BAB I
PENDAHULUAN

A. LATAR BELAKANG

Program Tabungan santri merupakan salah satu sarana untuk membiasakan para santri dalam mengelola keuangannya guna memenuhi kebutuhannya di Pondok Pesantren. Hal ini merupakan salah satu aspek yang begitu penting karena akan memberikan manfaat dalam pembentukan karakter santri yang disiplin, hemat dan suka menabung.

Sistem tabungan santri dapat mempermudah santri, wali santri, maupun pengelola pondok presantren dalam kegiatan pengelolaan keuangan tabungan. Tujuannya adalah untuk memberikan informasi dalam perencanaan, memulai, pengorganisasian, operasional sebuah perusahaan yang melayani sinergi organisasi dalam proses mengendalikan pengambilan (Kertahadi, 2007) .

Pondok Pesantren Asaasunnajaah adalah salah satu lembaga pendidikan non formal berbasis keagamaan Islam yang berada di Kecamatan Kesugihan. Selain kegiatan belajar mengajar, juga mengadakan program – program lainya. Salah satunya adalah program tabungan santri.

Media penyimpanan data yang tidak terkomputerisasi dan masih berupa arsip, membuat petugas kesulitan dalam hal pencarian data santri yang menabung, penghapusan dan pengeditan data tabungan (Wijaya, 2017). Adapun dalam pencatatan tabungan sering mengalami kendala seperti dalam perhitungan yang sering mengalami kesalahan, sehingga perlu perhitungan ulang.

Dari permasalahan diatas, penulis mencoba mencarikan solusi dengan membangun aplikasi yang dapat membantu petugas dalam pengentrian data atau pencarian data. Sehingga petugas dapat dengan mudah dalam pengelolaan tabungan santri tersebut.

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 mengamakan data. Algoritma AES adalah blok chipertext 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 sebagaiplaintext. 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**"

B. RUMUSAN MASALAH

Berdasarkan latar belakang yang telah diuraikan diatas maka, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana cara menerapkan algoritma AES-256 pada aplikasi tabungan santri di Pondok Pesantren Asaasunnajaah ?
2. Bagaimana cara menguji fitur keamanan AES-256 yang diterapkan pada data tabungan santri dalam aplikasi tabungan santri ?

C. TUJUAN PENELITIAN

Berdasarkan rumusan masalah, maka tujuan yang ingin dicapai pada penelitian ini antara lain:

1. Menerapkan metode algoritma AES-256 pada aplikasi tabungan santri di Pondok Pesantren Asaasunnajaah Kesugihan.
2. Mengetahui hasil pengujian fitur keamanan algoritma AES-256 pada aplikasi tabungan santri.

D. BATASAN PENELITIAN

Berdasarkan rumusan masalah maka, pada penelitian ini diperlukan batasan masalah agar tujuan penelitian ini dapat tercapai. Adapun batasan masalah pada pembahasan ini adalah sebagai berikut:

1. Objek penelitian adalah *database* aplikasi tabungan santri Pondok Pesantren Asaasunnajaah berbasis web.
2. Fitur keamanan aplikasi tabungan santri menggunakan metode algoritma kriptografi AES-256.

b. Aplikasi dibuat dengan menggunakan pemrograman PHP/framework Codeigniter versi 4 dengan database server MySQL.

c. Model diagram menggunakan UML Visio 2016

E. MANFAAT PENELITIAN

Manfaat yang diharapkan dari penelitian ini antara lain:

1. Bagi penulis
    a. Menambah pemahaman mengenai ilmu yang dipelajari, khususnya dalam pengembangan sistem informasi dan algoritma kriptofrafi AES.
    b. Sebagai tolak ukur penerapan ilmu pengetahuan kriptografi AES kedalam permasalahan data tabungan.
    c. Menambah pengalaman dalam perancangan sistem menggunakan bahasa pemrograman PHP dan MySQL.
2. Bagi Pembaca
    a. Menambah referensi mengenai pembuatan sistem dengan menggunakan bahasa pemrograman PHP dan MySQL bagi mahasiswa yang akan melakukan penelitian di masa yang akan datang.
    b. Penerapan Algoritma kriptografi AES untuk enkripsi dan dekripsi dalam pengembangan sistem.
3. Bagi Pondok Pesantren
    a. Menghasilkan suatu sistem yang menambah tingkat keamanan data tabungan santri.
    b. Membuat fitur pencatatan transaksi tabungan santri dari sisi admin menjadi lebih mudah dan efisien.

F. SISTEMATIKA PENULISAN

Secara garis besar, sistematika penulisan skripsi terbagi menjadi beberapa bagian:

1. Bagian awal

Bagian awal berisi dari halaman judul, halaman pengesahan, motto, kata pengantar, daftar isi, daftar gambar. daftar tabel dan abstrak

2. Bagian kedua

Bagian kedua yaitu bagian tengah yang terdiri dari bab I sampai bab dengan V, yaitu:

Bab I : Pendahuluan

Pada bab ini, terdapat latar belakang, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

Bab II : Landasan Teori

Pada bab ini berisi tentang pendeskripsian dari teori-teori yang berhubungan dengan pokok permasalahan diatas, mulai dari Telaah Pustaka, landasan Teori yang berisikan, pengertian kriptografi, algoritme *advance encryption standard,* dan aplikasi berbasis web.

Bab III : Metode Penelitian

Pada bab ini terdiri dari tahapan penelitian yang didalamnya terdapat *flowchart* tahapan penelitian, analisis kebutuhan, desain sistem yang terdiri dari *use case diagram, sequence diagram.*

Bab IV : Hasil Penelitian Dan Pembahasan

Pada bab ini berisi tentang penyusunan implementasi sistem dan implementasi algoritme kriptografi *advance encryption standard* pada aplikasi tabungan santri dan pengujian sistem

Bab V : Penutup

Pada bab ini berisi kesimpulan laporan isi penelitian dan saran-saran untuk menambah kesempurnaan sistem serta kata penutup.

3. Bagian Akhir

Bagian dari skripsi ini adalah berupa daftar pustaka dan lampiran-lampiran.