BAB II. TINJAUAN PUSTAKA

A. Penelitian Terdahulu

1. Sulaiman dkk. (2018) menyatakan bahwa telah melakukan pengujian pada perangkat lunak dengan menggunakan seribu (1000) karakter pada algoritma *Rivest Code* 4 (RC4) dan *Advanced Encryption Standard* (AES) untuk mengetahui tingkat kecepatan pada kedua algoritma, jika dimasukan kedalam gambar dengan menggunakan metode *Least Significant Bit* (LSB). Sehingga bisa dianalisis algoritma mana yang lebih unggul dalam hal kecepatan jika diterapkan kedalam metode *Least Significant Bit* (LSB) steganografi. Penerapan kriptografi dalam metode *Least Significant Bit* (LSB) telah banyak dilakukan, baik dengan menggunakan kriptografi simetris maupun asimetris.
2. Rihan dkk. (2015) menyatakan bahwa mengevaluasi dua algoritma yaitu AES dan DES. Ukuran kinerja skema enkripsi akan dilakukan dalam hal pemrosesan waktu, *throughput* enkripsi penggunaan CPU pada *Windows* dan *Platform Mac* untuk ukuran teks yang berbeda. Penggunaan CPU dan *throughput* enkripsi untuk dua enkripsi algoritma AES dan DES. Waktu enkripsi dianggap sebagai waktu yang diperlukan oleh algoritma enkripsi untuk menghasilkan teks penyandian dari *plaintext*. Waktu enkripsi digunakan untuk menghitung *throughput* dari skema enkripsi. Ini menandakan bahwa kecepatan enkripsi *throughput* dari enkripsi dihitung sebagai total *plaintext* dalam *byte* terenkripsi dibagi dengan waktu enkripsi. Penggunaan CPU adalah persentase waktu dimana CPU hanya berkomitmen

pada proses penghitungan tertentu. Ini mencerminkan penggunaan CPU yang digunakan dalam proses enkripsi, yang lebih tinggi adalah beban CPU. Proses ini dilakukan untuk mengukur dampak perubahan ukuran data dan platform untuk setiap algoritma kriptografi.

3. Kuswanto & Rachmad. (2018) menyatakan bahwa melakukan pengujian terhadap kombinasi AES dan Kode Turbo. Penujian ini dilakukan untuk menentukan kinerja kombinasi AES dan Turbo Code pada saluran AWGN dan saluran ideal dengan mengukur kinerja BER efek penurunan dan waktu eksekusi. Proses eksekusi enkripsi dan deskripsi dilakukan dengan membandingkan waktu untuk berbagai jenis data dan saluran. Input data yang digunakan yaitu jenis data (teks, gambar dan suara), SNR 15 dB dan 1 iterasi. Dalam pelaksanannya enkripsi dan deskripsi kombinasi AES dan Turbo Code pada AWGN diperlukan waktu yang lebih panjang dibandingkan dengan saluran ideal. Waktu yang dibutuhkan adalah sekitar 6 detik pada saluran ideal sementara untuk saluran AWGN adalah sekitar 32 detik.
4. Ashiru dkk. (2015) Menyatakan bahwa mengatasi masalah dalam menghitung peningkatan dan menghitung overhead komputasi, dengan menganalisis enkripsi standar (AES) dan dimodifikasi untuk meningkatkan kinerja enkripsi. Pengembangan dan implementasi peningkatan algoritma AES untuk semua jenis data. Algoritma AES yang sudah dimodifikasi dan disempurnakan dapat memberikan kecepatan enkripsi yang lebih baik. Untuk memeriksa seberapa cepat peningkatan algoritma AES maka dilakukan pengujian dengan menggunakan beberapa file. Algoritma modifikasi AES

akan dibandingkan dengan algoritma AES yang tidak dimodifikasi dalam proses pengujiannya menggunakan 16 byte teks dan membandingkan waktu kecepatannya. Dengan menggunakan algoritma AES yang sudah dimodifikasi peningkatan kecepatan enkripsi dan deskripsi data yang kompleks meningkat.

B. Landasan Teori

1. Virtual Private Network

Menurut Wijaya (2011) *Virtual Private Networ*k (VPN) adalah fasilitas yang memungkinkan koneksi jarak jauh (*remote access*) yang aman dengan menggunakan jaringan internet untuk akses ke LAN di kantor. Sebelum fasilitas VPN diciptakan, akses ke LAN dari jauh dilakukan menggunakan fasilitas *remote access* dial-up. Dengan fasilitas ini, pada LAN yang akan diakses sudah harus disediakan *remote access server* yang dapat dikoneksi dengan modem lewat jaringan telepon biasa, langsung dari laptop atau komputer pemakai. Demikian pula pada laptop atau computer pemakai tersebut harus diinstalasikan software *remote access client*.

2. Uji *Kruskal-Wallis*

Menurut Siregar (2013) Uji *Kruskal-Wallis* merupakan turunan dari uji Wilcoxon dengan kriteria lebih dari dua sampel bebas (K sampel). Uji di gunakan pada analisis Komperatif untuk menguji lebih dari dua sampel *independent* (bebas) dengan data berjenis ordinal dengan ukuran sampel tidak sama.

Beberapa tahap yang dilakukan adalah sebagai berikut:

a. Menentukan hipotesis

H_0: Tidak ada perbedaan antara rata-rata kecepatan pada algoritma AES128-SHA, AES128-SHA256, dan AES128-GCM-SHA256.

H_1: Ada perbedaan antara rata-rata kecepatan pada algoritma AES128-SHA, AES128-SHA256, dan AES128-GCM-SHA256.

b. Menentukan nilai alpha (α) (dalam penelitian ini digunakan α = 5%)

c. Kriteria pengujian

- H_0 diterima bila H hitung ≤ X^2 tabel
- H_0 ditolak bila H hitung > X^2 tabel

d. Menentukan H hitung.

$$H = \left[\frac{12}{N(N+1)}\right]\left[\sum \frac{R_k^2}{n_k}\right] - 3(N+1)$$

Di mana:

k = jumlah kelompok sampel.

R_k = jumlah rangking setiap sampel ke-k(sampel)

N = total sampel

e. Membandingkan F hitung dengan F tabel.

Tujuan membandingkan X^2 tabel dan H hitung adalah untuk mengetahui, apakah Ho ditolak atau diterima berdasarkan kaidah pengujian.

f. Pengambilan kesimpulan

Tujuan untuk menarik kesimpulan bahwa Ho menerima atau menolak.

3. Statistik

Menurut Taniredja & Mustafidah (2011) mendefinisikan bahwa statistika tidak lepas dengan adanya data. Diolah denganengan kata lain bahwa statistika berhubungan dengan pengolahan data. Dari sudut pandang statistik, data dapat dibagi menjadi dua, yaitu:

a. Data Kuantitatif

Data kuantitatif adalah data yang dinyatakan dalam bentuk angka. Misalnya: usia seseorang, tinggi seseorang, penjualan dalam sebulan, dsb.

b. Data Kualitatif

Data kualitatif adalah data yang dinyatakan dalam bentuk bukan angka. Misalnya: jenis pekerjaan (petani, nelayan, pegawai, dsb), status perkawinan, gender (jenis kelamin), kepuasan seseorang (tidur puas, cukup puas, sangat puas), dsb. Data jenis kualitatif ini harus dikuantifikasikan agar bisa diolah dengan statistika, karena statistik hanya bisa memproses data yang berupa angka.

4. SPSS

Menurut Taniredja & Mustafidah (2011) *Statistical Package for Social Science* (SPSS) merupakan paket statistika untuk ilmu-ilmu *social*, akan tetapi SPSS banyak juga digunakan untuk bidang-bidang lain yang memang membutuhkan statistika. Sejak dikeluarkannya SPSS dengan versi *under* DOS sampai sekarang dengan versi *under* windows, sudah dikembangkan SPSS sampai generasi atau *release* 17 yang paling baru dengan penambahan fasilitas yang makin lengkap seperti grafik pengendalian

untuk *quality control* dan penambahan fasilitas untuk *link S-Plus* yaitu *Package* Statistika terbaru yang sangat cocok untuk tujuan ilmiah dan pengembangannya, tidak hanya pengolahan data semata seperti *software* statistika yang lain. SPSS berfungsi untuk membantu memproses data-data statistik secara cepat dan tepat, serta menghasilkan berbagai *output* yang dikehendaki oleh para pengambil keputusan. Statistik dapat diartikan sebagai suatu kegiatan yang bertujuan untuk mengumpulkan data, meringkas, atau menyajikan data kemudian menganalisis data dengan menggunkanan metode tertentu, dan mengintrepretasikan hasil dari analisa tersebut.

5. Kriptografi

Menurut Munir (2006) Kriptografi (*cryptography*) berasal dari bahasa Yunani: "*cryptos"* artinya *"secret"* (rahasia), sedangkan *"graphein"* artinya *"writing"* (tulisan). Jadi, kriptografi berarti *"secret writing"* (tulisan rahasia). Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Kriptografi digunakan untuk keamanan komunikasi penting seperti komunikasi dikalangan militer, diplomat, dan mata-mata. Namun saat ini kriptografi lebih dari sekedar *privacy*, tetapi juga untuk tujuan *data integrity*, *authentication*, dan *non-repudiation*.

6. Algoritma

Menurut Ariyus (2006) Algoritma berasal dari nama penulis buku Arab yang terkenal yaitu Abu Ja'far Muhammad ibnu Musa al-Khuwarizmi dibaca oleh orang barat menjadi algorism). Kata algorism lambat laun berubah menjadi algorithm. Algoritma adalah urutan langkah-langkah logis untuk penyelesaian masalah yang disusun secara sistematis

7. *Advanced Encryption Standard* (AES)

Menurut Sadikin (2012) 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.