STORAGE – Jurnal Ilmiah Teknik dan Ilmu Komputer, Vol. 4 No. 2, Mei 2025, 111 - 119
e-ISSN: 2828-5344 | DOI: 10.55123

PERANCANGAN PENERAPAN ALGORITMA KRIPTOGRAFI AES 256 UNTUK KEAMANAN DATABASE APLIKASI MANAJEMEN SISWA

[1)]Dian Sri Purwanti, [2)]Muhammad Fadli, [3)]Muhammad Surono, [4)]Erliyan Redy Susanto
[1,2,3,4)] Fakultas Teknik dan Ilmu Komputer, Magister Ilmu Komputer, Universitas Teknokrat Indonesia
[2)] Jurusan Ekonomi dan Bisnis, Pengelolaan Perhotelan, Politeknik Negeri Lampung
[1)] dian_sri_purwanti@teknokrat.ac.id,[2)]muhammadfadliofficial@polinela.ac.id,
[3)]muhammadsurono@teknokrat.ac.id, [4)]erliyan.redy@teknokrat.ac.id

INFO ARTIKEL

Riwayat Artikel :
Diterima : 10 Mei 2025
Disetujui : 27 Mei 2025

Kata Kunci :
AES 256-256, Keamanan Data, Kriptografi, Sistem Informasi, Database

ABSTRAK

Mengelola sistem informasi berbasis web memerlukan keamanan data, terutama di institusi pendidikan di mana informasi pribadi siswa disimpan. Basis data aplikasi manajemen siswa di SMKN XYZ Bandar Lampung dibuat lebih aman dalam penelitian ini dengan memanfaatkan teknik kriptografi AES 256. Urgensi penelitian ini ditekankan oleh meningkatnya risiko terhadap sistem informasi akademik yang dapat mengakibatkan pelanggaran data dan penyalahgunaan. Implementasi dan analisis kinerja AES 256 untuk menjaga integritas dan keamanan data siswa adalah topik utama dari penelitian ini. Mengelola sistem informasi berbasis web memerlukan keamanan data, terutama di lembaga pendidikan di mana informasi pribadi siswa disimpan. Basis data aplikasi manajemen siswa di SMKN XYZ Bandar Lampung dibuat lebih aman dalam penelitian ini dengan memanfaatkan teknik kriptografi AES 256. Urgensi penelitian ini ditekankan oleh meningkatnya risiko terhadap sistem informasi akademik yang dapat mengakibatkan pelanggaran data dan penyalahgunaan. Implementasi dan analisis kinerja AES 256 untuk menjaga keamanan dan integritas data siswa adalah topik utama dari penelitian ini.

ARTICLE INFO

Article History :
Received : Mei 10, 2025
Accepted : Mei 27, 2025

Keywords*:*
AES 256-256, Data Security, Cryptography, Information Systems, Database

ABSTRACT

Overseeing a web-based data framework requires information security, particularly in instructive educate where students' individual data is put away. The database of understudy administration application at SMKN 4 Bandar Lampung is made more secure in this investigate by utilizing AES 256 cryptography procedure. The direness of this investigate is emphasized by the expanding dangers to scholastic data frameworks that can result in information breaches and abuse. The execution and execution examination of AES 256 to preserve the judgment and security of student information is the most subject of this investigate. Overseeing web-based data frameworks requires information security, particularly in instructive teach where students' individual data is put away. The database of understudy administration application at SMKN 4 Bandar Lampung is made more secure in this inquire about by utilizing AES 256 cryptographic procedure. The direness of this inquire about is emphasized by the expanding dangers to scholarly data frameworks that can result in information breaches and misuse. Implementation and execution investigation of AES 256 to preserve the security and judgment of understudy information is the most point of this study.

1. PENDAHULUAN

Dengan Seiring dengan perkembangan yang cepat di dunia digital, keamanan data merupakan komponen esensial dalam pengelolaan informasi. Kemajuan teknologi informasi juga membuat pengguna lebih mudah berkomunikasi melalui berbagai media, termasuk pengiriman dan penerimaan data dalam jumlah besar (Liwandouw & Wowor, 2017). Namun, kemudahan ini diiringi dengan peningkatan kemungkinan serangan siber yang dapat membocorkan data sensitif. Pelaku kejahatan siber sering menggunakan celah keamanan sistem informasi untuk mengakses, mencuri, atau memanipulasi data sensitif (Anwar, 2017)(Baso & L, 2024). Perkembangan dalam Teknologi dan data ini harus diperhatikan, terutama dalam hal keamanan data dan informasi (Setiawan & Fatimah, 2021)(Nizamuddin Aulia Kafa & Dolly Virgian Shaka Yudha Sakti, 2024). Pengamanan data dan informasi sangat penting untuk memastikan bahwa informasi atau pesan tidak bocor kepada orang yang tidak sah (Santoso et al., 2018)(Purnama & Rohayani, 2015)(Handoko & Rony, 2018). Oleh karena itu, untuk menjamin perlindungan dan pencegahan data akses yang tidak sah, langkah-langkah mitigasi risiko sangat penting (Santoso et al., 2018)(R. Andriyanto et al., 2020)(Priyadi et al., n.d.).

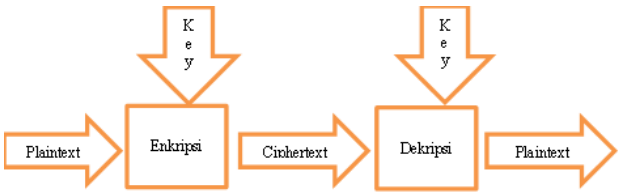
Dunia pendidikan adalah salah satu bidang yang paling rentan terhadap serangan siber karena lembaga pendidikan menyimpan banyak informasi pribadi, seperti data pribadi siswa, nilai akademik, dan riwayat pendidikan mereka. Di SMKN 4 Bandar Lampung, sistem manajemen data siswa berbasis web menghadapi masalah besar dalam menjaga keamanan data tersebut. Penyalahgunaan, manipulasi, atau bahkan pencurian identitas dapat terjadi jika data akademik jatuh ke tangan orang yang tidak bertanggung jawab. Untuk mengatasi masalah ini, metode keamanan yang dapat diandalkan dibutuhkan untuk memastikan kerahasiaan, integritas, dan autentikasi data yang ada di sistem informasi sekolah.

Mengubah data menjadi bentuk yang tidak dapat dibaca oleh orang yang tidak berwenang atau tidak sah dikenal sebagai kriptografi, sebuah alat penting untuk melindungi data(Saputra et al., 2024). Untuk meningkatkan keamanan data, berbagai algoritma telah dikembangkan, termasuk *Advanced Encryption Standard* (AES), yang sangat dikenal karena keamanannya. Dimana versi AES 256, yang menawarkan tingkat keamanan paling optimal yang memiliki panjang kunci 256-bit, melindunginya dari serangan *brute force* dan serangan kriptografi lainnya (Nagaraju et al., 2023)(M. R. Andriyanto & Sukmasetya, 2022)(Gunawan, 2021).

Penelitian ini bertujuan untuk menerapkan algoritma AES 256 untuk meningkatkan keamanan *database* aplikasi manajemen siswa berbasis web di SMKN 4 Bandar Lampung. Beberapa langkah penting akan dibahas dalam penelitian ini: pertama, desain sistem enkripsi dan dekripsi yang menggunakan AES 256; kedua, penerapan algoritma dalam aplikasi manajemen siswa; dan ketiga, pengujian kinerja enkripsi dan dekripsi dalam menangani data akademik.

2. METODE

Pada awalnya, kriptografi adalah ilmu yang mempelajari cara menyembunyikan pesan(Keamanan & Sosial, 2024). Namun, saat ini, kriptografi adalah ilmu yang menangani keamanan informasi seperti kerahasiaan, keutuhan, data, dan otentikasi entitas dengan menggunakan teknik matematika(Nanda et al., 2024)(Wahyu et al., 2024). Oleh karena itu, kriptografi modern mencakup lebih dari hanya menyembunyikan pesan; itu lebih tentang menggabungkan metode untuk menjaga keamanan informasi(Saputra et al., 2024). Proses kriptografi terdiri dari dua tahap utama: enkripsi dan deskripsi(Purnama & Rohayani, 2015)(Ginting et al., 2015)(Saleh & Windarto, 2018). Sistem ini mengenkripsi teks asli *(plaintext)* menjadi teks tersandi *(ciphertext)* (Liwandouw & Wowor, 2017)(Purnama & Rohayani, 2015). Kemudian, proses dekripsi menggunakan kunci yang sama untuk mengembalikan teks tersandi ke bentuk aslinya(Syahrani & Pramusinto, 2024). Gambar 1 berikut menunjukkan proses enkripsi dan dekripsi data:



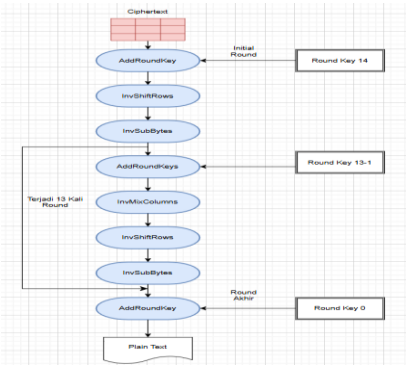
Gambar 1. Proses enkripsi dan dekripsi

Saat ini, algoritma Data Enkripsi Standar (DES) dianggap tidak aman untuk enkripsi sandi blok kunci simetrik 64-bit dan 56-bit karena ukuran kuncinya yang pendek rentan terhadap serangan *brute force*. *Advanced Encryption Standard* (AES 256) telah menggantikan DES beberapa tahun terakhir(Sidabutar et al., 2024). AES 256 menggunakan komponen yang selalu memiliki invers dengan panjang blok 128 bit; kuncinya dapat berukuran 128, 192, atau 256 bit (Algoritma et al., 2024). Metode berulang digunakan untuk menyalin AES 256 (R. Andriyanto et al., 2020).

Algoritma memulai dengan tahap utama yang terdiri dari tiga belas putaran. Setiap putaran mengandung transformasi yang disebutkan di bawah ini:

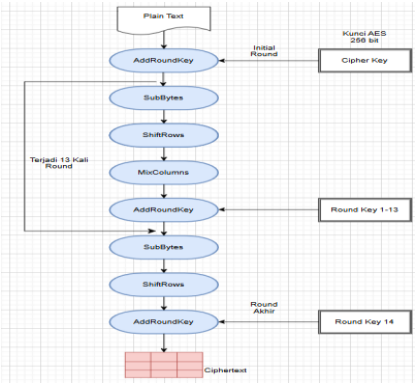
- *SubByte* untuk melakukan substitusi *byte*, gunakan *S-Box*. Ini meningkatkan kekacauan.
- *ShiftRows* mengubah baris matriks data untuk meningkatkan difusi.
- *MixColumns* melakukan operasi matriks untuk menyebarkan perubahan ke setiap kolom.
- *AddRoundKey* menggabungkan data dengan kunci enkripsi yang telah diperluas dari kunci awal.

Untuk menunjukkan bagaimana enkripsi AES dilakukan dapat dilihat pada gambar dibawah ini:



Gambar 2. Proses Enkripsi AES-256

Pada langkah awal, dekripsi dimulai dengan *AddRoundKey*, yang menggunakan *Round Key* 14 yang diperoleh dari proses ekspansi kunci. Kemudian, *InvShiftRows* dan *InvSubBytes* diubah, yang merupakan kebalikan dari operasi substitusi dan pergeseran yang dilakukan selama proses enkripsi. Operasi *AddRoundKey* kemudian dilakukan, yang menggunakan tombol *round* 13 hingga 1 dalam tiga belas putaran. Dalam setiap putaran, ada transformasi tambahan, seperti *InvMixColumns*, yang digunakan untuk menyebarkan perubahan di antara kolom matriks blok data. Prosedur berulang sebanyak tiga belas kali hingga mencapai tahap terakhir. Hanya tiga operasi-*InvShiftRows*, *InvSubBytes*, dan *AddRoundKey* digunakan pada round akhir, dengan menggunakan *Round Key* 0, yang merupakan kunci awal proses enkripsi. Proses ini berhasil mengembalikan *ciphertext* ke *plaintext* yang asli. Proses deskripsi AES 256 dapat dilihat sebagai berikut:



Gambar 3. Proses Dekripsi AES-256

Adapun langkah-langkah pada penelitian kali ini adalah sebagai Tinjauan penelitian tentang kriptografi, terutama teori tentang algoritma AES 256, eksperimen dengan algoritma enkripsi AES 256, membuat aplikasi untuk enkripsi AES 256 dan testing program enkripsi AES 256 dengan aplikasi yang telah dibuat.

3. HASIL DAN PEMBAHASAN

1. Analisis Advanced Encryption Standard (AES) 256

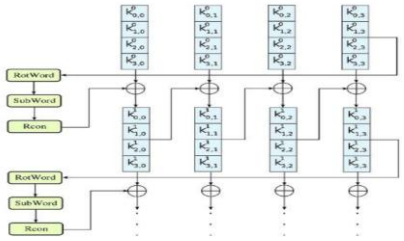
Studi ini menggunakan AES 256-bit yang setra dengan 64 karakter heksadesimal, Berikut adalah ilustrasi penggunaan AES 256 di karakter data siswa.

a. Definisikan *plaintext* dan *key*.
Plaintext= Muhammad Alfariz
Key= 3a 0f 6a 84 c0 2d 14 db 2f 8e 9c 46 5b 6d f6 6f
4b 64 f4 c9 3d 24 9c 0d 4b 92 78 65 42 09 29 b9

b. Konversi *plaintext* dan *key* diatas ke dalam nilai *hexadecimal*

Pada proses ini *key* utama akan diperbanyak sesuai dengan jumlah ukuran *key* yang digunakan dengan ukuran

32*byte* (256bit) yang memiliki 14 key yang berbeda untuk setiap roundnya. Berikut adalah gambaran *key expansion*



Gambar 4. key expansion AES

Langkah pertama merubah 16*byte* kunci utama ke dalam matrix 4x4, menggunakan AES-256, maka membuat matrix 4x8/ 2 matrix 4x4 seperti berikut:

Tabel 1. Matrix 4x4

3a	c0	2f	5b	4b	3d	4b	42
0f	2d	8e	6d	64	24	92	09
6a	14	9c	f6	f4	9c	78	29
84	db	46	6f	c9	0d	65	b9

Dikarenakan panjang kunci utama 256 bit (32*byte* atau 8*word* karena 1 *word* = 4 *byte*) jadi jumlah *word* (Nk) adalah 256:32 = 8*word* yang dibagi setiap *key* menjadi 4 *word* per *key*, dan AES 256 membutuhkan 15 *key* (14 putaran + 1 untuk tambahan per-*round*) maka jumlah *word* yang dibutuhkan dituliskan sebagai berikut: $(Nb \times (Nr + 1))$ Nb = Jumlah kolom di setiap *state matrix* (4), Nr = Jumlah putaran enkripsi (14), Jadi total *word* yang dibutuhkan = $(4 \times (14 + 1))$ = 60 *words*. Sedangkan Nk = 8 yang dibagi menjadi *word* hasilnya menjadi:

W0 = 3a0f6a84 W1 = c02d14db W2 = 2f8e9c46 W3 = 5b6df66f

W4 = 4b64f4c9 W5 = 3d249c0d W6 = 4b927865 W7 = 420929b9

- Proses *RotWord* yaitu memindahkan nilai posisi *byte* ke kiri secara sirkular dan pada posisi pertama akan mengambil nilai kolom terakhir dari matrix key utama.

$$\boldsymbol{RotWord}([\boldsymbol{b_0} \quad \boldsymbol{b_1} \quad \boldsymbol{b_2} \quad \boldsymbol{b_3}]) = [\boldsymbol{b_0} \quad \boldsymbol{b_1} \quad \boldsymbol{b_2} \quad \boldsymbol{b_3}]$$

Tabel 2. Proses *RotWord*

42	09
09	29
29	b9
b9	42

- Proses SubWord memetakan setiap *byte key* dengan menggunakan table S-Box AES.

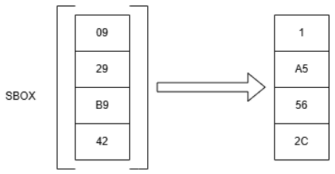
$$\boldsymbol{SubWord}([\boldsymbol{b_0} \quad \boldsymbol{b_1} \quad \boldsymbol{b_2} \quad \boldsymbol{b_3}]) = [\boldsymbol{S(b_0)} \quad \boldsymbol{S(b_1)} \quad \boldsymbol{S(b_2)} \quad \boldsymbol{S(b_3)}]$$

Tabel 3. S-box AES

	x0	x1	x2	x3	x4	x5	x6	7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	1	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	4	c7	23	c3	18	96	5	9a	7	12	80	e2	eb	27	b2	75
4x	9	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	0	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	2	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	6	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	8
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	3	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

Sehingga mendapatkan nilai:

Tabel 5. Nilai hasil S-Box AES



- Proses Rcon (*round constant*), dimana 4*byte* hasil sbox tadi akan di XOR menggunakan matriks konstan Rcon.

$$\boldsymbol{rcon_{i=}}[rc_i \quad 00_{16} \quad 00_{16} \quad 00_{16}]$$

$$\boldsymbol{rc_1}\begin{cases} \boldsymbol{1} & \boldsymbol{if\ i = 1} \\ \boldsymbol{2.rc_{i-1}} & \boldsymbol{if\ i > 1\ and\ rc_{i-1} < 80_{16}} \\ \boldsymbol{(2.rc_{i-1}) \oplus 11B_{16}} & \boldsymbol{if\ i > 1\ and\ rc_{i-1} \geq 80_{16}} \end{cases}$$

I adalah nomor *round* saat dilaksanakan. Pada AES-256 dibutuhkan 60 *words* sehingga Rcon digunakan hanya setiap 8 putaran sekali, sehingga hanya 7 elemen Rcon yang diperlukan, yaitu untuk posisi *word* ke-8, 16, 24, 32, 40, 48, dan 56.

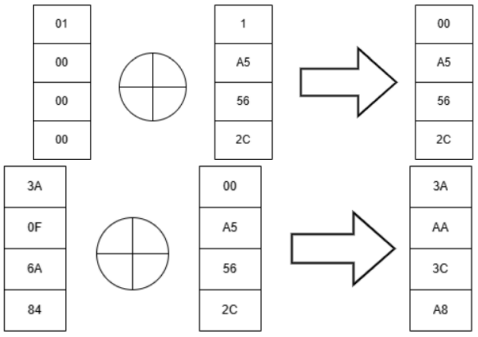
Berikut adalah matriks dari Rcon.

Tabel 5. Matrix Rcon (*round constant*)

	Round Constant													
Rcon	01	02	04	08	10	20	40	80	1B	36	6C	D8	AB	4D	9A
	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
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Proses mencari *word* ke 8, pada putaran 1 dengan matrix rcon menggunakan $[01 \quad 00 \quad 00 \quad 00]$kemudian XOR dengan hasil dari s-box sebelum nya. Hasil dari proses Rcon, hasil proses Rcon akan dilakukan-XOR-kan dengan *key* utama pada kolom 0 yaitu $[3a \quad 0f \quad 6a \quad 84]$.

Tabel 6. Proses pencarian *word* ke 8 dan hasil proses Rcon



Hasil XOR dengan *key* utama pada kolom 0, mendapat word ke-8, W8 = 3aaa3ca8d setelah itu dapat mencari *word* selanjutnya dengan rumus:

$w[i] = w[i-1] \oplus w[i-Nk]$

$w[i]$: *word* yang akan dihitung

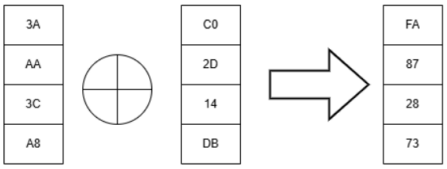
$w[i-1]$: *word* sebelumnya

$w[i-Nk]$: *word* yang terletak Nk langkah sebelum

w[i]

- Mencari word selanjutnya seperti word ke 9
  $w[9] = w[9-1] \oplus w[9-8]$ maka hasilnya $w[9] = w[8] \oplus w[1]$
- Mencari *word* ke 9 dilakukan XOR *word* ke 8, *word* ke 1.

Tabel 7. Pencarian *word* ke 9

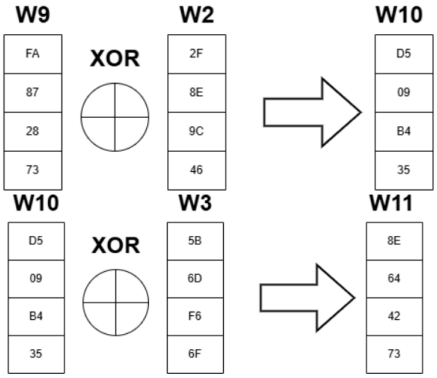


Karena setiap putaran memiliki 8 *word*, melakukan proses ini berulang hingga akhir perputaran. Di akhir setiap putaran, akan dilakukan proses penambahan kunci yang sama seperti yang disebutkan di atas, hanya mengambil kata terakhir dari setiap putaran untuk melakukan proses RotWord, SubWord, dan Rcon. Hasil dari perputaran pertama adalah seperti ini:

Tabel 8. Pencarian *word* ke 10,11

W10:

W11:



- Expansi kunci pada word 12,20,28,36,44,52

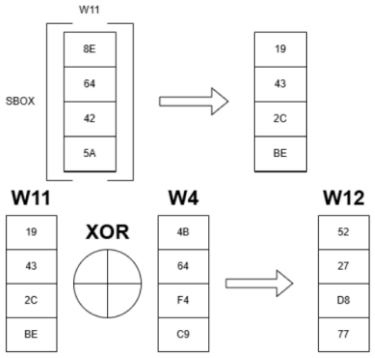
Aturan diterapkan pada *word* kelipatan 4 dengan tujuan meningkatkan keacakan kunci turunan. Fungsi ini tidak dilakukan *RotWord* atau XOR dengan Rcon, melainkan dengan melakukan *SubWord* sebelum melakukan XOR dengan word yang terletak Nk langkah sebelum i $w[i - Nk]$ dengan pengerjaan seperti: $w[12] = w'[11] \oplus w[4]$.

Proses *SubWord* pada W11 dengan menggunakan *S-Box* AES:

Tabel 9. *S-Box* AES

	x0	x1	x2	x3	x4	x5	x6	7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30		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	4	c7	23	c3	18	96	5	9a	7	12	80	e2	eb	27	b2	75
4x	9	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	0	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	2	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	6	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	8
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	3	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

Hasil :



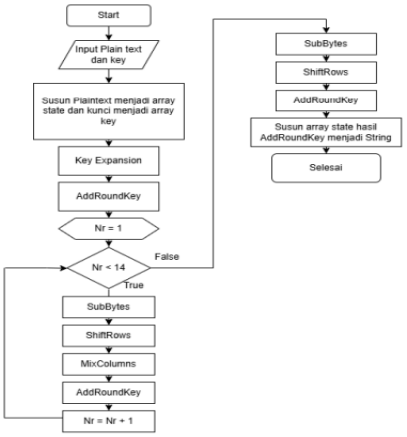
- Proses *SubWord* dilakukan seperti rumus XOR
- Tabel menunjukkan semua kunci yang telah diekspansi:

Tabel 11. Enkripsi key setiap putaran

Subkey - 0	3a0f6a84c02d14db2f8e9c465b6df66f
Subkey - 1	4b64f4c93d249c0d4b9278654209 29b9
Subkey - 2	3aaa3ca8fa872873d509b4358e64425a
Subkey - 3	5227d8776f03447a24913c1f669815a6
Subkey - 4	7ef3189b847430e8517d84dddf19c687
Subkey - 5	ccf36c60a3f0281a87611405e1f901a3
Subkey - 6	e38f126367fb228b3686a656e99f60d1
Subkey - 7	d228bc5e71d89444f6b98041174081e2
Subkey - 8	e2838a938578a818b3fe0e4e5a616e9f
Subkey - 9	6cc723851d1fb7c1eba63780fce6b662
Subkey - 10	7ccd2023f9b5883b4a4b8675102ae8ea
Subkey - 11	a622b802bb3d0fc3509b3843ac7d8c21
Subkey - 12	a3d4ddb25a615589102ad3fc00003b16
Subkey - 13	c5415a457e7c55862ee76dc5829ae3e4
Subkey - 14	5bc5b4a101a4e128118e32d4118e09c2

2. Proses Enkripsi AES 256

Diagram alur ini menggambarkan bagaimana data diubah secara bertahap melalui berbagai operasi matematika untuk meningkatkan keamanannya terhadap serangan kriptografi dapat dilihat pada gambar dibawah ini:



Gambar 5. Alur AES 256

- *AddRoundKey*, putaran 0

Pada proses melakukan XOR *Plain Text* dengan kunci initial/kunci utama atau *RoundKey* – 0

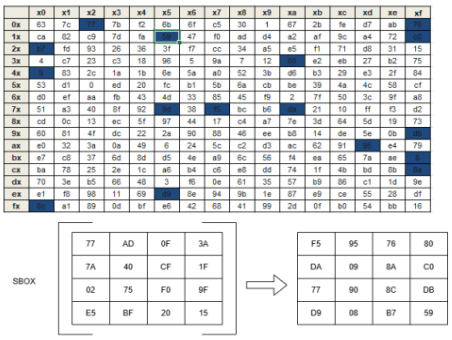
Tabel 12. *AddRoundKey*, putaran 0

- *Substitution Bytes*

Setelah melakukan XOR pada tahap *AddRoundKey*, selanjutnya melakukan *SubsByte* dengan proses yang sama seperti *key expansion*, yaitu hasil dari *AddRoundKey* akan dipetakaan pada tabel S-Box AES.

Tabel 10. Hasil *S-Box* AES

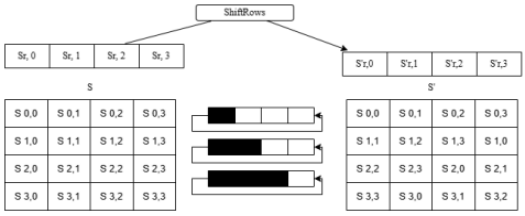
Tabel 13. S-Box AES



- Hasil *ShiftRow*

ShiftRow perpindahan *byte* ke kiri sebanyak nilai r, perpindahan r *byte* paling kiri ke ujung kanan baris. Baris pertama, di mana r = 0, tidak berubah atau tidak terjadi pergeseran.

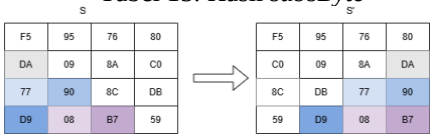
Tabel 14. Hasil *ShiftRow*



Pada ilustrasi di atas, dapat diketahui bahwa perpindahan baris mengikuti nilai r, pergeseran nya seperti baris Ke 2 << 1 kali baris Ke 3 << 2 kali baris Ke 4 << 3 kali.

- *ShiftRow* dari hasil *SubsByte*

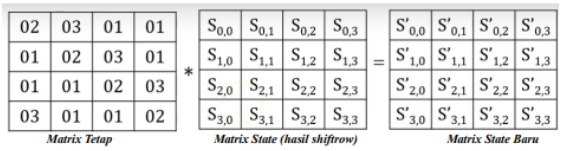
Tabel 15. Hasil *subsByte*



- *MixColumn*

Proses *MixColumn* ini menggunkan metode galois field yang dianotasikan sebagai GF(2^8). Operasi *MixColumn* menggabungkan matrix tetap dengan *Matrix State* dari proses *ShiftRow*.

Tabel 16. M*ix column*

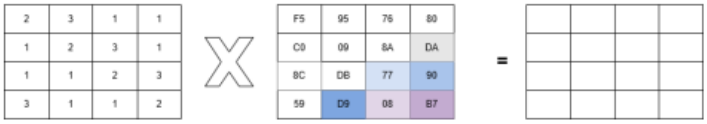


Pengoperasiannya dapat dirumuskan sebagai berikut :

$$S'_{0,c} = (\{02\} \circ S_{0,c}) \oplus (\{03\} \circ S_{1,c}) \oplus S_{2,c} \oplus S_{3,c}$$
$$S'_{1,c} = S'_{0,c} \oplus (\{02\} \circ S_{1,c}) \oplus (\{03\} \circ S_{2,c}) \oplus S_{3,c}$$
$$S'_{2,c} = S'_{0,c} \oplus S'_{1,c} \oplus (\{02\} \circ S_{2,c}) \oplus (\{03\} \circ S_{3,c})$$
$$S'_{3,c} = (\{03\} \circ S_{0,c}) \oplus S'_{1,c} \oplus S'_{2,c} \oplus (\{02\} \circ S_{3,c})$$

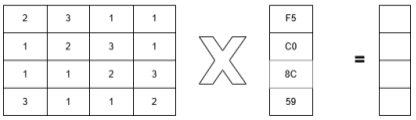
Perkalian pada kolom pertama dari hasil *ShiftRow*

Tabel 17. hasil *shiftrow*



Pencarian kolom pertama jadi akan terlihat seperti ini:

Tabel 18. Hasil *shiftrow* kolom pertama



Rumus yang digunakan:

$y_0(02.F5) \oplus (03.C0) \oplus (01.8C) \oplus (01.59)$

Proses perkalian pada *Galois Field* secara matematis dengan mengkonversikan bilangan Hexadesimal menjadi biner, dan ditransformasikan kedalam bentuk Polynomial-nya.

$\boldsymbol{F5}$=**11100101**$\rightarrow x^7 + x^6 + x^5 + x^4 + \dot{x}^2 + 1$

02 = **0000 0010** $\rightarrow x$

perkalian *polynomial*:

$\{02 * F5\} = x(x^7 + x^6 + x^5 + x^4 + \dot{x}^2 + 1)$

$\{02 * F5\} = x^8 + x^7 + x^6 + x^5 + \dot{x}^3 + x$

Dalam Galois Field dengan orde 2^8 jika mendapatkan hasil *polynomial* lebih dari x^7, perlu dilakukan pembagian modulus dengan menggunakan *irreducible polynomial* $\rightarrow x^8 + x^4 + x^3 + x \dot{+} 1$

$\{02 * F5\} = (x^4 + x^3 \dot{+} \dot{x} + 1) + x^7 +$

Sederhanakan menjadi: $\{02 * F5\} = x^7 + x^6 + x^5 + x^4 \dot{+} 1$

Konversikan kembali menjadi biner: : $\{02 * F5\} =$ 1111 0001 $\rightarrow$ F1 {0

Hal yang sama dengan baris selanjutnya:

03 = **0000 0011** $\rightarrow \boldsymbol{x + 1}$

$\boldsymbol{C0}$ = **1100 0000** $\rightarrow \boldsymbol{x\ 7 + x\ 6}$

Perkalian:$\{03 * C0\} = (x + 1) * (x^7 + x^6)\{03 * C0\} = x^8 + x^7 + x^7 + x^6 \rightarrow x^8 + x^6$ $(karena\ dalam\ GF(2), penjumlahan\ 1 + 1 = 0, jadi\ suku\ x\ 7 + x\ 7\ saling\ meniadakan)$.

$\{03 * C0\} = x^6 + x^4 + x^3 + x \dot{+} 1 \rightarrow$0101 1011

Mencari bilangan biner 2 baris terakhir

8C = 10001100

59 = 01011001

Selanjutnya dilakukan operasi XOR: 1111 0001 $\oplus$ 0101 1011 $\oplus$ 1000 1100 $\oplus$ 0101 1001 = 0111 1111 $\rightarrow$ 7F (dalam hex)

Sehingga mendapat hasil akhir berupa 7F.

- Operasi *MixColumn* untuk semua kolom pada matrix input.

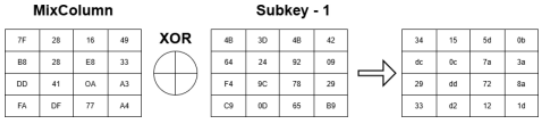
Tabel 19. Operasi *mixcolumn*

7F	28	16	49
B8	28	E8	33
DD	41	0A	A3
FA	DF	77	A4

- *AddRoundKey*

Transformasi *AddRoundKey* terjadi setelah transformasi *MixColums* dengan cara menggunakan proses XOR dengan sub kunci yang sesuai untuk setiap iterasi.

Tabel 20. Operasi *mixcolumn*



Hasil dari *AddRoundKey* akan digunakan kembali sebagai input proses enkripsi (*SubByte, ShiftRow, MixColumn, AddRoundkey*) selanjutnya. Seluruh proses akan diulang sampai ronde ketiga belas. Pada ronde keempat belas, proses tetap sama, tetapi proses MixColumn tidak dilakukan. Hasil enkripsi akan tampak seperti ini setelah perputaran 14 kali:

Tabel 21. Hasil ekripsi

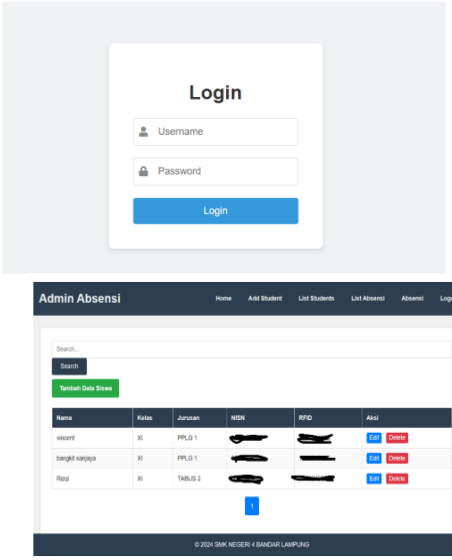
Cipher Text	3cdca53c0972e008d25c45cacbf7dc7ac660b3b62ca1

3. Implementasi dan Uji Coba Aplikasi

Tampilan Layar dapat diuraikan tentang tampilan layar mulai dari aplikasi dijalankan hingga selesai. Berikut ini adalah tampilan yang ada pada aplikasi ini.

a. Tampilan *Form Login* dan Tampilan *Menu Utama*

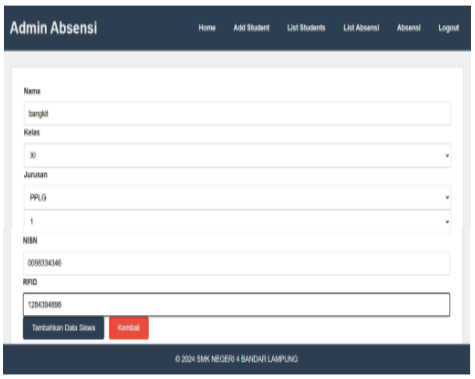
Tampilan login form dari aplikasi absensi SMK Negeri 4 Bandar Lampung dapat dilihat pada gambar dibawah ini:



Gambar 6. Tampilan login form dan Tampilan *Menu Utama* dari aplikasi absensi SMK Negeri 4 Bandar Lampung

4. Implementasi AES 256-256 pada Pengamanan Database

Gambar di bawah ini menunjukkan hasil input dan enkripsi data siswa:



Gambar 7. Tampilan menu utama dan input data siswa aplikasi absensi SMK Negeri 4 Bandar Lampung

Gambar dibawah ini database yang telah dienkripsi aplikasi absensi SMK Negeri 4 Bandar Lampung:

Tabel 22. Hasil enkripsi

Nama Siswa	RFID	NISN	ROMBEL
ADITYA MAHENDRA RAMADAN	iUhIRh30oXGivO3chVUETm0GwJOPj+miuI2r232	IhkklDCC0HpyTD+o5klX3vQIhoayFZky	XI PPLG 1
AHMAD NURIL ADINATA RAMADHAN	191FUiZd8w4WXu+o5K8WEVK/0QcYKGIPR/d6HU	2czYRJ7Yd2h/WRc7tMWXiTcbCMoQALLA6	XI PPLG 1
AL KHAIDAR AKBAR	X5uPzvAG6j96TA24uw7V7zws4dgLm1jq6vr	RswZ0dnwWqLeOjELi9yk0ujOny/b6p0e2	XI PPLG 1
ANDIKA KURNIAWAN	xPUEtusYgcgkjjb8RoP7sogO+zzUI+Yj8SqmtNubm	KY43hFKYeqbJ86N/2SXM2oEK/7XkBqBUsG	XI PPLG 1
BAGUS NAYOTTAMA	lyCm/J1/k5/xpir1y+stuujDeNT1jDffLCXuwWo4zp	A0AS/WsJqRMR9EKMepUhvrByHu+ax9Sd	XI PPLG 1
DWI AGUSTIN	FAAxg4QcTpmseZAx1rwQ256fB84XNjKJwUt9OQA	FuEbPNpF5v9QRGwDUzD4/kyWH23KUcgtt	XI PPLG 1
DZIDANE DARWIN WIJAYA	TdELWOfX4kipkYQxoR7i1xiFZxTJnwhBwHr0I/Oh	fiNYvWIz51XpDt3eHISxBVIYMJ4yf0RDOFX	XI PPLG 1
ERIC FRANSLIE	eQ2x6zkHBsQPWTnroEXP9420V7QrYCcnGrcy9LW	AWO2LQrUaAcKWdQ6/gX5Krqm19fY+kxBy	XI PPLG 1
FACHRY ADITIYA FIRMANSYAH	/5SohQE6wRSr+jszwuSa0bcMObTA51voUkf6UYa	nWkBAMciEH7Ur9oW02Hq9KqrhOTf5/aH	XI PPLG 1
FADIL PUTRA SUSELO	iVbed5iMmJRw6a52MCiNYq+m/Q8wJ0njuiTEW	s8jUdiFVFdelbuZTbBK8fbKfMjGIBgmaod	XI PPLG 1
FAHMI ILHAM JAYA	EFeFzPu450wYkrdHo6PbIWL2Sxc4x53wm57QBxb	HP5K87nvper79a1dNV9uTMtEKV6BTk1Zjv	XI PPLG 1
HAMDAN KURNIAWAN SEJATI	69DxWOWYwiO7657JdoCiuepeaXBW1c+NuMuB	78FtnJ5ppG2NolyqqSQbxZsaIsPmDCc7RI5	XI PPLG 1
ILHAM ZHAVA PRATA UTAMA	B8xxaKEYpSwGyT4/WVw1NA8YDzchgke7N23PfX	G2Z77DITLI88wsg0WG0PmIlkFPioO6xsOX	XI PPLG 1
INDRA IRAWAN	ORaLa+2SuWKh9C1aI+W1LItryCm447WWmDop	V/isLiYwop5gJ8fYc9iAq/Okydb//jy9u1hW	XI PPLG 1
JULIAN SAPUTRA	JjMvkwheOwup/tXMZfM5mqijW/wWHBbY2fRN	234HLb//jIet96+PvjBit31VvnIAg330MzP77	XI PPLG 1
JULIO ARDIKA P	K8MLrbIF5CeM+X3ewXnQuEsoTZkaYp3LMeF85	HZ0y+rGJtdz0iQcqQfBdPk180ZLTaj1d8L3k	XI PPLG 1
M. FAKHRI DHIYAULHAQ	VPs1mk4i9tHWUpPofyxKQhpNrHjYaU1fkK5QPjX	TDF/1ZRDrE0dTT9b9n0LTxsWYv4dLB3LO	XI PPLG 1
M. RAFII MAKARIM	NHTKzh1WIWtCFpATU5xOG9TSWIFEs+Y3vIMiH	68OExY7IsoUaDv5V181B4dxY0WRxrsE4XR	XI PPLG 1
M. RAYHAN KAMIL	JA+UDocwVbdFx7E1wtXUZqEYHJGHEQmWjZf3W	UJVC7tpVdgRT8hSqf6tFoMCz/sqN4Ci3Qx	XI PPLG 1
M. YUGA RAMA SAPUTRA	o6sbbzHof+h1fimnyQeXwdiCbIIP9tS8qtRBgeCN	vKEiVhO99Er17FIpJQ5/u3rZcy3LAMpZ3v2E	XI PPLG 1
MEISYA WULANDARI NASUTION	nfF/uv1qoKaNI69CJsUgp0e5diP6/Y+QCY5SQiHh	cd61Opba1HwLXYShzkYW7MZHLW7Duak	XI PPLG 1
MORENO RADITYA KUSUMA	zf4BGxANLfgKpUS5wJjBQDW83voDd4Bbbxc2g/u	0XEEoia5YRo27Dji/a7coyECuwmDCpgG/H	XI PPLG 1
MUHAMAD RIZQI WIRANSYAH	PQoL2spef74Dcpi+hwLr1vnimGt8dboNe/NP93c	rLcqA+wph2BirJybdCfuc9aKb7N965Egx2o	XI PPLG 1
MUHAMMAD BANGKIT SANJAYA	NZBTU6vEM2K5QxwdUhOdcjYqI5f8cOuk68Pe69f	UktZ1pbSpW3YOLirzehNw0iaUwrxrVoI+	XI PPLG 1
QUILA RENATA ATHALIE SUPOMO	d1Gn3upVvZTUuHJnBsHoNpqwHfwwZ8vZaYc7	dhKQOQa2YTI3p8law4dPsVEfVII1y2LodJ	XI PPLG 1
RADO RAMADHAN	2BcfNY4kSN9FAXNz6AwwmhQaATB/mnNOO1rs	pNaMyTYcMkjNe9PtGOA/kuObQk17xddr	XI PPLG 1

Berdasarkan tabel diatas data siswa yang dienkripsi terdiri dari empat komponen utama: nama siswa, RFID, NISN, dan rombel. Nama siswa ditampilkan secara terbuka untuk identifikasi visual, tetapi data RFID dan NISN telah dienkripsi untuk menjaga kerahasiaan dan keamanan data pribadi. Hasil enkripsi identifikasi berbasis radio frequency identification (RFID) ditampilkan dalam kolom RFID, yang biasanya digunakan dalam sistem kontrol akses otomatis atau absensi. Sementara itu, kolom NISN berisi hasil enkripsi dari Nomor Induk Siswa Nasional, yang unik untuk setiap siswa. Dalam kasus ini, seluruh siswa berada dalam kelas "X PPLG 1", Kolom Rombel (Rombongan Belajar) menunjukkan kelas atau kelompok belajar masing-masing siswa. Tujuan penggunaan enkripsi dalam tabel ini adalah untuk meningkatkan keamanan sistem informasi sekolah, mencegah data siswa disalahgunakan, dan memenuhi prinsip keamanan data sesuai dengan peraturan perlindungan data pribadi.

4. KESIMPULAN

Penelitian ini menunjukkan peningkatan keamanan *database* aplikasi manajemen siswa berbasis web di SMKN XYZ Bandar Lampung. Hasil eksperimen menunjukkan

bahwa sistem yang digunakan dapat dengan efektif menjaga kerahasiaan dan integritas data akademik siswa. Analisis kinerja menunjukkan bahwa AES 256 tetap efisien dalam enkripsi dan dekripsi data dan memberikan tingkat keamanan yang tinggi. Pengembangan sistem keamanan yang lebih fleksibel yang menggabungkan metode enkripsi lain, seperti *hybrid cryptography*, untuk meningkatkan efisiensi dan fleksibilitas dalam pengamanan data adalah topik penelitian masa depan. Selain itu, penerapan keamanan berbasis *blockchain* dapat menjadi alternatif yang menjanjikan untuk menjamin keabsahan dan ketertelusuran informasi akademik siswa. Studi tambahan juga dapat dilakukan untuk meningkatkan efisiensi komputasi AES 256 dalam aplikasi berbasis *cloud*, yang akan membuatnya lebih *scalable* dan hemat sumber daya.

5. DAFTAR PUSTAKA

Algoritma, K., Dan, K. A.-, Meningkatkan, S.-U., & Dokumen, K. (2024). *Kombinasi algoritma kriptografi aes-256 dan sha3-512 untuk meningkatkan keamanan dokumen pdf*. *11*(1), 46–54.

Andriyanto, M. R., & Sukmasetya, P. (2022). Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Keamanan Data Transaksi Pada Sistem E-Marketplace. *Journal of Computer System and Informatics (JoSYC)*, *4*(1), 179–187. https://doi.org/10.47065/josyc.v4i1.2451

Andriyanto, R., Khairijal, K., & Satria, D. (2020). Penerapan Kriptografi AES Class Untuk Pengamanan URL WEBSITE Dari Serangan SQL INJECTION. *Jurnal Unitek*, *13*(1), 34–48. https://doi.org/10.52072/unitek.v13i1.153

Anwar, S. (2017). Implementasi Pengamanan Data Dan Informasi Dengan Metode Steganografi LSB Dan Algoritma Kriptografi AES. *Jurnal Format*, *6*(1), 65–74.

Baso, F., & L, N. A. (2024). *Implementasi Teknik Kriptografi dengan Metode AES 256 untuk Keamanan File*. *3*(3), 84–87.

Ginting, A., Isnanto, R. R., & Windasari, I. P. (2015). Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email. *Jurnal Teknologi Dan Sistem Komputer*, *3*(2), 253. https://doi.org/10.14710/jtsiskom.3.2.2015.253-258

Gunawan, I. (2021). Peningkatan Pengamanan Data File Menggunakan Algoritma Kriptografi AES Dari Serangan Brute Force. *TECHSI - Jurnal Teknik Informatika*, *13*(1), 14. https://doi.org/10.29103/techsi.v13i1.2395

Handoko, H., & Rony, M. A. (2018). Implementasi Keamanan Database Dengan Enggunakan Metode Advanced Encryption Standard (Aes-256) Pada Sekolah Smk Islam Al Hikmah Jakarta Berbasis …. *Skanika*, *1*(3), 1137–1142.

Keamanan, A., & Sosial, J. (2024). *Technology Sciences Insights Journal*. 0–3.

Liwandouw, V. B., & Wowor, A. D. (2017). The Existence of Cryptography: A Study on Instant Messaging. *Procedia Computer Science*, *124*, 721–727. https://doi.org/10.1016/j.procs.2017.12.210

Nagaraju, S., Nagendra, R., Balasundaram, S., & Kiran Kumar, R. (2023). Biometric key generation and multi round AES crypto system for improved security. *Measurement: Sensors*, *30*(February), 100931. https://doi.org/10.1016/j.measen.2023.100931

Nanda, D., Herlambang, R., Pravitasari, N., Korespondensi, P., & Pendahuluan, I. (2024). Penerapan Kriptografi AES untuk Keamanan Data Aplikasi Pemesanan Bibit Ternak pada BPSI UAT. *Remik*, *8*, 29–44.

Nizamuddin Aulia Kafa, & Dolly Virgian Shaka Yudha Sakti. (2024). Implementasi Kriptografi Berbasis Web dengan Algoritma Advanced Encryption Standard (AES) 256 dan Kompresi Huffman untuk Pengamanan File di SMK Satria. *Jurnal Ticom: Technology of Information and Communication*, *12*(2), 50–55. https://doi.org/10.70309/ticom.v12i2.109

Priyadi, D. P., Budiyanto, U., Studi, P., Informatika, T., Informasi, F. T., Luhur, U. B., Utara, P., & Lama, K. (n.d.). *Pengecekan Keaslian Gambar Menggunakan Algoritma Kriptografi Advanced Encryption Standard 128 (Aes), Vigenere Cipher Dan Steganografi Least Significant Bit (Lsb) Berbasis Android Pada Cv . Wiratama*. *128*, 1–7.

Purnama, B., & Rohayani, A. H. H. (2015). A New Modified Caesar Cipher Cryptography Method with LegibleCiphertext from a Message to Be Encrypted. *Procedia Computer*

Science, *59*(Iccsci), 195–204. https://doi.org/10.1016/j.procs.2015.07.552

Saleh, M. R., & Windarto. (2018). Implementasi Algoritma Enkripsi AES 256 dan Vigenere Cipher untuk Mengamankan Dokumen Digital pada Aplikasi Penyimpan dan Berbagi Dokumen Digital Berbasis Web. *Skanika*, *1*(3), 1259–1266.

Santoso, A. R., Riski, A., & Kamsyakawuni, A. (2018). Implementasi Algoritma Reversed Vigenere Encryption pada Pengamanan Citra. *Berkala Sainstek*, *6*(2), 61. https://doi.org/10.19184/bst.v6i2.9224

Saputra, M. W. A., Ashari, S. A., & Larosa, E. (2024). Keamanan Data Sistem Informasi Akademik ITEkes Mahardika: Penerapan Sistem Pencadangan Basis Data dengan Enkripsi AES. *Inverted: Journal of Information Technology Education*, *4*(2), 79–85. https://doi.org/10.37905/inverted.v4i2.22969

Setiawan, A., & Fatimah, T. (2021). Implementasi Algoritma Kriptografi Rc4 Untuk Keamanan Database Aplikasi Penggajian Karyawan Berbasis Web Pada Pt. Trans Intra Asia. *Skanika*, *4*(1), 66–71. https://doi.org/10.36080/skanika.v4i1.2044

Sidabutar, L., Ramadhan, M., & Panjaitan, Z. (2024). *Implementasi Kriptografi Pengamanan Data Pemesanan Produk Menggunakan Meotode AES*. *3*, 440–449.

Syahrani, F. N., & Pramusinto, W. (2024). *DAN VIGENERE CIPHER PADA COFFEE SHOP NGOPI IMPLEMENTATION OF AES 128 AND VIGENERE CIPHER CRYPTOGRAPHIC ALGORITHMS IN NGOPI COFFEE SHOP WITH WEB-BASED APPLICATIONS*. *3*(September), 74–81.

Wahyu, I., Aji, K., & Santika, R. R. (2024). *UNTUK PENGAMANAN DATA PENJUALAN RUMAH MAKAN IMPLEMENTATION OF CRYPTOGRAPHY USING THE AES METHOD*. *3*(September), 224–233.