Jurnal Nasional Teknologi Komputer
Vol.x; No: x; Bulan 202x
Website: publikasi.hawari.id/index.php/jnastek
E-ISSN: 2808-4845; P-ISSN: 2808-7801

Makalah Penelitian

Implementasi Kriptografi Pengamanan Data File Dokumen Menggunakan Algoritma Advanced Encryption Standard Mode Chiper Block Chaining

Sahat Fernando Manullang[1], Allwine [2], Jakaria Sembiring [3]

[1]Teknik Informatika, STMIK Methodist Binjai.
[1]sahatfernandomanullang@gmail.com, [2]allwineamikmg@gmail.com, [3]jakariasembiring@gmail.com

Corresponding Author: write name of corresponding author

ABSTRACT

Improving the security aspects of data can be done by controlling cryptographic techniques. The AES (Advanced Encryption Standard) algorithm is cryptography that can be used to protect data or information by encrypting and decrypting data blocks of 128 bits with a key length of 128 bits, 192 bits, or 256 bits. The data security process can be carried out using the Cipher Block Chaining (CBC) method in its operating mode. In preparation for carrying out the encryption process used is a pdf document file. The first 16 bytes of data are read as the first block for the encryption process with the CBC method. The results of the research are being able to implement application programs using the Advanced Encryption Standard mode Cipher Block Chaining algorithm by encrypting and decrypting document files.

Keywords: *Cryptography, Encryption, Decryption, Advanced Encryption Standard, Cipher Block Chaining*

ABSTRAK

Dalam meningkatkan aspek keamanan suatu data dapat dilakukan dengan pengendalian teknik kriptografi. Algoritma AES (Advanced Encryption Standard) merupakan kriptografi yang dapat digunakan untuk melindungi data atau informasi dengan melakukan mengenkripsi dan mendekripsi blok data sepanjang 128 bit dengan panjang kunci 128 bit, 192 bit, atau 256 bit. Proses pengamanan data dapat dilakukan dengan menggunakan metode Chiper Block Chaining (CBC) dalam mode operasinya. Dalam persiapan untuk melakukan proses enkripsi yang digunakan adalah sebuah file dokumen pdf. Data 16 byte pertama dibaca sebagai blok pertama untuk proses enkripsi dengan metode CBC. Hasil dari penelitian yaitu dapat mengimplementasikan program aplikasi menggunakan algoritma Advanced Encryption Standard mode Chiper Block Chaining dengan melakukan enkripsi dan dekripsi file dokumen.

Kata Kunci: *Kriptografi, Enkripsi, Dekripsi, Advanced Encryption Standard, Chiper Block Chaining.*

1. Pendahuluan

Dalam meningkatkan aspek keamanan dan menjaga keutuhan dari suatu data dapat dilakukan sistem kriptografi, yaitu dengan menyandikan isi atau content file dokumen tersebut menjadi isi yang sulit bahkan tidak dapat dipahami melalui proses enkripsi dan untuk memperoleh kembali informasi yang asli dilakukan proses dekripsi .

Kriptografi merupakan salah satu cara yang dapat digunakan dalam melindungi kerahasiaan data dengan melakukan proses penyandian dengan penggunaan kode khusus terhadap data yang ingin diamankan sehingga makna asli dari data tidak lagi dapat dimengerti, pengamanan data kriptografi dilakukan dengan cara melakukan enkripsi data dengan kunci rahasia [1]. Algoritma kriptografi modern memiliki 2 jenis kunci, yaitu algoritma simetris (konvensional) dan algoritma asimetris (kunci publik) [2]. Algoritma simetris modern beroperasi dalam mode bit dan dapat dikelompokkan menjadi dua kategori, yaitu cipher aliran (stream cipher) dan cipher blok (block cipher)[3].

AES merupakan algoritma chiper yang aman untuk melindungi data atau informasi bersifat rahasia. AES dipublikasikan oleh NIST (National Institute of Standard and Technology) pada tahun 2001 untuk menggantikan algoritma DES (Data encryption Standard) [1].

Proses pengamanan data dengan mode operasi chiper blok dapat dilakukan dengan beberapa metode, yaitu metode Electronic Code Book (ECB), Chiper Feedback (CFB), Output Feedback (OFB), Chiper Block Chaining (CBC). Metode CBC merupakan salah satu mode operasi cipher blok yang menerapkan umpan balik pada sebuah blok, blok plaintext yang current di-XOR-kan terlebih dahulu dengan blok ciphertext hasil enkripsi sebelumnya, selanjutnya hasil peng XOR-an tersebut masuk ke dalam fungsi enkripsi [6]. Sedangkan pada proses dekripsi dilakukan dengan memasukkan blok ciphertext yang current ke fungsi dekripsi, kemudian meng-XOR-kan hasilnya dengan blok ciphertext sebelumnya pada sebuah blok data [4]. Sehingga proses kriptanalis menjadi lebih sulit, dalam hal ini dapat meningkatkan keamanan data.

2. Tinjauan Pustaka

Tinjauan pustaka menjadi landasan dalam melakukan penelitan dan penulis mengambil beberapa contoh penelitian terdahulu yang dapat dijadikan sebagai pertimbangan dan acuan dalam mendukung penulisan, maka dalam tinjauan pustaka penulis mencantumkan beberapa penelitian terdahulu, sebagai berikut:
"Penerapan Algoritma Advanced Encryption Standard (AES - 256) Dengan Mode CBC Dan Secure Hash Algorithm (SHA-256) Untuk Pengamanan Data File" (Ahmad Fathurrozi, 2021). Pada Penelitian tersebut melakukan penerapan algoritma AES-256 dengan mode CBC dan SHA-256 terhadap aplikasi yang telah dibuat yaitu dapat mengenkripsi file dengan berbagai ekstensi seperti file dokumen, file suara (voice note/mp3), file video serta file gambar dengan baik dan dapat didekripsikan kembali dengan kunci yang sama pada aplikasi.
"Enkripsi Dan Dekripsi Dengan Algoritma Aes 256 Untuk Semua Jenis File" (Voni Yuniati, et al, 2011). Dari hasil penelitian yang dilakukan bahwa isi file yang telah dienkripsi dengan algoritma AES 256 merupakan isi file dari file sumber, sehingga apabila akan dilakukan proses dekripsi, maka akan kembali seperti file sumber semula dan waktu yang diperlukan untuk proses enkripsi pada penelitian ini tidak sama dengan waktu proses dekripsi yang dikarenakan adanya pemakaian resource komputer.
"Keamanan Dokumen Menggunakan Algoritma Advanced Encryption Standard (Aes)" (Joko Handoyo, 2020). Pada penelitian ini, algoritma Advanced Encryption Standard (AES) diimplementasikan sebagai pengamanan form dokumen pada website. Dalam proses pengiriman dokumen, ketika dokumen dan password dimasukkan maka akan otomatis di enkripsi. Untuk memulai proses enkripsi siapkan 2 buah array berukuran 4x4 bernama Plaintext dan Key. Plaintext dan key tersebut dikonversikan ke dalam bentuk bit menggunakan kode ASCII. Lalu konversikan kode ASCII tersebut ke dalam heksadesimal.
"KombinasiAlgoritma Cipher Block Chaining (CBC) dan Mars Pada Penyandian File PDF" (Ridha Ismadiah, 2020). Pada penilitian ini membahas pengamanan file pdf berdasarkan kombinasi algoritma CBC dan Mars meliputi tahap, yaitu proses perluasan kunci (key expansion), proses enkripsi dan dekripsi. Hasil dari proses XOR tersebut yang kemudian di enkripsi. Dari Algoritma Mars ini proses yang akan di jalan kan terdiri dari ekspansi atau pembangkit kunci, pembangkit kunci disini menggunkan modifikasi dari Algoritma DES.

3. Metode Penelitian

3.1 Advanced Encryption Standart (AES)

Algortima AES menggunakan substitusi dan permutasi, dan sejumlah putaran (cipher berulang) setiap putaran mengunakan kunci internal yang berbeda (kunci setiap putaran disebut

round key). Garis besar Algoritma AES yang beroperasi pada blok 128-bit adalah sebagai berikut [5]:

1. Key Schedule: merupakan proses untuk membentuk kunci yang akan digunakan dalam proses enkripsi dan dekripsi. Pembentukan kunci terdiri dari beberapa tahapan yaitu RotWord, SubWord, XOR dengan nilai R-con, dan XOR dengan word sebelumnya.
2. AddRoundKey: melakukan XOR antara state awal (plaintext) dengan cipher key. Tahap ini disebut juga initial round.
3. Putaran sebanyak Nr – 1 kali. Proses yang dilakukan pada setiap putaran adalah:
   a. SubBytes: adalah operasi substitusi byte nonlinier yang menukar byte state secara independen menggunakan tabel S-Box. S-Box dihasilkan dari perkalian invers polynomial GF(2^8) [7].
   b. ShiftRows: pergeseran baris-baris array state secara wrapping dimana bit yang paling kiri dipindahkan menjadi bit yang paling kanan. Jumlah pergeseran tergantung pada nilai bari (r). Baris r = 1 digeser sejauh 1 byte, baris r = 2 digeser sejauh 2 byte, dan baris r = 3 digeser sejauh 3 byte. Baris r = 0 tidak digeser.
   c. MixColumns: mengoperasikan setiap elemen yang berada dalam satu kolom pada State. Perkalian elemen dengan polynomial a (x) mod (x4 + 1) pada kolom ditetapkan pada persamaan [5] :
      a (x) = {03}x3 + {01} x2 + {01} x + {02} (1)
   d. AddRoundKey: melakukan XOR antara state sekarang round key.
4. Final Round: proses untuk putaran terakhir tidak mengalami transformasi MixColumns:
   a. SubBytes
   b. ShiftRows
   c. AddRoundKey

3.2 Operasi Chiper Blok Chaining

Chiper 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 [8].

Rumus matematis untuk enkripsi pada mode CBC adalah:

$$C_i = E_k\,(P_i \oplus C_{i-1}),\ C_0 = IV \qquad (2)$$

sedangkan rumus matematis untuk dekripsi pada mode CBC adalah:

$$P_i = D_k\,(C_i) \oplus C_{i-1},\ _0 = IV \qquad (3)$$

Blok plaintext pertama menggunakan C_0 sebagai initialization vector atau IV yang diberikan secara acak dan digunakan menggantikan blok chipertext sebelumnya.

3.3 Algoritma

Untuk mengetahui bagaimana langkah-langkah algoritma *Advanced Encryption Standard* dalam mengenkripsi dan mendekripsi file dokumen, maka dibutuhkan algoritma untuk memecahkan masalah tersebut, yaitu:

Algoritma Enkripsi AES

```
Header      : Algoritma enkripsi advanced encryption standard
Deklarasi   : P, C : String, IV, K : Byte
Deskripsi   :
            Input  :
                    IV ← Initialization Vector
                    P ← Plaintext
                    K ← Key
            Output :
                    C ← Chipertext
            Proses :
                    Mulai
                       Memasukkan Ekspansi(K)
                       XOR (IV)
                       AddRoundkey
                       Putaran Transformasi
                       Subbytes;
                       Shiftrows;
                       Mixcolumns(P);
                       Addroundkey;
                    Selesai.
```

Algoritma Dekripsi AES

```
Header      : Algoritma enkripsi advanced encryption standard
Deklarasi   : P, C : String, IV, K : Byte
Deskripsi   :
            Input  :
                    C ← Chipertext
                    K ← Key
                    IV ← Initialization Vector
            Output :
                    P ← Plaintext
            Proses :
                    Mulai
                       Memasukkan Ekspansi(K)
                       AddRoundkey
                       InvSubBytes
                       InvShiftRows
                       AddRoundKey
                       InvMixColumns
                       XOR (IV)
                    Selesai.
```

4. Hasil

4.1 Enkripsi Advanced Encryption Standard

Proses enkrispi dari langkah-langkah algoritma Advanced Encryption Standard tersebut dilakukan sampai 10 kali putaran, pada proses terkahir yaitu tanpa MixColumns [5]. Proses terakhir yang dihasilkan adalah sebagai chipertext. Sebagai contoh dari sebuah plaintext yang dilakukan proses enkripsi menggunakan algoritma Advanced Encryption Standard metode Chiper Block Chaining dapat dilihat pada table 1.

Tabel 1. Plaintext dan Chipertext AES

Input	*Byte*
Plaintext	25 50 44 46 2D 31 2E 37 0D 0A 25 B5 B5 B5 B5 0D
IV	69 76 73 74 6D 69 6B 6D 65 74 68 6F 64 69 73 74
Key	70 72 6F 64 69 69 6E 66 6F 72 6F 61 74 69 6B 61
Output	*Byte*
Chipertext	1B 81 88 79 C1 FE 94 E7 A3 8B 7A E8 90 07 04 13

Key Schedule terdiri dari beberapa tahapan yaitu RotWord, SubWord, XOR dengan nilai R-con, dan XOR dengan word sebelumnya.

Tabel 2. Kunc Kunci (ChiperKey) dalam Heksadesimal

Kunci	Heksadesimal
prodiinformatika	70 72 6F 64 69 69 6e 66 6F 72 6F 61 74 69 6B 61

Tabel 2. Kunci dibagi 4 *byte*

W_{i-4}	W_{i-3}	W_{i-2}	W_{i-1}
70	69	6F	74
72	69	72	69
6F	6E	6F	6B
64	66	61	61

Tahapan selanjutnya adalah RotWord, yang dilakukan pada tahap RotWord adalah menggeser setiap byte pada kolom terakhir dari cipherkey secara siklik ke atas satu kali.

Tabel 3. RotWord W_{i-1}

W_{i-1}		W_{i-1}
74		69
69		6B
6B		61
61		74

Hasil dari RotWord W_{i-1} kemudian dilakukan pensubtitusian dengan tabel S-Box yang sudah ditetapkan

Tabel 4. Subtitusi W_{i-1}

W_{i-1}	Hasil SubtitusiW_{i-1}
74	F6
69	7F
6B	EF
61	92

Tahap terakhir untuk mendapatkan kunci kolom ke (W_1) yaitu proses XOR yang dilakukan terhadap hasil subword dengan nilai R-con yang bersesuaian, lalu XOR lagi dengan kolom (W_{i-4}), berikut adalah tabel R-con (Round Constant).

Tabel 5. *R-con* (*Round Constant*).

1	2	3	4	5	6	7	8	9	10
01	02	04	08	10	20	40	80	1B	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

Sebelum mendapatkan nilai matrik W_1 dengan melakukan $W_{i-1} \oplus W_{i-4} \oplus$ Rcon, bilangan heksadesimal dirubah dulu menjadi bilangan biner untuk dapat dilakukan operasi XOR.

Prosesnya adalah sebagai berikut:

$$\begin{bmatrix}70\\72\\6F\\64\end{bmatrix} \oplus \begin{bmatrix}F6\\7F\\EF\\92\end{bmatrix} \oplus \begin{bmatrix}01\\00\\00\\00\end{bmatrix}$$

Berikut bilangan heksadesimal yang diatas telah dirubah ke dalam bilang biner:

$$\begin{bmatrix}01110000\\01110010\\01101111\\01100100\end{bmatrix} \oplus \begin{bmatrix}11110110\\01111111\\11101111\\10010010\end{bmatrix} \oplus \begin{bmatrix}00000001\\00000000\\00000000\\00000000\end{bmatrix} = \begin{bmatrix}10000111\\00001101\\10000000\\11110110\end{bmatrix}$$

Selanjutnya untuk mendapatkan sub kunci pertama pada kolom kedua hingga keempat dilakukan operasi XOR antara W_i dengan kolom W_{i-1-3}, tanpa proses XOR *R-con,* Sehingga pada *round* pertama didapatkan

Key Schedul Round Pertama yaitu = $\begin{bmatrix}87 & EE & 81 & F5\\0D & 64 & 16 & 7F\\80 & EE & 81 & EA\\F6 & 90 & F1 & 90\end{bmatrix}$

Proses pengolahan nilai matrik W_1 dengan melakukan $W_{i-4} \oplus W_{i-1} \oplus Rcon$ dilakukan berulang sebanyak 10 iterasi sehingga menghasilkan 10 Round Key Schedule.

Operasi XOR IV adalah proses pertama dalam metode CBC dilakukan operasi XOR antara IV dengan plaintext blok pertama yang kemudian hasil operasi XOR tersebut dilakukan proses enkripsi AES, untuk proses operasi nya sebagai berikut:

$$\begin{bmatrix}25 & 2D & 0D & B5\\50 & 31 & 0A & B5\\44 & 2E & 25 & B5\\46 & 37 & B5 & 0D\end{bmatrix} \oplus \begin{bmatrix}69 & 6D & 65 & 64\\76 & 69 & 74 & 69\\73 & 6B & 68 & 73\\74 & 6D & 6F & 74\end{bmatrix} = \begin{bmatrix}4C & 40 & 68 & D1\\26 & 58 & 7E & DC\\37 & 45 & 4D & C6\\32 & 5A & DA & 79\end{bmatrix}$$

AddRoundKey melakukan XOR antara Hasil XOR Blok Pertama yang dinotasikan sebagai state awal (P_{i-1}) dengan key sehingga menjadi sebuah state 4x4.

$$\begin{bmatrix}4C & 40 & 68 & D1\\26 & 58 & 7E & DC\\37 & 45 & 4D & C6\\32 & 5A & DA & 79\end{bmatrix} \oplus \begin{bmatrix}70 & 69 & 6F & 74\\72 & 69 & 72 & 11\\6F & 6E & 6F & 6B\\64 & 66 & 61 & 61\end{bmatrix} = \begin{bmatrix}3C & 29 & 07 & A5\\54 & 00 & 0C & CD\\6F & 2B & 22 & AD\\56 & 3C & BB & 18\end{bmatrix}$$

Proses selanjutnya melakukan subtitusi Addroundkey sebelumnya dengan menggunakan Subtitution Box (S-Box) AES

$$\begin{bmatrix}3C & 29 & 07 & A5\\54 & 00 & 0C & CD\\6F & 2B & 22 & AD\\56 & 3C & BB & 18\end{bmatrix} \mathrm{S-Box} \begin{bmatrix}EB & A5 & C5 & 06\\20 & 63 & FE & BD\\A8 & F1 & 93 & 95\\B1 & EB & EA & AD\end{bmatrix}$$

Transformasi ShiftRows melakukan rotasi setiap baris. Baris ke 1 dirotasi 0 kali, baris ke 2 dirotasi 1 kali, baris ke 3 dirotasi 2 kali, dan baris ke 4 dirotasi 3 kali.

Tabel 6. Hasil Rotasi ShiftRows

SubBytes				Rotasi
EB	A5	C5	06	0 kali
63	FE	BD	20	1 kali
93	95	A8	F1	2 kali
AD	B1	EB	EA	3 kali

Kemudian p roses MixColumns melakukan perkalian setiap kolom dari array state polynomial a(x) mod ($x^4 + 1$)

$$\begin{bmatrix} EB & A5 & C5 & 06 \\ 63 & FE & BD & 20 \\ 93 & 95 & A8 & F1 \\ AD & B1 & EB & EA \end{bmatrix} \oplus \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} = \begin{bmatrix} 56 \\ 2E \\ 59 \\ 97 \end{bmatrix}$$

Berikut hasil keseluruhan dalam tahapan MixColoumns pada Round ke 1:

Tabel 7. Transformasi MixColoumns Round 1

56	7B	0E	77
2E	4D	AC	A4
59	A2	15	FA
97	E6	65	0C

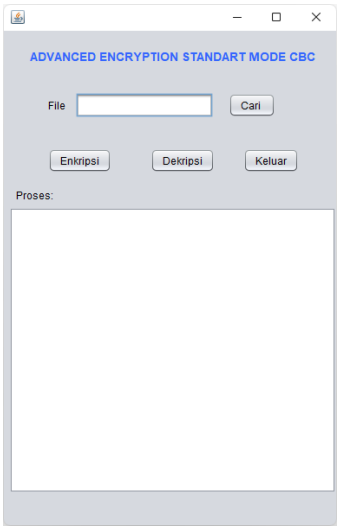
Proses AddRoundKey, SubBytes, ShiftRows, dan MixColoums yang dilakukan untuk Round ke 1 hingga Round ke 9 menggunakan cara yang sama dengan proses Round sebelumnya. Pada proses Round 10 yang terakhir tanpa transformasi MixColoumns, tahapan yang dilakukan adalah adalah SubBytes, ShiftRows dan AddRoundKey yang dihasilkan adalah sebagai chipertext 16 byte yang pertama, sehingga didapatkan hasil AddRoundKey terakhir sebagai chipertext adalah (1B 81 88 79 C1 FE 94 E7 A3 8B 7A E8 90 07 04 13).

Tabel 8. Hasil Tranformasi Round 10

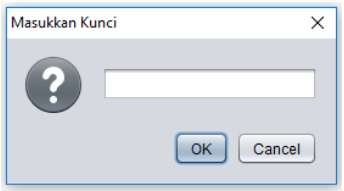
Key Schedule				*SubBytes*				*ShiftRows*				*AddRoundKey*			
07	B3	1E	D4	1C	72	BD	44	1C	72	BD	44	1B	C1	A3	90
9B	10	DA	8F	88	1A	EE	51	1A	EE	51	88	81	FE	8B	07
64	C6	76	C9	0C	CD	EC	52	EC	52	0C	CD	88	94	7A	04
C0	C1	71	7C	26	99	6F	B9	B9	26	99	6F	79	E7	E8	13

4.2 Implementasi Program

Program aplikasi yang dibuat menggunakan bahasa pemgroman java menggunakan perangkat lunak open-source Java Netbeans IDE 8.2 berupa Windows Application. Sistem yang telah dirancang mencakup dengan proses enkripsi dan dekripsi dengan menggunakan algoritma AES mode CBC. Tampilan program aplikasi pengamanan file yang dibangun terbagi atas dua form yaitu form menu utama, dan form input kunci. Form utama menampilkan kolom input file, tombol enkripsi, dekripsi dan hasil prosesnya.



Gambar 1. Tampilan Input File



Gambar 2. Tampilan Input Key

Dari program yang telah dibuat dilakukan pengujian enkripsi terhadap objek file dokumen "cobaenkrip.pdf" dilakukan proses enkripsi dengan pembentukan IV (Initialization Vector) secara acak pada program dan memberikan kunci sepanjang 16 byte "prodiinformatika".

Gambar 3. Tampilan Proses Enkripsi

Dari hasil pengujian untuk proses enkripsi berhasil dilakukan, dan lokasi *output* file yang telah di enkripsi tersimpan di folder yang sama dengan file asli. Untuk file enkripsi diberikan penambahan ekstensi ".aes" pada nama filenya.

5. Kesimpulan

Berdasarkan pembahasan yang telah diuraikan pada bab-bab sebelumnya, maka dapat diambil kesimpulan sebagai berikut:

1. Hasil dari penguncian enkripsi menggunakan algoritma AES mode CBC dari beberapa file dokumen menghasilkan ekstensi file baru sebagai chipertext yang isinya merupakan kode-kode dan karakter yang sulit dipahami.
2. Penerapan algoritma AES mode CBC dengan penyandian dokumen file dapat di proses tanpa merubah atau menghapus file aslinya.
3. Implementasi algoritma Advanced Encryption Standard mode Chiper Block Chaining dapat diterapkan pada program aplikasi menggunakan Java Netbeans IDE 8.2 yang mencakup proses enkripsi dan dekripsi.

REFERENSI

[1] Azhari, M., Mulyana, D. I., Perwitosari, F. J., & Ali, F. (2022). Jurnal Pendidikan Sains dan Komputer Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). Jurnal Pendidikan Sains dan Komputer.

[2] Munir, R. (2006). *Kriptografi*. Bandung: Informatika Bandung.

[3] R. Kristoforus JB, S. A. B. (2012). Implementasi Algoritma Rijndael untuk Enkripsi dan Dekripsi pada Citra Digital. Seminar Nasional Aplikasi Teknologi Informasi 2012, 2012(Snati), 15–16.

[4] Aliyah, J. (2020). Aplikasi Mobile Untuk Enkripsi Data Gambar Menggunakan Kombinasi Fungsi Xor Dan Mode Operasi Cbc. Jurnal Informatika, Teknologi Dan Sains, 2(4), 214–222.

[5] Bhaudhayana, G., & Widiartha, I. (2015). Implementasi Algoritma Kriptografi Aes 256 Dan Metode Steganografi Lsb Pada Gambar Bitmap. Jurnal Ilmu Komputer.

[6] Fathurrozi, A. (2021). Penerapan Algoritma Advanced Encryption Standard (AES-256) Dengan Mode CBC DanSecure Hash Algorithm (SHA-256) Untuk Pengamanan Data File. 2(2), 227–238.

[7] Wadi, S. M., & Zainal, N. (2014). High Definition Image Encryption Algorithm Based on AES Modification. Wireless Personal Communications, 79(2), 811–829.

[8] Henry, Kridalaksana, A. H., & Arifin, Z. (2016). Kriptografi Aes Mode Cbc Pada Citra Digital Berbasis Android. Seminar Ilmu Komputer Dan Teknologi Informasi, 1(1), 45–52.

[9] Dony Ariyus. (2008). Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi. Yogyakarta: Penerbit Andi.

[10] Maricar, M. A., & Sastra, N. P. (2018). Efektivitas Pesan Teks Dengan Cipher Substitusi, Vigenere Cipher, dan Cipher Transposisi. Majalah Ilmiah Teknologi Elektro.

[11] Jubilee Enterprise. (2016). Belajar Java, Database, dan Netbeans dari Nol. PT Elex Media Komputindo, Jakarta.

[12] Y. Supardi. (2010). Pemrograman Bahasa Java Bagi Pemula. Bandung: Informatika Bandung.

******