Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 8, Nomor 1, Januari 2024
http://doi.org/10.33395/remik.v8i1.13157
e-ISSN : 2541-1330
p-ISSN : 2541-1332

Penerapan Kriptografi AES untuk Keamanan Data Aplikasi Pemesanan Bibit Ternak pada BPSI UAT

[1]Dwi Nanda Rahmat Herlambang, [2] Nilma, [3]Norma Pravitasari
[1,2,3]Universitas Indraprasta PGRI
Jakarta, Indonesia

[1]dn.rahmath@gmail.com, [2] nilma23juli@gmail.com,
[3]Vytha.mipa12@gmail.com

*Penulis Korespondensi
Diajukan : 06/11/2023
Diterima : 12/12/2023
Dipublikasi : 01/01/2024

ABSTRAK
Kriptografi, sebagai cabang ilmu matematika yang mengkaji keamanan data, memiliki peran krusial dalam melindungi informasi sensitif di era digital yang penuh risiko. Tujuan utama kriptografi adalah memastikan bahwa data, baik dalam bentuk pesan asli maupun pesan sandi, hanya dapat diakses oleh penerima yang sah. Penelitian ini membahas konsep dasar kriptografi, jenis-jenis enkripsi, serta aplikasinya dalam kehidupan sehari-hari dan dunia teknologi informasi. Penerapan *Advanced Encryption Standard* (AES) dalam konteks keamanan data pemesanan bibit ternak di Balai Pengujian Standar Instrumen Unggas dan Aneka Ternak (BPSI UAT) menjadi fokus penelitian. 1blok plainteks berukuran 128 bit terlebih dahulu dikonversi kode ASCII menjadi matriks heksadesimal berukuran 4x4 yang disebut *state*. Setiap elemen state berukuran 1 byte. Proses *enkripsi* mengunakan 4 transformasi dasar dengan urutan trasformasi *subbytes*, *shiftrows*, *mixcolumns*, dan *addroundkey*. Sedangkan pada proses *dekripsi* mengunakan *invers* semua transformasi dasar pada algoritma AES kecuali *addroundkey* dengan urutan transformasi *invshiftrows*, *invsubbytes*, *addroundkey*,dan *invmixcolumns*. pada kriptografi AES menggunakan mode *Cipher Block Chaining* (CBC). Hasil dari penelitian ini menunjukkan keberhasilan konversi pesan asli menjadi pesan sandi yang digunakan dalam aplikasi pemesanan bibit ternak. Dalam kesimpulan, penelitian ini menggarisbawahi pentingnya penerapan kriptografi, khususnya AES, dalam menjaga keamanan data, seperti pemesanan bibit ternak.

Kata Kunci: AES, CBC, Flutter, Kriptografi

I. PENDAHULUAN

Perkembangan teknologi telah membawa dampak signifikan terutama dalam kegiatan proses pemesanan, dari yang dahulu masih menggunakan cara bertemu antar kedua belah pihak penjual dan pembeli, sampai saat ini yang telah dibuat sebuah software dengan bentuk aplikasi guna menunjang proses pemesanan antar kedua belah pihak. Software yaitu "*Computer programs and associated documentation.Software product may be developed for aparticular customer or may be developd for a general market* " yang dapat diartikan "Program komputer dan dokumentasi terkait. Produk perangkat lunak dapat dikembangkan untuk pelanggan tertentu atau dapat dikembangkan untuk pasar umum". (Sommerville, 2009, p. 6). Meskipun aplikasi untuk proses pemesanan lebih umum digunakan dalam konteks bisnis, penggunaannya masih terbatas di kalangan masyarakat karena kendala kompleksitas pembuatan dan tingginya biaya yang terkait dengan pengembangan aplikasi tersebut. Tetapi dengan adanya aplikasi dapat meminimalisir tindak kejahatan yang terjadi jika masih menggunakan cara lama.

BPSI UAT (Balai Pengujian Standar Instrumen Unggas dan Aneka Ternak) telah mengembangkan beberapa strategi untuk modernisasi proses pemesanan, menggantikan metode

e-ISSN : 2541-1330
p-ISSN : 2541-1332

tradisional yang melibatkan interaksi antar individu. Salah satu pendekatan melalui penggunaan aplikasi pihak ketiga. Meskipun demikian, penulis menemukan bahwa menggunakan aplikasi dari pihak ketiga dapat menimbulkan potensi risiko bagi pengguna, karena data tidak lagi dipegang oleh instansi itu sendiri, melainkan sepenuhnya dikelola oleh pihak ketiga. Kemudian penulis mendapati data belum melewati proses kriptografi ketika dilakukan penyimpanan. Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga.(Rosdiana, 2018, p. 21)

Dalam perkembangan kriptografi, banyak organisasi telah menciptakan algoritma dengan tujuan membuat algoritma baru atau memperbarui algoritma lama karena dianggap tidak lagi aman dalam mengatasi berbagai jenis serangan yang bertujuan membuka teks sandi tanpa memiliki kunci. *National Institute of Standards and Technology* (NIST), sebagai agensi Departemen Perdagangan AS melakukan sayembara dan menetapkan Algoritma Rijndael sebagai algoritma baru pengganti *Data Encryption Standard* (DES) karena sudah dianggap tidak aman dan kelak diberi nama *advanced encryption standard* (AES).(Munir, 2019, p. 274)

Berdasarkan hasil riset yang dilakukan oleh penulis, aplikasi pihak ketiga yang digunakan oleh BPSI UAT memiliki banyak cela yang terjadi jika tetap digunakan terutama pada bagian penyimpanan data yang dilakukan tanpa melewati proses kriptografi, oleh karena itu penulis mengambil judul "Penerapan Kriptografi AES Untuk Keamanan Data Aplikasi Pemesanan Bibit Ternak Pada BPSI UAT" hal ini sejalan untuk mengatasi masalah yang terjadi pada ruang lingkup instansi.

II. STUDI LITERATUR

Penelitian Terdahulu

Dalam penelitian ini penulis terinspirasi dan mereferensi dari penelitian-penelitian sebelumnya yang berkaitan dengan latar belakang masalah pada penelitian ini. Berikut ini penelitian terdahulu antara lain :

1. Skripsi
   Judul : IMPLEMENTASI ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) PADA LAYANAN SMS DESA.
   Penulis : Intan Fitriani
   Nim : 5302414018
   Tahun : 2020
   Fakultas : Pendidikan Teknik Informatika dan Komputer
   Universitas : Universitas Negeri Semarang
   Kesimpulan : Telah berhasil mengimplementasikan penggunaan algoritma *advanced encryption standard* (AES) pada layanan sms desa.
2. Skripsi
   Judul : IMPLEMENTASI ALGORITMA KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD PADA SISTEM INFORMASI PONDOK PESANTREN AN-NAJAH
   Penulis : Ivvan Nuzulul Huda
   Nim : 1508046027
   Tahun : 2021
   Fakultas : Sains dan Teknologi
   Universitas : UIN Walisongo Semarang
   Kesimpulan : Telah berhasil mengimplementasikan penggunaan algoritma *advanced encryption standard* (AES) pada sistem informasi pondok pesantren An-najah.
3. Skripsi
   Judul : PENERAPAN ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) PADA FITUR CHAT DALAM APLIKASI ASISTEN GURU (ASGUR)

e-ISSN : 2541-1330
p-ISSN : 2541-1332

Penulis	: Yogi Firdaus
Nim	: 15170195
Tahun	: 2021
Fakultas	: Teknik dan Informatika
Universitas	: Bina Sarana Informatika
Kesimpulan	: Telah berhasil menerapkan algoritma *Advanced Encryption Standard* (AES) pada fitur chat dalam aplikasi asisten guru (ASGUR).

Terminologi Kriptografi

- Kriptografi

Kriptografi merupakan suatu bidang keilmuan yang mempelajari teknik-teknik matematika yang berkaitan dengan aspek keamanan dengan cara mengubah pesan asli atau plainteks menjadi pesan disandi atau cipherteks begitu sebaliknya.

- Pesan, plainteks, dan cipherteks

Pesan berupa plainteks adalah teks awal yang belum melalu proses enkripsi. kemudian untuk ciipherteks adalah pesan yang butuh melalui proses dekripsi terlebih dahulu agar isi pesan dapat dilihat.

- Enkripsi dan dekripsi

Enkripsi adalah proses mengubah informasi atau data menjadi bentuk yang hampir tidak dikenali menggunakan algoritma tertentu, sedangkan dekripsi adalah proses mengembalikan bentuk tersamar tersebut menjadi informasi asalnya. Kedua pendapat ini menyatakan konsep yang sama, yaitu konversi data antara bentuk terenkripsi (cipherteks) dan bentuk asli (plainteks), dengan istilah yang berbeda seperti enkripsi dan dekripsi, atau enciphering dan deciphering.

- Pesan, plainteks, dan cipherteks

Pesan berupa plainteks adalah teks awal yang belum melalu proses enkripsi. kemudian untuk ciipherteks adalah pesan yang butuh melalui proses dekripsi terlebih dahulu agar isi pesan dapat dilihat.

Cipher, kode, dan kunci

Algoritma kriptografi untuk enkripsi dan dekripsi disebut juga cipher. Cipher dapat diartikan sebagai aturan untuk enchipering dan dechipering. Sedangkan cipher sendiri menurut Rifaldi Munir (Munir, 2019, p. 191) memiliki 2 kategori untuk cara melakukan proses kunci yaitu :

1. Cipher alir (*stream cipher*)
   Algoritma kriptografi yang memproses planteks/cipherteks dalam bentuk bit tunggal (atau *byte* tunggal), yang dalam hal ini cipher mengenkripsi (atau mendekripsi) satu bit atau satu *byte* setiap kali.
2. Cipher blok (*block cipher*)
   Algoritma kriptografi yang memproses plainteks/chipherteks dalam bentuk blok-blok bit (atau blok *byte*). Didalam cipher blok terdapat Lima mode operasi umu, diantaranya *Electronic Code Book* (ECB), *Cipher Block Chaining* (CBC), *Cipher Feedback* (CFB), *Output Feedback* (OFB), *Counter Mode.*

Perangkat Lunak (Software)

- Dart

Menurut (Syaputra & Putra Wira Ganda, 2019, pp. 4–5) menuturkan bahwa Dart adalah bahasa berorientasi objek (*Object Oriented*) dengan sintaksis (*Syntax*) *C-style*. Lalu ia juga menjelaskan terdapatnya fitur yang digunakan pada *Client Side Development* (Pengembangan dari sisi *client*) salah *Compile AoT* dan *JiT* yang membantu proses *compile* dari aplikasi yang dikembangkan.

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 8, Nomor 1, Januari 2024
http://doi.org/10.33395/remik.v8i1.13157
e-ISSN : 2541-1330
p-ISSN : 2541-1332

- Flutter

Syaputra dan Ganda (2019:18) menjelaskan Flutter merupakan sebuah *framework* aplikasi *mobile* yang bersifat *open source* (terbuka) yang diciptakan oleh Google. Flutter digunakan untuk mengembangkan aplikasi untuk *system* operasi Android dan iOS.

- Javascript (ECMAScript 6)

Javascript (ECMAScript 6) atau sering disingkat ES6 merupakan bahasa Standarisasi sebelumnya dilakukan pada tahun 2009 (dikenal dengan ECMAScript 5). Javascript telah mengalami perubahan yang berupa penambahanfitur-fitur baru seperti dukungan terhadap parameter opsional didalam fungsi, interpolasi variable didalam string, pembuatan string yang terdiri dari beberapa baris , pendefinisian kelas, pewarisan kelas, dan lain-lain. (Raharjo, 2019, p. 13).

- NodeJS

Node.js adalah perangkat lunak yang didesain untuk mengembangkan aplikasi berbasis web dan ditulis dalam sintaks bahasa pemrograman JavaScript. Bila selama ini kita mengenal JavaScript sebagai bahasa pemrograman yang berjalan di sisi *client* / *browser* saja, maka Node.js ada untuk melengkapi peran JavaScript sehingga bisa juga berlaku sebagai bahasa pemrograman yang berjalan di sisi server, sepertihalnya PHP, Ruby, Perl, dan sebagainya. (Kurniawan et al., 2020, p. 129).

- Mongodb

Mongodb merupakan salah satu dari sekian banyak penyimpanan data dalam sistem database NoSQL berupa kumpulan pasang kunci dan nilai (key-value store), kumpulan dokumen (document store), kumpulan tuple (tuple store), satu table dengan kolom yang sangat banyak (wide column store), dan lain-lain. (Raharjo, 2019, p. 193).

III. METODE

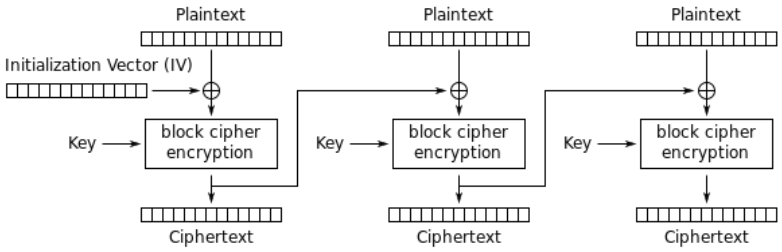
Mode CBC (*Cipher Block Chainning*)

Mode ini menerapkan mekanisme umpan-balik (*feedback*) pada sebuah blok, yaitu hasil enkripsi blok sebelumnya di umpan balikkan ke proses enkripsi blok yang sekarang. Caranya, blok plainteks yang sekarang di XOR-kan terlebih dahulu dengan blok cipherteks hasil sebelumnya. selanjutnya hasil peng-XOR-an ini masuk kedalam fungsi E. Dengan mode CBC, Setiap blok chipherteks bergantung tidak hanya pada blok plainteksnya tetapi juga pada seluruh plainteks sebelumnya. (Munir, 2019, pp. 212–213).

Menurut Henry dkk, (Henry et al., 2016, p. 47) Proses enkripsi pada mode CBC, dimana pada proses enkripsi dilakukan secara sekuensial dari blok data pertama hingga blok data terakhir.

Jika blok pertama memiliki indeks 1, maka rumus matematis untuk melakukan proses enkripsi pada mode CBC adalah :

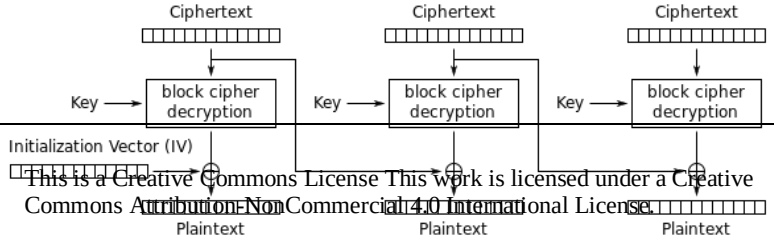
$$C_i = E_k\left(P_1 \oplus C_{i-1}\right), C_0 = IV$$



Gambar 1. Enkripsi Mode CBC
Sumber : (Henry et al., 2016, p. 47)

Sedangkan rumus matematis untuk melakukan proses dekripsi pada mode CBC adalah :

$$C_i = D_k\left(C_i\right) \oplus C_{i-1}, C_0 = IV$$



Remik: Riset dan E-Jurnal Manajemen In*forma*tika Komputer
Volume 8, Nomor 1, Januari 2024
http://doi.org/10.33395/remik.v8i1.13157
e-ISSN : 2541-1330
p-ISSN : 2541-1332

dimana :

C_i : *Ciphertext* pada blok i

P_i : *Plaintext* pada blok i

$E_k(...)$: Fungsi enkripsi yang digunakan

$D_k(...)$: Fungsi dekripsi yang digunakan

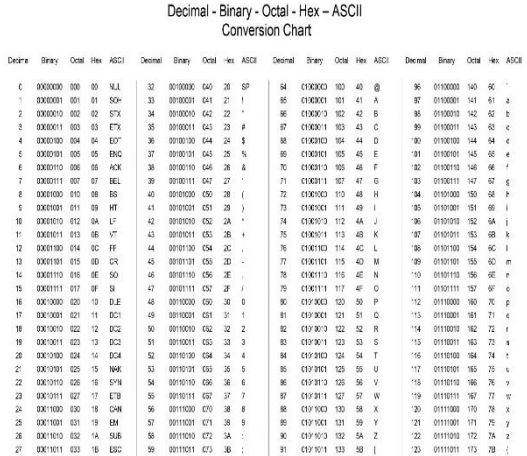
IV : Initialization Vector

Yang dalam hal ini, $C_0=IV$ (Initialization Vector). *IV* dapat diberikan oleh pengguna atau dibangkitkan secara acak oleh program. Jadi, untuk menghasilkan blok *ciphertext* pertama (C_1), *IV* digunakan untuk menggantikan blok *ciphertext* sebelumnya (C_0), Sebaliknya pada dekripsi, blok plainteks diperoleh dengan cara meng-XOR-kan *IV* dengan hasil dekripsi terhadap blok *ciphertext* pertama. Pada mode CBC, blok *Plaintext* yang sama menghasilkan blok *ciphertext* yang berbeda hanya jika blok-blok *Plaintext* sebelumnya berbeda. (Henry et al., 2016, p. 47).

Plaintext* menjadi *Hex

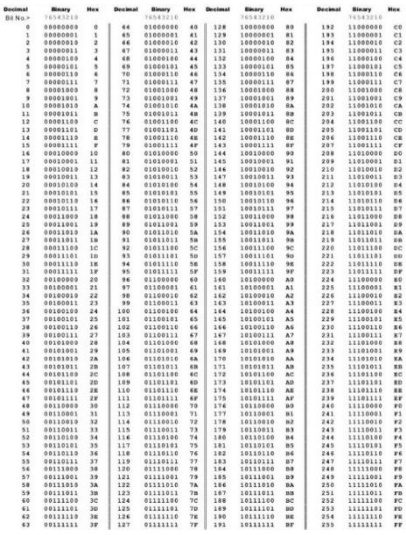
Pada awalnya plainteks atau pesan awal sebelum dieksekusi harus diubah terlebih dahulu menjadi bilangan *hex*adesimal lalu dapat dihitung. Cara mengubahnya dengan menggunakan table, seperti gambar berikut :

Table 2. ASCII to Hex 0-127



Sumber : (Weiman, 2009)

Table 1. Hex to Binary 0-255



Sumber : (Karl, 2011)

Ekspansi Kunci

Ekspansi kunci adalah melaksanakan kunci kode untuk menghasilkan suatu kunci skedul. Kunci ekspansi yang diperlukan algoritma AES yaitu Nb(Nr+1) kata dengan Nb adalah jumlah blok dan Nr adalah jumlah putaran sehingga untuk algoritma AES 128-bit memerlukan 4(10+1) = 44 kata. (Ivvan Nuzulul Huda, 2021, p. 71) .

Pembangkitan kunci putaran didalam Algoritma Rijndael tergolong rumit dan agak sukar diterangkan.Tinjau sebuah larik *key* yang panjangnya 16 *byte* (16 elemen) dan Nr = 10 putaran.

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 8, Nomor 1, Januari 2024
http://doi.org/10.33395/remik.v8i1.13157
e-ISSN : 2541-1330
p-ISSN : 2541-1332

sepuluh kunci akan disimpandidalam matriks rk. (Munir, 2019, p. 292).

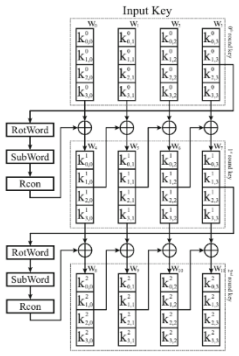
Algoritma ekspansi kunci adalah sebagai berikut:

- Salin elemen-elemen *key* ke dalam larik w[0], w[1], w[2], w[3]. Larik w[0] berisi empat elemen pertama *key*, w[1] berisi empat elemen berikutnya, dan seterusnya.
- Mulai dari i = 4 sampai 44, lakukan :
  - Jika i merupakan kelipatan 4, gunakan rumus berikut :
    w[i]= w[i-4] ⊕ *Subword*(*Rotword*(w[i-1])) ⊕ RC[i/4]
    1. *Rotword* , merupakan proses geser w[i-1] satu *byte* ke ke kiri secara sirkuler.
    2. *Subword* , merupakan proses subtitusi dengan *S-box* terhadap hasil pergeseran tersebut.
    3. RC (*Rcon*) , merupakan proses dimana tabel *Rcon* dilakukan XOR (⊕) dengan hasil *Subword* dan w[i-4]
  - Jika i bukan merupakan kelipatan 4, Maka gunakan rumus berikut :
    w[i]= w[i-1] ⊕ w[i-4]

Table 3. Tabel Rcon

Round	1	2	3	4	5	6	7	8	9	10
Rcon[]	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

Sumber : (Soliman & Abozaid, 2010, p. 52)



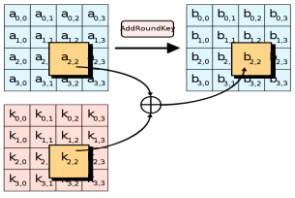
Gambar 3. key schedule of AES-128 algorithm.
Sumber : *(Kim et al., 2018)*

Kriptografi AES (*Advanced Encryption Standard*)

Algoritma *Advanced Encryption Standard* (AES) adalah algoritma enkripsi yang diterbitkan oleh *National Institute of Standards and Technology* (NIST) pada tahun 2000. Tujuan utama dari algoritma ini adalah untuk menggantikan algoritma DES setelah algoritma tersebut diketahui memiliki celah keamanan seiring dengan perkembangan kecepatan komputer. NIST mengundang para ahli yang bekerja pada bidang enkripsi dan keamanan data di seluruh dunia untuk mengembangkan algoritma *block* cipher untuk melakukan enkripsi dan dekripsi data yang lebih baik dari algoritma DES. (Ako didalam FIRDAUS, 2021, p. 8).

Menurut (Munir, 2019, p. 278), Garis besar Algoritma Rijndael atau yang sekarang disebut Algoritma AES (*Advanced Encryption Standard*) yang beroperasi pada blok 128-bit dengan kunci 128-bit adalah sebagai berikut (di luar proses pembangkitan *round key*):

- Putaran awal
  1. *AddRoundKey*: melakukan XOR antara *state* awal (plainteks) dengan *chipher key*.

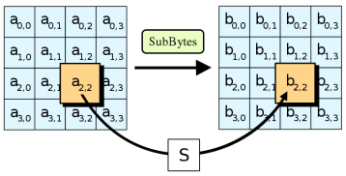


Gambar 4. Ilustrasi Transformasi AddRoundKey
Sumber : *(Asriyanik, 2017, p. 555)*

- Putaran sebanyak Nr-1 kali. Proses yang dilakukan pada setiap putaran adalah:

Remik: Riset dan E-Jurnal Manajemen In*forma*tika Komputer
Volume 8, Nomor 1, Januari 2024
http://doi.org/10.33395/remik.v8i1.13157
e-ISSN : 2541-1330
p-ISSN : 2541-1332

1. *SubBytes / InvSubByte*: subtitusi *byte* dengan menggunakan table substitusi (*S-box* / Inversi *S-box*).



Gambar 5. Ilustrasi Transformasi SubBytes
Sumber : *(Asriyanik, 2017, p. 555)*

Table 4. S-box didalam Rijndael

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0x	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1x	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2x	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3x	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4x	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5x	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6x	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7x	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8x	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9x	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
Ax	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
Bx	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
Cx	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
Dx	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
Ex	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
Fx	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Sumber : (Munir, 2019, p. 282)

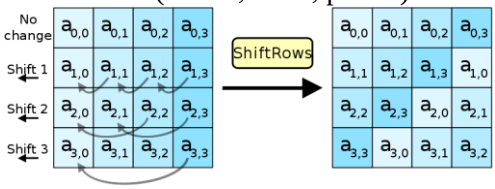
Table 5. Inversi S-box didalam Rijndael

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0x	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1x	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2x	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3x	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4x	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5x	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6x	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7x	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8x	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73

e-ISSN : 2541-1330
p-ISSN : 2541-1332

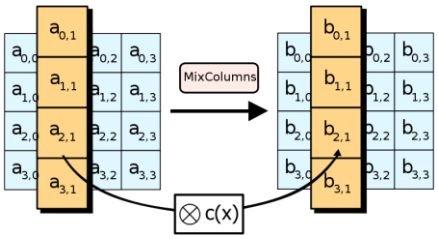
9x	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
Ax	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
Bx	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
Cx	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
Dx	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
Ex	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
Fx	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

2. *ShiftRows / InvShiftRow*: pergeseran baris-baris *array state* secara wrapping.
Sumber : (Munir, 2019, p. 296)



Gambar 6. Ilustrasi Transformasi ShiftRows
Sumber : *(Asriyanik, 2017, p. 555)*

3. *MixColumns / InvMixColumn*: mengacak data dimasing-masing kolom *array state*.



Gambar 7. Ilustrasi Transformasi MixColumns
Sumber : *(Asriyanik, 2017, p. 555)*

4. *AddRoundKey*: melakukan XOR antara *state* sekarang dengan *round key*.

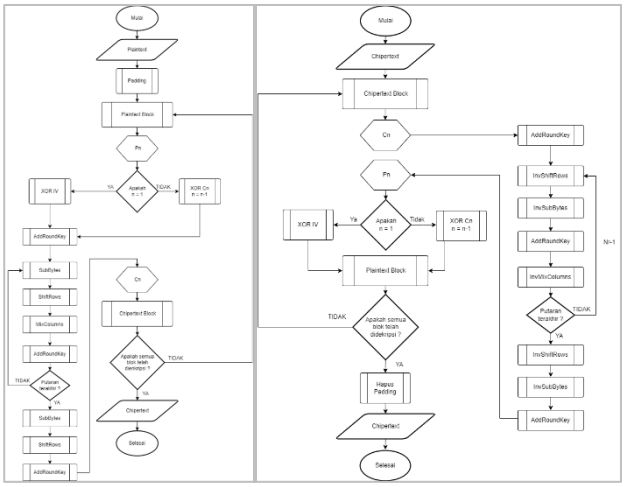
- Putaran terakhir
  1. *SubBytes / InvSubByte*
  2. *ShiftRows / InvShiftRow*
  3. *AddRoundKey*

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 8, Nomor 1, Januari 2024
http://doi.org/10.33395/remik.v8i1.13157
e-ISSN : 2541-1330
p-ISSN : 2541-1332

Hex menjadi *Base64*

Pada tahap ini peneliti akan melakukan convert kedalam *Base64* untuk menghindari tidak ditemukannya kode *hex* pada ASCII characters atau termasuk kedalam Extended ASCII characters yang berada diatas desimal 127.

Flowchart Enkripsi dan Dekripsi AES 128bit mode CBC



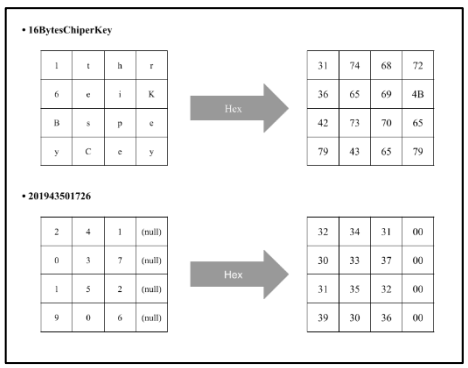
Gambar 8. Flowchart Enkripsi(Kiri) dan Dekripsi(Kanan) AES 128bit mode CBC
Sumber : *(Pakpahan & Prayino, 2021, pp. 6–7)*

IV. HASIL DAN PEMBAHASAN

Dengan menerapkan kriptografi *Advanced Encryption Standard* (AES) dalam proses enkripsi, aplikasi akan memberikan tingkat keamanan yang berbeda dibandingkan dengan aplikasi yang tidak melakukan enkripsi pada datanya. Hal ini dikarenakan *Plaintext* atau yang dikenal juga sebagai *value* awal sebelum enkripsi, akan berubah menjadi *ciphertext* yaitu value yang sudah melalui teknik-teknik matematika yang berkaitan dengan aspek keamanan informasi atau dikenal sebagai kriptografi.

Plaintext menjadi *Hex*

Pada gambar 9, merupakan proses mengubah *Plaintext* menjadi *hex* menggunakan tabel 1 ASCII to *Hex* 0-127 lalu kemudian disusun pada balok 4x4 atau 16 byte (16 elemen).



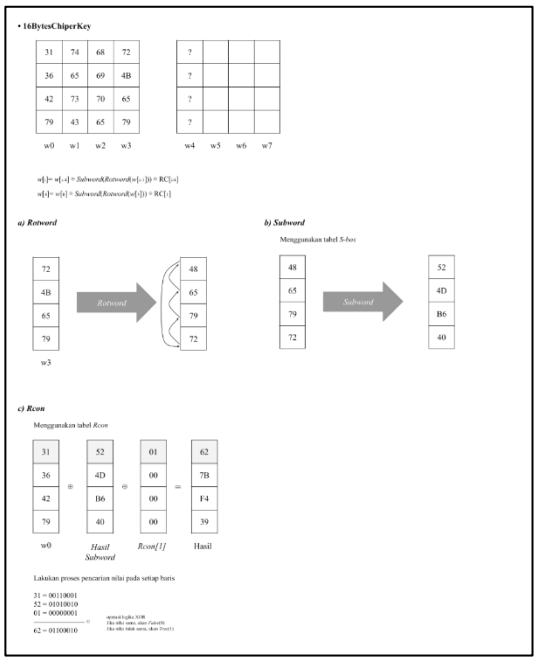
Gambar 9. *Plaintext* menjadi *Hex*
Sumber : (Penulis, 2023)

Remik: Riset dan E-Jurnal Manajemen In*forma*tika Komputer
Volume 8, Nomor 1, Januari 2024
http://doi.org/10.33395/remik.v8i1.13157
e-ISSN : 2541-1330
p-ISSN : 2541-1332

Ekspansi Kunci

- Larik kelipatan 4

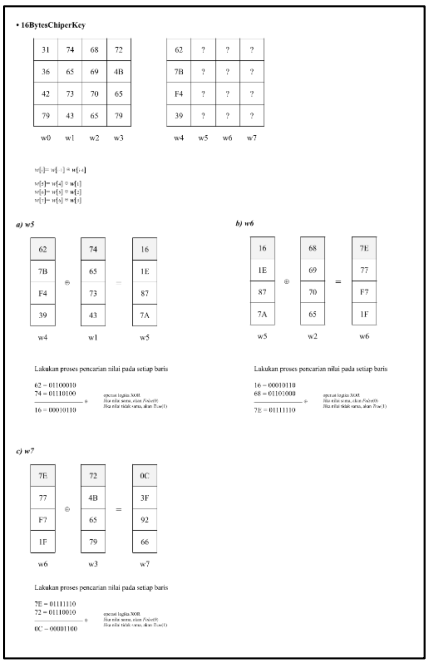
  Pada gambar 10, merupakan proses mengubah kunci "16BytesChiperKey" mejadi *hex* lalu dijadikan Ekspansi kunci awal yang akan dijadikan value untuk w[4] dan sebagai kunci bukan kelipatan 4.



Gambar 10. Ekspansi kunci larik kelipatan 4
Sumber : (Penulis, 2023)

- Larik selanjutnya

  Pada gambar 11, merupakan kelanjutan dari proses mendapatkan value untuk w[5], w[6], w[7] sebagai kunci bukan kelipatan 4. Dan akan menghasilkan kunci untuk menghitung w[8].

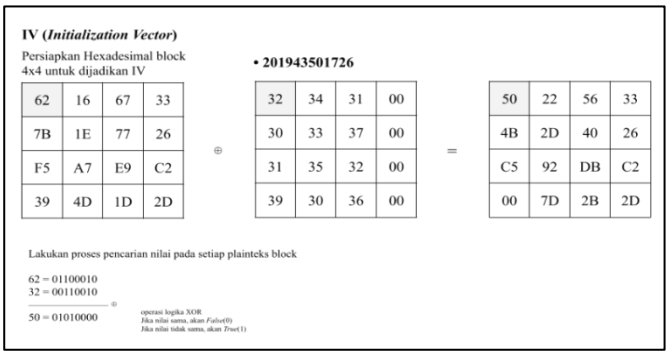


Gambar 11. Ekspansi kunci bukan larik kelipatan 4
Sumber : (Penulis, 2023)

Remik: Riset dan E-Jurnal Manajemen In*forma*tika Komputer
Volume 8, Nomor 1, Januari 2024
http://doi.org/10.33395/remik.v8i1.13157
e-ISSN : 2541-1330
p-ISSN : 2541-1332

- Hasil ekspansi
  Pada tabel 6, merupakan hasil dari ekspansi kunci.

Table 6. Table Output Kunci Ekspansi



Gambar 12. Putaran awal proses IV
Sumber : (Penulis, 2023)

Proses Algoritma

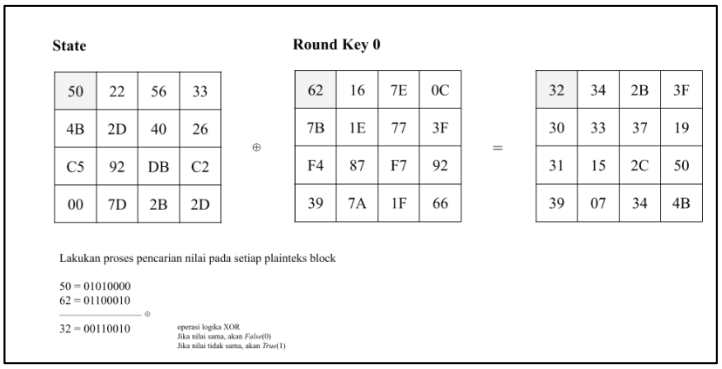
- Putaran awal
  1. IV (*Initialization Vector*)
     Pada gambar 12, merupakan proses IV (*Initialization Vector*) menggunakan *hex* yang telah disiapkan dan dilakukan pada AES mode CBC.

62	16	7E	0C	83	F7	9F	ED	6A	9D	02	EF
7B	1E	77	3F	7B	1E	77	3C	34	2A	5D	61
F4	87	F7	92	F4	87	F7	92	C7	40	B7	25
39	7A	1F	66	39	7A	1F	66	6C	16	09	6F
Ronde 0				Ronde 1				Ronde 2			
81	1C	1E	F1	2D	31	2F	DE	FA	CB	E4	3A
0B	21	7C	1D	71	50	2C	31	C2	92	BE	8F
6F	2F	98	BD	41	6E	F6	4B	20	4E	B8	F3
B3	A5	AC	C3	12	B7	1B	D8	0F	B8	A3	7B
Ronde 3				Ronde 4				Ronde 5			
A9	62	86	BC	B9	DB	5D	E1	E6	3D	60	81
CF	5D	E3	6C	3D	60	83	EF	97	F7	74	9B
01	4F	F7	04	DE	91	66	62	FA	6B	0D	6F
8F	37	94	EF	EA	DD	49	A6	12	CF	86	20
Ronde 6				Ronde 7				Ronde 8			
E9	D4	B4	35	13	C7	73	46				
3F	C8	BC	27	24	EC	50	77				
4D	26	2B	44	B8	9E	B5	F1				
1E	D1	57	77	88	59	0E	79				
Ronde 9				Ronde 10							

  2. *AddRoundKey*

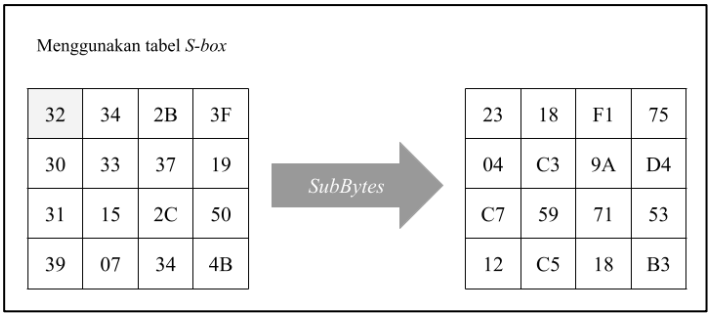
Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 8, Nomor 1, Januari 2024
http://doi.org/10.33395/remik.v8i1.13157
e-ISSN : 2541-1330
p-ISSN : 2541-1332

Pada gambar 13, merupakan proses *AddRoundKey*. *State* melakukan XOR dengan *RoundKey* ke 0.



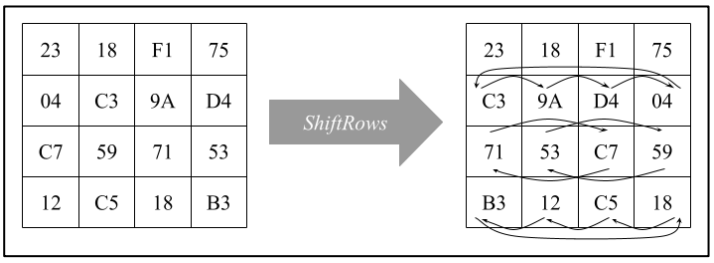
Gambar 13. Putaran awal proses *AddRoundKey*
Sumber : (Penulis, 2023)

- Putaran 1
  1. *SubBytes*
     Pada gambar 14, merupakan proses putaran 1 yaitu *SubBytes*. Untuk mengubah angka menggunakan tabel 4 yaitu *table S-box*.



Gambar 14. Putaran 1 proses *SubBytes*
Sumber : (Penulis, 2023)

  2. *ShiftRows*
     Pada gambar 15, merupakan proses putaran 1 yaitu *Shiftrow*. Untuk melakukan rotasi posisi angka dapat dilihat pada gambar.

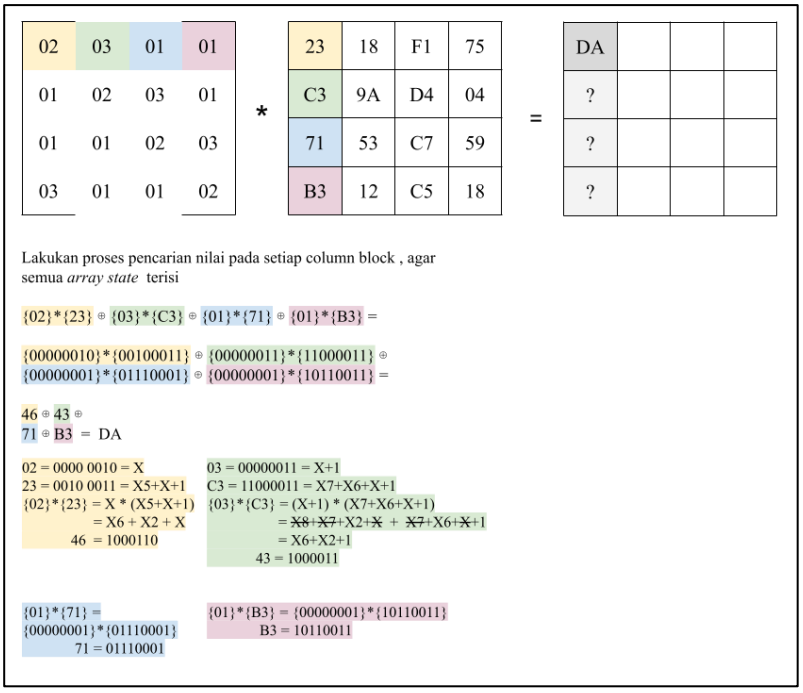


Gambar 15. Putaran 1 proses *ShiftRows*
Sumber : (Penulis, 2023)

  3. *MixColumns*

Remik: Riset dan E-Jurnal Manajemen In*forma*tika Komputer
Volume 8, Nomor 1, Januari 2024
http://doi.org/10.33395/remik.v8i1.13157
e-ISSN : 2541-1330
p-ISSN : 2541-1332

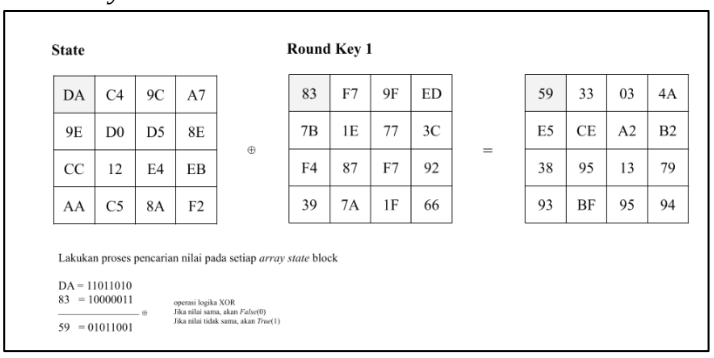
Pada gambar 16, merupakan proses putaran 1 yaitu *MixColumns*. Untuk melakukan XOR secara metriks dapat dilihat pada gambar.



Gambar 16. Putaran 1 proses *MixColumns*
Sumber : (Penulis, 2023)

4. *AddRoundKey*

Pada gambar 17, merupakan proses *AddRoundKey*. State melakukan XOR dengan *RoundKey* ke 1.



Gambar 17. Putaran 1 proses *AddRoundKey*
Sumber : (Penulis, 2023)

- Hasil Putaran

Remik: Riset dan E-Jurnal Manajemen In*forma*tika Komputer
Volume 8, Nomor 1, Januari 2024
http://doi.org/10.33395/remik.v8i1.13157
e-ISSN : 2541-1330
p-ISSN : 2541-1332

Pada tabel 7, merupakan hasil dari seluruh perputaran AES. Dan kemudian hasil akhir dijadikan *Base64* dan jadilah *Chipertext*.

Table 7. *Table Output Round* AES 128 CBC

Ronde	*Mulai Ronde*				*SubBytes*				*ShiftRows*				*MixColumns*				*Kunci*				*AddRoundKey*			
0	50	22	56	33													62	16	7E	0C	32	34	2B	3F
	4B	2D	40	26													7B	1E	77	3F	30	33	37	19
	C5	92	DB	C2													F4	87	F7	92	31	15	2C	50
	00	7D	2B	2D													39	7A	1F	66	39	07	34	4B
1	32	34	2B	3F	23	18	F1	75	23	18	F1	75	DA	C4	9C	A7	83	F7	9F	ED	59	33	03	4A
	30	33	37	19	04	C3	9A	D4	C3	9A	D4	04	9E	D9	D5	8E	7B	1E	77	9C	E5	CE	A2	B2
	31	15	2C	50	C7	59	71	53	71	53	C7	59	CC	12	E4	EB	F4	87	F7	92	38	95	13	79
	39	07	34	4B	12	C5	18	B8	B8	12	C5	18	AA	C5	8A	F2	39	7A	1F	66	93	BF	95	91
2	59	33	03	4A	CB	C3	7B	D6	CB	C3	7B	D6	54	B9	A0	C7	6A	9D	02	EF	3E	24	A2	2B
	E5	CE	A2	B2	D9	8B	3A	37	8B	3A	37	D9	63	AA	14	2B	34	2A	5D	61	57	80	49	4A
	38	95	13	79	07	2A	7D	B6	7D	B6	07	2A	DC	F1	5A	25	C7	40	B7	25	1B	B1	ED	00
	93	BF	95	94	DC	08	2A	22	22	DC	08	2A	F4	71	AD	C6	6C	16	09	6F	98	67	A4	A9
3	3E	24	A2	2B	B2	36	3A	34	B2	36	3A	34	B5	04	1F	04	81	1C	1E	F1	34	18	21	F5
	57	80	49	4A	5B	CD	3B	D6	CD	3B	D6	5B	1F	A3	E2	88	0B	21	7C	1D	14	82	9E	95
	1B	B1	ED	00	AF	C8	55	63	55	63	AF	C8	BB	01	3D	3F	6F	2F	98	BD	D4	2E	A5	82
	98	67	A4	A9	46	85	49	D3	D3	46	85	49	E8	8E	26	3D	B3	A5	AC	C3	5B	2B	8A	9E
4	34	18	21	F5	18	AD	FD	E6	18	AD	FD	E6	08	76	26	8D	2D	81	2F	DE	25	47	09	53
	14	82	9E	95	FA	13	0B	2A	13	0B	2A	FA	1F	B7	80	24	71	50	2C	31	4E	E7	AC	15
	D4	2E	A5	82	48	31	06	13	06	13	48	31	1A	CB	4F	FC	41	6E	F6	4B	5B	A5	B9	B7
	5B	2B	8A	9E	39	F1	7E	0B	0B	39	F1	7E	2B	86	87	06	12	B7	1B	D8	19	41	9C	DE
5	25	47	09	53	3F	A0	01	ED	3F	A0	01	ED	92	48	17	68	FA	CB	E4	3A	68	83	F3	52
	4E	E7	AC	15	2F	94	91	59	94	91	59	2F	EB	6B	3F	67	C2	92	BE	8F	29	F9	81	E8
	5B	A5	B9	B7	39	06	56	A9	56	A9	39	06	20	4E	78	B7	20	4E	B8	F3	00	00	C0	44
	19	31	9C	DE	12	C7	DE	1D	1D	12	C7	DE	B9	E7	F6	A2	0F	B3	A3	7B	B6	5F	55	D9
6	68	83	F3	52	45	EC	0D	00	45	EC	0D	00	B5	82	00	6B	A9	62	B6	BC	1C	E0	86	D7
	29	F9	81	E8	A5	99	0C	9B	99	0C	9B	A5	8C	97	4A	08	CF	5D	E3	6C	43	CA	A9	64
	00	00	C0	44	63	63	BA	1B	BA	1B	63	63	EC	04	1A	7C	01	4F	F7	04	ED	4B	BD	78
	B6	5F	55	D9	4E	CF	FC	35	35	4E	CF	FC	86	A4	6A	25	8F	17	94	EF	09	91	FB	CA
7	1C	E0	86	D7	9C	E1	44	0E	9C	E1	44	0E	9E	0A	C4	3A	B9	DB	3D	E1	27	D1	99	DB
	43	CA	A9	64	1A	74	D3	43	74	D3	43	1A	FF	82	E1	4F	3D	60	83	EF	C2	E2	62	A0
	ED	4B	BD	78	55	B3	55	BC	55	BC	55	B3	DE	52	D2	BF	DE	91	66	62	00	C3	B4	DD
	09	93	FL	CA	01	DC	BB	74	74	01	DC	BB	76	55	79	D6	EA	DD	49	A6	9C	88	30	70
8	27	D1	99	DB	CC	3E	EE	B9	CC	3E	EE	B9	EC	B6	5B	2C	E6	3D	60	81	0A	BB	3B	AD
	C2	E2	62	A0	25	98	AA	E0	98	AA	E0	25	3A	F7	54	85	97	F7	74	9B	AD	00	20	1E
	00	C3	B4	DD	63	2E	8D	C1	8D	C1	63	2E	A6	74	9F	CC	FA	6B	0D	6F	5C	1F	92	A3
	9C	88	30	70	DE	C4	04	51	51	DE	C4	04	F8	8E	89	D3	12	CF	86	20	EA	41	BF	F3
9	0A	BB	3B	AD	67	EA	E2	95	67	EA	E2	95	79	80	80	5D	E9	D4	B4	35	C0	54	34	68
	AD	00	20	1E	93	63	B7	72	63	B7	72	93	7D	06	5B	F7	3F	C8	BC	27	42	CE	E7	D0
	5C	1F	92	A3	4A	C0	4F	0A	4F	0A	4A	C0	8D	DB	9A	83	4D	26	2B	44	C0	FD	B1	C7
	EA	41	BF	F3	87	83	08	0D	0D	87	83	08	9F	8D	18	E1	1E	D1	57	77	81	5C	4F	96
10	C0	54	34	68	BA	20	18	45	BA	20	18	45					13	C7	73	46	A9	E7	6B	03
	42	CE	E7	D0	2C	8B	94	70	8B	94	70	2C					24	EC	50	77	AF	78	20	5B
	C0	FD	B1	C7	BA	54	C8	C6	C8	C6	BA	54					B8	9E	B5	F1	70	58	0E	A5
	81	5C	4F	96	0C	4A	84	90	90	0C	4A	84					88	59	0E	79	18	55	44	FD

Sumber : (Penulis, 2023)

Hex menjadi *Base64*

Pada gambar 18, merupakan proses *hex* menjadi *Base64* untuk mengatasi karakter ASCII diatas 127 yang tidak terdefinisi.

Gambar 18. *Hex to Base64* menggunakan cryptii
Sumber : (Penulis, 2023)

Implementasi pada Aplikasi

- Enkripsi

  Implementasi enkripsi terdiri dari beberapa bagian antara lain *Plaintext* dan *key*. Selanjutnya aplikasi akan diatur terlebih dahulu *key* dan kita coba melakukan *input Plaintext*, yang dimana :

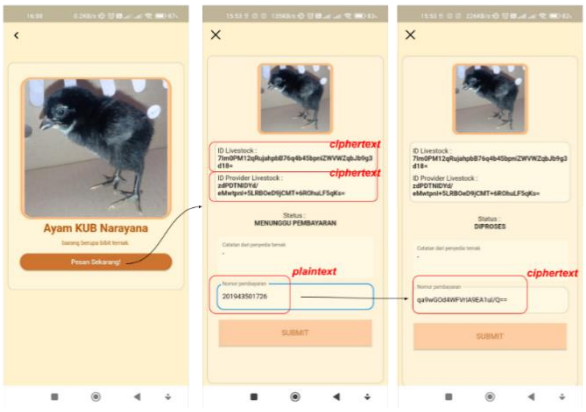
  key : 16BytesChiperKey
  Plaintext : 201943501726

  Pada gambar 19 diperlihatkan bahwa ketika aplikasi melakukan aksi “pesan sekarang!” maka akan membuat sebuah pesanan baru dengan ID Livestock dan ID Provider Livestock telah dilakukan enkripsi

  Selanjutnya diperlihatkan bahwa ketika *user* melakukan “submit”, Nomor Pembayaran yang telah diisi akan dienkripsi sehingga baik pada data ID Livestock, ID Provider Livestock dan Nomor Pembayaran akan tersimpan dalam bentuk *ciphertext*. dapat dilihat bahwa hasilnya sama dengan pada bagian *hex* menjadi *Base64*, yaitu :

  Chipertext : qa9wGOd4WFVrIA9EA1ul/Q==

Remik: Riset dan E-Jurnal Manajemen In*forma*tika Komputer
Volume 8, Nomor 1, Januari 2024 e-ISSN : 2541-1330
http://doi.org/10.33395/remik.v8i1.13157 p-ISSN : 2541-1332



Gambar 19. Tampilan Implementasi enkripsi pada aplikasi
Sumber : (Penulis, 2023)

- Dekripsi

  Sama seperti proses enkripsi, pada Implementasi dekripsi terdiri dari beberapa bagian antara lain *key*. Selanjutnya aplikasi akan diatur terlebih dahulu *key* yang sama, yang dimana :

  key : 16BytesChiperKey

  Pada gambar 20 diperlihatkan bahwa hasil dekripsi menghasilkan *Plaintext* berikut dapat dilihat bahwa hasilnya sama dengan *Plaintext* awal, yaitu :

  Plaintext : 201943501726

Gambar 20. Tampilan Implementasi dekripsi pada aplikasi
Sumber : (Penulis, 2023)

V. KESIMPULAN

Kesimpulan yang dapat diambil dari penerapan kriptografi *advanced encryption standard* (AES) untuk keamanan data aplikasi pemesanan bibit ternak pada BPSI UAT (Balai Pengujian Standar Instrumen Unggas dan Aneka Ternak) adalah Berhasilnya proses enkripsi dan dekripsi pada kriptografi AES menggunakan mode *Cipher Block Chaining* (CBC) dengan kunci awal "16BytesChiperKey" dan diujikan dengan pesan asli "201943501726" didapatkan pesan disandi "qa9wGOd4WFVrIA9EA1ul/Q==" menunjukkan bahwa pesan asli berhasil diubah menjadi pesan disandi hal ini merupakan salah satu hasil sebagai solusi bagi pihak perusahaan untuk meningkatkan keamanan pada saat penyimpanan data pemesanan bibit ternak sehingga data yang tersimpan didalam aplikasi sudah dalam bentuk enkripsi.

VI. REFERENSI

Asriyanik. (2017). Studi Terhadap Advanced Encryption Standard (Aes) Dan. *Jurnal Ilmiah Sains Dan Teknologi*, *7*(1), 553–561.

FIRDAUS, Y. (2021). *Penerapan Algoritma Advanced Encryption Standard (Aes) Pada Fitur Chat Dalam Aplikasi Asisten Guru (Asgur)*. https://repository.bsi.ac.id/index.php/repo/viewitem/31151%0Ahttps://repository.bsi.ac.id/index.php/unduh/item/332077/Skripsi-PENERAPAN-ALGORITMA-ADVANCED-ENCRYPTION-STANDARD-.pdf

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.

Ivvan Nuzulul Huda. (2021). *IMPLEMENTASI ALGORITMA KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD PADA SISTEM INFORMASI PONDOK PESANTREN AN-NAJAH*. 6.

Karl. (2011). *Decimal-Binary-Hexadecimal Conversion Chart*. https://www.scribd.com/document/69978100/Decimal-Binary-Hexadecimal-Conversion-Chart

Kim, P., Han, D., & Jeong, K. C. (2018). Time–space complexity of quantum search algorithms in symmetric cryptanalysis: applying to AES and SHA-2. *Quantum Information Processing*, *17*(12), 1–39. https://doi.org/10.1007/s11128-018-2107-3

Kurniawan, I., Humaira, & Rozi, F. (2020). REST API Menggunakan NodeJS pada Aplikasi Transaksi Jasa Elektronik Berbasis Android. *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi*, *1*(4), 127–132. https://doi.org/10.30630/jitsi.1.4.18

Munir, R. (2019). *KRIPTOGRAFI EDISI KEDUA* (KEDUA). Informatika Bandung.

Pakpahan, A. V, & Prayino, N. F. (2021). Implementasi Algoritma Rijndael Untuk Keamanan Login (Studi Kasus: Perangkat Lunak Keuangan Pemberian Tunjangan Di Kantor …. *... : Jurnal Teknik Mesin, Elektro Dan Ilmu ...*, *12*(1), 1–13. https://jurnal.umk.ac.id/index.php/simet/article/view/4442

Raharjo, B. (2019). *PEMROGRAMAN WEB DENGAN NODE.JS DAN JAVASCRIPT*. Informatika Bandung.

Rosdiana, R. (2018). Sekuritas Sistem Dengan Kriptografi. *Al-Khwarizmi: Jurnal Pendidikan Matematika Dan Ilmu Pengetahuan Alam*, *3*(1), 21–32. https://doi.org/10.24256/jpmipa.v3i1.216

Soliman, M. I., & Abozaid, G. Y. (2010). FastCrypto: Parallel AES pipelines extension for general-purpose processors. *Neural, Parallel and Scientific Computations*, *18*(1), 47–58. https://doi.org/10.1115/1.802977.paper114

Sommerville, I. (2009). *Software Engineering (9th ed.; Boston, Ed.). Massachusetts: Pearson Education.*

Syaputra, R., & Putra Wira Ganda, Y. (2019). *Happy Flutter* (Y. P. W. Ganda (ed.)). Al Qolam.

Weiman, D. (2009). *ASCII Conversion Chart*. https://web.alfredstate.edu/faculty/weimandn/miscellaneous/ascii/ascii_index.html