BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan data merupakan aspek yang sangat penting [1]. Keamanan dan kerahasiaan informasi sendiri adalah bagian penting dari informasi [2]. Karena data merupakan hal yang sensitif, maka keamanan data juga harus diperhatikan dan banyak masalah keamanan data yang dapat mengakibatkan pencurian atau kerusakan data oleh pihak yang tidak bertanggung jawab [3]. Bocornya data nasabah bank BSI oleh kelompok *hacker* LockBit pada Mei 2023 lalu menjelaskan betapa berharganya data dan pentingnya aspek keamanan data [4]. Selain itu, data yang disimpan umumnya merupakan informasi rahasia penting yang tidak boleh diketahui orang luar [5]. Sehingga keamanan data sudah seharusnya untuk diberikan perhatian lebih [6]. Data pada internet sendiri tersimpan dalam basis data.

Basis data atau *database* adalah media penyimpanan digital yang membagi data menjadi tabel-tabel yang dikelompokkan ke dalam kolom-kolom untuk memudahkan pemrosesan dan penyimpanan data [7]. Saat ini, *Database* telah menjadi bagian mendasar dari sistem informasi [8]. Salah satu jenis serangan yang umum terhadap basis data atau *database* adalah *SQL Injection*. *SQL Injection* bukanlah hal yang benar-benar baru di dunia peretasan dimana *SQL Injection* itu sendiri merusak basis data suatu situs web [9]. Berbagai macam jenis dan bentuk serangan menunut adanya sistem kemanan yang dapat menangkal berbagai macam bentuk serangan *database*. Terdapat berbagai macam metode yang umum digunakan untuk keamanan *database* seperti kriptografi.

Kriptografi sendiri dapat diartikan sebagai ilmu dan seni menjaga kerahasiaan pesan dalam bentuk data atau informasi yang bermakna atau berharga dengan cara menyembunyikan pesan dalam bentuk yang tidak dapat dipahami [10]. Dengan metode tersebut, penerapan kriptografi dapat mengamankan data dari sisi *database* agar para pihak yang tidak bertanggung jawab tidak dapat melihat atau mencuri data ketika melakukan serangan *SQL Injection*. Data yang sudah

terenkripsi menggunakan teknik kriptografi tertentu memberikan keamanan ekstra sehingga data akan menjadi lebih aman.

Berdasarkan latar belakang tersebut, peneliti akan berfokus pada perancangan sistem keamanan basis data atau *database* dengan menerapkan enkripsi dua tahap (*double encryption*) dengan menggunakan data kartu kredit dan nomor telepon sebagai kolom yang akan dienkripsi sebagai simulasi sistem keamanan data untuk nomor telepon dan kartu kredit. Enkripsi yang diimplementasikan adalah kombinasi antara enkripsi simetris, yakni AES-256, dengan enkripsi asimetris yaitu RSA yang dikombinasikan dengan *Openssl Library* sebagai *tools* untuk enkripsi dan dekripsi. Sistem akan dibangun menggunakan web server berbasis *PHP Native* dengan metode web hosting serta pengujian implementasi enkripsi pada data menggunakan serangan *SQL Injection*. Selain itu, dilakukan pengujian pada sisi dekripsi untuk memastikan implementasi dari enkripsi dua tahap tersebut berjalan pada sistem.

1.2 Perumusan Masalah

Rumusan masalah yang dapat diangkat dari penelitian ini adalah :

1. Bagaimana cara kerja metode enkripsi AES-256 dan RSA dalam mengamankan data pada *database*?
2. Bagaimana hasil pengujian serangan terhadap sistem yang sudah dibuat?
3. Apakah implementasi dari kombinasi AES-256 dan RSA dapat mengamankan data pada *database*?

1.3 Pertanyaan Penelitian

Pertanyaan penelitian yang ingin diketahui oleh peneliti dalam penelitian ini adalah :

1. Apakah enkripsi dua tahap menggunakan algoritma AES-256 dan RSA dapat diimplementasikan pada keamanan data pada *database*?
2. Apakah sistem enkripsi dua tahap yang sudah dibangun dapat melindungi data dari serangan *SQL Injection*?

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah :

1. Memahami bagaimana cara kerja kriptografi AES-256 dan RSA dalam mengamankan database.
2. Mengetahui hasil pengujian serangan *SQL Injection* terhadap sistem yang sudah dibangun.

1.5 Batasan Masalah

Batasan masalah dalam penelitian ini adalah :

1. Penelitian ini hanya berfokus pada aspek keamanan *database* dengan mengimplementasikan metode kriptografi *Advanced Encryption Standard* (AES) dan *Rivest Shamir Adleman* (RSA).
2. Penelitian ini hanya berfokus pada bagaimana hasil yang didapatkan menggunakan serangan SQL Injection pada sistem yang sudah dibangun menggunakan enkripsi dua tahap *Advanced Encryption Standard* (AES) dan *Rivest Shamir Adleman* (RSA).
3. Penelitian ini menggunakan skenario serendah-rendahnya sistem dengan menonaktifkan semua fitur keamanan seperti SSL/TLS, HTTPS, dan *Web Application Firewall*.

1.6 Manfaat Penelitian

Manfaat dari penelitian ini adalah memberikan persepektif baru dalam perkembangan ilmu teknologi khususnya di sektor keamanan dan dapat menjadi referensi bagi penelitian-penelitian selanjutnya. Selain itu, secara praktis, diharapkan nantinya peneliti dapat mengimplementasikan dengan baik algoritma yang digunakan yakni AES-256 dan RSA dalam penelitian ini.