BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi dan informasi saat ini telah memberikan dampak yang signifikan di dalam berbagai bidang. Termasuk salah satunya yaitu dalam hal pertukaran data, dimana kemampuan untuk mengakses suatu data dapat dilakukan dengan cepat dan akurat menjadi sangat esensial bagi sebuah organisasi maupun individu. Seiring dengan perkembangan tersebut, memungkinkan pengiriman data menjadi relatif lebih cepat dan murah. Dilain pihak, pengiriman data jarak jauh melalui jaringan internet, gelombang radio maupun media lain yang digunakan masyarakat luas sangat memungkinkan bagi pihak lain untuk menyadap dan mengubah data yang dikirim. Oleh sebab itu, proses enkripsi diperlukan untuk mengamankan data (informasi) yang dikirim dalam upaya mengatasi kejahatan yang bisa berupa pencurian data maupun manipulasi data oleh penjahat, maka akan diimplementasikan sebuah sistem keamanan yang bisa menjaga keamanan pengiriman data dari *client-server*, sehingga proses pembayaran akan bisa dilakukan dengan aman[5].

Terdapat banyak algoritma kriptografi, masing-masing algoritma memiliki karakter dan spesifikasi yang berbeda. Salah satu jenis algoritma kriptografi adalah blok *cipher* yang menggunakan kunci simetris, contoh: AES, DES, *Camellia*, Threefish, dan TDEA.

Dari algoritma kriptografi yang ada, dipilih algoritma kriptografi *Camellia*. *Camellia* dipilih karena sudah diakui oleh ISO (*International Organization for Standardization*) dan terpilih bersama tiga algoritma lain dari 42 algoritma yang diajukan pada proyek NESSIE yang diprakarsai oleh *Information Society Technologies* (IST) dari European Union (EU) [3]. Algoritma ini akan di uji implementasinya pada sistem *biometric payment* yang dibangun menggunakan bahasa pemrograman Java. Parameter performansi yang diukur dan dibandingkan meliputi waktu proses dan *avalanche effect.*

1.2 Rumusan Masalah

Masalah yang akan dibahas pada penelitian ini adalah sebagai berikut :

a) cara merancang dan membangun perangkat lunak kriptografi yang menggunakan algoritma *Camellia* untuk diterapkan pada sistem *biometric payment.*

b) cara mengukur performansi dari algoritma *Camellia* yang didapatkan melalui perangkat lunak berdasarkan waktu proses enkripsi dan dekripsi dan *avalanche effect.*

c) cara melakukan analisa performansi algoritma *Camellia* dan menentukan apakah algoritma kriptografi optimal untuk diterapkan pada sistem *biometric payment* melalui pengamatan parameter-parameter performansi.

1.3 Tujuan

Tujuan penyusunan penelitian ini adalah :

a) dapat merancang dan membangun perangkat lunak kriptografi yang menggunakan algoritma *Camellia* untuk diterapkan pada sistem *biometric payment.*

b) dapat mengukur performansi algoritma yang didapatkan melalui perangkat lunak berdasarkan waktu proses enkripsi dan dekripsi dan *avalanche effect.*

c) mendapatkan analisa dan kesimpulan akhir dari performansi algoritma.

1.4 Batasan Masalah

Pada penyusunan penelitian ini terdapat batasan masalah seperti berikut :

a) algoritma kriptografi yang digunakan adalah algoritma *Camellia.*

b) parameter yang digunakan adalah waktu proses enkripsi dan dekripsi dan *avalanche effect*.

c) bahasa pemrograman untuk pembangunan perangkat lunak simulasi proses kriptografi menggunakan bahasa Java.

d) tidak membahas pembobolan *server* dan keamanan pada *database*.

1.5 Metodologi Penelitian

Langkah yang ditempuh untuk menyelesaikan penelitian ini adalah :

a) studi literatur, mengumpulkan bahan referensi dari buku, jurnal, *ebook* dll yang berhubungan dengan penelitian ini.

b) analisa matematis mengenai struktur fungsi dari algoritma yang digunakan.

c) melakukan pengujian untuk proses enkripsi dan dekripsi data pada sistem *biometric payment* untuk mendapatkan data-data parameter analisa.

d) menganalisa hasil pengujian yang telah dilakukan.

1.6 Sistematika Penulisan

Tugas akhir ini dibagi dalam beberapa topik bahasan yang disusun secara sistematis sebagai berikut.

BAB 1 PENDAHULUAN

Berisi latar belakang, rumusan masalah, tujuan, batasan masalah, metodologi penelitian, dan sistematika penulisan.

BAB 2 DASAR TEORI

Berisi teori-teori dasar mengenai kriptografi, Algortima kriptografi kunci simetris secara umum serta konsep algoritma *Camellia*.

BAB 3 PERANCANGAN DAN IMPLEMENTASI

Berisi konfigurasi umum sistem, perancangan sistem, keluaran yang ingin dihasilkan

BAB 4 IMPLEMENTASI DAN PENGUJIAN SISTEM

Berisi data hasil pengujian dan analisis terhadap sistem yang telah dibangun.

BAB 5 KESIMPULAN DAN SARAN

Berisi kesimpulan dari penelitian yang sudah dilakukan dan saran pengembangan dan perbaikan selanjutnya.