BAB I
PENDAHULUAN

1.1 Latar Belakang

Kemajuan ilmu pengetahuan dan teknologi yang sangat cepat telah memberi pengaruh yang baik serta manfaat yang besar bagi manusia dalam berbagai bidang kehidupan. Keunggulan tersebut tidak lepas dari hasil penelitian dan percobaan oleh para ilmuwan dan *engineer*, yang selalu mencari terobosan dan temuan baru untuk menciptakan sesuatu yang baru bermanfaat dan berguna bagi kehidupan manusia.

Semakin berkembangnya ilmu pengetahuan dan teknologi, maka semakin tinggi dampak yang akan terjadi baik itu dampak positif dan dampak negatif. Dampak positifnya adalah semakin cepatnya dalam proses bertukar informasi karena sudah tidak terbatas oleh ruang dan waktu lagi. Sedangkan untuk dampak negatifnya dapat dilihat dari semakin meningkatnya tingkat kejahatan di internet, seperti *hacking, cracking, carding, phising, spamming, dan defacing*.

Keamanan data merupakan masalah yang sangat penting dalam perkembangan teknologi saat ini. Oleh sebab itu dibutuhkan sebuah cara yang dapat menjaga kerahasiaan dan keamanan merujuk pada perlindungan informasi dari penyingkapan pihak yang tidak sah. Salah satu mekanisme untuk meningkatkan keamanan data adalah dengan menggunakan teknik kriptografi. Ada berbagai macam algoritma dalam kriptografi diantaranya adalah Algoritma *Advance Encryption Standard* (AES) dan Algoritma *Blowfish*. Enkripsi adalah proses yang dilakukan untuk mengubah suatu informasi menjadi serangkaian kode

rumit (*ciphertext*) yang sulit diartikan. Dekripsi adalah proses yang mengembalikan informasi yang sudah dienkripsi menjadi sebuah informasi (*plaintext*).

Algoritma AES terdiri atas 3 blok cipher, yaitu AES-128, AES-192 dan AES-256. Algoritma tersebut memiliki tingkat keamanan yang cukup tinggi, karena sampai sekarang belum ditemukan algoritma / mesin yang mampu untuk memecahkan data hasil enkripsi algoritma kriptografi tersebut dengan cepat. Karena masih banyak orang yang kurang mengerti dengan cara kerja algoritma kriptografi tersebut. Jenis Algoritma lainnya adalah Algoritma *Blowfish*. Algoritma *Blowfish* merupakan algoritma simetri yang tergolong dalam metode *block cipher*. Ada dua tipe dasar algoritma simetris yaitu *block cipher* dan stream *cipher*. Sebuah block *cipher* memproses *block byte* pada satu waktu. Sebuah stream cipher memproses satu *byte* atau bahkan satu bit pada suatu waktu.

Dari permasalahan yang ada sangat dibutuhkan suatu sistem yang dapat membandingkan algoritma mana yang lebih unggul baik dalam hal enkripsi dan dekripsi. Oleh sebab itu peneliti berinisiatif mengambil judul penelitian "Analisis Perbandingan Performa Enkripsi dan Dekripsi Menggunakan Algoritma AES-256 dan Algoritma *Blowfish*".

1.2 Perumusan Masalah

Berdasarkan latar belakang masalah tersebut, dapat dibuat suatu rumusan masalah, yaitu "Bagaimana cara merancang sebuah system berbasis PHP yang dapat mensimulasikan masing-masing cara kerja dan membandingkan algoritma

AES-256 dan Algoritma *Blowfish* mana yang lebih unggul baik dalam *performa* enkripsi dan dekripsi pada *file* dengan *size* yang berbeda,?".

1.3 Batasan Masalah

Demikian luas cakupan penelitian, sehingga demi mencegah adanya penyimpangan dari judul yang telah ditentukan, maka penulis perlu membatasi ruang lingkup kegiatan penelitian ini pada :

1) Metode kriptografi yang digunakan adalah metode kunci simetri dengan algoritma kriptografi *Advanced Encryption Standard* (AES) 256 bit dan Algoritma *Blowfish*.
2) Aplikasi bahasa pemrograman yang digunakan adalah bahasa pemrograman PHP.
3) Penelitian berfokus pada Analisis Perbandingan Performa Dari Hasil Enkripsi Dan Dekripsi AES dan *Blowfish* pada *File* dokumen dengan ekstensi *word* dengan format *docx*.
4) Pada penelitian ini yang menjadi standar perbandingan antara algoritma AES 256 dan *Blowfish* adalah waktu dalam proses enkripsi dan dekripsi.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini yaitu menghasilkan sistem yang dapat menganalisa perbandingan performa antara algoritma kriptografi *Advanced Encryption Standard* (AES) dengan *Blowfish* dan mengimplementasikan dengan bahasa pemrograman PHP.

1.5 Manfaat Penelitian

Dengan adanya penelitian ini diharapkan bisa memberikan manfaat antara lain sebagai berikut:

1) Dapat memberikan pembelajaran dalam bentuk simulasi mengenai cara kerja algoritma kriptografi *Advanced Encryption Standard* (AES) 256 dengan *Blowfish*.
2) Mengetahui perbandingan performa antara algoritma kriptografi *Advanced Encryption Standard* (AES) 256 dengan *Blowfish*.

1.6 Metodologi Penelitian

1.6.1 Tempat dan Waktu Penelitian

Penelitian ini dilaksanakan pada semester ganjil Tahun Akademik 2018/2019, yaitu antara bulan November 2018 sampai dengan bulan Agustus 2019. Penelitian ini dilaksanakan di Kec. Sekayu, Kab. Musi Banyuasin, Prov Sumatera Selatan.

1.6.2 Data Penelitian

Data penelitian yang menjadi objek penelitian dalam studi kasus Analisis Perbandingan Performa Algoritma Kriptografi *Advanced Encryption Standard* (AES) 256 bit dengan Algoritma *Blowfish* yaitu data-data jenis *file word* dengan format *docx* yang akan di gunakan dalam proses enkripsi dan dekripsi.

1.6.3 Metode penelitian

Penelitian ini dalam menjelaskan permasalahan menggunakan metode deskriptif. Dimana metode deskriptif merupakan metode dalam meneliti status sekelompok manusia, suatu objek, suatu set kondisi, suatu sistem pemikiran ataupun suatu kelas peristiwa pada masa sekarang. Tujuan dari penelitian deskriptif ini adalah untuk membuat deskripsi, gambaran, atau lukisan secara sistematis, faktuan dan akurat mengenai fakta-fakta, sifat-sifat serta hubungan antar fenomena yang diselidiki.

1.6.4 Metode Pengumpulan Data

Adapun metode pengumpulan data yang digunakan dalam penelitian adalah sebagai berikut:

1) Data Primer

   Data primer yaitu data atau informasi yang diambil langsung dari subjek penelitian.

   a) Pengambilan data melalui wawancara secara langsung dengan sumber datanya, melalui tatap muka, dengan mewawancarai narasumber terkait studi kasus penelitian.
   b) Observasi merupakan teknik pengumpulan data yang tidak hanya mengukur sikap dari responden (wawancara) namun juga merekan fenomena yang terjadi (situasi kondisi).

2) Data Sekunder

Data sekunder yaitu sumber data penelitian yang diambil secara tidak langsung melalui media perantara (diperoleh dan dicatat oleh pihak lain) yaitu dari dokumen dan studi pustaka, baik yang dipublikasikan maupun yang tidak dipublikasikan.

a) Mencari masalah-masalah serta melengkapi data-data yang diperlukan dalam penulisan penelitian ini.
b) Studi pustaka digunakan untuk pengumpulan informasi dengan mempelajari buku-buku, jurnal, *website*, dan referensi yang berhubungan dengan sistem ini.

1.6.5 Metode Pengembangan Sistem

Menurut A.S., Rossa dan M. Shalahuddin **(2018: 28)** model *waterfall* adalah model klasik yang bersifat sistematis, berurutan dalam membangun *software*. Tahapan dalam model *waterfall* menurut referensi Pressman:

1) Analisis kebutuhan perangkat lunak

   Sebelum memulai pekerjaan yang bersifat teknis, sangat diperlukan adanya komunikasi dengan customer demi memahami dan mencapai tujuan yang ingin dicapai. Hasil dari komunikasi tersebut adalah inisialisasi proyek, seperti menganalisis permasalahan yang dihadapi dan mengumpulkan data-data yang diperlukan, serta membantu mendefinisikan fitur dan fungsi *software*. Pada tahap ini telah dilakukan analisis kebutuhan pengguna yakni tentang apa yang diperlukan untuk menyelesaikan permasalahan yang ada dan juga

mengumpulkan data baik dari buku, jurnal, artikel dan internet yang berkaitan dengan judul penelitian.

2) Desain

Pada tahapan perancangan dan permodelan sistem yang berfokus pada perancangan struktur data, s*oftware*, tampilan *interface*, dan algoritma program. Tujuannya untuk lebih memahami gambaran besar dari apa yang akan dikerjakan.

3) Pengkodean

Pada tahapan ini proses penerjemahan bentuk desain menjadi kode atau bentuk/bahasa yang dapat dibaca oleh mesin. Setelah pengkodean selesai, dilakukan pengujian terhadap sistem dan juga kode yang sudah dibuat. Tujuannya untuk menemukan kesalahan yang mungkin terjadi untuk nantinya diperbaiki.

4) Pengujian

Tahapan yang terakhir adalah implementasi *software* ke customer, pemeliharaan *software* secara berkala, perbaikan *software*, evaluasi *software*, dan pengembangan *software* berdasarkan umpan balik yang diberikan agar sistem dapat tetap berjalan dan berkembang sesuai dengan fungsinya.

1.7 Sistematika Penulisan

Untuk mempermudah penulisan skripsi ini, penulis membuat suatu sistematika penulisan yang terdiri dari:

BAB 1 : PENDAHULUAN

Bab ini berisikan latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat, metodologi, dan sistematika penulisan.

BAB 2 : TINJAUAN PUSTAKA

Bab ini menjelaskan teori-teori singkat tentang hal-hal yang berhubungan dengan judul, pembahasan bahasa pemrograman dan lain sebagainya.

BAB 3 : ANALISIS DAN PERANCANGAN

Bab ini membahas mengenai analisis kebutuhan untuk perancangan sistem yang akan dibuat sesuai dengan metode pengembangan sistem yang digunakan.

BAB 4 : HASIL DAN PEMBAHASAN

Bab ini membahas mengenai hasil implementasi analisis dan perancangan sistem yang dilakukan, serta hasil pengujian sistem untuk mengetahui apakah perancangan sistem yang dibuat sudah memenuhi kebutuhan.

BAB 5 : PENUTUP

Bab terakhir ini penulis akan menguraikan kesimpulan dan saran yang mencakup hasil dari pengujian. Pada bagian saran berisi saran-saran yang dapat menjadi pertimbangan untuk penelitian-penelitian berikutnya.