BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi khususnya teknologi internet pada dasawarsa terakhir membuat orang dari dunia pendidikan mempunyai banyak pilihan dalam memanfaatkan teknologi tersebut. Sistem informasi akademik pada dunia pendidikan merupakan sesuatu yang sangat penting bagi para civitas akademik. Sistem informasi akademik dibangun untuk memberikan kemudahan kepada para pelajar dalam kegiatan administrasi pendidikannya secara *online*. Sistem informasi akademik sangat membantu dalam pengelolaan data nilai pelajar, mata pelajaran, data *staff* pengajar serta administrasi agar mampu mengefektifkan waktu dan menekan biaya operasional.

Setiap sistem informasi akademik pasti telah mempunyai sistem pengamanannya sendiri, namun dalam pengamanannya pasti mempunyai suatu kelemahan. Salah satunya adalah kelemahan keamanan pada saat *login*. Kelemahan sistem keamanan *login* sistem informasi akademik bisa di masuki oleh orang-orang yang tidak berkepentingan.

Proses *login* tersebut bisa dimanfaatkan oleh orang-orang yang tidak memiliki wewenang untuk masuk dan melakukan pencurian data maupun perubahan data-data dalam sistem informasi akademik. Untuk *login* dalam sistem informasi akademik hanya perlu mengetahui nomor induk pelajar dan *password* saja, sistem tidak akan mengetahui apakah benar si pemilik yang *login* ke dalam sistem atau bukan. Dengan begitu, proses *login* pada sistem informasi akademik masih memiliki kekurangan dalam hal keamanan sistem.

Ada beberapa metode untuk melakukan autentikasi, salah satunya adalah menggunakan *password*, namun penggunaan *password* belum menjamin keamanan dan kerahasiaan sebuah data maupun informasi. Sistem *login* yang menggunakan *database* sebagai autentikasi *user* dan *password* sangat rentan untuk diretas.

Kerahasiaan merupakan faktor penting untuk menjaga isi informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka

informasi. Salah satu cara untuk mengatasi hal ini adalah dengan teknik penyandian data atau yang lebih dikenal dengan kriptografi.

Disinilah kriptografi berperan menjaga informasi-informasi rahasia tersebut agar pengguna atau pihak yang berhak saja yang dapat mengetahui informasi tersebut. Salah satu dari kriptografi yang dapat digunakan adalah *One Time Pad* (OTP). Metode penyandian *One Time Pad* (OTP) dikenal sebagai sebuah metode penyandian yang sangat kuat sehingga tidak mudah dipecahkan. Metode penyandian *One Time Pad* (OTP) merupakan salah satu variasi dari metode penyandian substitusi dengan cara memberikan syarat-syarat khusus terhadap kunci yang digunakan yaitu terbuat dari karakter / huruf yang acak dan algoritma ini menggunakan kunci yang sama dalam proses enkripsi maupun dekripsi. Algoritma ini akan mengharuskan pengirim dan penerima menyetujui suatu *key* tertentu sebelum terjadi komunikasi diantara kedua belah pihak. Oleh karena itu, untuk lebih mengamankan pada proses *login* di sistem informasi akademik bisa dengan menggunakan kriptogafi *One Time Pad* ini

Berdasarkan latar belakang permasalahan tersebut, penelitian ini mengusulkan untuk menggunakan kriptografi *One Time Pad* sebagai solusi dalam penambahan pengamanan *login* di sistem informasi akademik. Sehingga penelitian ini mengambil judul **"PENGAMANAN AUTENTIKASI SISTEM INFORMASI AKADEMIK MENGGUNAKAN KRIPTOGRAFI *ONE TIME PAD*".** Dalam penulisan ini akan menjelaskan tentang kriptografi *One Time Pad* dalam pengamanan autentikasi sistem informasi akademik.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas, terdapat rumusan masalah, yaitu :

a. Apakah implementasi kriptografi *one time pad* dalam pengamanan proses *login* pada sistem informasi akademik sudah sesuai ?
b. Apakah kriptografi *one time pad* dapat menambah pengamanan pada sistem *login* di sistem informasi akademik ?
c. Apakah *one time pad* dapat mencegah orang yang tidak berkepentingan untuk *login* ke sistem informasi akademik ?

1.3 Tujuan Penelitian

Berdasarkan latar belakang, rumusan masalah, dan ruang lingkup maka tujuan penelitian dalam menunjang penulisan skripsi ini adalah:

a. Mengimplementasikan kriptografi *one time pad* pada sistem informasi akademik dalam melakukan proses enkripsi pada halaman *login* sistem informasi akademik untuk menjaga kerahasiaan data maupun informasi dari serangan yang dilakukan oleh orang yang tidak berkepentingan.
b. Algoritma *one time pad* ini dapat menjadi suatu *alternative* sistem enkripsi dan dekripsi yang lebih baik.
c. Mengetahui sejauh mana proses *one time pad* dalam meningkatkan keamanan pada sistem informasi akademik.
d. Sistem ini dapat menjadi salah satu *alternative* untuk penyandian data pada *database* dengan kebutuhan proses dan waktu yang relatif singkat.

1.4 Manfaat Penelitian

Sesuai dengan permasalahan dan tujuan penelitian yang telah disebutkan diatas, maka penelitian dapat dirumuskan sebagi berikut :

a. Penelitian ini dapat dijadikan sebagai bahan pertimbangan atau dikembangkan lebih lanjut, serta sebagai bahan referensi terhadap penelitian tentang pengamanan autentikasi sistem informasi akademik menggunakan kriptografi *one time pad*.

b. Penelitian ini dapat meningkatkan sistem keamanan dan menjaga kerahasiaan tentang sistem informasi akademik agar data-data maupun informasi tentang pelajar aman dari orang-orang yang tidak memiliki wewenang untuk mengetahui data maupun informasi dari para pelajar.
c. Untuk mengukur sejauh mana kriptografi *one time pad* dalam mengamankan sistem informasi akademik

1.5 Ruang Lingkup

Agar pembahasan dalam skripsi ini dapat mencapai hasil yang optimal, maka penulis membatasi ruang lingkup pembahasan sebagai berikut :

a. Sistem yang digunakan berbasis *web*.
b. kriptografi yang digunakan untuk sistem informasi akademik ini menggunakan kriptografi *one time pad.*
c. Proses enkripsi data dilakukan di dalam *Form* Registrasi *one time pad*.
d. *One time pad* hanya digunakan untuk melakukan proses enkripsi pada saat pelajar melakukan registrasi pada form *registrasi one time pad*.
e. Bahasa pemrograman yang digunakan adalah PHP dengan menggunakan XAMPP dan *MySQL* sebagai *database*nya.

1.6 Luaran Yang Diharapkan

Luaran yang diharapkan dalam penelitian ini adalah menghasilkan sebuah aplikasi pengamanan autentikasi sistem informasi akademik menggunakan kriptografi *one time pad*.

1.7 Sistematika Penulisan

Untuk memberikan gambaran yang lebih jelas dan sistematis, Penulis akan memberikan gambaran mengenai isi dari penulisan tugas akhir ini, berikut ini adalah sistematika dari tugas akhir ini :

BAB I Pendahuluan

Bab ini menjelaskan latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, ruang lingkup, luaran yang diharapkan, dan sistematika penulisan.

BAB II Tinjauan Pustaka

Bab ini berisi uraian teori-teori yang mendasari penelitian secara detail, dapat berupa metode, model, algoritma, teknik, konsep, prosedur, atau definisi yang berkaitan dengan topik penelitian.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan tahapan penelitian, deskripsi pendekatan teoritis, *desain eksperimen*, delineasi wilayah kajian, sumber data, teknik pengumpulan data, teknik pengolahan data, dan teknik analisis data, yang digunakan untuk mencapai tujuan penelitian. Untuk setiap proses yang dijalankan, harus dijelaskan dasarnya.

BAB IV HASIL DAN PEMBAHASAN

Bab ini terdiri atas analisa permasalahan tentang semua hal terkait pengumpulan data yang diperlukan dalam perancangan sistem informasi akademik menggunakan kriptografi *one time pad*. Analisa perancangan aplikasi dan pembahasan berisikan tentang ide-ide penulis yang dituangkan dalam suatu rancangan aplikasi untuk memecahkan suatu masalah yang ada.

BAB V PENUTUP

Bab ini menjelaskan kesimpulan yang didapat dari hasi penelitian dan saran guna proses pengembangan selanjutnya.

DAFTAR PUSTAKA

RIWAYAT HIDUP

LAMPIRAN