(2024), 2 (3): 205–217 **Scientica** 3021-8209
Jurnal Ilmiah Sain dan Teknologi

PENGGUNAAN QR CODE BERBASIS KRIPTOGRAFI ALGORITMA ADVANCED ENCRYPTION STANDARD DAN SHA-512 UNTUK APLIKASI PENCATATAN BIAYA PENDIDIKAN BERBASIS WEB DI SMK PUSDIKHUBAD

Alfian Rahman[1)], Ade Kania Ningsih[2)], Ridwan Ilyas[3)]
Sains Dan Informatika, Teknik Informatika, Universitas Jenderal Achmad Yani, Kota Cimahi, Indonesia
Email: alfianrahman18@if.unjani.ac.id[1)], ade.kanianingsih@lecture.unjani.ac.id[2)], ilyas@lecture.unjani.ac.id[3)]

Abstract (English)
Vocational Education Expense Recording Data can contain some important information, such as the student's identity, parent/guardian, address and payment history for approximately 3 years the student has attended school. Where the data must be guaranteed security because the data is sensitive if there is data manipulation it will greatly impact students and schools. Therefore, data security is needed to keep data confidential and prevent unauthorized parties from misusing the data. The purpose of this research is to help with this problem by building a web-based Education Fee Recording system based on a case study at PUSDIKHUBAD Vocational School, using the Advanced Encryption Standard (AES-256) algorithm to encrypt and decrypt student billing data, and SHA-512 to encrypt key that will be used by AES-256, the result of the encryption will be converted into a QR Code. The QR Code will be used by students to make payments to TU staff. To test how effective the Advanced Encryption Standard (AES-256) algorithm is, the Avalanche Effect calculation method is used, where if the results obtained are more than 50% then the cryptography used is good because small changes to the plaintext can impact the ciphertext because there are several bits that change resulting in a change that makes it more secure.

Article History
Submitted: 1 Februari 2024
Accepted: 12 Februari 2024
Published: 13 Februari 2024

Key Words
Cryptography; SHA-512; Advanced Encryption Standard (AES-256); Avalanche Effect; NIS

Abstrak (Indonesia)
Data Pencatatan Biaya Pendidikan di SMK dapat memiliki beberapa informasi penting, seperti identitas siswa, orangtua/wali, alamat dan riwayat pembayaran selama kurang lebih 3 tahun siswa tersebut bersekolah. Dimana data tersebut diharuskan terjamin keamanannya dikarenakan data tersebut bersifat sensitif jika adanya manipulasi data maka akan sangat berdampak bagi siswa maupun sekolah. Oleh karena itu maka dibutuhkan keamanan data untuk menjaga data agar terjaga kerahasiaannya dan juga mencegah pihak yang tidak berwenang untuk menyalahgunakan data tersebut. Tujuan dari penelitian ini adalah untuk membantu persoalan tersebut dengan membangun sebuah sistem Pencatatan Biaya Pendidikan berbasis web berdasarkan studi kasus di SMK PUSDIKHUBAD, dengan menggunakan algoritma Advanced Encryption Standard (AES-256) untuk mengenripsi maupun dekripsi data tagihan siswa, dan SHA-512 untuk mengenkripsi key yang akan digunakan oleh AES-256, hasil dari enkripsi tersebut akan diubah menjadi sebuah QR Code. QR Code akan digunakan siswa untuk melakukan pembayaran kepada staff TU. Untuk pengujian seberapa efektifnya algoritma Advanced Encryption Standard (AES-256) maka digunakan metode perhitungan Avalanche Effect, dimana jika hasil yang didapat lebih dari 50% maka kriptografi yang digunakan adalah baik dikarenakan perubahan kecil pada plainteks dapat berdampak ke cipherteks sebab terdapat beberapa bit yang berubah yang mengakibatkan perubahan yang membuat lebih aman.

Sejarah Artikel
Submitted: 1 Februari 2024
Accepted: 12 Februari 2024
Published: 13 Februari 2024

Kata Kunci
Kriptografi; SHA-512; Advanced Encryption Standard (AES-256); Avalanche Effect; NIS

PENDAHULUAN

SMK Pusdikhubad merupakan sebuah sekolah menengah kejuruan yang berada di Kecamatan Cimahi Tengah. Sekolah ini, pada proses Pencatatan Biaya Pendidikan hanya

menggunakan excel dalam melakukan rekap pembayaran siswa, Dan siswa hanya menerima laporan “Lunas” melalui kartu SPP yang cara penggunaannya masihlah tradisional yaitu tertulis tangan dan cap di kartu SPP mereka.

Proses digitalisasi menjadi salah satu bentuk pembaruan untuk permasalahan tersebut. Namun dalam digitalisasi terdapat beberapa permasalahan baru terkait dengan keamanan data, untuk menjaga privasi dan mencegah penyalahgunaan data, diperlukan metode-metode yang dapat digunakan untuk mengamankan data secara efektif.[1]. Guna mencegah ancaman kejahatan cyber seperti akses yang tidak sah atau ketidak tepatannya data tersebut ditujukan, pencurian, dan pemalsuan data, diperlukan upaya untuk menjaga keamanan dan integritas data.

Faktor keamanan data memang sangat penting dalam mengatasi masalah pembajakan dan penyalahgunaan data. Hal ini diperlukan agar data tetap bersifat rahasia dan tidak jatuh ke tangan yang salah.

Berdasarkan pembahasan diatas, kriptografi merupakan salah satu pendekatan yang digunakan untuk menjaga keamanan dan kerahasiaan data dengan mengubah data asli menggunakan algoritma khusus. Melalui proses ini, data diubah menjadi bentuk yang tidak dapat dikenali oleh siapa pun atau perangkat digital apa pun. Secara umum, kriptografi sering dikaitkan dengan konsep "tulisan rahasia". Namun, dalam pengertian yang sebenarnya, kriptografi adalah ilmu yang mempelajari tentang menjaga kerahasiaan data agar tetap aman, valid, dan terjaga keasliannya.

Hal ini mendorong penelitian untuk membuat sistem dimana siswa dan bendahara dapat terlibat langsung dengan sistem yang akan dibuat, dimana siswa dapat melihat riwayat pembayaran dan daftar tagihan mereka secara langsung melalui gadget/smartphone mereka namun tidak mempersulit siswa dalam cara penggunaannya. Untuk mensiasati permasalahan tersebut dibuatlah halaman

khusus yang bisa diakses oleh siswa dalam aplikasi yang akan dibangun, dimana siswa akan mendapatkan akun yang sudah disiapkan oleh sistem dan data riwayat pembayaran tersebut dapat diakses. Siswa juga dapat melakukan pembayaran tagihan dengan cara mengunduh QR yang disediakan oleh sistem dan menunjukkannya kepada Bendahara yang nantinya akan langsung diproses oleh bendahara.

Berdasarkan pada latar belakang yang telah dijabarkan diatas, maka pada penelitian ini akan melakukan pembangunan sistem Pencatatan Biaya Pendidikan bebasis Web berdasarkan studi kasus di SMK PUSDIKHUBAD yang dilengkapi dengan keamanan tambahan menggunakan kriptografi dengan metode AES-256 dan penggunaan SHA-512 untuk mengamankan key yang akan digunakan oleh AES-256 serta menggunakan QR Code dalam pengaksesannya. Keamanan akan berfokus pada data tagihan siswa, dimana setiap kali siswa akan melakukan pembayaran, siswa diharuskan untuk mengunduh QR pada aplikasi sesuai dengan akun yang dimiliki. QR Code berisikan data NIS yang nantinya akan dienkripsi dengan AES-256 menggunakan kode yang sudah ditentukan oleh bendahara sebelumnya. Bendahara nantinya akan memindai isi QR dan mendekripsikan isinya menggunakan kode yang sudah diatur. Jika proses dekripsi berhasil, maka data siswa beserta data tagihan siswa tersebut akan muncul, selanjutnya bendahara cukup mengkonfirmasi pembayaran siswa dan tagihan pun dinyatakan lunas. Siswa dapat melihat status tagihan melalui aplikasi sesuai dengan akun yang dimiliki.

AES-256 dipilih sebagai algoritma yang akan mengenkripsi data Nomor Induk Siswa dengan gabungan key yang ditentukan oleh bendahara ketika akan membuat QR Code melalui aplikasi menggunakan akun yang digunakan oleh siswa. Key akan dienkripsi menggunakan SHA-512 dan disimpan kedalam basis data, hasil dari enkripsi AES-256 akan dimasukkan kedalam QR Code yang nantinya akan digunakan siswa untuk melakukan pembayaran tagihan.

Pemilihan AES-256 dibandingkan AES-128 adalah dikarenakan jumlah putaran yang digunakan. AES-256 memiliki putaran yang lebih banyak dibandingkan AES-128 yaitu 14 putaran sedangkan AES-128 menggunakan 12 putaran. Putaran ini menghasilkan seberapa

kompleksnya enkripsi yang digunakan, semakin banyak putaran maka semakin kompleks dalam memecahkan enkripsinya.
Pada pemilihan SHA-512 juga mengacu pada alasan permasalahan yang sama, dimana semakin panjang nilai hash yang dihasilkan maka tingkat keamanan yang digunakan lebih tinggi.

A. Rumusan Masalah

Berdasarkan dari latar belakang yang sudah dijelaskan sebelumnya, terdapat beberapa masalah yang dapat dirumuskan. Beberapa rumusan masalah tersebut ialah :

1. Bagaimana penerapan algoritma AES-256 (Advanced Encryption Standard) untuk melakukan pengamanan data tagihan siswa dan SHA-512 untuk mengamankan kunci AES ?
2. Seberapa efektif penggunaan AES-256 untuk mengamankan data berdasarkan perhitungan Avalanche Effect ?

B. Batasan Masalah

Batasan masalah yang ada hanya dibatasi pada :

1. Program yang digunakan adalah berbasis web dengan bahasa pemrograman PHP native.
2. Algoritma enkripsi dan dekripsi data yang digunakan adalah AES-256 dan untuk penyamaran kunci menggunakan SHA-512.
3. Studi kasus dan objek penelitian ini adalah implementasi keamanan pada data tagihan yang dimiliki oleh siswa di SMK PUSDIKHUBAD.
4. Untuk pengujian seberapa efektif penggunaan algoritma AES-256 menggunakan metode perhitungan Avalanche Effect.

C. Tujuan Penelitian

Adapun Tujuan pada penelitian ini yang ingin dicapai adalah :

1. Untuk menyelesaikan permasalahan keamanan data pada aplikasi Sistem Pencatatan Biaya Pendidikan di SMK PUSDIKHUBAD dengan mengimplementasikan metode kriptografi algoritma AES-256 dan SHA-512 untuk menyamarkan data dan sebuah QR Code yang berfungsi untuk melakukan pembayaran tagihan siswa.
2. Menguji seberapa efektif algoritma AES-256 menggunakan perhitungan Avalanche Effect.

D. Keluaran Dan Manfaat

Luaran dan manfaat dari penelitian ini adalah sebagai berikut :
Luaran yang didapatkan dari penelitian ini adalah :

1. Terimplementasinya keamanan data pada aplikasi Pencatatan Biaya Pendidikan di SMK PUSDIKHUBAD pada bagian pembayaran tagihan siswa.
2. Persentase hasil perhitungan dari pengujian AES-256 menggunakan metode Avalanche Effect untuk menguji keamanan data pada aplikasi Pencatatan Biaya Pendidikan di SMK PUSDIKHUBAD.

Manfaat dari penelitian ini yaitu :

1. Membantu menjaga keamanan data pembayaran tagihan siswa pada aplikasi Pencatatan Biaya Pendidikan di SMK PUSDIKHUBAD.
2. Dapat mengetahui seberapa efektifnya algoritma AES-256.

(2024), 2 (3): 205–217 Scientica 3021-8209
Jurnal Ilmiah Sain dan Teknologi

METODOLOGI PENELITIAN

Gambar 1 Metodologi Penelitian

2.1 Metodologi Penelitian

Metode Pada penelitian ini dilakukan 6 tahapan untuk mencapai tujuan pembuatan sistem Pencatatan Biaya Pendidikan di SMK PUSDIKHUBAD. Tahapan - tahapan ini ditunjukkan pada Gambar 1.

2.1.1 Studi Pustaka

Tahap awal dalam proses penelitian ini ialah menjalankan analisis literatur atau studi pustaka. Tindakan analisis literatur dilaksanakan sebagai fondasi rujukan bagi kerangka teori yang akan diterapkan dalam penelitian ini. Beberapa sumber analisis literatur mencakup artikel jurnal, studi sebelumnya, serta beragam sumber lainnya.

2.1.2 Analisa Kebutuhan

Analisa kebutuhan dilaksanakan sebagai bagian dari proses awal dalam mengidentifikasi segala kebutuhan yang diperlukan untuk menjalankan sistem dengan efisien. Data yang menjadi kebutuhan meliputi rincian siswa, informasi perwalian, dan rekam jejak transaksi pembayaran.

2.1.3 Pengumpulan Data

Dalam rangka mencapai tujuan penelitian, dilakukan pengumpulan data guna memperoleh informasi yang dibutuhkan. Teknik pengumpulan data yang akan digunakan meliputi studi pustaka yang telah ada dan wawancara dengan tenaga administrasi SMK PUSDIKHUBAD sebagai sumber data yang relevan.

2.1.4 Pengembangan Sistem

Dalam pengembangan sistem, data yang diperoleh dari narasumber akan diimplementasikan dan dianalisis untuk menciptakan sistem yang sesuai dengan kebutuhan dan kondisi di lapangan. Dalam hal ini, sistem yang akan dikembangkan akan menggunakan php native.

2.1.5 Pengujian Keamanan Data

Pengujian keamanan sistem yang telah dibuat dilakukan dengan menerapkan perhitungan Avalanche Effect. Pengujian menggunakan perhitungan Avalanche Effect dilakukan dengan cara merubah 1 karakter pada plainteks yang akan diuji. Hasil ciphertext dari plainteks asli dan plainteks yang sudah diubah 1 karakter akan dibandingkan dengan perhitungan Avalanche effect. Hasil yang didapatkan pada pengujian ini adalah persentase hasil perhitungan dimana hasil tersebut akan menentukan seberapa bagus tidaknya penggunaan kombinasi kriptografi yang digunakan.

2.1.6 Laporan Dan Publikasi

Dokumentasi merupakan tahap terakhir dari penelitian ini, pada tahap ini melakukan penulisan hasil penelitian yang telah dilakukan dengan membuat laporan penelitian. Hasil dari tahapan ini berupa Laporan Tugas Akhir.

2.2 Kriptografi

Kriptografi merupakan ilmu yang mempelajari teknik penyandian dengan mengubah dan mengacak plaintext atau teks asli menggunakan kunci dan algoritma khusus. Tujuannya adalah menghasilkan ciphertext atau teks acak yang sulit dikenali dan tidak dapat dibaca oleh pihak yang tidak memiliki kunci untuk mengembalikan informasi ke bentuk aslinya.[3]

Gambar 2 Alur Kriptografi

2.3 Secure Hash Algorithm

SHA atau Secure Hashing Algorithm merupakan fungsi kriptografi yang dirancang khusus oleh penyedia otoritas kemanan internet untuk menjaga keamanan data. SHA ini bekerja dengan cara melakukan transformasi data menggunakan fungsi HASH. Secure Hash Algorithm dikembangkan pada tahun 1993 dan diterbitkan oleh NIST dengan nama Federal Information Processing Standard (FIPS PUB 180). Awalnya, SHA disebut sebagai SHA-0 kemudian versi SHA yang direvisi muncul pada tahun 1995 dan dinamai sebagai SHA-1 yang desainnya sangat mirip dengan keluarga fungsi hash MD-4.[5]

2.4 AES (Advanced Encryption Standar)

Algoritma Advanced Encryption Standard atau disingkat AES adalah salah satu algoritma enkripsi cipher blok yang diterbitkan oleh National Institute Of Standards and Technology (NIST) pada tahun 2000.[6] Algoritma AES merupakan algoritma kriptografi dengan kunci simetris di mana kunci yang digunakan untuk enkripsi sama dengan kunci yang digunakan untuk dekripsi. Algoritma AES memiliki tiga kategori kunci, yaitu AES 128 bit, 192 bit, dan 256 bit. Pada algoritma AES 128 bit, setiap blok data asli dengan ukuran 128 bit diubah menjadi bentuk state yang merupakan matriks heksadesimal berukuran 4x4. Putaran enkripsi dan dekripsi dalam algoritma AES dipengaruhi oleh panjang kunci yang digunakan. Oleh karena itu, ketika menggunakan kunci 128 bit, proses enkripsi atau dekripsi menjadi lebih cepat karena jumlah putaran yang lebih sedikit.[7]

Algorithm	Key length (bits)	Block size (bits)	No of round
AES- 128	128	128	10
AES- 192	192	128	12
AES- 256	256	128	14

Gambar 3 AES

2.5 QR Code

QR Code adalah sebuah gambar matriks dua dimensi yang memiliki fungsi untuk menyimpan data di dalamnya. QR Code merupakan pengembangan dari kode batang (barcode)[8]. Karena QR Code merupakan matriks dua dimensi, maka penyimpanan data dilakukan secara vertikal dan horizontal.

QR Code bekerja menggunakan cara yang sama seperti barcode yang cara kerjanya berupa bentuk pola yang bisa diterjemahkan[9]. Data ini dapat berisi apa saja, mirip sebuah

URL pada situs Web, data geolokasi yang digunakan pada peta. Data tersebut dapat berupa apa saja selama dapat ditulis di bawah 4.000 karakter atau lebih (tergantung pada jenis data) [10].

2.6 Avalanche Effect

Pengujian Avalanche Effect menurut A.F. Webster dan Stafford E. Tavares pada tahun 1985 dianggap baik apabila terjadi perubahan bit yang menunjukkan persentase minimal di angkat 50% [12], Perubahaan persentase sebesar itu akan mengakibatkan masalah yang cukup sulit untuk para pembobol melakukan serangan. Rumus perhitungan Avalanche effect sesuai pada persamaan (1).

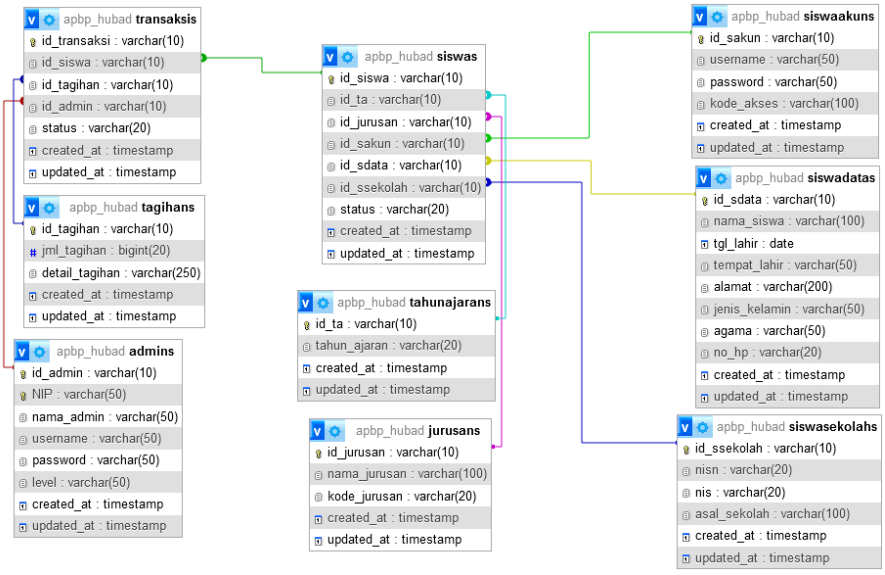
$$Avalanche\ Effect = \frac{jumlah\ bit\ berbeda}{total\ panjang\ bit}\ x\ 100\% \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$

HASIL DAN PEMBAHASAN

Implementasi dilakukan menggunakan komputer pribadi guna mempermudah dalam proses pengujian. Perangkat lunak yang dibangun yaitu berbasis web dengan menggunakan bahasa pemrograman PHP dengan Tools Visual Studio Code, menggunakan Google Chrome sebagai media web browser, serta menggunakan basis data MySQL dan Web Server Apache yang terdapat dalam aplikasi XAMPP..

3.1 Implementasi Basis Data

Implementasi basis data dibangun berdasarkan perancangan database yang telah dirancang. Analisis dan Perancangan. Database dibuat dengan menggunakan MySQL. Implementasi dari masing-masing tabel yang terdapat pada sistem yang dibangun.



Gambar 4 Database

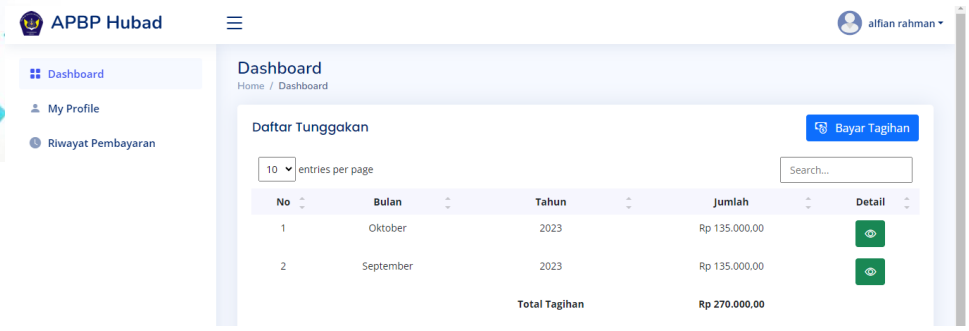
3.2 Implementasi Antarmuka

Implementasi antarmuka adalah representasi dari perancangan antarmuka yang sudah dibuat sebelumnya.

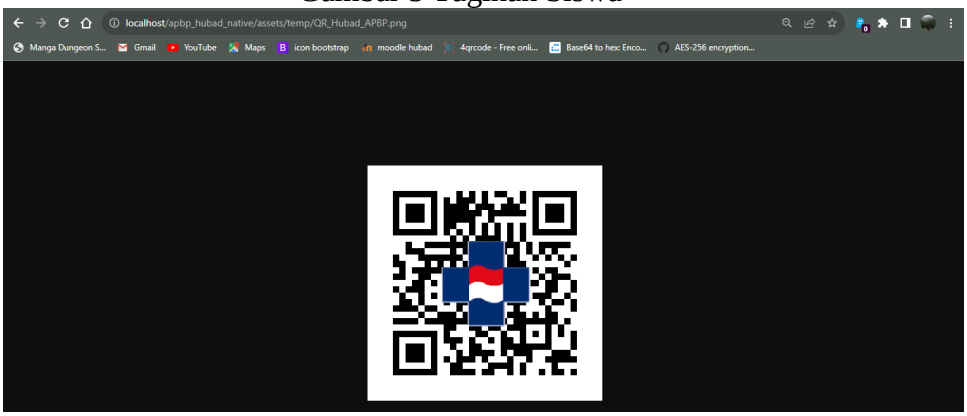
A. Siswa

Pada halaman user akses siswa, terdapat menu daftar tunggakan yang berisikan daftar tunggakan siswa tersebut. Terdapat tombol “Bayar Tagihan” dimana jika ditekan maka akan memunculkan QR Code berisikan kode tagihan yang harus siswa tunjukkan kepada staff tu/bendahara sekolah.

(2024), 2 (3): 205–217 Scientica 3021-8209
Jurnal Ilmiah Sain dan Teknologi



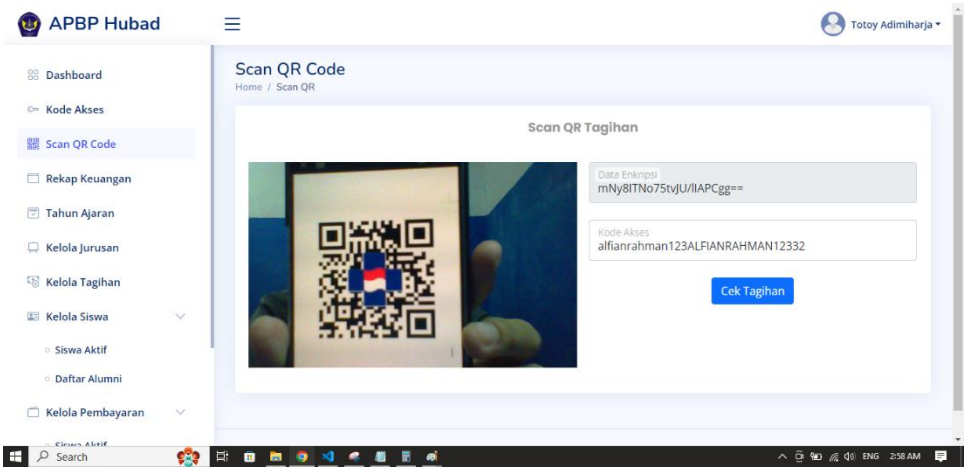
Gambar 5 Tagihan Siswa



Gambar 6 QR Code

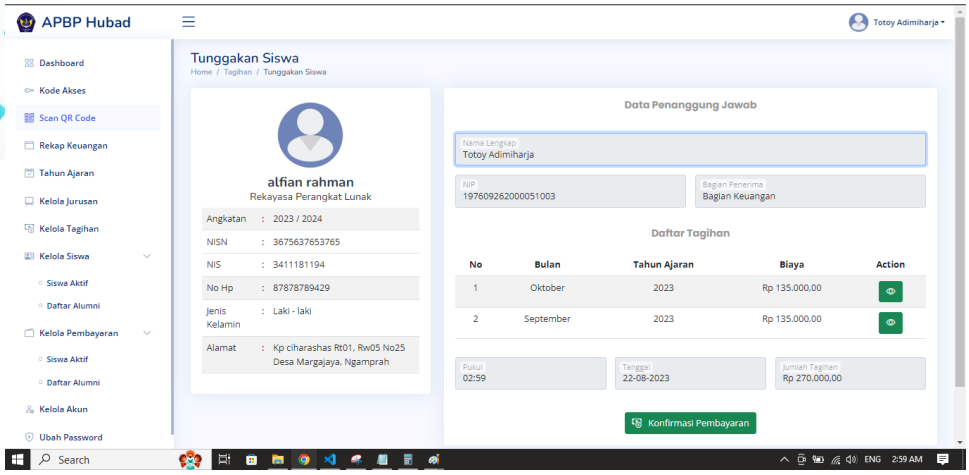
B. Staff TU

Pada halaman akun admin/staff tu, terdapat menu Scan QR, dimana proses pengecekan data tagihan siswa akan dilaksanakan. Staff TU diminta untuk memasukkan kode akses dan menscan QR Code yang diberikan siswa.



Gambar 7 Scan QR

Setelah proses berjalan dengan lancar maka akan muncul data siswa beserta tagihan yang dimiliki siswa. Pada bagian ini, staff tu dapat menekan tombol konfirmasi yang menandakan bahwa siswa telah melakukan pembayaran dan tagihan akan dinyatakan "Lunas".



Gambar 8 Detail Tagihan Siswa

3.3 Implementasi AES-256 dan SHA-512

A. AES-256

AES-256 digunakan untuk menyamarkan data NIS. Dimulai pada halaman "Kode Akses" pada level akses Staff TU. Staff TU diminta untuk memasukkan kode akses dengan panjang 32 digit karakter yang merepresentasikan bahwa key yang digunakan yaitu 32 karakter (256 Bit).

Selanjutnya kode akses yang dimasukkan akan dikombinasikan dengan plainteks yaitu NIS dan hasil dari enkripsi akan disimpan pada tabel QR yang mengacu kepada setiap siswanya.

Tabel 1 Source Code AES-256 (Enkripsi)

Source Code AES-256 (enkripsi)
$key = $_POST['key']; //query untuk get NIS siswa … $NIS = $data[‘NIS’]; … $method = 'aes-256-cbc'; $iv = chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0); $encrypted = base64_encode(openssl_encrypt($NIS, $method, $key, OPENSSL_RAW_DATA, $iv));

$key merupakan variabel dari kode akses yang dimasukkan staff TU, $NIS merupakan data nomor induk siswa yang sebelumnya sudah terdaftar didalam database (didapatkan dengan cara menggunakan query perulangan) yang akan disamarkan. $method merupakan variabel yang mendefinisikan method aes yang akan digunakan, yaitu aes 256 cbc. CBC menunjukkan bahwa tiap blok dari plainteks dilakukan XOR dengan hasil cipherteks dari blok sebelumnya yang kemudian dilakukan enkripsi. $iv merupakan blok – blok yang akan digunakan dalam pengenkripsian aes, terdapat 16 blok atau 128 bit. $encrypted merupakan variabel yang berisikan pengolahan atau proses enkripsi akan dijalankan, hasil enkripsi akan diubah menjadi base64. Hasil dari enkripsi tersebut nantinya akan dimasukkan kedalam basis data pada tabel qr.

(2024), 2 (3): 205–217 Scientica 3021-8209
Jurnal Ilmiah Sain dan Teknologi

	id_qr	enkripsi
Edit Copy Delete	1	pltmx6b63r+sOd/47Rgemw==
Edit Copy Delete	2	1PFWtVzdYej0jcVdJGAa5w==
Edit Copy Delete	3	CnNMUnDaeExqtlvpeeUQcw==
Edit Copy Delete	4	EhkPGiZb59n+ud4zJriTQA==

Gambar 9 Tabel Enkripsi

Selanjutnya data hasil enkripsi tersebut akan diakses oleh siswa pada halaman "Dashboard (lihat tagihan)" pada level akses Siswa (Gambar 5). Siswa dapat menekan tombol "Bayar Tagihan". Sistem akan otomatis memasukkan data hasil enkripsi sebelumnya sesuai dengan user siswa yang menekan tombol "Bayar Tagihan" (Gambar 5). Data enkripsi tersebut akan dimasukkan kedalam QR Code yang nantinya siswa tersebut harus menunjukkannya kepada staff TU untuk melakukan pembayaran

Gambar 10 Isi QR Code

Untuk dekripsi data, saat siswa berhasil mengunduh QR Code dan menunjukkannya kepada Staff TU. Staf TU akan memindai QR Code tersebut pada halaman "Scan QR" pada level akses Staff TU (Gambar 4.18). sistem akan membaca isi didalam QR, setelah isi dalalam QR muncul, staff TU diminta untuk memasukkan kode akses yang sebelumnya dimasukkan oleh staff TU. Proses dekripsi akan dimulai ketika staff TU menekan tombol "Cek Tagihan".

Tabel 2 Source Code AES-256 (Dekripsi)

Source Code AES-256 (dekripsi)
$qr = $_POST['enkripsi']; $ka = $_POST['kode_akses']; $method = 'aes-256-cbc'; $iv = chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0); $decrypted = openssl_decrypt(base64_decode($qr), $method, $ka, OPENSSL_RAW_DATA, $iv);

$qr merupakan data yang sudah di enkripsi sebelumnya, sedangkan $ka merupakan kode akses yang diinputkan setelah melakukan scan. Terdapat $method dan $iv yang memiliki fungsi yang sama seperti enkripsi, sedangkan proses dekripsi terjadi pada $decrypted, dimana proses ini akan menyandingkan data yang telah dienkripsi dengan kunci yang dimasukkan setelah melakukan scan qr.

B. SHA-512

SHA-512 digunakan untuk menyamarkan kode akses sebelum dimasukkan kedalam database. Proses ini dilakukan pada saat staff TU memasukkan kode akses (Gambar 4.17).

Tabel 3 Source Code SHA-512

Source Code SHA-512
$key = $_POST['key']; $hashing = hash('sha512', $key); $kunci = password_hash($hashing, PASSWORD_DEFAULT);

$key merupakan kode akses yang diinputkan pada Gambar 4.17. $hashing merupakan proses hash menggunakan SHA-512 terhadap data didalam variabel $key. $kunci merupakan pendeskripsian hasil hash yang nantinya digunakan untuk verifikasi pencocokan data pada proses dekripsi AES-256.

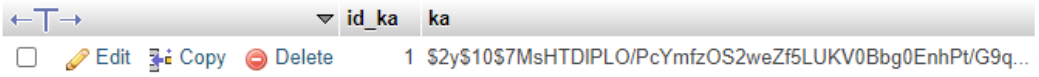
Selanjutnya pada proses dekripsi AES-256, kunci yang diinputkan akan dilakukan pencocokan data dengan kunci yang sudah didaftarkan sebelumnya yang tersimpan didalam database

Tabel 4 Source Code Verifikasi

Source Code Verifikasi

$ka = $_POST['kode_akses'];
//query get kode akses
….
$kode_akses = $data['kode_akses'];
$verify = hash('sha512', $ka);
$verify1 = password_verify($verify, $kode_akses);
if($verify1==TRUE){
  …..
}

$ka merupakan kode akses yang diinputkan sebelumnya, sedangkan $kode_akses merupakan kode akses yang sudah dihash dan dimasukkan kedalam database. $verify merupakan proses hash dari $ka, selanjutnya $verify1 merupakan proses pencocokan antara kode akses yang diinputkan dan dengan kode akses yang terdaftar pada basis data.



Gambar 11 Tabel Kode Akses

3.4 Pengujian Avalanche Effect

Pengujian Avalanche Effect (AE) dilakukan dengan menganalisis perubahan nilai bit dari hasil enkripsi pada sistem. Terdapat 3 percobaan yang dilakukan dengan menggunakan data dan ketentuan sebagai berikut :

Tabel 5 Avalanche Effect

Plainteks	:	3411181194
Key	:	alfianrahman123ALFIANRAHMAN12332
Kriptografi	:	AES 256-bit-cbc

1. Percobaan ke-1
   a. Plainteks

Tabel 6 Plainteks Percobaan ke-1

Sebelum	3411181194
Sesudah	341118119a

b. Chiperteks

Tabel 7 Chiperteks Percobaan ke-1

Sebelum	mNy8ITNo75tvJU/lIAPCgg==
Sesudah	UHW1kxiSbWt96e4M2/Kqhg==

b. Konversi Base64 dalam Bit

Tabel 8 Konversi Percobaan ke-1

Sebelum	10011000 11011100 10111100 00100001 00110011 01101000 11101111 10011011 01101111 00100101 01001111 11100101 00100000 00000011 11000010 10000010
Sesudah	01010000 01110101 10110101 10010011 00011000 10010010 01101101 01101011 01111101 11101001 11101110 00001100 11011011 11110010 10101010 10000110

c. Perhitungan Avalanche Effect

$$Avalanche\ Effect = \frac{59}{128}\ x\ 100\%$$

= 46,09%

1. Percobaan ke-2

a. Plainteks

Tabel 9 Plainteks Percobaan ke-2

Sebelum	3411181194
Sesudah	3411a81194

b. Chiperteks

Tabel 10 Chiperteks Percobaan ke-2

Sebelum	mNy8ITNo75tvJU/lIAPCgg==
Sesudah	NHD+1MBMMtAZuo9MoC0p5A==

c. Konversi Base64 dalam Bit

Tabel 11 Konversi Percobaan ke-2

Sebelum	10011000 11011100 10111100 00100001 00110011 01101000 11101111 10011011 01101111 00100101 01001111 11100101 00100000 00000011 11000010 10000010
Sesudah	00110100 01110000 11111110 11010100 11000000 01001100 00110010 11010000 00011001 10111010 10001111 01001100 10100000 00101101 00101001 11100100

d. Perhitungan Avalanche Effect

$$Avalanche\ Effect = \frac{66}{128}\ x\ 100\%$$

= 51,56%

2. Percobaan ke-3

a. Plainteks

Tabel 12 Plainteks Percobaan ke-3

Sebelum	3411181194
Sesudah	a411181194

b. Chiperteks

Tabel 13 Chiperteks Percobaan ke-3

Sebelum	mNy8ITNo75tvJU/lIAPCgg==
Sesudah	ptq6DrO65cwLuKoo5ujrZA==

c. Konversi Base64 dalam Bit

Tabel 14 Konversi Percobaan ke-3

Sebelum	10011000 11011100 10111100 00100001 00110011 01101000 11101111 10011011 01101111 00100101 01001111 11100101 00100000 00000011 11000010 10000010
Sesudah	10100110 11011010 10111010 00001110 10110011 10111010 11100101 11001100 00001011 10111000 10101010 00101000 11100110 11101000 11101011 01100100

d. Perhitungan Avalanche Effect

$$Avalanche\ Effect = \frac{62}{128}\ x\ 100\%$$

= 48,43%

Berdasarkan 3 percobaan diatas didapatkan nilai AE pada percobaan ke 1 sebesar 46.09%, percobaan ke-2 sebesar 51.56% dan pada percobaan ke-3 sebesar 48.43 %. Jika dihitung nilai rata – rata yang didapat sebesar 48.69%. Berdasarkan perhitungan rata – rata dapat disimpulkan bahwa nilai pengujian AE cukup memadai karena berada dalam rentang 45% - 60% (Sutanto et al., 2015).

KESIMPULAN

Berdasarkan hasil implementasi pada sistem APBP Hubad dan analisis algoritma AES menggunakan Avalanche effect, dapat ditarik beberapa kesimpulan penting :

1. Penerapan algoritma AES pada sistem APBP Hubad dapat memberikan tingkat keamanan yang memadai terhadap proses pembayaran siswa di SMK Pusdikhubad.
2. Hasil pengujian menunjukkan bahwa chiper text yang dihasilkan setelah proses enkripsi menggunakan algoritma AES memiliki tingkat keamanan yang memadai. Pengujian avalanche effect menunjukkan bahwa enkripsi AES 256-bit memiliki tingkat avalanche effect sebesar 48,69%. Selain itu, hasil uji kelayakan sistem menggunakan blackbox menunjukkan bahwa sistem APBP Hubad memiliki tingkat persentase 100% dan layak digunakan.

Perlu diperhatikan bahwa kesimpulan di atas didasarkan pada hasil implementasi dan analisis khusus pada sistem APBP Hubad dan mungkin tidak dapat diterapkan secara umum untuk setiap implementasi algoritma AES. Penting untuk melakukan evaluasi dan analisis yang cermat terhadap implementasi spesifik dalam konteks yang relevan.

REFERENCES

[1] A. Ajmera, S. S. Ghosh, and T. Vijayetha, “Secure LSB Steganography over Modified Vigenère-AES Cipher and Modified Interrupt Key-AES Cipher,” in *2018 IEEE Punecon*, 2018, pp. 1–7, doi: 10.1109/PUNECON.2018.8745393.

[2] A. Karima and M. N. Diyatan, “Algoritma Kriptografi Gost Dengan Implementasi MD5 Untuk Meningkatkan Nilai Avalanche Effect,” *J. Techno.COM*, vol. 15, no. 4, pp. 292–302, 2016.

[3] W. S. Sari, E. H. Rachmawanto, D. R. I. M. Setiadi, and C. A. Sari, “A Good Performance OTP encryption image based on DCT-DWT steganography,” *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 15, no. 4, pp. 1987–1995, 2017, doi: 10.12928/TELKOMNIKA.v15i4.5883.

[4] F. Ferdiansyah, A. Id Hadiana, and F. Rakhmat Umbara, “Penggunaan QR Code Berbasis Kriptografi Algoritma AES (Advanced Encryption Standard) Untuk Administrasi Rekam Medis,” *J. Inf. Technol.*, vol. 3, no. 2, pp. 20–27, 2021, doi:

10.47292/joint.v3i2.64.
[5] V. Kaur and A. Singh, “An Encryption Scheme Based on AES and SHA-512,” 2015. [Online]. Available: http://www.ripublication.com.
[6] M. R. Hidayatsyah, “Penerapan Metode Decision Tree Dalam Pemberian Pinjaman Kepada Debitur Dengan Mhd . Rido Hidayatsyah,” vol. 5, p. 22, 2013.
[7] A. T. Utomo and R. Pradana, “IMPLEMENTASI ALGORITMA ADVANCED ENCRYPTION STANDARD (AES-128) UNTUK ENKRIPSI DAN DEKRIPSI FILE (AES-128) ALGORITHM FOR FILE ENCRYPTION AND DECRIPTION,” no. September, pp. 268–276, 2022.
[8] H. A. Alfatihah, I. Fitri, and A. Andrianingsih, “Sistem Presensi dan Sertifikasi Elektronik Memanfaatkan QR Code Menggunakan Algoritma AES,” *Smatika J.*, vol. 11, no. 02, pp. 70–80, 2021, doi: 10.32664/smatika.v11i02.580.
[9] I. Qr, C. Dan, A. Vigenere, C. Pada, and S. Manajemen, “Nanda Dwi Wicaksono-142410101072,” 2019.
[10] S. Saghranie and Widyaiswara, “Hubungan antara QR Code dan Dunia Industri dan Perdagangan,” *Pusdiklat Ind.*, vol. 1, no. 1, pp. 1–11, 2020.
[11] A. Z. Hasibuan, M. S. Asih, and H. Harahap, “Penerapan QR Code dan Vigenere Cipher Dalam Sistem Pelaporan Juru Parkir Ilegal,” *Query J. Sist. Inf.*, vol. 3, no. 1, pp. 2579–5341, 2019.
[12] A. R. Tulloh, Y. Permanasari, and E. Harahap, “Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen,” *J. Mat. UNISBA*, vol. 2, no. 1, pp. 118–125, 2016, [Online]. Available: https://ejournal.unisba.ac.id/index.php/matematika/article/view/4067.
[13] A. Rahardiansyah, A. Rusman, A. H. Kahfi, and U. N. Mandiri, “Sistem Penunjang Keputusan Siswa Berprestasi Metode AHP di SMP Era Informatika,” vol. 10, no. 1, p. 2022, 2022.
[14] Haviluddin, “Memahami Penggunaan UML (Unified Modelling Language),” *Memahami Pengguna. UML (Unified Model. Lang.*, vol. 6, no. 1, pp. 1–15, 2018.
[15] A. H. Khan and I. Porres, “Consistency of UML class, object and statechart diagrams using ontology reasoners,” *J. Vis. Lang. Comput.*, vol. 26, pp. 42–65, 2015, doi: 10.1016/j.jvlc.2014.11.006.
[16] L. Febriani, “Sistem Perhitungan Premi Asuransi Mitra Beasiswa Berencana pada AJB Bumiputera 1912 Kantor Cabang Tanjung Karang,” *J. Ilmu Data*, vol. 2, no. 2, pp. 1–10, 2022.
[17] S. P. Sangian, H. Toba, F. T. Informasi, and U. K. Maranatha, “Integrasi Proses Akademik dan Keuangan Dalam Pengajuan Beasiswa Universitas Kristen Maranatha,” vol. 4, 2022.
[18] Supriyono, “Software Testing with the approach of Blackbox Testing on the Academic Information System,” *Int. J. Inf. Syst. Technol.*, vol. 3, no. 36, pp. 227–233, 2020.