4th Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
27 Maret 2024 – Jakarta, Indonesia
Volume 3, Nomor 1, April 2024 - ISSN 2962-8628 (*online*

IMPLEMENTASI KRIPTOGRAFI MENGGUNAKAN ALGORITMA AES (ADVANCED ENCRYPTED STANDARD) UNTUK PENGAMANAN DATABASE BERBASIS WEB PADA TK ANNIDA

[1*]**Akbar Liyan Arfiyan,** [2]**Sri Mulyati,** [3]**Pipin Farida Ariyani**, [4]**Noni Juliasari**

[1,2,3,4]Teknik informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta, Indonesia

Email: [1*]1711500106@student.budiluhur.ac.id, [2]sri.mulyati@budiluhur.ac.id, [3]pipin.faridaariyani@budiluhur.ac.id, [4]noni.juliasari@budiluhur.ac.id
(* : corresponding author)

Abstrak- Dalam sejarah kehidupan manusia ada banyak macam peninggalan yang bersejarah dengan metode unik dalam mengamankan sebuah data agar tidak dengan mudah dapat diakses oleh entitas yang tidak memiliki akses yang seharusnya. Salah satu metodenya yaitu kriptografi, seiring berkembangnya waktu maka kriptografi pun menjadi bermacam – macam metodenya. Walaupun begitu, semua harus diseimbangi dengan dekripsi yang membaca enkripsi karena dengan dekripsi itu enkripsi tidak dapat dibaca oleh siapapun yang membutuhkanya. Juga dekripsi sebagai pelengkap dalam pengambilan data enkripsi jika diperlukan dalam berbagai hal keamanan misalnya kantor administrasi, pendidikan, keuangan dan juga instansi yang berbidang dalam teknologi informasi. Di setiap sekolah pasti ada data murid yang merupakan data yang sensitif dan hanya dapat di akses atau dilihat oleh pihak yang berwenang dan data tersebut memerlukan sebuah "pengamanan", Saat ini masih ada beberapa sekolah salah satunya TK Annida yang tidak menyimpan data muridnya dengan aman, tujuan dari penelitian yang saya buat ini bertujuan untuk mengamankan data murid dan mempermudah pengelolaan data di TK Annida seperti, data murid, data nilai matapelajaran dan juga data kelas murid, sehingga lebih mudah di Kelola dan lebih aman dari yang namanya pencurian data sehingga jika data yang dicuri atau dibaca tidak dapat di terjemakhan, dengan metode enkripsi menggunakan algoritma AES (Advanced Encryption Standard), dengan adanya sistem informasi pengamanan data enkripsi menggunakan algoritma AES berbasis web yang saya buat pada TK Annida data murid yang tersimpan lebih aman dan lebih terorganisir, sistem informasi yang saya buat sudah berhasil mengamankan data yang terdapat pada database dengan cara enkripsi menggunakan AES, juga sudah berhasil menterjemahkan data yang sudah terenkripsi dengan melakukan dekripsi, sehingga dapat dibaca oleh staff yang memiliki akses ke sistem informasi yang saya buat untuk TK Annida.

Kata kunci : Kriptografi, Advanced Encryption Standard (AES) , Enkripsi, Dekripsi

IMPLEMENTATION CRYPTOGRAPHY USING AES ALGORITHM (ADVANCED ENCRYPTED STANDARD) TO SECURING A WEB-BASED DATABASE IN ANNIDA KINDERGARTEN

Abstract- *In the history of human life there are many kinds of historical relics with unique methods of securing data so that it cannot be easily accessed by entities that do not have proper access. One method is cryptography. As time develops, cryptography has become various methods. However, everything must be balanced with decryption which reads encryption because with decryption the encryption cannot be read by anyone who needs it, also decryption as a complement to retrieving encryption data if needed in various security matters, for example administrative offices, education, finance and also agencies in the field of information technology. In every school there must be student data which is sensitive data and can only be accessed or seen by authorized parties and this data requires "security". Currently there are still several schools, one of which is Annida Kindergarten, which does not store its student data safely. The aim of the research that I created is to secure student data and make it easier to manage data at Annida Kindergarten, such as student data, subject grade data and also student class data, so that it is easier to manage and safer from data theft so that if the data is stolen or read and cannot be translated, with an encryption method using the AES (Advanced Encryption Standard) algorithm, with an encryption data security information system using a web-based AES algorithm that I created at Annida Kindergarten, student data that is stored is safer and more organized, the information system What I created has succeeded in securing the data contained in database by encrypting it using AES, and I have also succeeded in translating the encrypted data by decrypting it, so that it can be read by staff who have access to the information system that I created for TK Annida.*

Keywords *: Cryptography, Advanced Encryption Standard (AES), Encryption, Decryption*

1. PENDAHULUAN

Dalam organisasi, data sensitif dan hanya dapat diakses atau dilihat oleh pihak berwenang saja tentunya memerlukan sebuah "pengamanan". Data-data sensitif tersebut dapat berupa data pribadi, data keuangan, data rahasia, dan lain-lain [1], [2]. Sebab, pada perkembangan zaman yang sangat pesat saat ini, banyak sekali pencurian terhadap benda atau hal berharga [3], salah satunya adalah data [4]. Dengan banyaknya kemudahan–kemudahan layanan pada saat ini, data merupakan alat yang cukup sering dimanfaatkan untuk keperluan pribadi oleh pihak yang tidak bertanggung jawab, contohnya melakukan penipuan dengan data palsu, pencairan pinjaman tunai daring, dan masih banyak lagi [5]. Dengan adanya kejahatan-kejahatan di atas, muncul masalah yang harus bisa diatasi oleh pemilik data, yaitu masalah pengamanan data [6]. Banyak hal dapat dilakukan untuk mengamankan data, pada literatur ilmu pendidikan menerangkan bahwa ilmu untuk mempelajari tentang proses keamanan data adalah kriptografi [7]. Cara agar dapat memproteksi keamanan dan kerahasiaan data, salah satunya menggunakan teknik enkripsi dan dekripsi, tekntik tersebut juga memiliki banyak sekali Algoritma, diantaranya terdapat Algoritma AES (*Advanced Encryption Standard)* adakah algoritma enkripsi blok simetrik yang dipakai secara luas di seluruh dunia. Algoritma ini memiliki tingkat keamanan yang tinggi dan telah diuji coba secara ekstensif. Selain itu implementasinya dapat diterapkan dalam berbagai macam jenis data, sebagai contoh keamanan data pada Database [8].

Pada TK Annida penyimpanan data siswa/i bahkan beserta nilai dari mata pelajarannya masih disimpan dalam bentuk file excel, yang dimana jika file tersebut tercuri atau dilihat oleh pihak tidak berwenang secara sengaja atau tidak sengaja akan dimanfaatkan untuk hal-hal yang bisa merugikan. Hal tersebut sangatlah riskan, serta belum lagi untuk pengelolaan file-filenya yang makin lama semakin banyak hingga menumpuk dan sulit untuk dikelola, perlu dibuat sistem informasi untuk memudahkan pihak yang berhak untuk mengelolanya serta tersimpan ke dalam Database, yang dilengkapi dengan keamanan berupa pengenkripsian pada isi Database dengan menggunakan metode Algoritma AES [9], penggunaan enkripsi ini tentunya dapat membuat data sistem informasi tersebut ditingkatkan keamanannya.

Penelitian sebelumnya tentang Implementasi Algoritma *Advanced Ecryption Standard* dilakukan oleh Fandi Ahmad Sitorus dkk, dengan judul “Implementasi Algoritma Advanced Encryption Standard (AES) 128 Bit Untuk Keamanan Data Transaksi Penjualan Pada PT. MITSUBISHI ELECTRIC INDONESIA.” [10]. Penelitian ini bertujuan mengamankan data yang berisi beberapa data peribadi seperti nama customer, alamat customer, nomor handphone customer, dan lain-lain yang bersifat rahasia. Sedangkan di penelitian ini di peruntungkan untuk murid taman kanak kanak yang lebih riskan dicuri untuk tujuan yang membayakan murid dan orangtua murid di TK ANNIDA, maka dariitu penelitian ini dibuat untuk mengamankan data murid dari pencurian data yang tidak di inginkan.

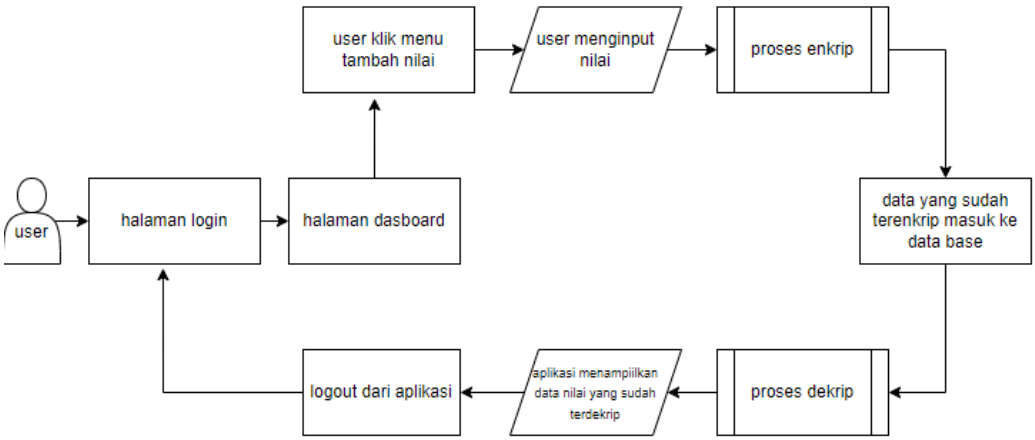
2. METODE PENELITIAN

2.1 Data Penelitian

Pengujian aplikasi sistem informasi ini menggunakan data siswa, data mata pelajaran, dan data nilai dimana data tersebut tersimpan di dalam *database*.

2.2 Penerapan Metode AES

Advanced Encryption Standard atau dalam singkatannya yaitu AES bentuk algoritma kriptografi dalam penggunaannya pada pengamanan suatu data. Algoritma AES dapat dikatakan blok chipertext simetrik bisa untuk enkripsi (encipher) serta pendekripsian (decipher) informasi. Dalam enkripsi terdapat ciphertext yang membuat data sulit untuk dapat dibaca dengan merubahnya dan dekripsi merupakan perubahan dari ciphertext data menjadi bentuk awal alias bentuk semula (plaintext), pada gambar 1berikut adalah penjelasan singkat perihal implementasi metode enkripsi maupun dekripsi data memakai algoritma *Advanced Encryption Standard* (AES).



Gambar 1. Ilustrasi Prosedur Enkripsi AES

2.3 Rancangan Pengujian

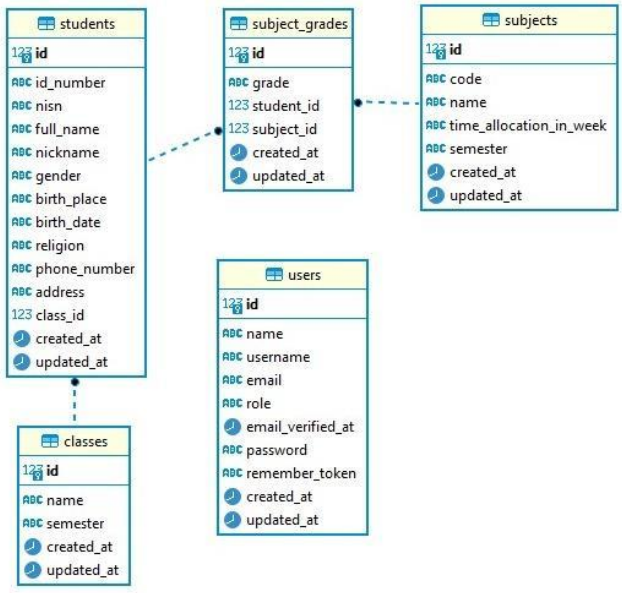
Rancangan pengujian ini dilakukan untuk memastikan implementasi proses enkripsi dan dekripsi algoritma AES bekerja dengan baik. Percobaan implementasi enkripsi dan dekripsi algoritma AES dibutuhkan untuk melihat apakah algoritma bekerja sesuai dengan yang dibutuhkan dan tidak terdapat error saat dijalankan dan memastikan data yang masuk ke data base telah terenkripsi.

2.4 Rancangan Basis Data

Untuk pengujian aplikasi sistem informasi ini adalah menggunakan data siswa, data mata pelajaran, dan data nilai dimana data tersebut tersimpan di dalam database, berikut rancangan basis data yang digunakan.

2.4.1 Class Diagram

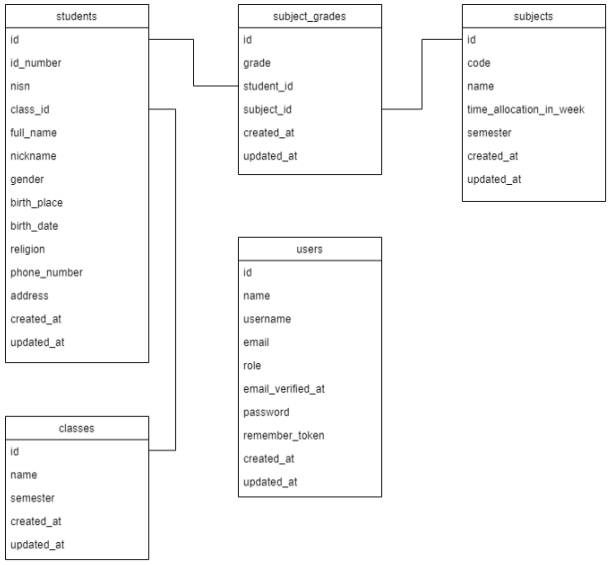
Berikut adalah gambar dari Class Diagram yang digunakan.



Gambar 2. Class Diagram

2.4.2 LRS (*Logical Record Structure*)

Berikut adalah gambar dari LRS (*Logical Record Structure*) yang digunakan.



Gambar 3. LRS *(Logical Record Structure*)

3. HASIL DAN PEMBAHASAN

3.1 Lingkungan Percobaan

Percobaan pertama yang dilakukan, telah disiapkan juga 2 komponen penting yakni Software dan Hardware yang akan digunakan untuk implementasi. Perlu ditentukannya spesifikasi pada kedua komponen tersebut, yang memiliki tujuan agar mendukung proses percobaan diharapkan bisa berjalan dengan baik dan mendapat hasil baik sesuai apa yang diinginkan. Berikut merupakan rinciannya :

3.1.1 Spesifikasi Software

Berikut penggunaan (*Software*) yang digunakan :

a. Sistem operasi Windows 11
b. Microsoft Office 2016
c. Google Chrome 120.0.6099.130
d. Visual Studio Code 1.41.1
e. Xampp 7.3.11

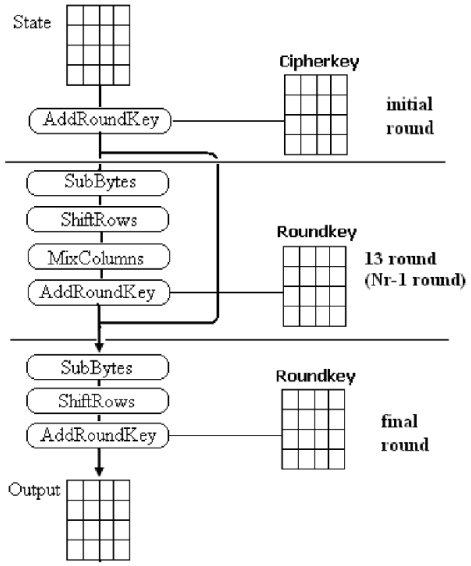
3.1.2 Spesifikasi Hardware

Berikut penggunaan (*Hardware*) yang digunakan :

a. Processor : Intel® Core™ i5-8250U 1.60GHz
b. Memory : 8 GB
c. Hardisk : 1 TB
d. Keyboard
e. Mouse

3.2 Implementasi Metode

Berikut adalah penjelasan singkat perihal implementasi metode enkripsi maupun dekripsi data, menggunakan algoritma *Advanced Encryption Standard* (AES).
Enkripsi algoritma AES memiliki prosedur diantaranya terdapat 4 macam perubahan bytes, yaitu *SubBytes*, *ShiftRows*, *Mixcolumns, dan AddRoundKey*. Langkah pertama kali pengenkripsian, input yang sudah disalin ke bagian state akan mendapatkan perubahan *byte AddRoundKey*. Kemudian, state tersebut akan mendapatkan perubahan *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* secara terus-menerus sejumlah *Nr*. Proses ini yang pada algoritma AES di sebut juga dengan *round function. Round* yang terbelakang memiliki perbedaan oleh *round-round* lebih dahulu yang mana dalam round terbelakang, *state* tidak terjadinya perubahan *MixColumns*. [7]
Berikut merupakan Ilustrasi dari prosedur pengenkripsian AES yang digambarkan didalam Gambar 4 berikut :



Gambar 4. Penggamabaran Prosedur Enkripsi AES.

3.2.1 Algoritma Enkripsi dengan Algoritma AES

Algoritma 1 ini menjelaskan bagaimana proses membuat data dienkrip yang selanjutnya dimasukan ke dalam Database. Hasil ditunjukan pada table 1

Algoritma 1. Proses Enkripsi

1. #start
2. Memasukan kunci enkrip pada sistem dan *Plaintext*
3. Inisialisasi terhadap state sebelum dienkripsi dengan algoritma AES, yang disebut penjadwalan kunci
4. Data dienkripsi dengan algoritma AES
5. Menghasilkan *Chipertext* data
6. Hasil chipertext data dimasukan ke dalam *Database*
7. #finish

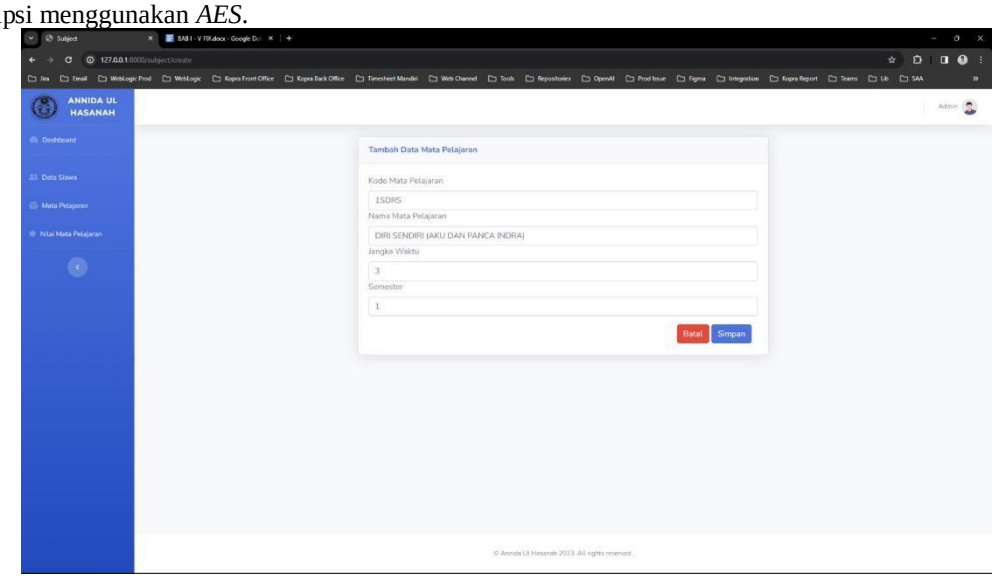
Table 1 di bawah menunjukan hasil dari algoritma 1 dan meampilkan hasil dari enkripsi yang berhasil

Tabel 1. Hasil Enkripsi

No	Keterangan Data	Data Masukan	Data Hasil	Ukuran Data (Kb)	Status
1	Kode Mata Pelajaran	1SDRS	WuyHbvVPTCz/sx9WCRvRbcV WTF7Q5/PSdVTsN+8GiXOxiiat 4InIEn0caAXy4/p7p9AzLMppG 0K1K4HCJMqfJA==	89	Berhasil
2	Nama Mata Pelajaran	DIRI SENDIRI (AKU DAN PANCA INDRA)	9U1pwienhWcmCVtDNBu6Zod vhlkCDuaO0ObgZa7oqPqvsvb6b B/KiDUnOWFcdlgVnF4D14l0u8 Hr/buPQcDYHt+SomcOz4BhYG uaDqmeq0mCS4ZJUgqyQkuboF 3X90S/	132	Berhasil
3	Jangka Waktu	3	uri33gQCbB7YFOQfJW1dEF2Y t9AGnwCmGnLgcohTGH+oQE G2SEkixaIYmotsEDahkYgdNaZ	89	Berhasil

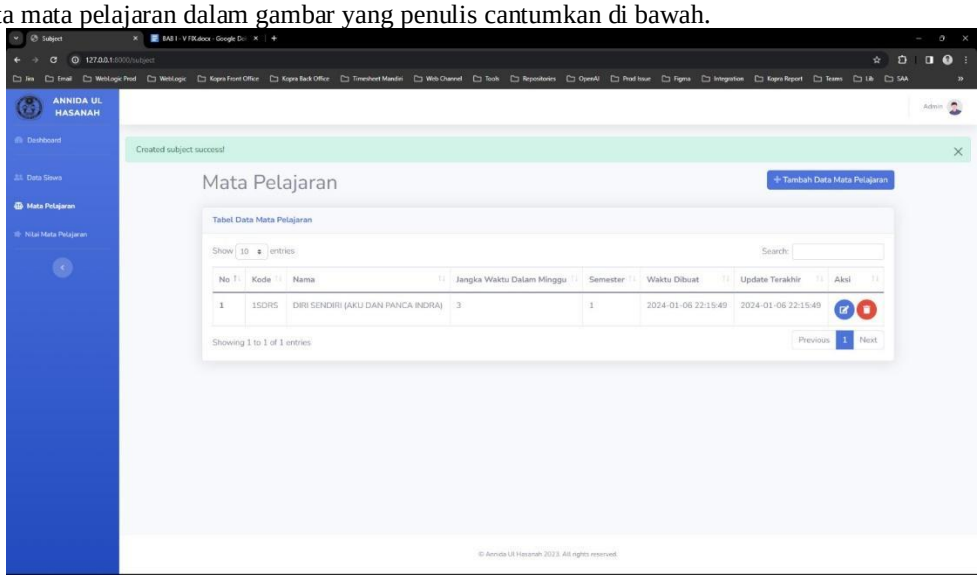
			YJRj12av1INESJg==		
4	Semester	1	Dg5R+gCrj7mSWZPkiaAaaWoa B5m2nKPOPPNmQDlUylTfPAi mTZhrGH9fVgPQ9FdWU59BQ S1GQ4SmhyDNuW681w==	89	Berhasil

Pada gambar 5 adalah input data mata pelajaran yang sudah terisi dalam form yang disediakan sebelum dienkripsi menggunakan *AES*.



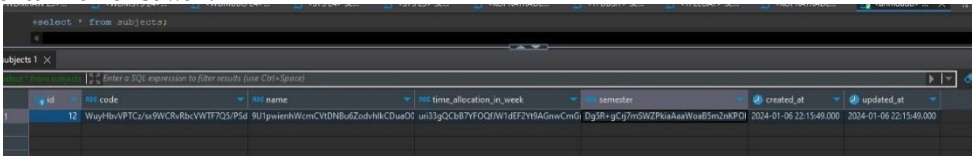
Gambar 5. Pengujian proses Enkripsi input

Gambar 6 berikut saat data disimpan akan tampil notifikasi sukses tersimpan dan data bisa dilihat pada tabel data mata pelajaran dalam gambar yang penulis cantumkan di bawah.



Gambar 6. Pengujian proses Enkripsi input sukses

Pada akhirnya jika kita lihat pada *database*, data yang terinput sudah terenkripsi seperti pada gambar 7 yang dicantumkan di bawah.



Gambar 7. Pengujian proses Enkripsi *database*

3.2.2 Algoritma Dekripsi dengan Algoritma AES

Algoritma 2 ini menjelaskan bagaimana proses merubah data yang sudah dienkripsi kemudian didekripsi sehingga menjadi Plaintext. Hasil ditunjukan pada Table 2.

Algoritma 2. Proses Dekripsi

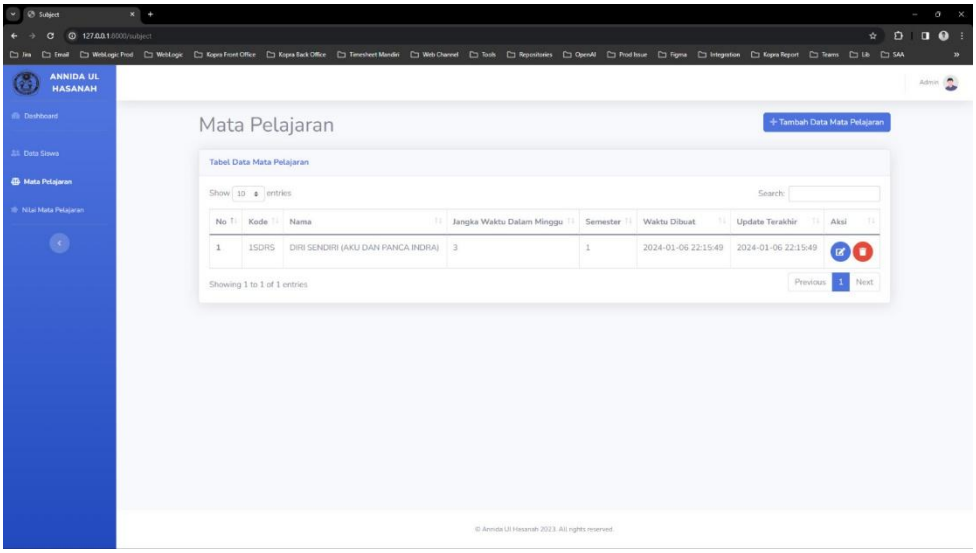
1. #start
2. Masukan kunci
3. Penjadwalan kunci
4. Dekripsi dengan algoritma AES
5. Menhasilkan *Plaintext*
6. #finish

Table 2 di bawah menunjukan hasil dari algoritma 2 dan meampilkan hasil dari dekripsi yang berhasil bisa dilihat di data hasil pada tabel.

Tabel 2. Hasil Dekripsi

No	Keterangan Data	Data Masukan	Data Hasil	Ukuran Data (Kb)	Status
1	Kode Mata Pelajaran	WuyHbvVPTCz/sx9WCRvRbcVWTF7Q5/PSdVTsN+8GiXOxiiat4InIEn0caAXy4/p7p9AzLMppG0K1K4HCJMqfJA==	1SDRS	89	Berhasil
2	Nama Mata Pelajaran	9U1pwienhWcmCVtDNBu6ZodvhlkCDuaO0ObgZa7oqPqvsvb6bB/KiDUnOWFcdlgVnF4D14l0u8Hr/buPQcDYHt+SomcOz4BhYGuaDqmeq0mCS4ZJUgqyQkuboF3X90S/	DIRI SENDIRI (AKU DAN PANCA INDRA)	132	Berhasil
3	Jangka Waktu	uri33gQCbB7YFOQfJW1dEF2Yt9AGnwCmGnLgcohTGH+oQEG2SEkixaIYmotsEDahkYgdNaZYJRj12av1INESJg==	3	89	Berhasil
4	Semester	Dg5R+gCrj7mSWZPkiaAaaWoaB5m2nKPOPPNmQDlUylTfPAimTZhrGH9fVgPQ9FdWU59BQS1GQ4SmhyDNuW681w==	1	89	Berhasil

Bisa terlihat dalam gambar 7 di atas sebelumnya, terhadap data yang tersimpan sudah terenkripsi, selanjutnya jika kita membuka halaman Mata Pelajaran akan tampil data yang sudah didekripsi seperti pada gambar 8 di bawah ini.



Gambar 8. Pengujian proses dekripsi

4. KESIMPULAN

Berdasarkan dari kajian bab yang dijabarkan sebelumnya terhadap permasalah serta aplikasi yang telah dikembangkan, maka dapat diberikan kesimpulan mengenai proses enkripsi dan dekripsi atau masalah keamanan data, antara lain :

a) Sistem informasi yang dibuat sudah berhasil mengamankan data yang terdapat pada *database* dengan cara enkripsi menggunakan *AES*.
b) Sistem informasi yang dibuat sudah berhasil menterjemahkan data yang sudah terenkripsi dengan melakukan dekripsi.
c) Jenis data yang dapat dienkripsi dan didekripsi berupa jenis data teks.
d) Sistem informasi yang dibuat dapat diakses hanya oleh staff yang sudah memiliki *email* dan *password* terdaftar saja.

8. DAFTAR PUSTAKA

[1] W. Putra *et al.*, "*Implementasi Algoritma Advanced Encryption Standard Untuk Kemanan Dokumen*," *Teknologi Dan Informasi V*, vol. 1, no. 2, pp. 76–83, 2023, [Online]. Available: https://journal.grahamitra.id/index.php/jurikti

[2] N. Ubay Baidoi, M. Hardjianto, and A. Wibowo, "*2 nd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) 21 Maret 2023-Jakarta*," 2023.

[3] M. R. Andriyanto and P. Sukmasetya, "*Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Keamanan Data Transaksi Pada Sistem E-Marketplace*," *Journal of Computer System and Informatics (JoSYC)*, vol. 4, no. 1, pp. 179–187, Dec. 2022, doi: 10.47065/josyc.v4i1.2451.

[4] M. Fakhriza, "*IMPLEMENTASI ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) E-ASPIRASI MAHASISWA PADA FAKULTAS SAINS DAN TEKNOLOGI BERBASIS WEB*," *JISTech (Journal of Islamic Science and Technology) JISTech*, vol. 7, no. 1, pp. 1–14, 2022. [Online]. Available: http://jurnal.uinsu.ac.id/index.php/jistech

[5] A. Tumanggor, H. Rumapea, A. Silalahi, and H. Artikel, "*Implementasi Algoritma Advance Encryption Standard (AES) Pada Keamanan Dokumen Keuangan (Studi Kasus : CV.Multikreasi Bersama)*," 2023. [Online]. Available: http://ojs.fikom-methodist.net/index.php/methotika

[6] M. Azhari, J. Perwitosari, and F. Ali, "*Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma* Kriptografi *Advanced Encryption Standard (AES),*" *Jurnal Pendidikan Sains dan Komputer*, vol. 2, no. 1, pp. 2809–476, 2022, doi: 10.47709/jpsk.v2i1.1390.

[7] N. Cristy and F. Riandari, "*Niolinda Cristy 1 , Fristi Riandari 2 [Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan*," vol. 4, no. 2, p. 75, 2021.

[8] 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*," *Applied Information System and Management (AISM)*, vol. 3, no. 2, pp. 69–78, Jan. 2021, doi: 10.15408/aism.v3i2.14722.

[9] Y. Putra, Y. Yuhandri, and S. Sumijan, "*Meningkatkan Keamanan Web Menggunakan Algoritma Advanced Encryption Standard (AES) terhadap Seragan Cross Site Scripting*," *Jurnal Sistim Informasi dan Teknologi*, pp. 56–63, Jun. 2021, doi: 10.37034/jsisfotek.v3i2.44.

[10] F. Ahmad Sitorus, N. Budi Nugroho, U. Fatimah Sari Sitorus Pane, P. Studi Mahasiswa, S. Triguna Dharma, and P. Studi Dosen Pembimbing, "*Implementasi Algoritma Advanced Encryption Standard (AES) 128 Bit Untuk Keamanan Data Transaksi Penjualan Pada PT. MITSUBISHI ELECTRIC INDONESIA*," 2020. [Online]. Available: https://ojs.trigunadharma.ac.id/