BAB I

PENDAHULUAN

1.1. Latar Belakang

Data merupakan hal yang sangat penting dan berharga bagi organisasi karena mengandung informasi-informasi yang bersifat sensitif maupun rahasia (Nolin, 2019). Saat terjadi proses transmisi data, diperlukan beberapa prosedur pengamanan agar keaslian data tetap terjaga dan tidak bocor ke pihak yang tidak memiliki kewenangan maupun kontrol atas data tersebut.

Adapun aspek yang harus diperhatikan saat melakukan transmisi data adalah *Confidentiality, Integrity, Availability* (Pesante, 2008), *Accounting, Authentication, Authorization* (Sinuraya, 2020) dan *Non-Repudiation* agar keamanan serta kerahasiaan data bisa terjamin. Salah satu cara untuk meningkatkan keamanan transmisi data yaitu dengan mengenkripsi data tersebut menjadi teks acak sehingga keamanan dan kerahasiaan data bisa terjaga.

Beberapa percobaan untuk mengamankan data pada saat proses transmisi telah dilakukan dalam penelitian sebelumnya, di antaranya menggunakan algoritma: DES (Adhar, 2019; Primartha, 2011), ROT (Aresta et al., 2020; Pratiwi, 2017) dan RC6 (Khairuman, 2013; Saputra, Sasmita and Wiranatha, 2017).

Algoritma DES berhasil diterapkan untuk mengamankan data yang digunakan pada sektor perbankan dan militer (Danuri, 2011). ROT merupakan algoritma yang umum digunakan pada *UNIX* (Sinaga and Mesran, 2017). DES memiliki kekurangan yaitu masih menggunakan blok kunci 64 bit dan ukuran kunci 56 bit (Danuri, 2011). Algoritma ROT rentan terhadap serangan maupun kebocoran

data karena tidak memiliki kunci untuk melakukan proses enkripsi maupun dekripsi sehingga tidak disarankan digunakan untuk proses transmisi data (Sinaga and Mesran, 2017). Serangan yang populer dilakukan pada algoritma RC6 adalah *exhaustive search* untuk mencari kunci dan *exhaustive search* tidak mungkin bisa diterapkan pada algoritma AES karena panjang kunci yang dimilikinya (Panggabean, 2007).

Adapun algoritma AES adalah versi terbaru dari DES yang meningkatkan blok kunci menjadi 128 bit serta ukuran kuncinya menjadi 3 varian agar keamanan algoritma AES lebih kuat (Hameed, Ibrahim and Manap, 2018). Algoritma AES dipilih untuk digunakan pada penelitian ini, karena keamanan menjadi faktor penting saat melakukan proses transmisi data.

AES-256 mode CTR memiliki kelemahan *reused key attack* yaitu kelamahan yang dapat mengembalikan kunci yang digunakan menjadi terlihat dan dapat digunakan kembali (Hammond, 2021).

Proses enkripsi data akan dilakukan menggunakan algoritma AES-256 serta akan dilakukan uji coba dengan diintegrasikan menggunakan OpenSSL sehingga dapat terjadi peningkatan keamanan pada proses transmisi data. Kunci akan di *hash* terlebih dahulu dan menggunakan fungsi *hex2bin* agar menjadi binary agar tidak *printable* sehingga dapat mengurangi resiko serangan *reused key attack*. Serangan *man-in-the-middle* (MITM) akan mencoba dilakukan untuk melihat perbedaan keamanan data yang sudah dienkripsi dengan yang tidak dienkripsi.

1.2. Rumusan Masalah

Berdasarkan latar belakang penelitian yang telah diungkapkan, maka penulis merumuskan masalah sebagai berikut.

1. Bagaimana mengintegrasikan algoritma AES-256 dan OpenSSL untuk proses enkripsi dan dekripsi data?
2. Bagaimana mengurangi resiko serangan *reused key attack?*
3. Bagaimana mengukur kecepatan proses enkripsi dan dekripsi data?
4. Bagaimana mengukur tingkat keamanan integrasi algoritma AES-256 dan OpenSSL pada saat transmisi data?

1.3. Tujuan Penelitian

Berdasarkan rumusan masalah penelitian di atas, penulis menentukan tujuan penelitian sebagai berikut.

1. Melakukan integrasi antara algoritma AES-256 dan OpenSSL untuk proses enkripsi dan dekripsi data.
2. Mengurangi resiko serangan *reused key attack.*
3. Mengukur kecepatan proses enkripsi dan dekripsi data.
4. Mengukur tingkat keamanan integrasi algoritma AES-256 dan OpenSSL pada saat transmisi data.

1.4. Manfaat Penelitian

Penelitian yang penulis lakukan diharapkan memberi manfaat secara teoritis maupun praktis.

1. Dapat melakukan integrasi antara algoritma AES-256 dan OpenSSL untuk proses enkripsi dan dekripsi data.

2. Dapat mengurangi resiko serangan *reused key attack.*
3. Dapat mengukur kecepatan proses enkripsi dan dekripsi data.
4. Dapat mengukur tingkat keamanan integrasi algoritma AES-256 dan OpenSSL pada saat transmisi data.

1.5. Batasan Masalah

Penelitian ini difokuskan pada dua bidang yaitu kriptografi (enkripsi dan dekripsi) dengan algoritma AES-256 dan transmisi data yang dilakukan dari OS Windows ke OS Linux. Data uji di unduh dari situs https://file-examples.com/ dengan menggunakan jenis berkas dengan ekstensi zip, mp4, png, jpg, mp3, pdf, ppt, docx, csv, xlsx, dan xml serta ukuran yang berbeda.

Hash yang digunakan pada penelitian ini yaitu *sha512* dengan serangan yang dilakukan menggunakan *man-in-the-middle* (MITM).