Sehingga mampu meningkatkan pengoperasian sistem secara *real time* dan cukup cepat. Kini AES mendukung beberapa ukuran blok kunci dalam menentukan proses komputasi ketika enkripsi dan dekripsi, perbandingan tersedia pada Tabel 1.

Tabel 1. Perbandingan Penggunaan Bit blok pada AES

| Bit Blok | Nb *(Number of bit)* | Nk *(Number of key)* | | Nr *(Number of rounds)* |
|---|---|---|---|---|
| | | Row | Column | |
| 128 | 4 | 16 | 4 | 10 |
| 192 | 4 | 24 | 6 | 12 |
| 256 | 4 | 32 | 8 | 14 |

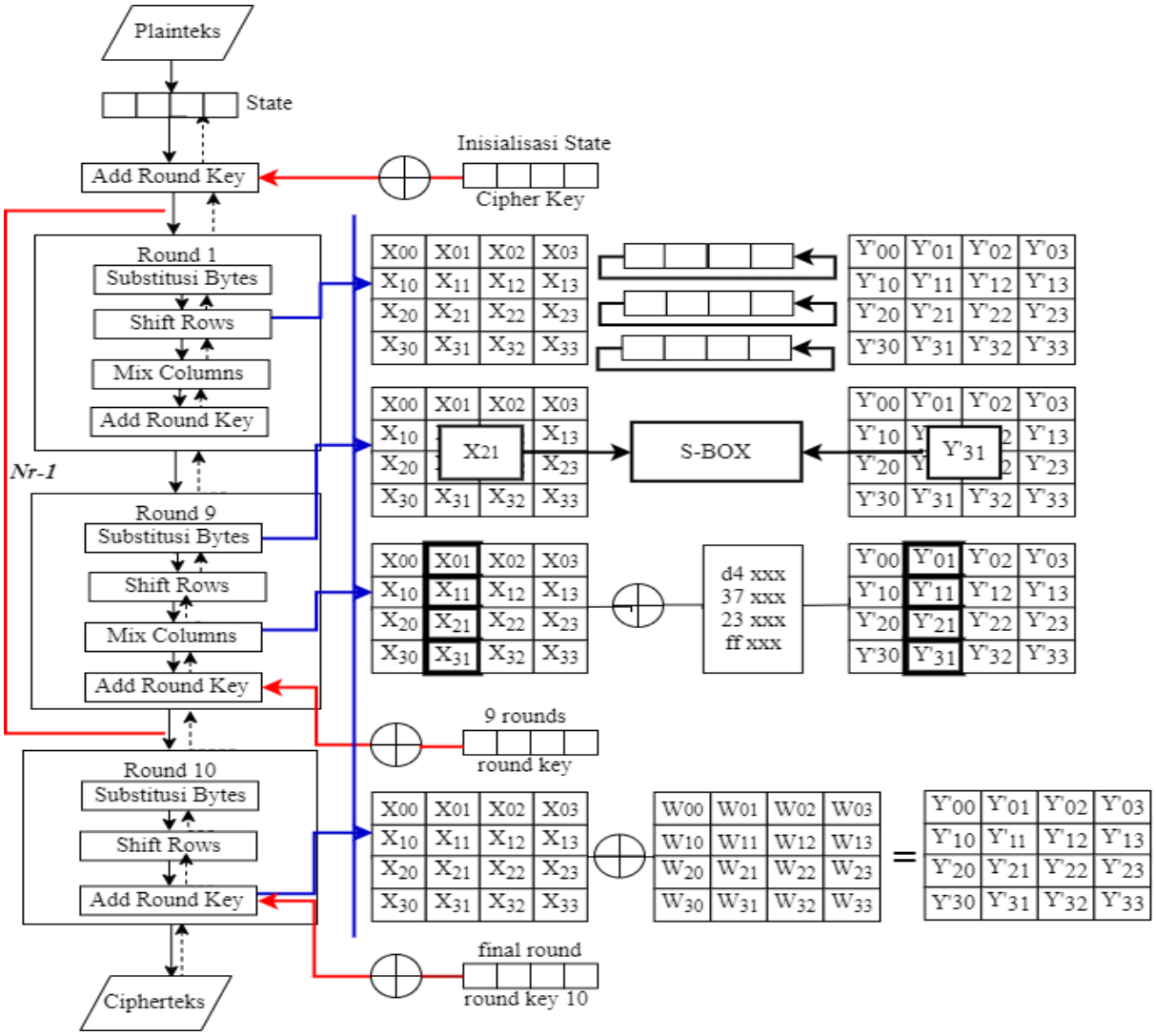



Gambar 2. Alur Kinerja Kriptografi AES

Penjelasan dari Gambar 2. proses enkripsi pada AES menerima teks sehingga diproses pada algoritma menyesuaikan dengan bit yang digunakan, kemudian hasil tiap enkripsi pada *plaintext* melakukan XOR antar *state* sehingga di menghasilkan pesan baru tak bermakna. Secara umum proses algoritma AES tertera pada Gambar 3.

Penggambaran algoritma AES pada Gambar 3. Sebagai berikut :

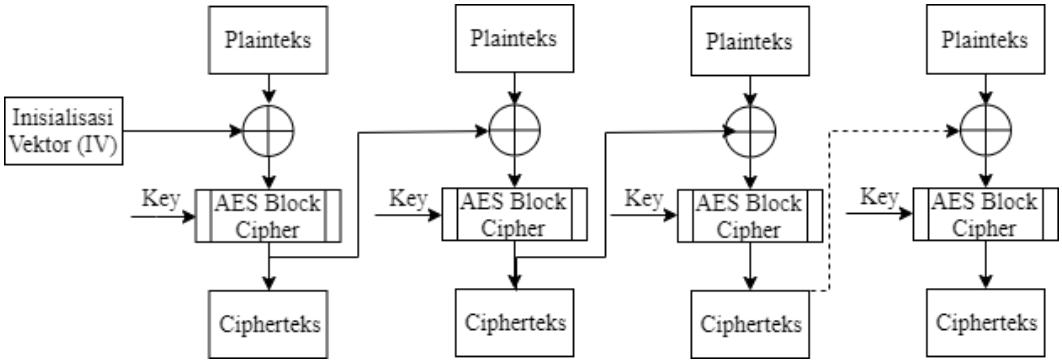
1) Add Round Key : *initialization* state dengan melakukan XOR, dengan mengoperasikan *array* dengan *row* 16 dan *column* 4, dimana hasil operasi ini menghasilkan *cipher key*.
2) Round 1 dan Round 9 : Putaran dengan perhitungan *Number of Round* (*Nr)*-1 kali, dimana tiap putaran tersebut memproses 4 tahapan pada AES, yaitu :
   a. Tahap *Sub Bytes substitution* dengan tabel (*S-Box*).
   b. Tahap *Shift Rows* melakukan pergeseran pada baris *array*, menyesuaikan dengan nilai baris.
   c. Tahap *Mix Columns* melakukan perkalian dengan kolom tiap *array state.*
   d. Tahap *Add Round Key* akan melakukan XOR antara *state* yang paling terbaru sampai mencapai akhir.
3) Hingga pada tahap *Final Round* kembali ke proses *Substitution Bytes*, *Shift Rows* dan *Add Round Key* terakhir tanpa melakukan *Mix Column* hingga mencapai putaran ke -10.




Gambar 3. Algoritma Metode AES pada 128 bit

**Modifikasi Advance Encryption Standard (AES) mode Cipher Block Cipher (CBC)**

Kriptografi AES mode CBC menjadi algoritma yang melibatkan nilai Inisialisasi Vektor (IV) pada blok cipher [30]. IV berdasarkan ukuran pada setiap blok masukan *plaintext*-nya. Pada rangkaian bit pada *plaintext* akan dibagi menjadi blok yang sama hingga memiliki ukuran yang serupa. Kinerja dari AES sesuai pada Gambar 3. kemudian diadopsi dengan mode *block chaining* dalam menghasilkan *ciphertext*.




Gambar 4. Algoritma Enkripsi AES mode CBC

Gambar 4. menjelaskan jika cara kerja dari modifikasi AES dengan CBC bekerja secara sekuensial, dimana blok data pertama mempengaruhi hasil blok yang kedua dan seterusnya. Awal pengoperasian peneliti memanfaatkan nilai pada data IV di blok dengan awal hasil AES Blok Cipher. Kinerja dari blok tersebut memanfaatkan AES dengan 128 bit yaitu dengan penggunaan kunci 16 karakter, 192 bit untuk kunci 24 karakter dan 256 bit menggunakan kunci 32 karakter. Fungsi matematis persamaan sebagai berikut:

$$C_0 = E_K(P_0 \oplus IV) \quad (1)$$
$$C_i = E_{Ki}(Pi \oplus C_{i-1}) \quad (2)$$
$$Ci+1 = EKx(Pi+1 \oplus Ci-1) \quad (3)$$
$$C_n = E_{Ky}(P_n \oplus C_{i-1}) \quad (4)$$

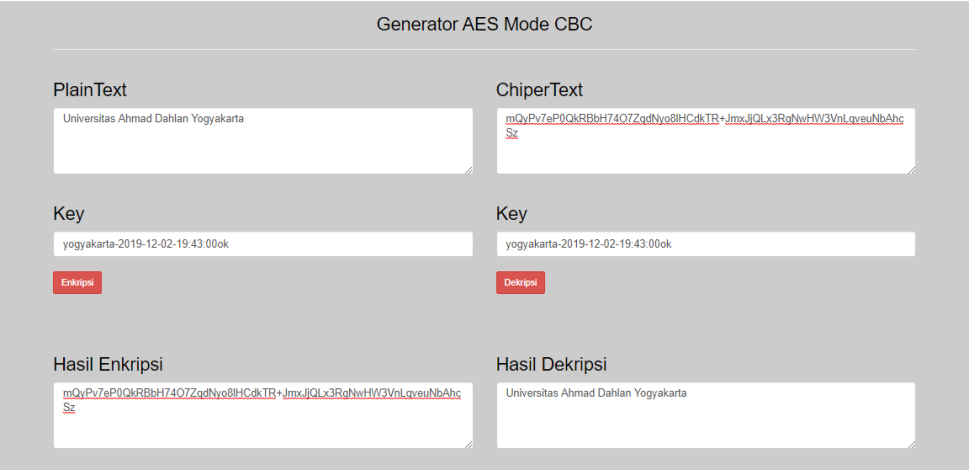
Dimana, pengoperasian enkripsi pada fungsi persamaan (1)(2)(3)(4) nilai *EKx* nilai *x,y* mewakili indek dari *plaintext* dari nilai 1 sampai *n* di nilai *EKx.* Nilai pada IV di inisiasi sesuai bit blok yang digunakan. Sedangkan untuk fungsi matematis persamaan proses dekripsi AES CBC modifikasi sebagai berikut :

$$P_0 = D_K(C_0 \oplus IV) \quad (5)$$
$$P_i = D_{Ki}(C_i \oplus C_{i-1}) \quad (6)$$
$$Pi+1 = DKx(Ci+1 \oplus Ci-1) \quad (7)$$
$$P_n = D_{Ky}(C_n \oplus C_{i-1}) \quad (8)$$

Pengoperasian pengembalian *ciphertext* ke *plaintext* atau proses dekripsi pada rumus persamaan (5)(6)(7)(8) nilai *DKx* nilai *x,y* mewakili indek dari enkripsi dari nilai 1 sampai *n* di nilai *DKx.*

## III. HASIL DAN PEMBAHASAN

Implementasi pengamanan informasi dengan kriptografi modifikasi AES mode CBC digunakan untuk generator dengan desain antar muka pada Gambar 5. Generator pada sistem ini terdiri dari masukan *Plaintext* kemudian user dapat memasukan *key* (kunci) hingga menampilkan hasil enkripsi. Pengembalian pesan selanjutnya terdapat pada menu *Ciphertext* kemudian masukan *key* (kunci) maka pesan tersebut dapat kembali seperti semula.




Gambar 5. Desain Antar Muka Kriptografi Modifikasi AES mode CBC

**Pengujian Waktu Eksekusi Enkripsi dan Dekripsi**

Pengujian eksekusi dilakukan dengan Postman [31] dalam menguji kecepatan waktu eksekusinya ketika proses enkripsi dan dekripsi. Fungsi utama dari Postman adalah untuk melakukan *testing* pada ketahanan enkripsi yang buat pada *Application Programming Interface* (API). Dimana API tersebut menyimpan data-data berupa *code* yang memiliki informasi [32]. Pengujian ini dilakukan untuk mengetahui tingkat kecepatan dalam waktu enkripsi dan dekripsi, seperti tertera pada Tabel 2. Fungsi enkripsi tidak akan berhasil jika tidak adanya kecocokan kunci pada bit blok yang sesuai.

**DOI: http://dx.doi.org/10.22441/fifo.2020.v12i1.002**

Tabel 2. Hasil Uji Coba Pengujian Waktu Eksekusi Enkripsi dan Ukuran

| No. | Panjang Karakter Plaintext | Panjang Karakter Ciphertext | Kecepatan (ms) | | | Ukuran (Byte) | | |
|---|---|---|---|---|---|---|---|---|
| | | | 128 bit | 192 bit | 256 bit | 128 bit | 192 bit | 256 bit |
| 1. | 5 | 24 | 13 | 11 | 10 | 271 | 271 | 273 |
| 2. | 24 | 44 | 12 | 12 | 10 | 292 | 292 | 292 |
| 3. | 45 | 64 | 17 | 11 | 14 | 312 | 312 | 313 |
| 4. | 5 | 24 | 21 | 10 | 17 | 271 | 271 | 272 |
| 5. | 20 | 44 | 11 | 11 | 10 | 291 | 291 | 292 |
| 6. | 47 | 64 | 11 | 14 | 18 | 311 | 311 | 313 |
| Rata-rata | | | 14,2 | 11,5 | 13,2 | 291,5 | 291,3 | 292,5 |

Hasil uji coba pengujian Tabel 2. didapatkan rata-rata kecepatan proses enkripsi yaitu pada blok 128 bit adalah 14,2 ms, sedangkan blok 192 bit adalah 11,5 ms, dan blok 256 bit adalah 13,2 ms. Dalam segi ukuran hasil dari proses enkripsi pada blok 128 bit mendapatkan rata-rata 291,5 *Byte*, sedangkan blok 192 bit mendapatkan rata-rata 291,3 *Byte*, dan blok 256 bit mendapatkan rata-rata 292,5 *Byte*.

Tabel 3. Fungsi dekripsi tidak akan berhasil jika tidak adanya kecocokan antara *ciphertext* dengan kunci pada bit blok yang sama.

Tabel 3. Hasil Uji Coba Pengujian Waktu Eksekusi Dekripsi dan Ukuran

| No. | Panjang Karakter Plaintext | Panjang Karakter Ciphertext | Kecepatan (ms) | | | Ukuran (Byte) | | |
|---|---|---|---|---|---|---|---|---|
| | | | 128 bit | 192 bit | 256 bit | 128 bit | 192 bit | 256 bit |
| 1. | 5 | 24 | 13 | 19 | 11 | 251 | 251 | 251 |
| 2. | 24 | 44 | 14 | 13 | 17 | 271 | 271 | 271 |
| 3. | 45 | 64 | 17 | 11 | 23 | 292 | 292 | 292 |
| 4. | 5 | 24 | 11 | 13 | 14 | 251 | 251 | 251 |
| 5. | 20 | 44 | 10 | 12 | 14 | 267 | 267 | 267 |
| 6. | 47 | 64 | 19 | 11 | 20 | 294 | 294 | 293 |
| Rata-rata | | | 14 | 13,2 | 16,5 | 271 | 271 | 270,8 |

Hasil uji coba pengujian Tabel 3. didapatkan rata-rata kecepatan proses dekripsi yaitu pada blok 128 bit adalah 14 ms, sedangkan blok 192 bit adalah 13,2 ms, dan blok 256 bit adalah 16,5 ms. Dalam segi ukuran hasil dari proses dekripsi pada blok 128 bit mendapatkan rata-rata 271,5 *Byte*, sedangkan blok 192 bit mendapatkan rata-rata 291,3 *Byte*, dan 256 bit mendapatkan rata-rata 292,5 *Byte*.

**Pengujian Keamanan Sistem dengan Frekuensi Keamanan Kata**

Pengujian ini untuk membuktikan keamanan sistem yang ditinjau dari frekuensi pengulangan karakter pada hasil *ciphertext* yang kerap muncul. Pengujian ini dilakukan karena sesuai dengan Kitab oleh Al-Kindi jika memecahkan kode pada pesan tak bermakna bisa dilakukan dengan teknik frekuensi kemunculan pada informasi [15][33]. Hasil uji coba pengujian keamanan terdapat pada Tabel 4.

Hasil uji coba pengujian Tabel 4. didapatkan rata-rata frekuensi perulangan karakter *chipertext* yaitu 9% dengan menerima huruf, simbol dan angka menunjukkan algoritma ini memiliki kemungkinan kecil untuk dapat dipecahkan melalui pembacaan kemunculan karakter.

**Pengujian Validasi**

Pengujian ini perlu dilakukan untuk mengetahui jika kinerja algoritma Kriptografi ini bisa bekerja dengan benar pada sistem. Skenario uji pada sistem ini menggunakan fungsionalitas ketika proses pengubahan *plaintext* ke *ciphertext* (enkripsi) atau sebaliknya yaitu proses *ciphertext* ke *plaintext* (dekripsi). Tabel 5. disajikan pengujian dengan beberapa macam skenario, baik pada *plaintext*, *ciphertext* dan kunci (*key*) menggunakan kombinasi huruf kapital, huruf kecil, simbol, angka dan spasi.

Tabel 4. Hasil Uji Coba Pengujian Keamanan Kriptografi Modifikasi AES mode CBC

| No | Plaintext | Bit Blok | Kunci | Ciphertext | Kemunculan Karakter | Total Karakter | Persentase Perulangan Karakter |
|---|---|---|---|---|---|---|---|
| 1. | Universitas Ahmad Dahlan | 128 | yogyakarta-2019- | 6TR9u6Yj56Jm+y8oDnjSQ2/ap0qsMkTgS2g69By25gg= | “6” dan “g” kemunculan 4 kali | 44 karakter | 9 % |
| 2. | Universitas Ahmad Dahlan 1960 Yogyakarta | | | 6TR9u6Yj56Jm+y8oDnjSQ0aFV7Zgwm6t3wDf7B46d4E/yaQeNnb0wE9SJGqrgiel | “6” kemunculan 5 kali | 64 karakter | 8 % |
| 3. | Universitas Ahmad Dahlan 1960 Yogyakarta Indonesia | | | 6TR9u6Yj56Jm+y8oDnjSQ0aFV7Zgwm6t3wDf7B46d4F0+jnmrmwD2yhGqaPzfVLLEnzTMqyLIMnExdzx+R5x4Q== | “6”, “m”, dan “n” kemunculan 4 kali | 88 karakter | 5 % |
| 4 | Universitas Ahmad Dahlan 1960 | | yogyakarta190704 | 6TR9u6Yj56Jm+y8oDnjSQ2ceQQQWQfsc2w9+zy8lII8= | “Q” kemunculan 5 kali | 44 karakter | 11 % |
| 5. | Universitas Ahmad Dahlan 1960 | 192 | yogyakarta-2019-12-02-19 | MCbUe08sdoNUQ8HIlUDU7wfEGL+7lryNf0g6IFO70qQ= | “U” kemunculan 4 kali | 44 karakter | 9 % |
| 6. | Universitas Ahmad Dahlan 1960 Yogyakarta | | | MCbUe08sdoNUQ8HIlUDU7+1qpfAN+CpFU2RH8S2xWymudV8bQd2PfrWqzrgWIPVk | “U” kemunculan 5 kali | 64 karakter | 8 % |
| 7. | Universitas Ahmad Dahlan 1960 Yogyakarta Indonesia | | | MCbUe08sdoNUQ8HIlUDU7+1qpfAN+CpFU2RH8S2xWymwFsEldtAiyyP0OT6CnzYuiio955h7SC/uxmj2hSTZcQ== | “U” kemunculan 5 kali | 88 karakter | 6 % |
| 8. | Universitas Ahmad Dahlan | | | MCbUe08sdoNUQ8HIlUDU75BfoPlm3Et6roPZFuvldv8= | “U” kemunculan 4 kalo | 44 karakter | 9 % |
| 9. | Universitas Ahmad Dahlan 1960 | 256 | yogyakarta-2019-12-02-19:43:00ok | mQyPv7eP0QkRBbH74O7ZqXNnoCap2gy/RfVCCch63vU= | “7” dan “C” kemunculan 3 kali | 44 karakter | 7 % |
| 10. | Universitas Ahmad Dahlan 1960 Yogyakarta | | | mQyPv7eP0QkRBbH74O7ZqXZpJOD9MTNxf0jHDlA/YQLDQlKBJDhhDpgsGPW5YnLX | “D” kemunculan 5 kali | 64 karakter | 8 % |
| 11. | Universitas Ahmad Dahlan 1960 Yogyakarta Indonesia | | | mQyPv7eP0QkRBbH74O7ZqXZpJOD9MTNxf0jHDlA/YQIjRSdCIFe+X0Z+PyYJjKbcqPu/M07go3BRL9+vicNF7g== | “7” kemunculan 5 kali | 88 karakter | 6 % |
| 12. | Universitas Ahmad Dahlan | | | mQyPv7eP0QkRBbH74O7ZqeYDxhs7fSBILDKPjtBZgPE= | “P” dan “7” kemunculan 4 kali | 44 karakter | 9 % |
| | | | | Rata-rata | | | 9% |

Tabel 5. Hasil Uji Coba Pengujian Proses Enkripsi & Dekripsi

| Proses Enkripsi | | | | Proses Dekripsi | | | |
|---|---|---|---|---|---|---|---|
| Masukkan Plaintext | Bit Blok | Key | Hasil Ciphertext | Masukkan Ciphertext | Key | Hasil Plaintext | Hasil |
| Uad&* | 128 | yogyakarta-2019- | L7Bw+UKhLGmbvC1rx0gkdA== | L7Bw+UKhLGmbvC1rx0gkdA== | yogyakarta-2019- | Uad&* | Berhasil |
| universitas Ahmad dahlan Yogyakarta Indonesia | 128 | yogyakarta-2019- | h1x6oDRUzWt+u83FMLfA2yCqgYIL/r3BF8OMN+0X/rVvxFxPAJXpQNVhSPNNxU2D | h1x6oDRUzWt+u83FMLfA2yCqgYIL/r3BF8OMN+0X/rVvxFxPAJXpQNVhSPNNxU2D | yogyakarta-2019- | universitas Ahmad dahlan Yogyakarta Indonesia | Berhasil |
| universitas Ahmad dahlan 1960&* | 128 | yogyakarta-2019- | h1x6oDRUzWt+u83FMLfA2194wljbI5xhmAXo68+luM4= | h1x6oDRUzWt+u83FMLfA2194wljbI5xhmAXo68+luM4= | yogyakarta-2019- | universitas Ahmad dahlan 1960&* | Berhasil |
| Universitas Ahmad Dahlan 1960 | 128 | yogyakarta-2019- | 6TR9u6Yj56Jm+y8oDnjSQ2ceQQQWQfsc2w9+zy8lII8= | 6TR9u6Yj56Jm+y8oDnjSQ2ceQQQWQfsc2w9+zy8lII8= | yogyakarta-2019- | Universitas Ahmad Dahlan 1960 | Berhasil |
| Uad&* | 192 | yogyakarta-2019-12-02-19 | gSJPTvZK3fnPgqNQSpIGKg== | gSJPTvZK3fnPgqNQSpIGKg== | yogyakarta-2019-12-02-19 | Uad&* | Berhasil |
| universitas Ahmad dahlan Yogyakarta Indonesia | 192 | yogyakarta-2019-12-02-19 | UA0tFYYwykanwo0z3Ozmoz2JQIrajqI5Nbu/ByUa76YbOhKLSMLQ4C1i06MDYYnW | UA0tFYYwykanwo0z3Ozmoz2JQIrajqI5Nbu/ByUa76YbOhKLSMLQ4C1i06MDYYnW | yogyakarta-2019-12-02-19 | universitas Ahmad dahlan Yogyakarta Indonesia | Berhasil |
| universitas Ahmad dahlan 1960&* | 192 | yogyakarta-2019-12-02-19 | UA0tFYYwykanwo0z3Ozmo4JNWDabBcrXbom9fycu+e0= | UA0tFYYwykanwo0z3Ozmo4JNWDabBcrXbom9fycu+e0= | yogyakarta-2019-12-02-19 | universitas Ahmad dahlan 1960&* | Berhasil |
| Universitas Ahmad Dahlan 1960 | 192 | yogyakarta-2019-12-02-19 | MCbUe08sdoNUQ8HIlUDU7wfEGL+7lryNf0g6IFO70qQ= | MCbUe08sdoNUQ8HIlUDU7wfEGL+7lryNf0g6IFO70qQ= | yogyakarta-2019-12-02-19 | Universitas Ahmad Dahlan 1960 | Berhasil |
| Uad&* | 256 | yogyakarta-2019-12-02-19:43:00ok | IXW9UVKo3Uub/1Uhtb3TAw== | IXW9UVKo3Uub/1Uhtb3TAw== | yogyakarta-2019-12-02-19:43:00ok | Uad&* | Berhasil |
| universitas Ahmad dahlan Yogyakarta Indonesia | 256 | yogyakarta-2019-12-02-19:43:00ok | GNuBUoa6Vf22/qJrz0xrTVwvwJLwNdkGLPzD8DGvkTglh4Jf4wWmuM34I/jckR7t | GNuBUoa6Vf22/qJrz0xrTVwvwJLwNdkGLPzD8DGvkTglh4Jf4wWmuM34I/jckR7t | yogyakarta-2019-12-02-19:43:00ok | universitas Ahmad dahlan Yogyakarta Indonesia | Berhasil |
| universitas Ahmad dahlan 1960&* | 256 | yogyakarta-2019-12-02-19:43:00ok | GNuBUoa6Vf22/qJrz0xrTfnDo/anVrn7WrpJUyQl1Ec= | GNuBUoa6Vf22/qJrz0xrTfnDo/anVrn7WrpJUyQl1Ec= | yogyakarta-2019-12-02-19:43:00ok | universitas Ahmad dahlan 1960&* | Berhasil |
| Universitas Ahmad Dahlan 1960 | 256 | yogyakarta-2019-12-02-19:43:00ok | mQyPv7eP0QkRBbH74O7ZqXNnoCap2gy/RfVCCch63vU= | mQyPv7eP0QkRBbH74O7ZqXNnoCap2gy/RfVCCch63vU= | yogyakarta-2019-12-02-19:43:00ok | Universitas Ahmad Dahlan 1960 | Berhasil |

Berdasarakan Tabel 5. akan disusun pengujian validasi dengan skenario uji data *palintext* maupun *ciphertext* dan menggunakan *key* benar, selain itu *key* yang disengaja kurang tepat. Hal tersebut untuk mengukur ketahanan algoritma dalam mempertahankan keaslian pesan didalamnya.

Tabel 6. Hasil Uji Coba Pengujian Validitas Ketahanan Kriptografi

| No. | Skenario Input | Key | Bit Blok | Hasil Ouput | Hasil Kesesuaian Harapan |
|---|---|---|---|---|---|
| 1. | Masukkan plaintext | Key benar | Blok benar | Menampilkan hasil enkripsi benar | Sesuai |
| | Masukkan chipertext | Key benar | Blok benar | Menampilkan hasil dekripsi benar | Sesuai |
| 2. | Masukkan plaintext | Key benar | Blok benar | Menampilkan hasil enkripsi benar | Sesuai |
| | Masukkan chipertext | Key salah | Blok benar | Menampilkan hasil dekripsi salah | Sesuai |
| 3. | Masukkan plaintext | Key salah | Blok salah | Menampilkan hasil key blok tidak sesuai | Sesuai |
| | Masukkan chipertext | Key salah | Blok salah | Menampilkan hasil key blok tidak sesuai | Sesuai |

Pengujian validasi pada Tabel 5. dan Tabel 6. menunjukkan bahwa kinerja algoritma Kriptografi ini bekerja dengan benar pada sistem, hal ini dibuktikan pada keberhasilan saat proses enkripsi atau sebaliknya yaitu proses dekripsi dan dari skenario uji 6 input pada sistem menghasilkan nilai 100% dengan *output* sesuai dengan yang diharapkan.

## IV. KESIMPULAN

Hasil uji coba pengujian enkripsi diketahui rata-rata kecepatan algoritma modifikasi AES mode CBC dihasilkan waktu tertinggi yaitu pada blok 128 bit yaitu 14,2 ms, blok 256 bit 13,2 ms dan terakhir blok 192 bit yaitu 11,5 ms. Sedangkan hasil uji coba pengujian dekripsi didapatkan rata-rata waktu tertinggi yaitu pada blok 256 bit yaitu 16,5 ms, blok 128 bit yaitu 14 ms dan terakhir blok 192 bit yaitu 13,2 ms. Pada penelitian ini blok pada kunci kurang berpengaruh pada waktu eksekusi, namun lebih dipengaruhi oleh lalu lintas jaringan. Sehingga diperlukannya simulasi pengujian dengan karakter yang lebih panjang. Pengujian dengan pola kemunculan frekuensi rata-rata dihasilkan 9%, dengan menerima huruf, simbol dan angka menunjukan algoritma ini memiliki kemungkinan kecil untuk dapat dipecahkan melalui pembacaan kemunculan karakter. Dari pengujian validasi menghasilkan nilai 100% dimana pengujian fungsionalitas tersebut menunjukkan hasil yang sesuai diharapkan. Pada kehidupan sehari-hari, penerapan algoritma dibutuhkan untuk dimanfaatkan dalam mengamankan data dan informasi pada sistem web dan mobile. Pada sisi web pengamanan bisa diterapkan dalam proses login, sedangkan untuk mobile bisa diterapkan dalam pembutan API-nya. Selain itu algoritma ini diharapkan bisa dimanfaatkan juga untuk proses mengamankan file dokumen penting, sehingga keabsahan informasi tetap terjaga dan tidak bisa disalahgunakan oleh pihak tidak berwenang.

## V. DAFTAR PUSTAKA

[1] A. Solichin, *Pemrograman web dengan PHP dan MySQL*. Penerbit Budi Luhur, 2016.
[2] W. Komputer, *Panduan Praktis Menguasai Pemrograman Web dengan JavaScript 2009*. Penerbit Andi, 2010.
[3] S. T. Edy Winarno, M. Eng, A. Zaki, and others, *Pemrograman Web Berbasis Html 5, php, dan Javascript*. Elex Media Komputindo, 2014.
[4] M. Saefuloh, A. Fadlil, and I. Riadi, "Pengembangan Sistem Informasi Penentuan Jalur Lokasi Penjemputan Menggunakan Algoritma Dijkstra Dan Algoritma," pp. 55–60, 2018.
[5] G. B. Davis, "Information Systems Conceptual Foundations: Looking Backward and Forward," in *Organizational and social perspectives on information technology*, Springer, 2000, pp. 61–82.
[6] S. A. Moscove, M. G. Simkin, and N. A. Bagranoff, *Core concepts of accounting information systems*. John Wiley & Sons, Inc., 1996.
[7] M. B. Romney, P. J. Steinbart, and B. E. Cushing, *Accounting Information Systems*, vol. 2. Prentice Hall Upper Saddle River, NJ, 2000.
[8] E. R. Indrajit, "Pengantar Konsep Dasar Manajemen Sistem dan Teknologi Informasi." Aptikom, 2001.
[9] N. Rochmah and Ardiansyah, "Desain Kriptografi CBC Modifikasi pada Proses Pengamanan Pesan melalui Email," *Semin. Nas. Teknol. Inf. dan Multimed.*, vol. 2, no. 1, pp. 1–6, 2016.
[10] D. Ariyus, *Computer Security*. 2006.
[11] B. Rahardjo, "Keamanan Sistem Informasi Berbasis Internet," *Jakarta PT INDOCISC*, 2005.
[12] D. Stiawan, *Sistem Keamanan Komputer*. Elex Media Komputindo, 2005.
[13] A. Zelvina, S. Effendi, and D. Arisandi, "Perancangan Aplikasi Pembelajaran Kriptografi Kunci Publik ElGamal Untuk Mahasiswa," *Dunia Teknol. Informasi-Jurnal Online*, vol. 1, no. 1, 2012.

[14] A. Prayogo, I. Riadi, and A. Luthfi, "Mobile Forensics Development of Mobile Banking Application using Static Forensic," *Int. J. Comput. Appl.*, vol. 160, no. 1, pp. 5–10, 2017.
[15] R. Munir, "Kriptografi," *Inform. Bandung*, 2006.
[16] A. G. Konheim, *Computer Security and Cryptography*. John Wiley & Sons, 2007.
[17] B. A. Forouzan, *Cryptography & network security*. McGraw-Hill, Inc., 2007.
[18] N. R. P. Dyah, "Perancangan Modifikasi Kriptografi Modern CBC Untuk Pengamanan Data/File Text," 2013.
[19] V. U. Sastry, N. R. Shankar, and S. D. Bhavani, "A Modified Hill Cipher Involving Interweaving and Iteration," *Int. J. Netw. Secur.*, vol. 11, no. 1, pp. 11–16, 2010.
[20] R. K. Meenakshi and A. Arivazhagan, "RTL Modelling for the Cipher Block Chaining Mode (CBC) for Data Security," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 8, no. 3, pp. 709–711, 2017.
[21] Henry, A. H. Kridalaksana, and Z. Arifin, "Kriptografi Aes Mode Cbc Pada Citra Digital Berbasis Android," *Semin. Ilmu Komput. dan Teknol. Inf.*, vol. 1, no. 1, pp. 45–52, 2016.
[22] A. F. Ramdhansya, E. Ariyanto, and H. H. Nuha, "Implementasi Advanced Encryption Standard (Aes) Pada Sistem Kunci Elektronik Kendaraan Berbasis Sistem Operasi Android Dan Mikrokontroler Arduino," *Semin. Nas. Inform.*, vol. 2014, no. semnasIF, pp. 92–98, 2014.
[23] F. A. Sianturi, "Perancangan Aplikasi Pengamanan Data Dengan Kriptografi Advanced Encryption Standard ( AES)," *Pelita Inform. Budi Darma*, vol. 4, no. 1, pp. 42–46, 2013.
[24] D. E. Erlianto and Painem, "Aplikasi Kriptografi Pengamanan Database Menggunakan Metode AES Dan Vigenere Berbasis Desktop Pada Pada Divisi Pencegahan Dan Penanggulangan Hiv Aids Yayasan Kapeta Aplikasi Kriptografi Pengamanan Database Menggunakan Metode AES dan Aplikasi Kriptografi P," *SKANIKA*, vol. 1, no. 2, pp. 772–779, 2018.
[25] D. Surian, "Algoritma Kriptografi AES Rijndael," *TESLA*, vol. 8, no. 2, pp. 97–101, 2006.
[26] D. T. Yuwono, A. Fadlil, and S. Sunardi, "Performance Comparison of Forensic Software for Carving Files using NIST Method," *J. Teknol. dan Sist. Komput.*, vol. 7, no. 3, p. 89, 2019.
[27] Imam Riadi, Abdul Fadlil, and Ammar Fauzan, "Evidence Gathering and Identification of LINE Messenger on Android Device," *Int. J. Comput. Sci. Inf. Secur.*, vol. 16, no. 5, pp. 201–205, 2018.
[28] Y. Kurniawan, "Kriptografi Keamanan Internet dan Jaringan Komunikasi," *Bandung Inform.*, 2004.
[29] Hermansa, R. Umar, and A. Yudhana, "Analisis Sistem Keamanan Teknik Kriptografi Dan Steganografi Pada Citra Digital ( Bitmap )," *Semin. Nas. Teknol. Fak. Tek. Univ. Krisnadwipayana*, pp. 1–9, 2019.
[30] M. M. Bace, "Cipher block chaining decryption." Google Patents, 2007.
[31] A. Rahmatulloh, H. Sulastri, and R. Nugroho, "Keamanan RESTful Web Service Menggunakan JSON Web Token (JWT) HMAC SHA-512," *J. Nas. Tek. Elektro dan Teknol. Inf.*, vol. 7, no. 2, 2018.
[32] M. I. Mazdadi, I. Riadi, and A. Luthfi, "Live Forensics on RouterOS using API Services to Investigate Network Attacks," *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 2, 2017.
[33] R. Munir, "Pengantar Kriptografi," *ITB, Bandung*, 2006.