

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

Keamanan sistem komputer menjadi semakin penting seiring dengan berkembangnya proses bisnis yang terkomputerisasi. Keamanan sistem komputer yang menjadi sorotan bukan hanya dari perangkat komputernya saja, namun juga keamanan jaringan, *software* atau program aplikasi dan juga keamanan *database*. Begitu juga dengan keamanan *database* yang menjadi pertahanan terakhir ketika suatu sistem komputer mengalami serangan dari pihak luar setelah menembus keamanan jaringan, keamanan sistem operasi dan *software*. Misalnya pada usaha dibidang penjualan dan kredit elektronik dimana di dalam *database*-nya akan menyimpan data-data diri pelanggan, termasuk *account login* pelanggan.

Keamanan *database* dapat dilakukan dengan berbagai cara, dimulai dari pembatasan hak akses *user* terhadap *database* itu sendiri, penggunaan nama *field* yang hanya dimengerti oleh administrator. Tidak semua pegawai yang diberi izin mengakses *database* mengerti alur *database* yang ada untuk menghindari pencurian data, perusakan data dan lain sebagainya, hingga pengimplementasian algoritma kriptografi untuk mengamankan data/*password* terhadap *record* dalam *database*-nya. Keamanan *database* dibuat dengan tujuan membuat *record* yang tersimpan menjadi lebih rahasia dan sulit dibaca oleh pihak lain.

Beberapa pengguna bahkan menggunakan *password* yang lemah, sehingga lebih rentan untuk dibobol. Hal tersebut menyebabkan kurangnya keamanan terhadap data *user* tersebut. Melihat permasalahan tersebut, maka digunakan algoritma kriptografi TEA (*Tiny Encryption Algorithm*) untuk meningkatkan tingkat keamanan data *user*, sehingga meminimalisir terjadinya pembobolan data *user login*.

Algoritma kriptografi TEA (*Tiny Encryption Algorithm*) adalah algoritma kriptografi yang simpel tetapi cepat dan merupakan kriptografi yang kuat. Algoritma kriptografi TEA ini di desain oleh *Wheeler* dan *Needham*. TEA adalah

sebuah kriptografi *block cipher* yang dikenal dengan kriptografi yang simpel dalam deskripsi dan implementasinya<sup>[1]</sup>

Beberapa penelitian terkait dengan yang penulis lakukan diantaranya adalah, Penelitian yang dilakukan oleh<sup>[2]</sup> yang berjudul “Implementasi Kombinasi *Tiny Encryption Algorithm* (TEA) Dan Algoritma *Least Significant Bit* (LSB) Untuk Keamanan *File Text*”. Penelitian<sup>[3]</sup> yang berjudul “*Design And Implementation Of Tiny Encryption Algorithm*”. Penelitian<sup>[4]</sup> yang berjudul “*A Crypt Analysis Of The Tiny Encryption Algorithm In Key Generation*”. Penelitian<sup>[5]</sup> yang berjudul “Kriptografi File Citra Menggunakan Algoritma *Tea* (*Tiny Encryption Algorithm*)”. Penelitian<sup>[6]</sup> berjudul “Implementasi Notifikasi Dengan SMS Pada *The Dude Network Monitoring*”.

Selain menggunakan algoritma kriptografi TEA untuk keamanan data *user login*, penulis juga menambahkan pengiriman sms kode otentikasi pada saat melakukan proses *login* yang akan dikirimkan ke *handphone user*. Dengan adanya aplikasi pengamanan data *user login* kriptografi dan notifikasi SMS untuk sistem *login* ini maka akan membuat sistem informasi lebih aman karena *password* akan dienkrip di *database* dan kode otentikasi untuk *login* akan dikirimkan ke nomor *handphone user* melalui SMS. Berdasarkan masalah diatas, maka penulis mengangkat judul penelitian “**Penerapan Algoritma Kriptografi TEA Dengan Notifikasi SMS Untuk Pengamanan Data User Login**”.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas, dapat dirumuskan permasalahan sebagai berikut:

1. Bagaimana cara meningkatkan keamanan data *user login*?
2. Bagaimana menerapkan algoritma kriptografi TEA dengan notifikasi SMS dalam proses pengamanan data *user login*?

## 1.3 Batasan Masalah

Untuk mempermudah dan membatasi masalah dalam pembuatan aplikasi, maka diberikan batasan-batasan sebagai berikut:

1. Algoritma yang digunakan adalah algoritma kriptografi TEA.

2. Proses SMS yang terdapat pada sistem digunakan untuk mengirim pesan kode otentikasi.
3. Penerapan algoritma kriptografi TEA dilakukan pada aplikasi berbasis PHP.
4. Kode otentikasi yang akan dikirimkan setelah melakukan *login* berjumlah 5 karakter.
5. Kekuatan sinyal berpengaruh terhadap pengiriman data.

## **1.4 Tujuan dan Manfaat Penelitian**

### **1.4.1 Tujuan Penelitian**

Setiap penelitian yang dilakukan memiliki manfaat maksud dan tujuan yang jelas, adapun tujuan dibuatnya penelitian ini adalah sebagai berikut:

1. Menerapkan algoritma kriptografi TEA untuk mengamankan *password* pada data *user login* dalam *database*.
2. Membuat sistem informasi lebih aman karena *password* akan dienkrip di *database* dan kode otentikasi untuk *login* akan dikirimkan ke nomor *handphone user* yang bersangkutan.

### **1.4.2 Manfaat Penelitian**

Adapun manfaat dari penelitian ini adalah:

1. Terjaminnya data *user login* di dalam *database* karena data akan disimpan dalam bentuk *ciphertext* yang sulit dipahami.
2. Memudahkan proses *login* dengan tingkat keamanan yang lebih tinggi karena menggunakan media *handphone* sebagai penerima kode otentikasi secara *real time* untuk melengkapi rangkaian proses *login*.

## **1.5 Sistematika Penulisan**

Sistematika penulisan laporan skripsi ini bertujuan untuk dapat memahami lebih jelas mengenai hal-hal dan proses pembuatan dalam laporan ini. Adapun sistematika penulisan laporan ini terdiri dari lima bab, yaitu:

### **BAB I PENDAHULUAN**

Bab ini menjelaskan tentang latar belakang, rumusan masalah, batasan masalah, manfaat dan tujuan penelitian, dan sistematika penulisan.

**BAB II      LANDASAN TEORI**

Bab ini menjelaskan mengenai definisi dan teori-teori dari berbagai sumber dan referensi yang membahas tentang peranan algoritma kriptografi TEA dengan notifikasi SMS untuk pengamanan data *user login*.

**BAB III     METODOLOGI PENELITIAN**

Bab ini berisi tentang metode-metode apa saja yang digunakan penulis dalam melakukan penelitian ini.

**BAB IV     HASIL DAN PEMBAHASAN**

Bab ini membahas tentang analisis, rancangan dan juga implementasi dalam pembuatan aplikasi, serta pembahasan mengenai algoritma kriptografi TEA.

**BAB V      PENUTUP**

Bab ini berisi kesimpulan dan saran yang didapat dari pembahasan bab-bab sebelumnya.

