BAB I. PENDAHULUAN

A. Latar Belakang

Pesatnya perkembangan teknologi informasi saat ini memudahkan manusia dalam melakukan komunikasi dan berbagi informasi. Salah satu kemajuan teknologi komunikasi yaitu proses pengiriman data (pesan). Pengiriman data (pesan) terdapat beberapa hal yang harus diperhatikan, yaitu: kerahasiaan, integritas data, autentikasi dan non repudiasi. Namun, dengan adanya kemudahan tersebut membuat kebanyakan orang lupa bahwa keamanan dan privasi data merupakan bagian yang sangat penting dalam berkomunikasi. Oleh karenanya dibutuhkan suatu proses penyandian atau pengkodean data sebelum dilakukan proses pengiriman. Sehingga data yang dikirim terjaga kerahasiaannya dan tidak dapat dengan mudah diubah untuk menjaga integritas data tersebut.

Terdapat beberapa algoritma yang disediakan oleh softether dalam pengenkripsian data. Softether VPN adalah perangkat lunak VPN generasi baru yang menawarkan stabilitas, fleksibilitas, dan perluasan, dan kompatibel dengan semua jaringan canggih yang menghasilkan bandwidth lebar, beban tinggi yang dibutuhkan oleh perusahaan besar dan penyedia Internet serta jaringan untuk perorangan dan rumah serta jaringan untuk kecil dan bisnis skala menengah.

AES merupakan sistem penyandian blok yang bersifat non-Feistel karena AES menggunakan komponen yang selalu memiliki invers kunci bit 128, 192, dan 256 bit. Penyandian AES menggunakan proses yang berulang yang disebut

dengan ronde. Jumlah ronde yang digunakan oleh AES tergantung dengan panjang kunci yang digunakan. Setiap ronde membutuhkan konci ronde dan masukan dari ronde berikutnya. Kunci ronde dibangkitkan berdasarkan kunci yang diberikan (Sadikin, 2012).

Dalam penelitian ini algoritma yang diambil adalah AES128-SHA, AES128-SHA256, dan AES128-GCM-SHA256 sebagai objek penelitian dalam menganalisis kecepatan pada proses enkripsi dan deskripsi. Pengujian dilakukan pada *Webserver StressTool* 8 dengan 100, 300, dan 500 *user*. Kemudian akan didapatkan kecepatan proses enkripsi dan deskripsi yang terbaik antara algoritma AES128-SHA AES128-SHA256 dan AES128-GCM-SHA256.

B. Perumusan Masalah

Berdasarkan latar belakang diatas dapat dirumuskan suatu permasalahan yang akan diselesaikan dalam penelitian ini adalah belum diketahui kecepatan proses enkripsi dan deskripsi pada algoritma AES128-SHA, AES128-SHA26, dan AES128-GCM-SHA256 saat proses enkripsi dan deskripsi.

C. Batasan Masalah

Dalam penelitian perlu adanya pembatasan masalah agar pembahasan dapat mencapai hasil yang optimal. Adapun batasan yang digunakan dalam penelitian ini adalah sebagai berikut:

1. *Request* yang diuji hanya 100, 300 dan 500 *user*.
2. Data yang digunakan saat pengujian memiliki ukuran dan jenis yang sama.

D. Tujuan Penelitian

Tujuan yang akan dicapai dari penelitian ini adalah menganalisis kecepatan proses enkripsi dan deskripsi algoritma AES128-SHA, AES128-SHA256, dan AES128-GCM-SHA256 dengan jumlah pengguna 100, 300, 500 *user*.

E. Manfaat Penelitian

Manfaat yang diharapkan dari hasil penelitian ini sebagai berikut:

1. Digunakan sebagai acuan atau bahan pertimbangan dalam memilih algoritma yang akan digunakan pada saat proses enkripsi dan deskripsi.
2. Proses transmisi data lebih cepat pada saat dilakukan enkripsi dan deskripsi.