PENGAMANAN *DATABASE* PERPUSTAKAAN DENGAN ALGORITMA *AES-128* PADA SMA WASKITO

Muhammad Thoriq Ardian[1*], Wahyu Pramusinto[2]

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

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

Abstrak-Perkembangan teknologi informasi saat ini telah berkembang dengan pesat dan dinamis, khususnya pada sektor pendidikan. Perpustakaan sekolah pun pada saat ini mulai banyak memakai aplikasi berbasis website sebagai tempat untuk mengelola data-data yang ada di perpustakaan. Perpustakaan menggunakan sistem komputerisasi, dapat membantu sekolah dalam kegiatan dilingkungan sekolah, SMA WASKITO merupakan lembaga di bidang pendidikan Sekolah Menengah Atas, dan belum memilik sistem informasi untuk membantu pengolahan data-data perpustakaan sekolah, dengan keamanan kriptografi yang baik untuk mengolah dan mengamankan data-data tersebut.kriptografi sendiri adalah teknik untuk mengacak data menjadi data yang tidak dapat dibaca oleh manusia dan hanya bisa diterjemahkan oleh komputer. Perpustakaan sekolah berbasis website akan dibuat dengan bahasa pemrogramman *php* dengan keamanan menggunakan metode kriptografi *AES-128* untuk keamanan *database*. Algoritma AES adalah algoritma enkripsi yang aman untuk melindungi data dan informasi sensitif. Dirilis oleh NIST (National Institute of Standards and Technology) pada tahun 2001, AES digunakan untuk menggantikan algoritma DES, yang dianggap lebih tua dan lebih mudah untuk diretas. Lalu akan dilakukan pengujian proses enkripsi dan dekripsi untuk memastikan apakah algoritma kriptografi berjalan dengan baik. Dari hasil pengujian diketahui bahwa jumlah karakter asli dapat mempengaruhi jumlah karakter hasil enkripsi. Kesimpulan akhir yang dicapai dalam penelitian ini adalah aplikasi dapat mengamankan data perpustakaan sekolah.

Kata Kunci: AES-128, perpustakaan, berbasis website

LIBRARY DATABASE SECURITY WITH AES-128 ALGORITHM ON WASKITO HIGH SCHOOL

The development of information technology is currently growing rapidly and dynamically, especially in the education sector. The school library is now starting to use a lot of website-based applications as a place to manage the data in the library. The library uses a computerized system, can help schools in activities in the school environment, WASKITO High School is an institution in the field of high school education, and does not yet have an information system to help process school library data, with good cryptographic security to process and secure data. Cryptography itself is a technique to scramble data into data that cannot be read by humans and can only be translated by computers. The website-based school library will be created with the PHP programming language with security using the AES-128 cryptographic method for database security. The AES algorithm is a secure encryption algorithm to protect sensitive data and information. Released by NIST (National Institute of Standards and Technology) in 2001, AES is used to replace the DES algorithm, which is considered older and easier to hack. Then the encryption and decryption process will be tested to ensure whether the cryptographic algorithm works well. From the test results it is known that the number of original characters can affect the number of characters from the encryption results. The final conclusion reached in this research is the application can secure school library data..

***Keywords**: AES-128, library, web-based*

1. PENDAHULUAN

Perkembangan teknologi informasi saat ini telah berkembang sangat pesat. *Website* adalah salah satu sarana untuk menyampaikan informasi dengan cepat. Proses mendapatkan informasi dari *website* lebih cepat dan juga lebih *up to date*. *Website* menjadi sarana infomasi yang sangat digemari *user* untuk saat ini karena, sangat mudah untuk diakses. Aplikasi *website* sendiri adalah aplikasi yang diakses menggunakan *browser* melalui jaringan internet. [1]

Perkembangan teknologi sangat membantu dalam satu dan lain hal, misalnya dalam bidang pendidikan. Pendidikan merupakan bidang yang saat ini sangat diprioritaskan pada perkembangan teknologi informasi untuk mendukung proses belajar. Fasilitas perpustakaan dibangun untuk menampung koleksi buku dan sumber bacaan. Koleksi bukunya selalu update dengan perkembangan ilmu pengetahuan. Sekolah merupakan salah satu contoh lembaga yang membutuhkan perpustakaan. Meningkatkan efisiensi dan efektifitas proses belajar khususnya pemanfaatan perpustakaan sebagai media pembelajaran. Perpustakaan sekolah juga membutuhkan aplikasi

perpustakaan berbasis web untuk menciptakan perpustakaan yang tertata dengan baik dan sistematis. Perpustakaan berbasis situs membutuhkan tampilan yang memungkinkan pengguna untuk melihat data buku dengan mudah. Perpustakaan juga membutuhkan sistem database yang baik agar semua data dapat tertata dengan baik. [2]

Sistem *database* berfungsi sangat penting untuk menyimpan data-data atau informasi. *Database* salah satu kunci penting dalam membuat sebuah *website.* Perpustakaan harus mempunyai sebuah database karena untuk memudahkan mencari buku-buku yang ada di perpustakaan tersebut. informasi *user* dan pelanggan juga ada di dalam *database*. Database juga harus ditambahkan sistem keamanan yaitu bisa dengan cara enkripsi data. Banyak sekali metode yang bisa dipakai untuk mengenkripsi sebuah data contohnya dengan menggunakan algoritma. Beberapa algoritma yang bisa dipakai untuk enkripsi dan dekripsi sebuah data salah satu contohnya adalah algoritma *Advanced Encryption Standart* (*AES).* [3]

Kriptografi berasal dari bahasa Yunani yaitu crypto dan graffia. Crypto artinya rahasia dan graffia artinya tulisan. Menurut istilah, enkripsi adalah ilmu dan teknologi untuk menjaga keamanan pesan saat dikirim dari satu tempat ke tempat lain. Enkripsi awalnya digambarkan sebagai studi tentang cara menyembunyikan pesan. Namun, kriptografi dalam pengertian modern adalah ilmu yang didasarkan pada metode matematika untuk menangani keamanan informasi contohnya kerahasiaan, integritas data, dan otentikasi entitas. [4]

Secara historis, kriptografi berada di masa kejayaannya bagi orang Yunani sekitar 400 SM. cukup terkenal. Alat yang digunakan untuk membuat pesan tersembunyi selama peradaban Yunani disebut Scytale. Bentuk scytale sendiri adalah batang silindris yang terdiri dari 18 kombinasi huruf. Selama pemerintahan Julius Caesar di Kekaisaran Romawi, penggunaan kriptografi menjadi lebih luas untuk alasan stabilitas nasional. Dengan demikian, berdasarkan aspek tersebut, walaupun klasik maupun modern, kriptografi memiliki tujuan yang sama yaitu sebagai sistem keamanan. [5]

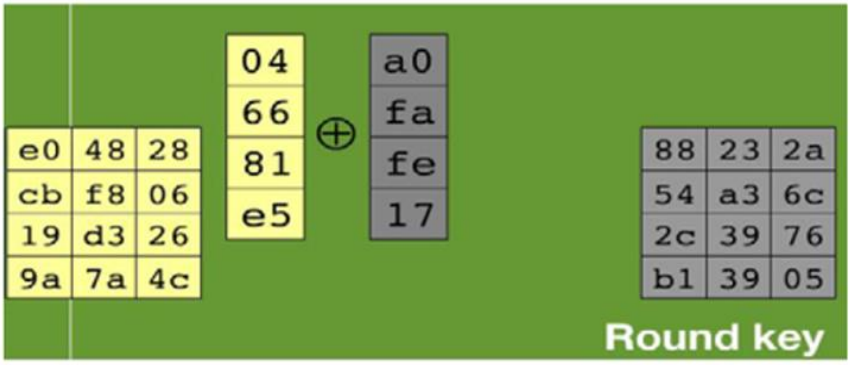
Algoritma AES adalah algoritma enkripsi yang aman untuk melindungi data dan informasi sensitif. Dirilis oleh NIST (National Institute of Standards and Technology) pada tahun 2001, AES digunakan untuk menggantikan algoritma DES, yang dianggap lebih tua dan lebih mudah untuk diretas. Jumlah putaran yang dilakukan oleh AES tergantung pada ukuran kunci yang digunakan. Misalnya, jika ukuran kunci adalah 128, ukuran blok tetap 128 bit berarti 10 putaran, 192 bit berarti 12 putaran, dan 256 bit berarti 14 putaran. Algoritma AES-128 adalah jenis enkripsi simetris. Ini berarti menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi informasi. Selain itu, pengirim dan penerima data memerlukan salinan data untuk mendekripsinya. [6]

Pada Proses enkripsi awalnya teks asli dibentuk sebagai sebuah state. Kemudian sebelum ronde 1 dimulai blok teks asli dicampur dengan kunci ronde ke-0 (transformasi ini disebut AddRoundKey). Setelah itu, ronde ke-1 sampai dengan ronde ke-(Nr-1) dengan Nr adalah jumlah ronde. AES menggunakan 4 jenis transformasi yaitu: *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*. Pada ronde terakhir, yaitu ronde ke-Nr dilakukan transformsi serupa dengan ronde lain namun tanpa transfomasi serupa dengan ronde lain namun tanpa transformasi MixColumns. [7]

Algoritma dekripsi AES menggunakan kebalikan dari semua transformasi dasar yang digunakan dalam algoritma enkripsi AES. Setiap transformasi dasar dari algoritma enkripsi AES memiliki transformasi terbalik: InvSubBytes, InvShiftRows, dan InvMixColumns. AddroundKey adalah transformasi pembalik diri jika Anda menggunakan kunci yang sama. [8]

1. *AddRoundKey*

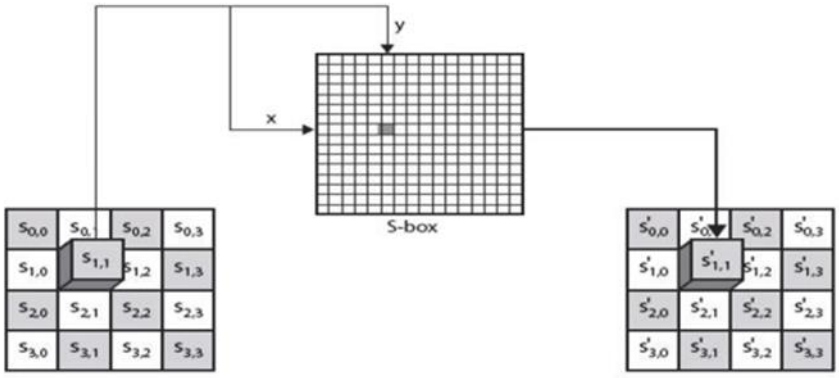
Fase AddRoundKey ini pertama-tama memperluas kunci kriptografi yang ada untuk mendapatkan *roundkey* yang akan digunakan dalam proses berikut. Kemudian setiap byte dari state matrix dari proses MixColumns di-XOR dengan setiap byte dari round key. Proses putaran atau proses SubBytes, ShiftRows, MixColumns dan AddRoundKey dilakukan dengan cara yang sama hingga putaran ke-n. Di sisi lain, di babak final (juga disebut babak final), proses SubBytes, ShiftRows, dan AddRoundKey terus berjalan, tetapi proses MixColumns tidak. [9]



Gambar 1. *AddRoundKey*

2. *SubBytes*

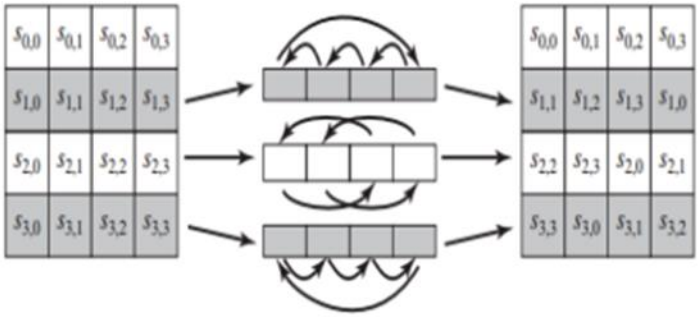
SubBytes yaitu transformasi byte di mana setiap elemen state dipetakan menggunakan tabel pengganti (S-Box). Ini karena setiap byte state diwakili oleh S`[r, c]. S`[r,c] adalah elemen dari tabel permutasi yang merupakan perpotongan baris (x) dan kolom (y). [9]



Gambar 2. *SubBytes*

3. *ShiftRows*

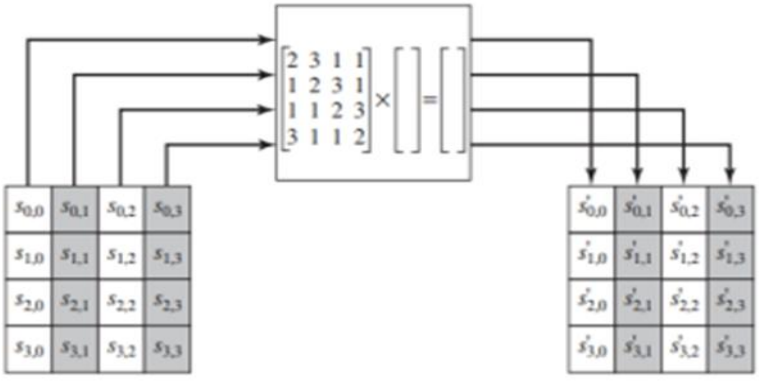
Shiftrows pada dasarnya adalah proses pergeseran bit dimana bit paling kiri digeser ke bit paling kanan (rotasi bit). Namun, jumlah shift yang dilakukan bervariasi dari baris ke baris. Baris pertama tidak dipindahkan. Setiap byte di baris kedua dari matriks status digeser ke kiri satu byte. Kemudian baris ketiga digeser ke kiri sebesar 2 byte, dan baris keempat digeser ke kiri sebesar 3 byte. Proses ini bertujuan untuk menciptakan difusi dengan mendistribusikan efek transformasi nonlinier ke baris-baris matriks keadaan putaran berikutnya. [9]



Gambar 3. *ShiftRows*

4. *MixColumn*

Proses *MixColumns mengalikan setiap kolom dari matriks. Tujuannya adalah untuk mendistribusikan* efek dari semua bit plaintext dan kunci enkripsi pada ciphertext yang dihasilkan pada kolom-kolom matriks. Setiap kolom matriks *state* diperlakukan sebagai polinomial 4 suku di bidang Galois dan dikalikan modulus (X8 + X4 + X3 + X + 1). Operasi MixColumns dapat dilihat sebagai perkalian matriks. [10]



Gambar 4. *MixColumn*

2. METODE PENELITIAN

Metode penelitian untuk membangun sistem ini menggunakan metode menganalisa data,rancangan algoritma dan tahap implementasi yang menggunakan Bahasa pemrograman PHP, lalu dilanjutkan dengan tahap pengujian.

2.1 Analisis Masalah

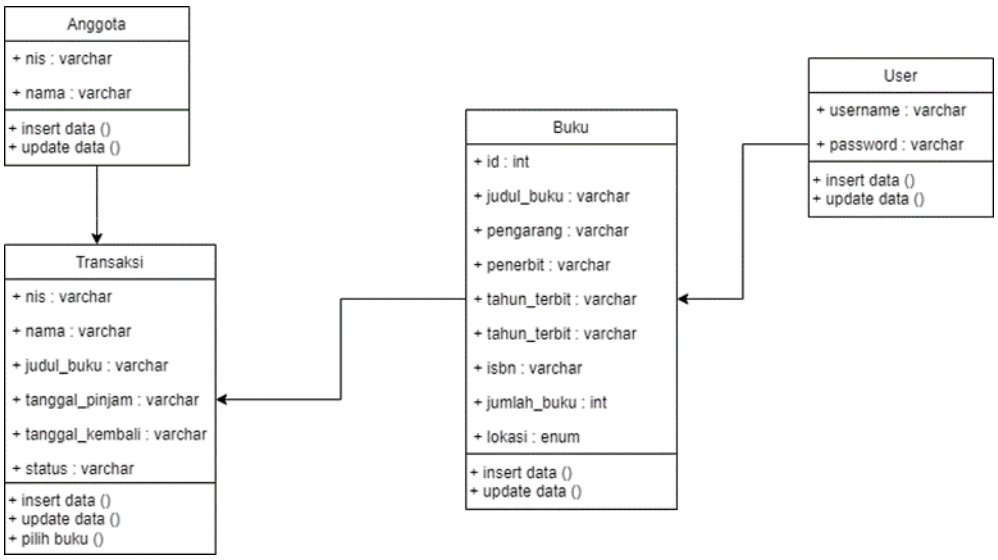
Sebuah sekolah yang ada di Tangerang Selatan yaitu SMA WASKITO memiliki masalah dalam masalah keamanan database dan memanajemen perpustakaan mereka agar sistematis. Pengamanan yang belum ada di sekolah ini adalah di sektor perpustakaan dalam mengamankan data-data sekolah yang disimpan dalam perpustakaan.

2.2 Rancangan Sistem

Rancangan sistem ini menjelaskan tentang bagaimana proses enkripsi dan dekripsi data yang diinput oleh admin, menggunakan pemanggilan fungsi enkripsi dan dekripsi.

2.3 *Class Diagram*

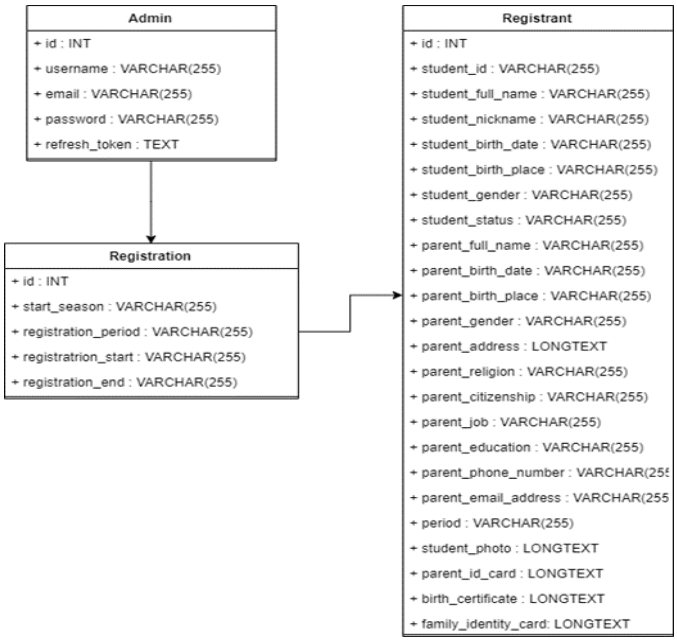
Diagram ini menunjukkan apa yang termasuk dalam sistem yang dimodelkan dengan komponen yang berbeda. Komponen yang berbeda ini dapat mewakili kelas yang diprogram, objek utama, atau interaksi antara kelas dan objek.



Gambar 5. *Class Diagram*

2.4 *Logical Record Structure* (LRS)

Gambaran susuna *record* dalam sebuah tabel yang terbentuk dari hasil hubungan antar himpunan. Di bawah ini adalah gambar *LRS* dari komponen *class diagram*.



Gambar 6. *Logical Record Structure* (LRS)

3. HASIL DAN PEMBAHASAN

3.1 Implementasi Metode

Penerapan metode kriptografi AES-128 pada bagian implementasi metode yang akan dijabarkan di bawah ini. Kita ambil contoh proses enkripsi dan dekripsi pada tambah data anggota dan tampil data anggota.

3.2 Proses Enkripsi

Proses pertama dalam enkripsi adalah pembuatan *EncryptBlock*, Proses ini adalah membuat metode enkripsi data dalam blok untuk menghasilkan *ciphertext* menggunakan kunci kritografi. Proses lainnya yaitu pemanggilan proses AES.

```
public function encryptBlock($x)

    $y = ''; // 16-byte string

    // place input x into the initial state matrix in column order
    for ($i = 0; $i < 4 * self::$Nb; $i++) {
        // we want integerger division for the second index
        $this->s[$i % 4][($i - $i % self::$Nb) / self::$Nb] = ord($x[$i]);

    // add round key
    $this->addRoundKey(0);
    end for

    for ($i = 1; $i < $this->Nr; $i++) {
        // substitute bytes
        $this->subBytes();

        // shift rows
        $this->shiftRows();

        // mix columns
        $this->mixColumns();

        // add round key
        $this->addRoundKey($i);
    end
```

Gambar 7. *EncryptBlock*

```
KeyExpansion (byte key[4*Nk], word w[Nb* (Nr+1)), Nk)
begin
    word temp

    i = 0
   while (i < Nk)
   w[i] = word (key[4*i], key[4*1+1], key[4*1+2], key[4*1+31)
   i= i+1
   end while

   1 = Nk
  while (i< Nb*(Nr+1)]
   temp = w[i-1)
   if (i mod Nk = 0)
      temp = Subword (RotWord (temp) ) xor Rcon[i/Nk)
   else if (Nk > 6 and i mod Nk=4)
   temp = Subword (temp)
   end if
   w[i] = W[i-Nk] xor temp
    i=i+1
   end while
end
```

Gambar 8. Pemanggilan proses AES

3.3 Proses Dekripsi

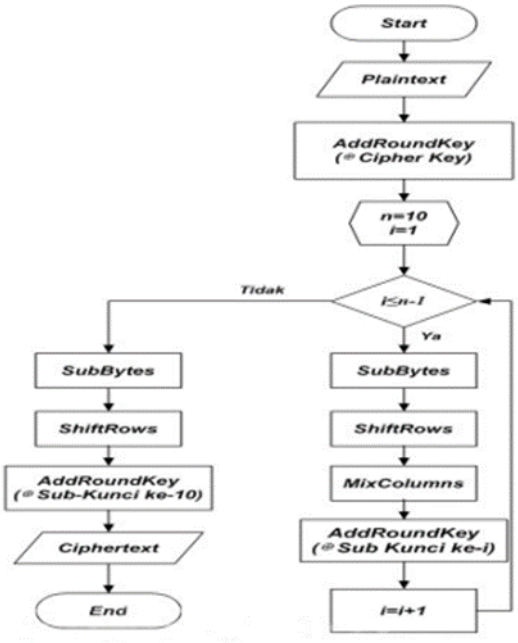
Proses dekripsi ini digunakan untuk mengubah *ciphertext* menjadi *plaintext*.

```
public function decryptBlock($y)
  {
     $x = ''; // 16-byte string

     // place input y into the initial state matrix in column order
     for ($i = 0; $i < 4 * self::$Nb; $i++) {
        $this->s[$i % 4][($i - $i % self::$Nb) / self::$Nb] = ord($y[$i]);
     end for

     // add round key
     $this->addRoundKey($this->Nr);

     for ($i = $this->Nr - 1; $i > 0; $i--) {
        // inverse shift rows
        $this->invShiftRows();

        // inverse sub bytes
        $this->invSubBytes();

        // add round key
        $this->addRoundKey($i);

        // inverse mix columns
        $this->invMixColumns();
     end
```

Gambar 9. Proses *DecryptBlock*

3.4 *Flowchart* Enkripsi dan Dekripsi

Flowchart sistem menggunakan algoritma kriptografi *Advanced Enryption System 128 (AES-128).*



Gambar 10. *Flowchart* Enkripsi

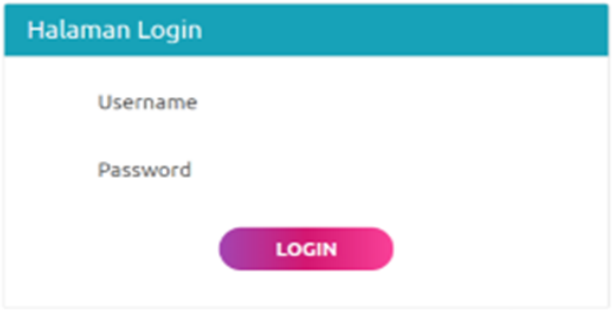
Gambar 11. *Flowchart* Dekripsi

3.5 Tampilan Layar

Di bawah ini adalah tangkapan layar dari sistem perpustakaan berbasis situs web yang dibuat menggunakan algoritma keamanan kriptografi AES-128 untuk melindungi data.

1. Halaman *Login*

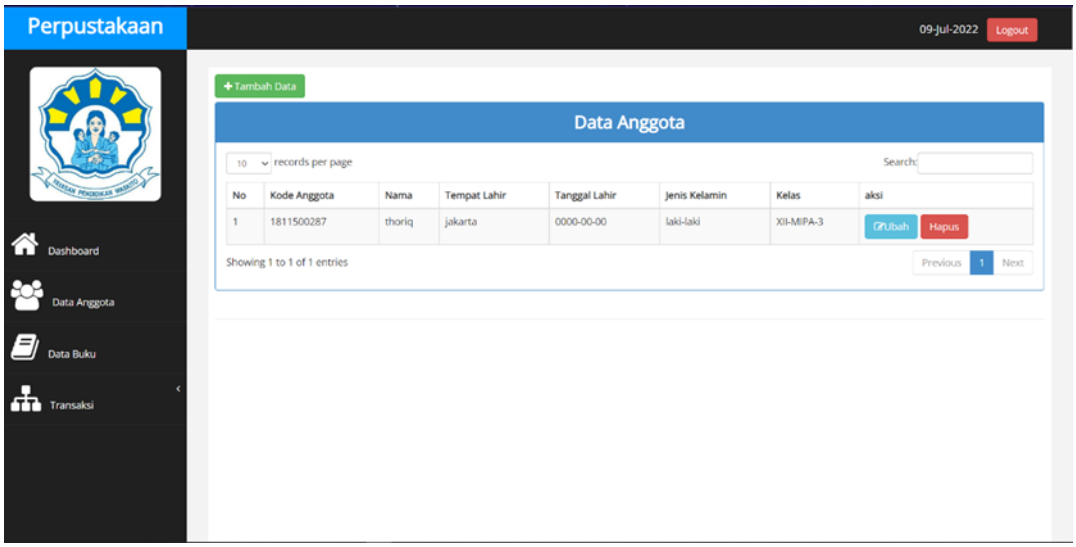
Berikut ini adalah tampilan layar dari halaman *login*, terdapat input *field username* dan *password*.



Gambar 12. Halaman *login*

2. Halaman Utama Anggota

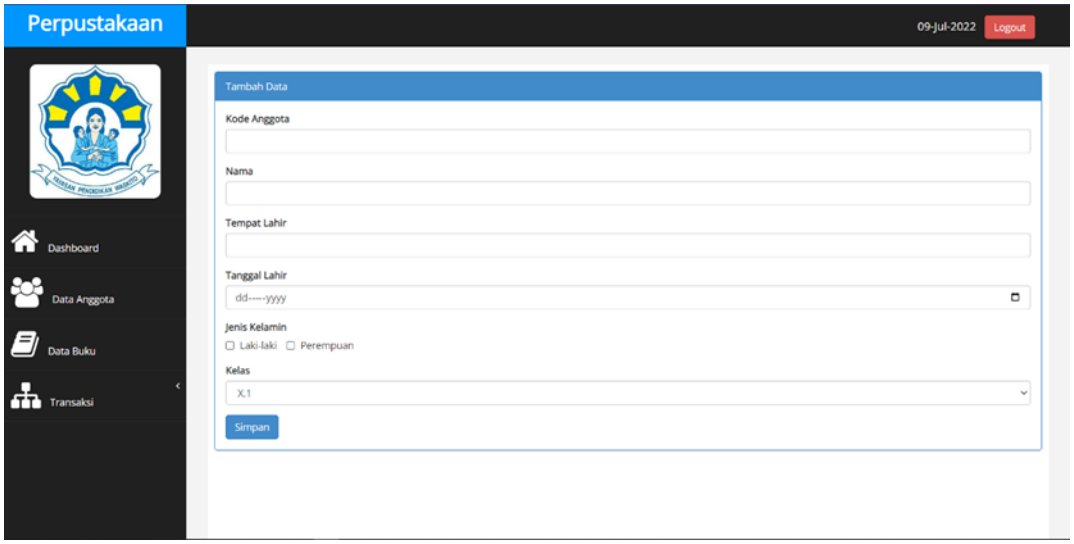
Halaman anggota berisikan data anggota yang telah terdaftar didalam database. Terdapat juga dua button untuk proses ubah dan hapus data.



Gambar 13. Halaman anggota

3. Halaman Tambah Data Anggota

Halaman ini ditampilkan setelah mengklik tombol Tambah Data. Halaman Tambah Data memiliki form untuk data anggota.



Gambar 14. Halaman tambah data anggota

3.6 Pengujian

Pengujian ini akan memfokuskan terhadap sisi kecepatan dan hasil enkripsi yang berupa berapa banyak karakter dan berapa ukuran data sebelum dan setelah dienkripsi menggunakan algoritma enkripsi Advanced Encryption Standard 128.

Tabel 1. Pengujian Kriptografi Data *String*

Karakter Asli	Hasil Enkripsi	Jumlah Karakter (*Bit*)		Waktu	
		Asli	Enkripsi	Enkripsi	Dekripsi
Muhammad Thoriq Ardian	pVCsb23QbojptILhKj3tEsum5kQP hAx5qsIg4IzHTu8=	20	44	6.027937 ms	0.283003 ms
Nurahman Latip	r1JVhjyDWR+9yizYS4QCSQ==	14	24	3.56602668 76 ms	0.1728534 698 ms

Karakter Asli	Hasil Enkripsi	Jumlah Karakter (*Bit*)		Waktu	
		Asli	Enkripsi	Enkripsi	Dekripsi
Nanda Reza Alfian	xfKwg22OGlTgBOoCLoPuE+KdDyqwPBisXfNHbUhCq0o=	17	44	4.22286987 3 ms	0.8120536 804 ms
Maghvira Ramadhanty	D89wtB6ny299D5pIG0zGKaE8lqZ6Bkq11u8mNeDw2LI=	19	44	5.03706932 07 ms	0.5900859 833 ms
Rizky	ps8o5nYSQVaOfz7AqGabEg==	5	24	3.63898277 28ms	0.1659393 311 ms
Rayhan Davon	uojTlKEhPNUrUlpiMUl4mg==	12	24	4.33397293 09 ms	0.2539157 867 ms
Faddlurohman	UjGx9CXF7wsXL2S02jtCxg==	12	24	4.79412078 86 ms	0.1559257 507 ms
Rizky Aditya	Mu4jyBB+fD/GriMmsveVgg==	12	24	4.50491905 21 ms	0.1688003 54ms
Anto Juniarto	uPLFmnmKyfQy8yp82HgWKw==	13	24	5.15294075 01 ms	0.1480579 376 ms
Achmad Kosasi	nE7RqcEDgJiLsswKx0KTEA==	13	24	3.31091880 8 ms	0.4060268 402 ms

4. KESIMPULAN

Setelah membangun sistem melalui tahap desain, dilanjutkan ke tahap implementasi dapat disimpulan bahwa, sistem ini digunakan untuk mengamankan data perpustakaan pada SMA WASKITO, data yang terenkripsi ini adalah kumpulan kombinasi karakter yang tidak dipahami oleh manusia. Hal ini dikarenakan hasil enkripsi selalu sama dengan hasil dekripsi menggunakan kunci yang sama. Setelah penelitian ini dilakukan sistem ini dapat membantu pihak sekolah dalam mengelola data mereka dan data tersebut dapat disimpan dengan aman.

DAFTAR PUSTAKA

[1] A. L. Gadja And Y. S. Belutowe, "Pengamanan Website Pengarsipan Dokumen Penting Di Polda Nusa Tenggara Timur Dengan Algoritma Aes-128," *Sekolah Tinggi Manajemen Informatika & Komputer (STIKOM) Uyelindo Kupang*, 2018.

[2] I. Chaidir, D. W. Aditya and Sumarna, "Rancang Bangun Sistem Informasi Perpustakaan Berbasis Web Pada Mts Al – Husna Depok," *Jurnal Informatika Merdeka Pasuruan,* vol. 5, 2020.

[3] M. Azhari, D. I. Mulyana, F. J. Perwitosari and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *Jurnal Pendidikan Sains dan Komputer,* vol. 2, 2022.

[4] P. Aji, "Rancang Bangun Sistem Informasi Perpustakaan Berbasis Web (Studi Kasus: Universitas Kuningan)," *Jurnal Cloud Information,* vol. 3, 2018.

[5] N. Rohmah, H. Aryadita and A. H. Brata, "Pengembangan Sistem Informasi Perpustakaan Berbasis Web Pada Perpustakaan Kecamatan Bungah," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer* , vol. 3, pp. 2225-2234, 2019.

[6] T. B. Tahir, M. A. HS and M. Rais, "Sistem Informasi Encrypt Dan Decrypt Dengan Algoritma AES Menggunakan Framework Laravel," *Patria Artha Technological Journal,* 2020.

[7] W. T. Ningsih, Y. Yunus and P. Radyuli, "Perancangan dan Pembuatan Sistem Informasi Perpustakaan Berbasis Web dengan PHP dan MySQL (Studi Kasus SMK Negeri 7 Padang)," *Jurnal Pendidikan Teknologi Informasi,* vol. 7, pp. 60-69, 2020.

[8] D. Widyawan and Imelda, "Pengamanan File Menggunakan Kriptografi Dengan Metode Aes-128 Berbasis Web Di Komite Nasional Keselamatan Transportasi," *SKANIKA,* vol. 4, pp. 15-22, 2021.

[9] R. Nuari and N. Ratama, "Implementasi Algoritma Kriptografi AES (Advanced Encryption Standard) 128 Bit Untuk Pengamanan Dokumen Shipping," *Journal Of Artificial Intelligence And Innovative Applications,* vol. 1, 2020.

[10] I. A. R. Simbolon, I. Gunawan, I. O. Kirana, R. Dewi and S. Solikhun, "Penerapan Algoritma AES 128-Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantar," *Journal of Computer System and Informatics (JoSYC)*, vol. 1, pp. 54-56, 2020.