

PENGUJIAN APLIKASI TABUNGAN SANTRI BERBASIS WEB DENGAN MENGUNAKAN ALGORITMA KRIPTOGRAFI ADVANCE ENCRYPTION STANDARD (AES) 256.

Muhamad Hasanudin ¹⁾, Lasimin ²⁾, M. Noviansyah Dasaprawira ³⁾

¹⁾ Universitas Nahdlatul Ulama AL ghazali cilacap

²⁾ Universitas Nahdlatul Ulama AL ghazali cilacap

³⁾ Universitas Nahdlatul Ulama AL ghazali cilacap

Email -¹⁾, lasimin@unugha.id ²⁾ viarprawira93@unugha.id ³⁾

ABSTRACT

This study aims to test the security of the web-based student savings application using an advanced encryption cryptographic algorithm using the PHP and MySQL programming languages. This research method uses SDLC (Software Development Life Cycle) software development using Agile Software Development. While the system security testing method uses the AES algorithm. Testing using AES with two events, namely testing the database server, and testing brute force.

Keywords: web, PHP, MySQL, Agile Software Development, AES

ABSTRAK

Penelitian bertujuan untuk menguji keamanan pada aplikasi tabungan santri berbasis web dengan menggunakan algoritma kriptografi advance encryption menggunakan Bahasa pemrograman PHP dan MySQL. Metode penelitian ini menggunakan pengembangan perangkat lunak SDLC (software Development Life Cycle) menggunakan Agile Software Development. Sedangkan metode pengujian keamanan system menggunakan Algoritma AES. Pengujian menggunakan AES dengan dua acara yaitu pengujian database server, dan pengujian brute force.

Kata Kunci : web, PHP, MySQL, Agile Software Development, AES

1. PENDAHULUAN

Dalam membangun aplikasi harus memperhatikan bagian keamanan data dan dokumen. Kerahasiaan dari data atau informasi merupakan suatu kelengkapan pelayanan yang dibuat untuk menjaga agar informasi yang tersimpan tidak dapat dibaca atau dibuka oleh pihak yang tidak berhak (Prameshwari, 2018).

Kerahasiaan dari data atau informasi merupakan suatu kelengkapan pelayanan yang dibuat untuk menjaga agar informasi yang tersimpan tidak dapat dibaca atau dibuka oleh pihak yang tidak berhak. Upaya dalam menjaga kerahasiaan dari data informasi tersebut sudah tercetus sejak jaman dahulu tepatnya pada jaman romawi dengan metode pergeseran huruf atau karakter dengan dasar nilai tertentu (Prameshwari, 2018).

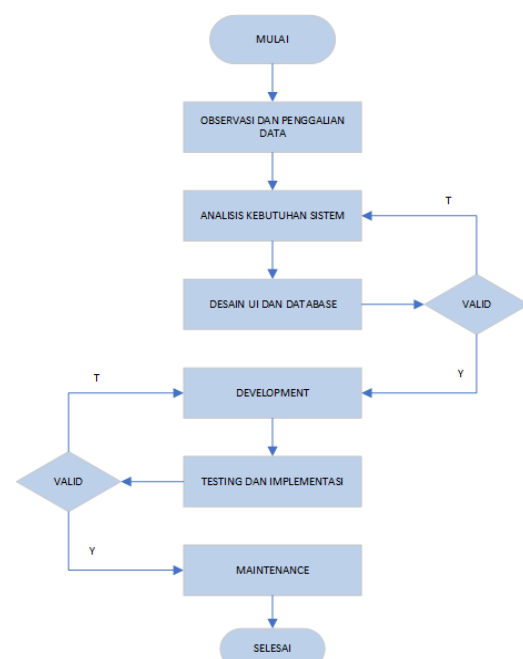
Advanced Encryption Standard (AES) merupakan algoritma *cryptographic* yang dapat digunakan untuk mengamankan data. Algoritma AES adalah blok ciphertext simetrik yang dapat mengenkripsi (encipher) dan dekripsi (decipher) informasi. Enkripsi merubah data yang tidak dapat lagi dibaca disebut ciphertext; sebaliknya dekripsi adalah merubah ciphertext data menjadi bentuk semula yang kita kenal sebagaipaintext. Algoritma AES is mengunkan kunci kriptografi 128, 192, dan 256 bits untuk mengenkrip dan dekrip data pada blok 128 bits (Zacky, 2016). Dilihat dari segi jenis kunci yang simetri maka

AES kecepatan operasi (komputasi) lebih tinggi bila dibandingkan dengan algoritma asimetrik sehingga dapat digunakan pada sistem realtime seperti GSM (Asriyani, 2017).

Berdasarkan permasalahan diatas untuk mempermudah proses pengelolaan data tabungan santri dengan mempertimbangkan aspek keamanan maka penulis berkeinginan membuat aplikasi tabungan santri dengan mengambil judul “**Algoritma Kriptografi *Advanced Encryption Standard* (AES) 256 Pada Aplikasi Tabungan Santri Berbasis Web**”

2. METODE

Penelitian Metodologi penelitian adalah serangkaian langkah-langkah yang sistematis/terstruktur yang dilakukan oleh peneliti untuk menemukan jawaban yang tepat atas pertanyaan pada objek penelitian (Prawiro, 2019). Dalam penelitian ini metodologi penelitian dijelaskan dalam bentuk diagram alir dibawah ini :



3. HASIL DAN PEMBAHASAN

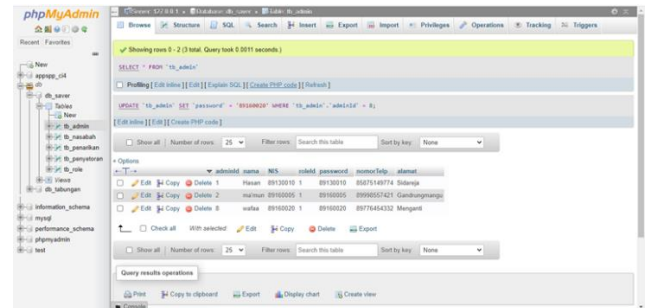
Pada tahap implementasi sistem menghasilkan aplikasi berbasis web untuk memproses enkripsi dan dekripsi menggunakan algoritma AES. Dalam proses pengerjaannya penelitian ini menggunakan metode CBC.

Mode *Cipher Block Chaining* (CBC) menerapkan mekanisme umpan-balik (*feedback*) pada sebuah blok, yang dimana hasil enkripsi blok sebelumnya diumpan-balikkan ke dalam enkripsi blok yang *current*. Caranya, blok plaintext yang *current* di-XOR-kan terlebih dahulu dengan blok *ciphertext* hasil enkripsi sebelumnya, selanjutnya hasil peng-XOR-an ini masuk ke dalam fungsi enkripsi. Pada mode *Cipher Block Chaining* (CBC), setiap blok *ciphertext* bergantung tidak hanya pada blok *plaintext* tetapi juga pada seluruh blok *plaintext* sebelumnya. Dekripsi dilakukan dengan memasukkan blok *ciphertext* yang *current* ke fungsi dekripsi, kemudian meng-XOR-kan hasilnya dengan blok *ciphertext* sebelumnya. Dalam hal ini, Blok *ciphertext* sebelumnya berfungsi sebagai umpan maju (*feed forward*) pada akhir proses dekripsi. dapat diketahui apa yang digunakan saat pengerjaan.

Dibawah ini merupakan *script* untuk menambah *user* tanpa menggunakan AES 256

```
Script Menambah User tanpa AES 256
public function simpan()
{
    $data = [
        'adminId' => $this->request->getVar('adminId'),
        'nama' => $this->request->getVar('nama'),
        'password' => $this->request->getVar('password'),
        'NIS' => $this->request->getVar('NIS'),
        'roleId' => $this->request->getVar('roleId'),
        'nomorTelp' => $this->request->getVar('nomorTelp'),
        'alamat' => $this->request->getVar('alamat'),
    ];
    $simpan = $this->model->simpan($data);
    if ($simpan) {
        return redirect()->to('/Admin');
    }
}
```

Hasil dari *password* yang belum terenkripsi yang tersimpan di *database*.



Berikut merupakan *script* yang digunakan untuk mengenkripsi yang tersimpan di *database*.

```
Script Algoritma AES Proses Enkripsi dan dekripsi

$password = $this->request->getVar("password");

$plaintext = $password;

$key = '1234567890';

$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);

$encrypted = base64_encode(openssl_encrypt($plaintext,
    $method, $key, OPENSSL_RAW_DATA, $iv));
```

Dibawah ini merupakan hasil dari enkripsi yang ada di beberapa tabel di database tabungan santri.

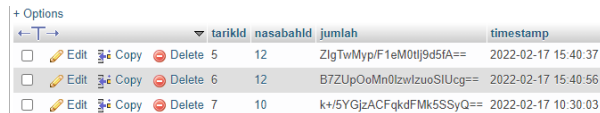
1. Database Tabel Admin



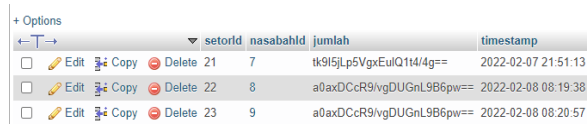
2. Database Tabel Nasabah



3. Database Tabel Penarikan



4. Database Tabel Penyetoran



A. Pengujian

Pengujian merupakan proses pengekskusi dari implementasi yang telah dilakukan untuk menilai dan menemukan kesalahan - kesalahan yang terdapat pada sistem. Dengan adanya pengujian diharapkan sistem memiliki kualitas yang baik dan dapat dijadikan bahan referensi dalam proses pengembangan sistem lebih lanjut. Pada pengujian ini akan dibagi menjadi dua, yaitu :

1. Pengujian Keamanan Database Server

Pada tahap ini dilakukan pengujian *database* dengan melakukan *sql injection* untuk mendapatkan isi dari *database* yang diinginkan dengan menggunakan tool *sqlmap* versi 1.5.12. Berikut merupakan proses *sql injection* dengan *sqlmap*, yaitu dengan mengetikkan perintah berikut *sqlmap -u https://tabungan.manuruliman*
clp.sch.id/index.php?id=1 --batch

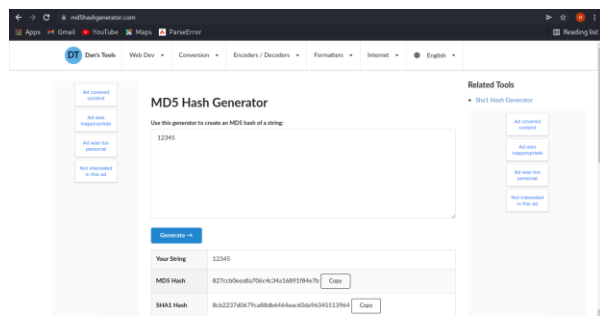


2. Pengujian Brute Force

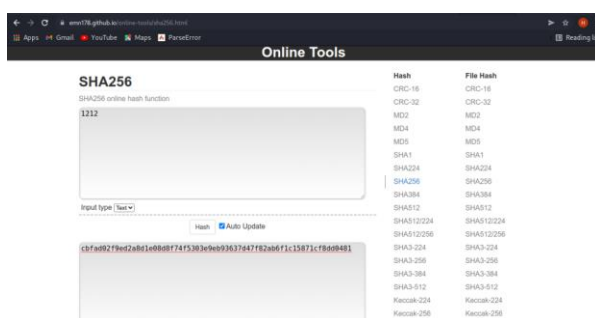
Serangan *brute force* adalah upaya mendapatkan akses sebuah akun dengan menebak username dan password yang digunakan. Salah satu metode yang digunakan adalah metode *rainbow table*. Metode ini merupakan metode *brute force* yang paling unik, yaitu dengan tidak menebak password tapi melakukan dekripsi proteksi hash hasil enkripsi dari sebuah password. Pada tahap pengujian ini menggunakan tool *Crack Station*.

Crack Station adalah proyek *security awareness* yang dimulai oleh *Defuse Security*. Tujuannya adalah untuk meningkatkan kesadaran tentang password yang aman di aplikasi web. Tahap pengujian ini yaitu dengan membandingkan hasil dari crack hash pada MD5, SHA256 dan AES-256.

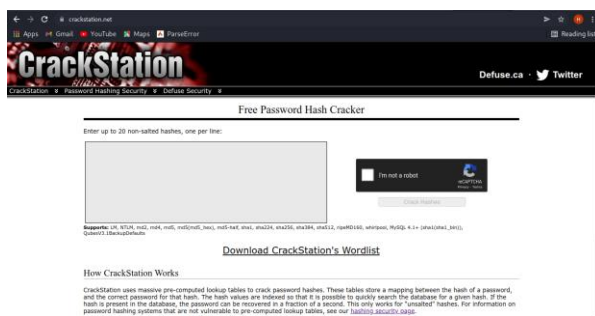
Langkah awal yaitu membuat enkripsi MD5 di web md5hashgenerator.com. Diketahui hasilnya pada gambar dibawah ini.



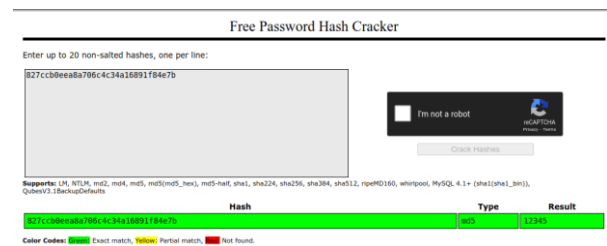
Selanjutnya yaitu membuat enkripsi menggunakan SHA256 melalui web emn178.github.io/online-tools/sha256.html. Diketahui hasilnya pada gambar dibawah ini.



Tahap berikutnya yaitu proses *hash code* menggunakan *crack station*, dengan mengunjungi web crackstation.net.



Kemudian *copy paste* hasil enkripsi pada web MD5 ke halaman *crack station*. maka hasil yang didapat yaitu enkripsi MD5 dapat dipecahkan, dapat dilihat dari warna kode berupa hijau dan menampilkan hasil serta tipenya



Langkah berikutnya *copy paste* hasil enkripsi pada web SHA256 ke halaman *crack station*. maka hasil yang didapat yaitu enkripsi SHA256 dapat dipecahkan, dapat dilihat dari warna kode berupa hijau dan menampilkan hasil serta tipenya.



Langkah terakhir yaitu *copy paste* hasil enkripsi pada enkripsi AES-256 yang berada di database ke halaman *crack station*. maka hasil yang didapat yaitu enkripsi AES-256 tidak dapat dipecahkan, dapat dilihat dari warna kode berupa merah dan tidak menampilkan hasil serta tipenya



Dapat disimpulkan bahwa dari hasil pengujian dengan crack station MD5 dan SHA256 dapat dipecahkan, sedangkan AES-256 tidak dapat dipecahkan.

B. Maintenance

Tahap pemeliharaan dilakukan setelah tahap implementasi dan pengujian. Pemeliharaan sistem informasi adalah suatu upaya untuk memperbaiki, menjaga, menanggulangi, mengembangkan sistem yang ada. Pemeliharaan ini di perlukan untuk meningkatkan efisiensi dan efektivitas kinerja sistem yang ada agar dalam penggunaannya dapat optimal (Idha, 2018). Pemeliharaan sistem meliputi :

1. System Back-Up

Membuat Salinan/*copy* untuk data-data penting yang ada pada komputer *user* maupun *server* ke dalam *backup storage (External Disk)*.

2. System Optimization

Melakukan Defragmentasi data dan membuang sampah-sampah yang ada pada komputer, serta memperbaiki kesalahan *setting* sehingga computer dapat berjalan normal.

3. System Rebuild

Membangun dan menata ulang kembali sistem yang rusak oleh faktor yang tidak disengaja, agar sistem dapat bekerja normal kembali.

4. System Upgrade

Menambah fungsi, memperbaharui sistem yang ada sesuai dengan kebutuhan, serta melakukan testing stabilitas untuk hardware dan software.

5. Training dan Pelatihan

Memberikan Pengarahan dan konsultasi kepada operator komputer, sehingga operator dapat mengoperasikan computer sesuai dengan prosedur pengoperasian komputer yang baik dan benar.

6. System Security

Pemasangan *Firewall* dan sistem autentifikasi untuk pengamanan sistem dan data penting dari orang luar yang tidak berkepentingan

4. PENUTUP

4.1. Kesimpulan

Dari Berdasarkan hasil dari penelitian yang telah dilakukan dapat disimpulkan bahwa:

1. Algoritma AES-256 merupakan menjadi salah satu alternatif untuk proses keamanan saat *login* dan keamanan data dalam hal ini enkripsi dan dekripsi data yang berada di *database*, hal ini berdasarkan hasil dari *chipper text* yang tidak dapat dipecahkan dengan menguji ketahanan terhadap serangan *brute force* menggunakan *software* penyerang *CrackStation*.
2. Keamanan dari hasil enkripsi dapat dijamin selama *symmetry key encryption* tidak bocor ke pihak yang tidak bertanggung jawab

4.2. Saran

Saran yang diberikan untuk pengembangan penelitian lebih lanjut adalah sebagai berikut:

1. Pada aplikasi tersebut belum diimplementasikan *login multi level*, sehingga hanya admin saja yang masih bisa mengakses. Untuk penelitian selanjutnya diharapkan *login* bisa dikembangkan supaya semua *user* baik admin maupun nasabah bisa mengakses.
2. Pada penelitian selanjutnya, harapkan sistem dapat dikembangkan dari berbasis web ke basis yang lain, seperti berbasis *mobile*.

5. DAFTAR PUSTAKA

- Adani, M. R. (2018, 10 24). *Aplikasi Berbasis Web*. From Sekamedia: <https://www.sekawanmedia.co.id/aplikasi-berbasis-web/>
- Adani, M. R. (2020, Agustus 8). *Metodologi Agile*. From Sekawan Media: <https://www.sekawanmedia.co.id/blog/metode-agile-development/>
- Adani, M. R. (2021, juni 21). *Mengenal Apa itu Use Case dan Teknik Pembuatannya*. From sekam media: [sekawanmedia.co.id/use-case-diagram/](https://www.sekawanmedia.co.id/use-case-diagram/)
- Agustina, E. (2011). *ANALISIS DAN PERANCANGAN SISTEM INFORMASI PENJUALAN BARANG PADA LEEKOFIBER*. Yogyakarta: Naskah Publikasi.
- Asriyani. (2017). STUDI TERHADAP ADVANCED ENCRYPTION STANDARD(AES) DAN ALGORITMA KNAPSACK DALAM PENGAMANAN DATA. *Jurnal SANTIKA : Jurnal Ilmiah Sains dan Teknologi-ISSN 2088-5407*, 556.
- Fitriani, I. (2020). *IMPLEMENTASI ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) PADA LAYANAN SMS DESA*.
- Hidayatulloh, H. (2017). *Implementasi Algoritma AES-128 dan QR Code untuk validasi tiket pada perusahaan travel PT. Bumindo Jaya Cemerlang*. Jember.
- Idha. (2018). *Makalah Pemeliharaan Sistem*. Lombok Timur: January.
- Kertahadi. (2007). *Manajemen, Sistem Informasi*. Jakarta: PT Pustaka Binaman Pressindo.
- Prameshwari, A. (2018). *Implementasi Algoritma Advanced Encryption*

- Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen . *JURNAL EKSPLORA INFORMATIKA*, 52-58.
- Prasetyo, M. s. (2016). *IMPLEMENTASI ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) RIJNDAEL UNTUK PROTEKSI FILE AUDIO*. Medan.
- Prawiro, M. (2019, Januari 30). *Metode Penelitian: Pengertian, Macam-Macam, dan Contoh Metode Penelitian*. From Maxmanroe: <https://www.maxmanroe.com/vid/umum/metode-penelitian.html>
- Rivian Nuari, N. P. (2020). Implementasi Algoritma Kriptografi AES (Advanced Encryption Standard) 128 Bit Untuk Pengamanan Dokumen Shipping. *Journal Of Artificial Intelligence And Innovative Application*, 1-5.
- Sadikin, R. (2012). *Kriptografi untuk Keamanan Jaringan*. Yogyakarta: Penerbit Andi.
- Setiawan, R. (2021, Agustus 21). *Apa Itu Sequence Diagram dan Contohnya* . From Dicoding: dicoding.com/blog/apa-itu-sequence-diagram/
- Sugiyono. (2012). *Metode Penelitian Kuantitatif Kualitatif dan R&B*. Bandung: Alfabeta.
- Widoyoko. (2014). *Teknik Penyusunan Instrumen Penelitian*. Yogyakarta: Pustaka Belajar.
- Wijaya, A. (2017). PERANCANGAN PROGRAM APLIKASI TABUNGAN MENGGUNAKAN SERVER NGINX (Studi Kasus Madrasah Ibtidayah Negeri 01 Kota Bengkulu). *Jurnal Pseudocode*, 29.
- Zacky. (2016, 3 23). *Kriptografi*. From KRIPTOGRAFI & JARINGAN KOMPUTER: <http://kriptografijaringan.blogspot.com/2016/03/enkripsi-algoritma-aes-advanced.html>