IMPLEMENTASI ALGORITMA *AES-128* UNTUK PENGAMANAN *DATABASE* PADA SMA *ISLAMIC CENTRE*

Reyhan Davon Ardiya[1*], Wahyu Pramusinto[2]

[1,2]Fakultas Teknologi Informasi, Teknik Informatika, Universitas Budi Luhur, Jakarta, Indonesia

Email: [1*]averuzmaximuz@gmail.com, [2]wahyu.pramusinto@budiluhur.ac.id
(* : corresponding author)

Abstrak-Kemajuan teknologi informasi saat ini telah membawa manfaat yang sangat besar bagi dunia pendidikan saat ini, keamanan merupakan hal yang mutlak dalam dunia penyimanan data, karena data merupakan hal-hal yang bersifat sensitif dan tidak boleh sembarangan dapat mengakses data-data tersebut agar tidak disalahgunakan, begitu juga di dalam dunia pendidikan, dalam suatu instansi sekolah terdapat beberapa data-data penting seperti data siswa, data guru, data nilai siswa, data administratif sekolah, semua data-data tersebut merupakan data yang penting dan sensitif, maka sistem keamanan sangat dibutuhkan pada kemajuan teknologi seperti sekarang. SMA *Islamic Centre* memiliki data siswa dan nilai yang tersimpan di dalam *database*. Data-data tersebut merupakan data sensitif dan tidak boleh diambil oleh orang yang tidak berhak. Oleh karena itu data tersebut perlu diberikan pengamanan khusus agar tidak bisa dimanipulasi oleh orang lain. Salah satu cara untuk melindungi data adalah dengan menggunakan metode kriptografi. Kriptografi merupakan metode untuk mengubah data asli yang bisa dibaca (*plain text*) menjadi data acak yang tidak bisa dibaca (*cipher text*). Pada penelitian ini digunakan algoritma kriptografi *AES-128* dengan bahasa pemrograman *PHP* dan *database MySQL*. Hasil akhirnya berupa aplikasi yang bisa mengamankan database yang berkaitan dengan sistem informasi penilaian. Aplikasi yang dibuat mampu menginput data ke dalam database dalam bentuk cipher text dan mampu mengembalikan data ke dalam bentuk plain text.

Kata Kunci: *AES-128*, pengamanan *database*, kriptografi

IMPLEMENTATION OF AES-128 ALGORITHM FOR DATABASE SECURITY AT SMA ISLAMIC CENTRE

Abstract- *Advances in information technology today have brought enormous benefits to the world of education today, security is an absolute thing in the world of data storage, because data are sensitive matters and should not be able to access the data indiscriminately so that it is not misused, as well as in the world of education, in a school agency there are some important data such as student data, teacher data, student grade data, school administrative data, all of these data are important and sensitive data, so a security system is needed at advances in technology as it is today. SMA Islamic Center has student data and grades stored in the database. These data are sensitive data and should not be taken by unauthorized persons. Therefore, the data needs to be given special security so that it cannot be manipulated by others. One way to protect data is to use cryptographic methods. Cryptography is a method for converting readable original data (plain text) into unreadable random data (cipher text). This research uses AES-128 cryptographic algorithm with PHP programming language and MySQL database. The end result is an application that can secure databases related to the assessment information system. The application made is able to input data into the database in the form of cipher text and is able to return data into plain text form.*

Keywords*: AES-128, database security, cryptography*

1. PENDAHULUAN

Semakin majunya teknologi manusia sering kali lalai dalam keamanan, keamanan merupakan suatu hal yang penting untuk diperhatikan, sistem keamanan merupakan gerbang dari seluruh data-data yang telah disimpan, tanpa adanya sistem keamanan yang baik data-data sering kali dicuri dan disalahgunakan pihak yang tidak bertanggung jawab.

Keamanan data merupakan hal yang perlu di perhatikan, khususnya pada sekolah SMA *Islamic Centre* karena merupakan suatu lembaga pendidikan yang menyimpan banyak informasi penting seperti data guru, data siswa, dan data nilai siswa, data-data tersebut merupakan data yang sensitif karena jika data tersebut jatuh ke orang yang tidak bertanggung jawab data tersebut bisa disalahgunakan untuk hal-hal yang berorientasi negatif, seperti penipuan.

SMA *Islamic Centre* belum memiliki aplikasi keamanan *database* untuk menjaga agar data-data siswa dan guru tetap aman, dengan demikian maka dibutuhkan suatu sistem pengamanan yang memiliki tingkat kemanan yang cukup tinggi untuk menjamin kerahasiaan data atau informasi penting tersebut agar tidak dicuri atau dimanipulasi. Dengan cara menjaga kerahasiaan data penting tersebut dan menyembunyikannya. Kriptografi merupakan salah satu metode yang digunakan dalam penelitian ini untuk menajaga kerahasiaan data sensitif. Data yang disimpan dalam database dimodifikasi sedemikian rupa sehingga tidak dapat dengan mudah dibaca [1]. Enkripsi adalah proses melindungi informasi dengan membuatnya tidak dapat dibaca tanpa bantuan pengetahuan khusus [2].

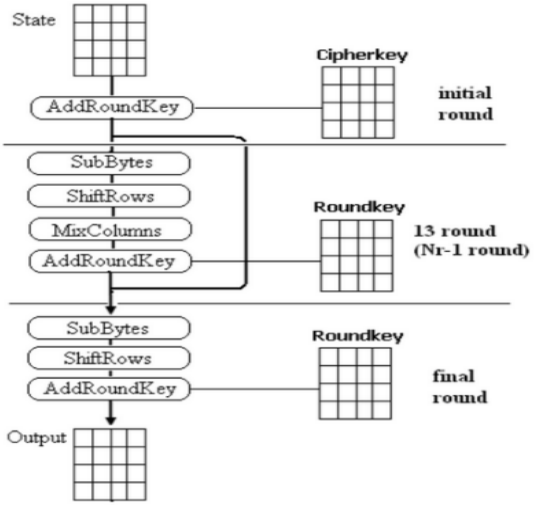
Kriptografi berasal dari bahasa Yunani, *crypt* dan *graffia*. *Crypto* artinya rahasia dan *graffia* artinya tulisan [3]. Enkripsi adalah ilmu dan teknologi yang ditujukan untuk menjaga keamanan pesan (enkripsi adalah seni dan ilmu untuk menjaga keamanan pesan). Secara umum kriptografi adalah teknologi keamanan informasi yang mengubah informasi dengan kunci tertentu dengan cara mengenkripsinya untuk menciptakan informasi baru yang tidak dapat dipahami oleh orang yang tidak berhak, dan hanya dapat diketahui oleh orang yang menerimanya. Anda berhak menerimanya melalui dekripsi [4].

Kriptografi adalah cabang ilmu yang mempelajari bagaimana menjaga informasi sensitif agar tidak dibaca dan dikirim kembali kepada siapa pun selain pemiliknya atau seseorang yang tidak berkepentingan. [5].

Kriptografi adalah ilmu dan seni menjaga kerahasiaan pesan dengan mengenkripsinya dalam bentuk yang tidak lagi dapat dipahami. Enkripsi memiliki dua proses: enkripsi dan dekripsi. Sebuah pesan yang dienkripsi disebut plaintext [6]. Kriptografi adalah ilmu dan teknologi untuk menjaga keamanan pesan. Kriptografi merupakan salah satu cabang matematika yang memiliki banyak fungsi dalam keamanan data [7].

Algoritma *Advanced Encryption Standard (AES)* merupakan algoritma enkripsi blok yang memiliki sifat simetris dengan menggunakan kunci simetris pada proses enkripsi dan dekripsi [8].

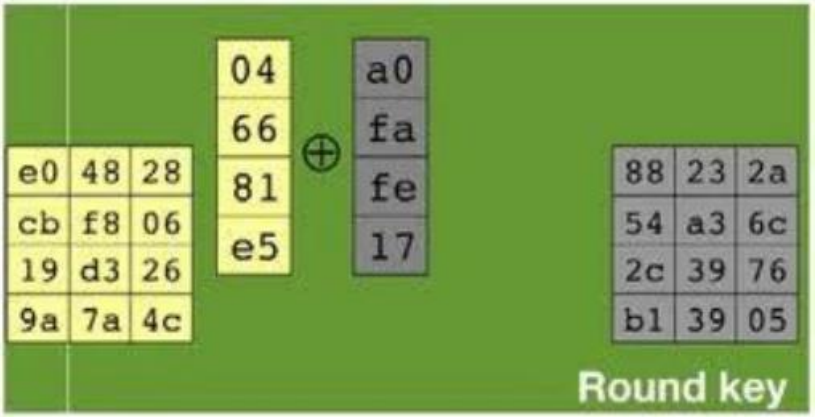
Proses enkripsi algoritma *AES* terdiri dari empat jenis transformasi *byte* : *SubBytes*, *ShiftRows*, *Mixcolumns*, dan *AddRoundKey*. Pada awal proses enkripsi, input yang disalin ke status mengalami konversi *byte AddRoundKey*. Status Nr kemudian digilir melalui transformasi *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*. Proses dalam algoritma *AES* ini disebut fungsi pembulatan. Babak terakhir sedikit berbeda dengan babak sebelumnya dimana keadaan babak terakhir belum mengalami transformasi *MixColumns*. Diagram proses enkripsi AES ditunjukkan di bawah ini.[6].



Gambar 1. Illustrasi Proses Enkripsi AES

1. *AddRoundkey*

Untuk proses enkripsi dan dekripsi *AES*, proses *AddRoundKey* adalah sama, menambahkan kunci bulat ke status melalui operasi XOR. Setiap *roundkey* terdiri dari Nb kata, setiap kata adalah [s`o,c , s`1,c , s`2,c , s`3,c] [so ,c , s1,c , s2 ,c , s3 ,c] [wround*Nb+c] untuk 0≤c≤Nb [wi] adalah kata kunci yang sesuai. di mana i = bulat*Nb+c. Transformasi AddRoundKey pada proses enkripsi pertama dengan putaran = 0, putaran berikutnya = putaran + 1, putaran selanjutnya pada proses dekripsi pertama dengan putaran = 14 putaran = putaran - 1. Ciphertext di sebelah kiri dan kunci bulat di sebelah kanan. XOR dilakukan kolom demi kolom. Artinya, kolom 1 ciphertext dari XOR dengan kunci bulat kolom 1, dan seterusnya. [6].



Gambar 2. *AddRoundKey*

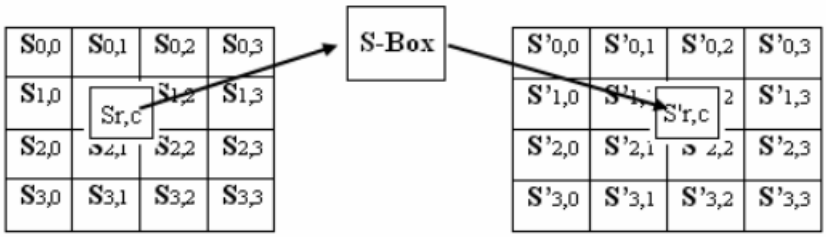
2. *SubBytes*

SubBytes adalah transformasi byte dimana setiap elemen dipetakan menggunakan tabel pengganti (S-Box). Tabel substitusi S-Box ditunjukkan pada gambar.

	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

Gambar 3. *SubBytes*

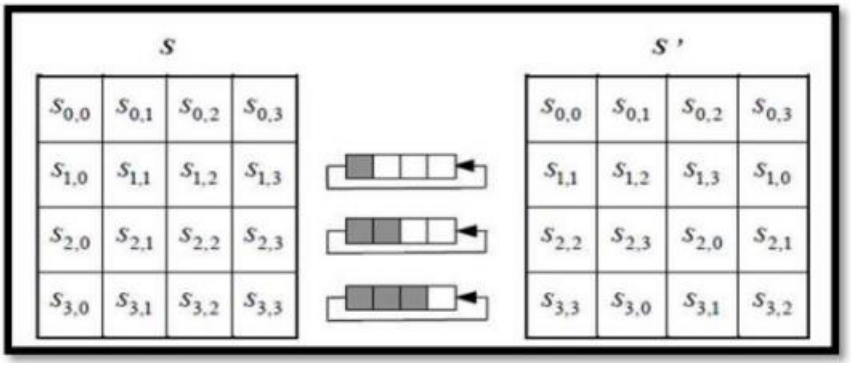
Untuk setiap byte dalam array status *subbyte* S-Box, misalkan [r,c]=xy. dimana xy dalam hal ini adalah bilangan heksadesimal dari nilai S[r,c] dan kemudian nilai pengganti S[r,c], adalah elemen tabel permutasi, efek peta byte pada setiap byte dan status. [6].



Gambar 4. Pemetaan pada setiap byte dalam state

3. *ShiftRows*

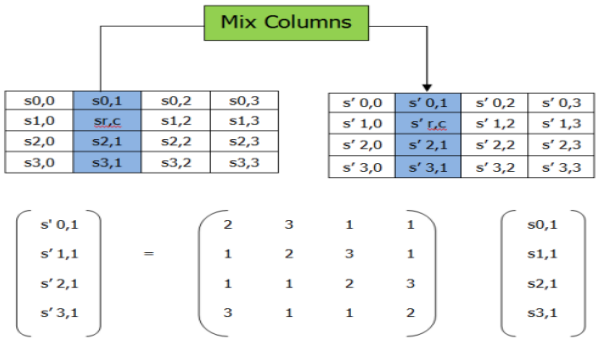
Transformasi Shiftrows pada dasarnya adalah proses pergeseran bit dimana bit paling kiri digeser ke bit paling kanan (rotasi bit) [6]. Proses pergerakan *shiftrow* ditunjukkan pada gambar di bawah ini. ;



Gambar 5. Transformasi *ShiftRows*

4. *Mix Columns*

Pada saat *MixColumn* mengalikan setiap elemen cipher blok dengan matriks yang ditunjukkan pada gambar di bawah. Tabel sudah ditentukan sebelumnya dan siap digunakan. Perkalian dilakukan seperti perkalian matriks biasa, yaitu dengan hasil kali dalam, dan kedua hasil kali tersebut dimasukkan ke dalam block cipher yang baru. Digambarkan di bawah bagaimana perkalian ini harus dilakukan. Dengan demikian, seluruh rangkaian proses yang terjadi di AES dijelaskan. [6].

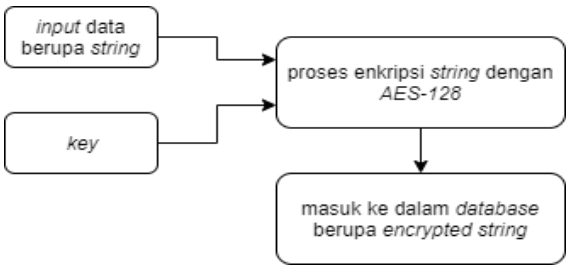


Gambar 6. Perkalian Matriks

2. METODE PENELITIAN

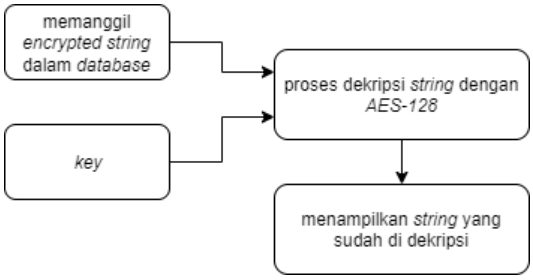
2.1 Metode Enkripsi.

Metode Enkripsi yang akan diimplementasikan pada aplikasi ini adalah pada saat admin memasukkan data ke dalam *database* siswa, guru, dan nilai, admin akan memasukkan beberapa string yang akan dienkripsi menggunakan metode *AES-128*, berikut gambar di bawah merupakan illustrasi singkat dari proses enkripsi yang akan digunakan.



Gambar 7. Illustrasi Enrkipsi

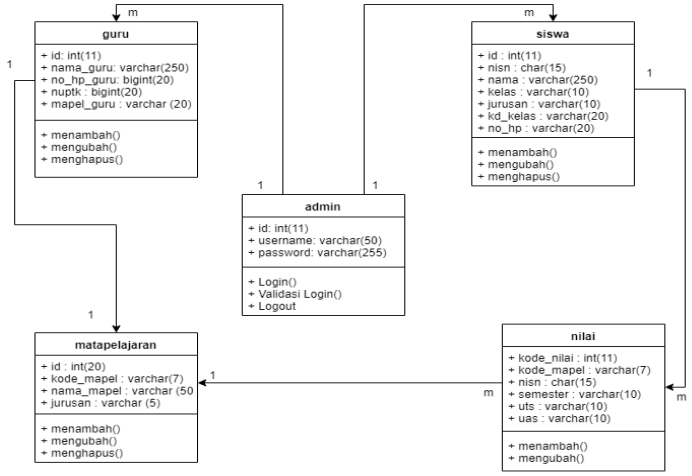
Sedangkan pada proses dekripsi, *string* akan otomatis di dekripsikan dan di tampilkan pada setiap halaman-halaman *website*.



Gambar 8. Illustrasi Dekripsi

2.2 *Class Diagram*

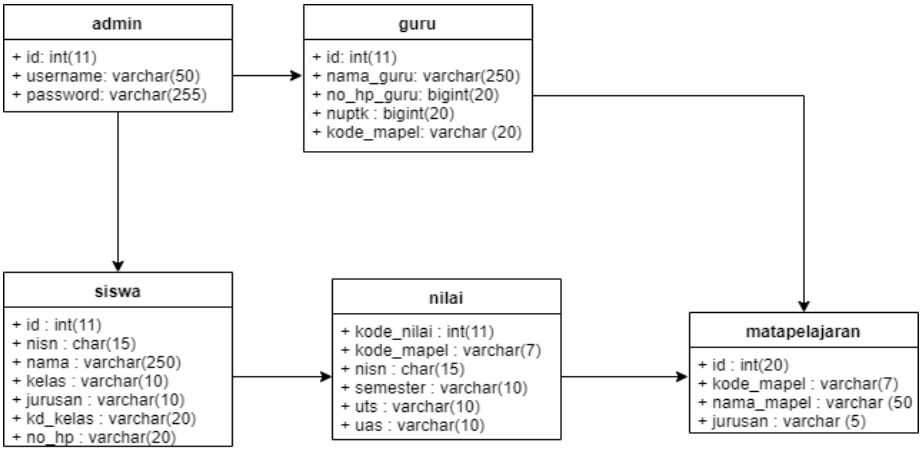
Class diagram merupakan model yang menggambarkan struktur dan deskripsi kelas dan hubungan antara kelas lain. Class diagram menggambarkan model yang digunakan untuk mendesain atribut dan fungsi yang digunakan untuk membuat desain rancangan sistem baru [9].



Gambar 9. Rancangan *Class Diagram*

2.3 *Logical Record Structure*

Logical record structure adalah struktur catatan dalam tabel yang terbentuk dari hasil seluruh kumpulan entitas. Memiliki aturan dasar yang sangat dipengaruhi oleh faktor utama yang menjadi titik perhatian utama [10].



Gambar 10. Rancangan *Logical Record Structure*

3. HASIL DAN PEMBAHASAN

3.1 Proses Enkripsi

a. Pembuatan *Object AES* dan *Key*

Proses pertama yang dilakukan yaitu membuat *variable object aes* dari *class AES*, dan memasukkan parameter *$key* dipenelitian ini hanya membuat 1 *key* statis yang akan digunakan untuk seluruh *key* pada proses enkripsi.

Gambar 11. Pembuatan *Object* dan *Key*

b. Proses Enkripsi

Proses kedua yaitu prosese enkripsi dan memasukkan hasil enkripsi ke dalam *database*.

Gambar 12. Proses Enkripsi

3.2 Proses Dekripsi

a. Pemanggilan *Object AES* dan *Key*, pada proses dekripsi yang dilakukan pertama kali adalah pemanggilan *Object* dan *Key* yang telah diinisialisasikan sebelumnya.

Gambar 13. Pemanggilan *Object* dan *Key*

b. Proses Dekripsi

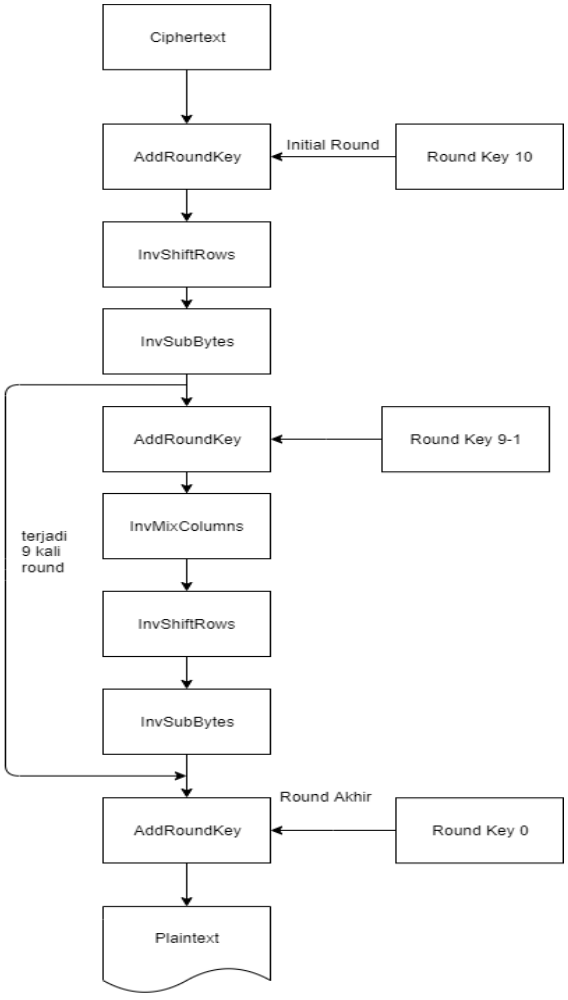
Proses kedua yaitu prosese pemanggilan fungsi dekripsi.

```
<td> <?= $object->decrypt(base64_decode($row["nama"])); ?></td>
<td> <?= $row["nisn"] ?></td>
<td> <?= $row["kelas"] ?></td>
<td> <?= $row["kd_kelas"] ?></td>
<td> <?= $object->decrypt(base64_decode($row["no_hp"])); ?></td>
```

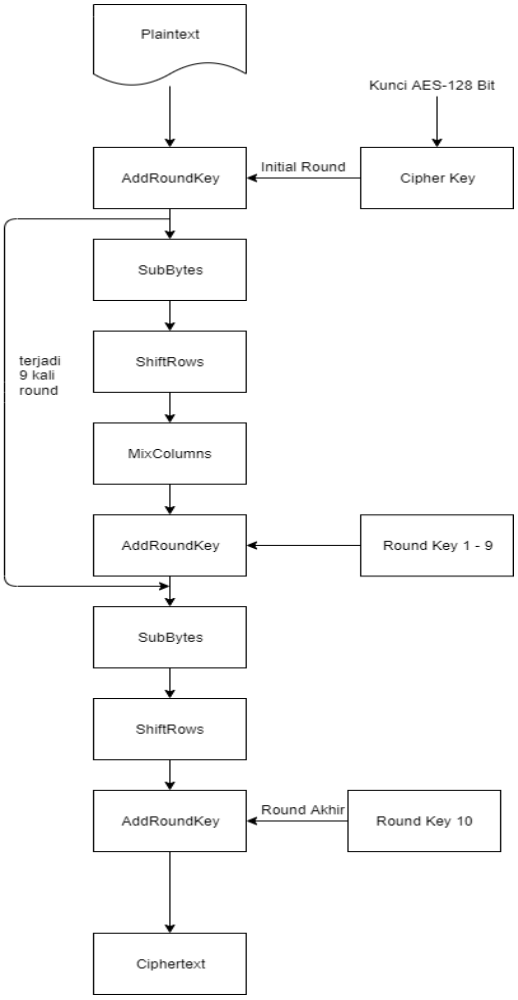
Gambar 14. Proses Dekripsi

3.3 *Flowchart* Enkripsi & Dekripsi

Flowchart atau alur website aplikasi pengamanan database pada SMA *Islamic Centre* menggunakan algoritma kriptografi *Advanced Enryption System 128 (AES-128).*



Gambar 15 *Flowchart* Enkripsi



Gambar 16 *Flowchart* Dekripsi

3.4 Tampilan Layar

Hasil tampilan layar aplikasi pengamanan *database* pada SMA *Islamic Centre*

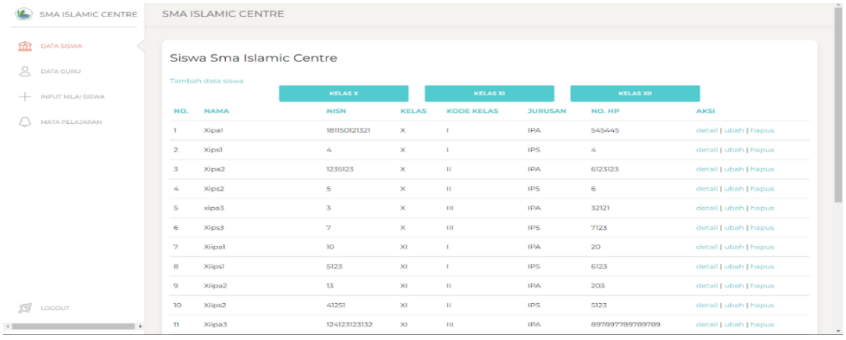
3.4.1 Tampilan Layar *Login*

Berikut ini merupakan tampilan layar *login* dari halaman dari admin untuk dapat mengakses halaman *index*.

Gambar 17. Tampilan Login

3.4.2 Tampilan Layar *Index*

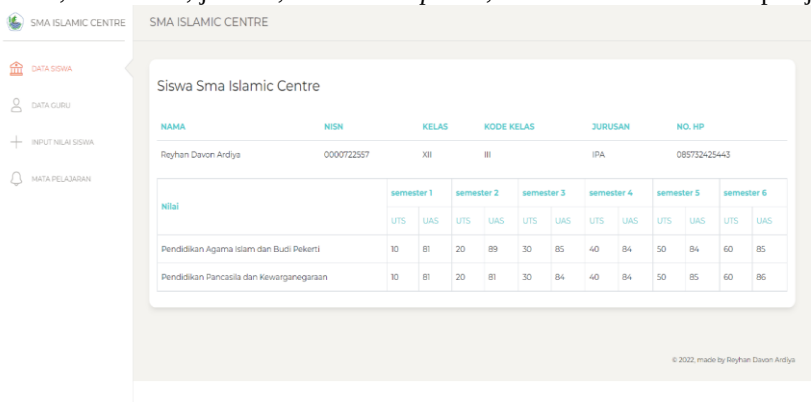
Tampilan layar *index* merupakan tampilan layar *index* halaman utama layar index menampilkan seluruh data siswa, dan terdapat beberapa *menu* seperti tambah siswa, ubah siswa, *menu* data guru, *menu* input nilai, *menu* mata pelajaran.



Gambar 18. Tampilan *Index*

3.4.3 Tampilan Layar *Detail* Siswa

Tampilan layar *detail* siswa merupakan tampilan layar *detail* siswa, untuk menampilkan seluruh detail siswa seperti nama, nisn, kelas, kode kelas, jurusan, nomer *handphone*, dan nilai-nilai dari mata pelajaran siswa.



Gambar 19. Tampilan Layar *Detail* Siswa

3.5 Pengujian

Dari pengujian yang telah dilakukan dengan memfokuskan terhadap sisi kecapatan dan hasil enkripsi yang berupa banyak karakter sebelum dan sesudah dienkripsi menggunakan algoritma kriptografi *AES-128*.

Tabel 1 Pengujian Enkripsi dan Dekripsi Data Siswa

Karakter Asli	Hasil Enkripsi	Jumlah Karakter		Waktu	
		Asli	Enkripsi	Enkripsi	Dekripsi
Davina Roza Arkananta	A3x/qzIoICKjvX6qn5fKf7Rb6rpzgBSEVRgeDTAiXZM=	21	44	0.016764879226685 ms	0.000321865081 78711 ms
Farhah Diniyah Rachmasani	JSmLsVmGl8nvJLpFguZuY554f0yWDgaTOswJoRcBwWk=	25	44	0.018707036972046 ms	0.000338077545 16602 ms
Javier Fadhal Firdaus	dXntalFENMqbdyUp4iZQkKGcfp9s9VtvwPKeZQ72KrQ=	21	44	0.017846107481 291 ms	0.000265836715 69824 ms

Tabel 2 Pengujian Enkripsi dan Dekripsi Data Guru

Karakter Asli	Hasil Enkripsi	Jumlah Karakter		Waktu	
		Asli	Enkripsi	Enkripsi	Dekripsi
Indra Priharstyadi	9OBL+aa00SEG5wvaSZGlSxAblFhSzNpCG2Sf24Jbh6o=	18	44	0.0267839 4317627 ms	0.00058412 551879883 ms
Fitriana Kartika	/+4UEgWwl+LWekcr0ltf6w==	16	24	0.028037071228027 ms	0.000157833099 36523 ms
Shamday Nura	tg/4SvgwgxDc/CfpC7c6kA==	12	24	0.012700796127319 ms	0.000126123428 34473 ms

4. KESIMPULAN

Setelah selesai melakukan tahap desain dan pembangunan sistem, kemudian dilanjutkan dengan tahap implementasi dan pengujian dapat disimpulkan bahwa sistem ini memudahkan input data siswa, guru, dan nilai siswa. Sistem ini berbasis *website* untuk administrator yang dibuat menggunakan bahasa pemrogramman PHP dan dengan pengamanan *database* yang menggunakan keamanan *AES-128*, untuk mengamankan *database* yang berisi tentang seluruh data inputan yang sudah telah di masukkan administrator.

DAFTAR PUSTAKA

[1] S. Natanael, H. Nurul, and S. Eka "Implementasi Kriptografi Hybrid Menggunakan Algoritma Aes-128 Dan Algoritma Rabin Untuk Mengamankan Data Dalam Database" *Student Online Journal (SOL)*, vol. 3, no. 1, pp. 178–183, 2022.

[2] T. Bin Tahir, M. A. Hadi Sirad, and M. Rais, "Sistem Informasi Encrypt Dan Decrypt Dengan Algoritma AES Menggunakan Framework Laravel," *Patria Artha Technol. J.*, vol. 4, no. 1, pp. 41–46, 2020.

[3] M. Sihombing, J. N. Sitompul, and T. A. Putri, "Implementasi Metode Kriptografi Advanced Encryption Standard (AES) untuk Proteksi Pesan Audio," *MEANS (Media Inf. Anal. dan Sist.*, vol. 4, no. 1, pp. 37–45, 2019.

[4] A. Prayitno and N. Nurdin, "Analisa Dan Implementasi Kriptografi Pada Pesan Rahasia," *J. Elektron. Sist. Inf. dan Komput.*, vol. 3, no. 1, pp. 1–11, 2017.

[5] D. I. Saragih and P. M. Hasugian, "Enkripsi Database Sekolah SMK Pembangunan Dengan Algoritma IDEA," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 4, no. 1, pp. 50–56, 2021.

[6] A. Eka Putri, A. Kartikadewi, and L. A. Abdul Rosyid, "Implementasi Kriptografi dengan Algoritma Advanced Encryption Standard (AES) 128 Bit dan Steganografi menggunakan Metode End of File (EOF) Berbasis Java Desktop pada Dinas Pendidikan Kabupaten Tangerang," *Appl. Inf. Syst. Manag.*, vol. 3, no. 2, pp. 69–78, 2021.

[7] Nuraini and S. Amini, "Implementasi AES-256 untuk Mengamankan Database E-Commerce," *J. Skanika*, vol. 1, no. 1, pp. 217–223, 2018.

[8] N. Cristy and F. Riandari, "Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan," *JIKOMSI [Jurnal Ilmu Komput. dan Sist. Informasi]* , vol. 4, no. 2, pp. 75–85, 2021.
[9] W. Alakel, "Sistem Informasi Akuntansi Persediaan Obat Metode First in First Out (Studi Kasus: Rumah Sakit Bhayangkara Polda Lampung)," *J. Tekno Kompak*, vol. 13, no. 1, p. 36, 2019.
[10] A. Taufik, "Perancangan Sistem Informasi Penjualan Makanan Kucing dan Anjing Berbasis Web," *J. Manaj. Inform.*, vol. 6, no. 2, pp. 61–70, 2019.