BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang semakin pesat tidak dapat dipungkiri telah mengubah cara kerja berbagai kegiatan dalam bidang kehidupan manusia mulai dari perusahaan sampai pemerintah. Dengan perkembangan teknologi saat ini pertukaran informasi antar pihak sangat diperlukan. Jika keamanan pertukaran informasi tidak bisa di jaga, maka pihak lain dapat memanfaatkan informasi tersebut sehingga akan merugikan pihak-pihak yang berhak atas informasi tersebut.

Foodmochi merupakan sebuah layanan jasa yang bergerak dalam pesan antar makanan *online*. Transaksi pemesanan dilakukan secara *online*. Kegiatan ini tentu saja akan menimbulkan resiko apabila data transaksi tidak terdapat perlindungan keamanannya.

Ada beberapa bentuk ancaman terhadap pertukaran informasi seperti penyadapan, pencurian dan pemalsuan informasi. Dalam aspek layanan keamanan jaringan, pada tahun 1991 lembaga intenasional yang bernama *Ineternational Telecommunication Standardiation Sector* (ITU-T) telah mendefinisikan jenis layanan dan mekanisme keamanan jaringan, untuk itu keamanan dari pertukaran informasi tersebut sangatlah diperlukan. Kriptografi adalah salah satu solusi yang tepat untuk menjaga kerahasiaan dan keaslian data.

Metode yang digunakan dalam penelitian sebelumnya untuk pengamanan data antara lain menggunakan algoritma *Rivest Code 5* (RC5) (Suryawan & Hamdani, 2013), *Rivest Shamir Adleman* (RSA) (Erika, Rachmawati, & Surya, 2012), *Advanced Encrption Standard* (AES) (Pabokory, Astuti, & Kridalaksana, 2015). Dalam penelitian ini akan menggunakan kombinasi dari algoritma RSA dan AES 256 karena algortima RSA mempunyai kemampuan yang cukup baik karena mempunyai kunci autentikasi 2 arah yaitu *public key* dan *private key* jadi lebih aman. Sedangkan algoritma AES *256* memiliki tingkat keamanan yang lebih baik karena proses putaran enkripsi lebih banyak sehingga mempersulit dalam pembacaan data.

Berdasarkan dari latar belakang tersebut, diperlukan sebuah keamanan data untuk menjaga kerahasiaan, keaslian data dan meningkatkan keamanan pada data transaksi dengan menggunakan kombinasi algortima RSA dan AES 256.

1.2 Perumusan Masalah

Perumusan masalah yang akan diungkapkan penulis adalah bagaimana merancang, membangun dan mengimplementasikan kombinasi algoritma RSA dan AES 256 pada data transaksi Foodmochi Sukoharjo.

1.3 Pembatasan Masalah

Untuk mempermudah penelitian, penulis membatasi permasalahan pada pengamanan *database* transaksi pada Foodmochi Sukoharjo yang meliputi :

1. Algoritma kriptografi yang digunakan dalam pengamanan data transaksi adalah RSA dan AES 256.
2. Sistem yang digunakan dalam penelitian ini menggunakan sistem yang sudah ada dalam Foodmochi yang berbasis web dan data yang akan di enkripsi meliputi data pada tabel user, temptransaksi, dan order karena tabel ini berhubungan langsung dengan data transaksi dan pelanggan.
3. *Database* yang digunakan adalah MySQL.
4. Bahasa pemrogrampan yang dipakai adalah PHP.

1.4 Tujuan Penelitian

Tujuan lainnya adalah terciptanya keamanan data transaksi dengan kombinasi algoritma RSA dan AES 256 pada Foodmochi Sukoharjo sehingga kedepannya data transaksi yang disimpan dalam *database* akan sulit diakses oleh orang yang tidak memiliki hak jadi kerahasiaan data, keaslian data terjamin.

1.5 Manfaat Penelitian

Penyusunan skripsi ini diharapkan dapat memberikan manfaat untuk perusahaan Foodmochi.

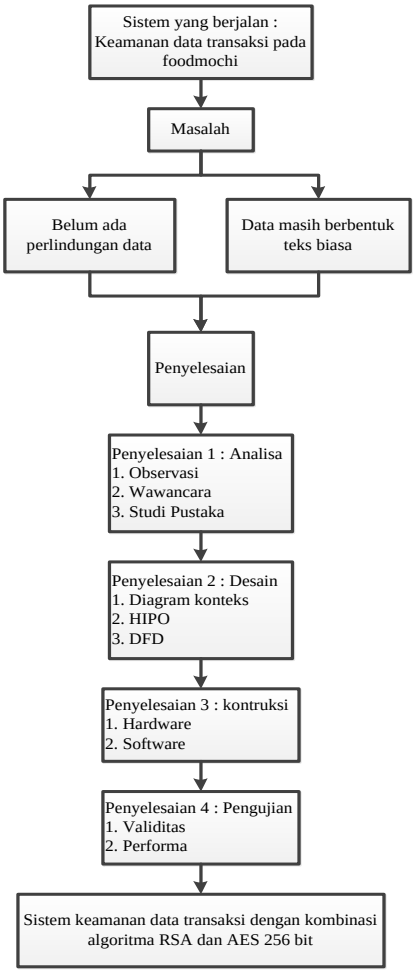
1.5.1 Manfaat Bagi Perusahaan

Berikut adalah manfaat bagi perusahaan :

a. Menjadi alat bantu untuk mengamankan data transaksi sehingga keutuhan data terjamin dari user yang tidak mempunyai hak ataupun kepentingan.

b. Meningkatkan kontruksi keamanan yang digunakan sebelumnya.

1.6 Kerangka Pikir



Gambar 1.1 Kerangka Pikir

1.7 Sistematika Penulisan

Untuk memberikan gambaran tentang pembahasan penelitian ini, maka secara garis besar sistematika penulisan sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi latar belakang, rumusan masalah, pembatasan masalah, tujuan penelitian, manfaat penilitian, kerangka piker, sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab ini menyajikan tentang pembahasan teori – teori yang berkaitan langsung dengan penyusunan laporan skripsi secara menyeluruh tentang tinjauan pustaka pada metode *Rivest Shamir Adleman* (RSA) dan *Advanced Encrption Standard* (AES).

BAB III METODE PENELITIAN

Pada bab ini dijelaskan tentang metode-metode yang digunakan dalam membuat sistem pengamanan data dengan kombinasi algoritma RSA dan AES : meliputi metode pengumpulan data, analisa data, analisa kebutuhan sistem, perancangan dan desain sistem.

BAB IV GAMBARAN PENELITIAN

Pada bab ini akan diuraikan tentang tinjauan pustaka dimana dibahas perbedaan dan persamaan dengan penelitian terdahulu,

data penelitian dan keamanan data yang meliputi enkripsi dan dekripsi.

BAB V PEMBAHASAN

Pada bab ini menguraikan tentang pembahasan mengenai diagram konteks, HIPO, diagram alir data dan *flowchart*.

BAB VI PENUTUP

Pada bab ini berisi tentang kesimpulan dan saran-saran yang diharapkan dapat memberi manfaat bagi pihak-pihak yang terkait.

DAFTAR PUSTAKA

LAMPIRAN