BAB I
PENDAHULUAN

1.1 Latar Belakang

E-commerce merupakan singkatan dari *Electronic Commerce* yang di definisikan sebagai proses pembelian dan penjualan produk, jasa, dan informasi yang dilakukan secara elektronik menggunakan salah satu jaringan yaitu internet. *Electronic Commerce* merupakan bagian dari *Electronic Bussiness* yaitu bisnis yang dilakukan dengan menggunakan *electronic transmission* (Hildamizanthi, 2011).

Dewi Irmawati (2011), mengemukakan manfaat yang diberikan dari *E-commerce* bagi aktivitas pemasaran diantaranya:

1. Promosi produk dan jasa menjadi lebih mudah karena penawarannya yang interaktif dan *real time*.
2. Pelayanan pelanggan yang lebih responsif karena mendapatkan informasi atau berkomunikasi dengan penjual atau *customer service* secara *online*.
3. Penghematan waktu dan biaya dalam melayani pemesanan.

Situs web *E-commerce* semakin canggih dengan mengadopsi system pelayanan pelanggan berbasis teknologi yang sebelumnya tidak tersedia karena terkendala oleh teknologi yang belum memadai (Froehle, 2006). Salah satu contohnya adalah *live chat* system. Dengan teknologi *live chat* ini, perusahaan yang menyediakan layanan *E-commerce* berusaha untuk memberikan sensasi berbelanja di toko *off-line* untuk dapat berkomunikasi dengan *customer service* (Andrews & Haworth, 2002). Penggunaan *chat* secara *real time* sering kali terbukti lebih efektif dibandingkan dengan saluran komunikasi yang lain seperti email atau *FAQ* untuk mempertahankan komunikasi dengan pelanggan (Qiu & Benbasat, 2005). *Live chat* juga terbukti menangani transaksi yang lebih kompleks

daripada *FAQ* atau komunikasi secara *email*. Dengan *live chat* juga terbukti memberikan kepuasan pelanggan yang lebih tinggi[1].

System informasi pelayanan pelanggan ini, dipercaya dapat meningkatkan pelayanan perusahaan kepada pelanggan melalui fitur *live chat* dan memudahkan pelanggan juga dalam memberikan kritik dan saran kepada perusahaan (Teddy & Ricoida, 2016).

Menurut Santoso (2015), penyerangan yang dapat dilakukan ketika seseorang menerima pesan pada saluran komunikasi adalah sebagai berikut:

1. *Sniffing*; ini merupakan serangan mengendus pesan.
2. *Replay attack*; ini merupakan serangan yang dilakukan setelah penyerang berhasil melakukan *Sniffing*, lalu menyamar sebagai pengirim atau penerima pesan untuk melakukan *replay attack*.
3. *Spoofing*; jenis penyerangan ini dilakukan setelah *replay attack* berhasil, dan penyerang berusaha meyakinkan bahwa dia bukan seorang penyerang melainkan pengirim atau penerima pesan.
4. *Man in the middle*; jenis penyerangan ini dilakukan secara paralel dalam komunikasi dua arah atau lebih.

Menurut penelitian yang dilakukan Elmorshidy dkk (2015), *e-commerce* yang menyediakan *live chat* system mungkin akan meminta pelanggannya untuk saling berbagi informasi pribadi, maka dari itu kebutuhan untuk menjaga informasi pribadi yang akurat akan meningkat. Dengan demikian penyedia layanan *live chat customers service* pada *e-commerce* harus memberikan jaminan informasi mereka aman dengan cara meningkatkan *firewall* dan teknologi enkripsi pada *live chat*.

Keamanan informasi data yang kita buat sangat berperan penting, untuk menjamin keaslian data agar tidak mudah disalah gunakan oleh tangan-tangan jahil yang tidak bertanggung jawab. Banyak sekali permasalahan seperti perubahan data atau penyalahgunaan data, meskipun telah menggunakan

[1] http://solutions.liveperson.com/sb/channel

pengamanan data. Dengan demikian, maka akan lebih baik jika menggunakan pengamanan data yang sulit ditembus seperti enkripsi data dengan menggunakan kriptografi (Kurniawan, 2004). Salah satu antisipasi dari resiko-resiko yang ditimbulkan live chat, yaitu membuat sebuah protocol keamanan alternatif dengan menggunakan algoritma kriptografi.

Kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan. Kriptografi dalam bahasa Inggris berarti *secret writing*. Sehingga kriptografi dapat juga disebut sebagai sesuatu yang tertulis secara rahasia. Beberapa tujuan kriptografi yang dibutuhkan pada live chat adalah *Confidentiality* dan *Data Integrity* yang dapat dipenuhi dengan enkripsi dan fungsi *hash*. Enkripsi pada data teks bertujuan untuk melindungi data tersebut agar tidak ada yang mencuri data tersebut. Fungsi *hash* dilakukan untuk mencegah perubahan suatu data oleh orang-orang yang tidak terkait. Kriptografi yang akan digunakan pada penelitian kali ini yaitu kriptografi *hybrid*, dimana kripotografi *hybrid* adalah penggabungan antara kriptografi kunci simetri dan asimetri. Kriptografi kunci simetri yang akan digunakan adalah algoritma Rijndael, dan kriptografi kunci asimetri yang akan digunakan adalah kriptografi RSA. Penulis menggabungkan kedua algoritma ini karena kunci simetri harus dikirim lewat saluran yang sangat aman untuk sampai ke penerima, ini menjadi salah satu kelemahan dari algoritma simetri. Untuk itu diperlukan algoritma yang berguna untuk mengamankan kunci simetri yaitu dengan menggunakan algoritma kunci *public* atau RSA.

Algoritma RSA tidak dapat digunakan untuk data yang berukuran besar, dan AES memiliki kelemahan dalam mengirimkan kunci. Dalam penelitiannya yaitu merancang web service, harus mempertimbangkan solusi keamanan yang akan mengatasi kelemahan RSA dan AES. Untuk menjaga integritas data, solusi yang mereka kemukakan adalah dengan mengkombinasikan algoritma RSA dan AES dengan teknik hashing SHA 256 (Kadam & Khaimar, 2015).

Beberapa peneliti menemukan adanya celah pada enkripsi AES yang memungkinkan memecahkan kunci rahasia lebih cepat dari sebelumnya, meskipun AES dinyatakan telah melalui berbagai macam tes (Nugroho, Judhie Putra, & Ramadhan, 2016).

Menurut penelitian Anggita (2017), modifikasi algoritma rijndael 256 bits yang telah dimodifikasi bagian *S-box* dan *Shiftrow* menggunakan pengujian *Avanche Effect*, menunjukkan bahwa modifikasi pada bagian *ShiftRow* memberikan hasil yang lebih baik sebesar 50.2232% dibandingkan modifikasi di bagian *S-box*.

Berdasarkan masalah dan studi literatur yang telah dijelaskan di atas. peneliti akan memodifikasi algoritma Rijndael di bagian *S-Box* dan *ShiftRow* dengan menggunakan panjang kunci 256 bits, karena jika menggunakan 256 bits memiliki ekspansi kunci 14 putaran yang akan menambah kompleksitas menjadi lebih tinggi dibandingkan dengan penelitian sebelumnya. Untuk mengamankan kunci akan menggunakan kombinasi algoritma RSA dan SHA256. Kunci yang akan digunakan untuk proses enkripsi dan dekripsi adalah kunci yang menggunakan algoritma RSA, demi keamanan dalam proses pengiriman kunci. Fungsi hash akan dilakukan pada proses sebelum pengiriman pesan dan juga setelah pesan diterima, lalu akan dibandingkan apakah hasil hash sama atau tidak ketika pesan sudah dikirim dan diterima. Jika fungsi hash tidak sama pada kedua belah pihak, maka terjadi perubahan pada data. Ini berguna untuk menyulitkan pihak ketiga untuk melakukan perubahan terhadap data. Pada penelitian inipun akan dilakukan perbandingan terhadap teori *chaos* yang akan digunakan, antara lain Henon Map dan Logistic Map dan agar dapat memberikan integritas data integritas data dan atau melindungi data per-*session*. Dengan menerapkan algoritma tersebut diharapkan dapat menambah keamanan data untuk data teks pada aplikasi *live chat e-commerce* berbasis web dibandingkan dengan penelitian sebelumnya.

1.2 Rumusan Masalah

Berdasarkan permasalahan yang ada, maka dirumuskan beberapa masalah yang akan diselesaikan, yaitu :

1. Bagaimana melakukan proses modifikasi algoritma Rijndael untuk menambah kompleksitas pada proses enkripsi pesan?
2. Bagaimana cara menerapkan hasil modifikasi algoritma Rijndael pada live chat?

3. Bagaimana cara menguji keamanan pesan yang telah terenkripsi pada sistem aplikasi live chat?
4. Bagaimana hasil perbandingan teori chaos yang akan digunakan antara Logistic Map dan Henon Map?

1.3 Tujuan

Beberapa tujuan yang ingin dicapai oleh peneliti pada penelitian ini adalah sebagai berikut :

1. Memodifikasi algoritma Rijndael untuk menambah kompleksitas pada proses enkripsi pesan pada live chat.
2. Melakukan perbandingan terhadap teori chaos yang digunakan antara Logistic Map dan Henon Map menggunakan *Randomness Test*.
3. Menambah kompleksitas pada keamanan sistem *live chat* dengan mengimplementasikan algoritma Rijndael ke dalam sistem *live chat*.

1.4 Batasan Masalah

Adapun batasan masalah pada penelitian ini, diantaranya:

1. Aplikasi *live chat* berbasis web yang akan dibuat menggunakan bahasa pemrograman PHP.
2. Pengujian modifikasi algoritma Rijndael menggunakan pengujian yang berupa *Avalanche effect*, dan *Randomness test*.
3. Pengujian keseluruhan aplikasi menggunakan teknik pengujian *man-in-the-middle-attack.*

1.5 Sistematika Penulisan Skripsi

Adapun sistematika penulisan skripsi ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi latar belakang mengenai pemilihan tema penelitian, rumusan masalah pada penelitian, batasan masalah pada penelitian, tujuan penelitian yang akan dilakukan, dan sistematika penulisan skripsi.

BAB II TINJAUAN PUSTAKA

Bab ini berisi penjelasan mengenai teori-teori dan konsep algoritma yang digunakan dalam penelitian yang bersifat induktif. Teori-teori yang digunakan antara lain mengenai Komunikasi, Keamanan Informasi, E-Commerce, Live Chat, Kriptografi, AES(Advanced Encryption Standard), Rijndael, RSA, Fungsi Hash, Teori Chaos, dan Brute Force.

BAB III METODOLOGI PENELITIAN

Bab ini berisi penjelasan langkah-langkah yang akan dilakukan dalam penelitian, dan diuraikan dalam bentuk bagan Desain Penelitian dan model pengembangan perangkat lunak yang digunakan yaitu Waterfall.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Bab ini berisi uraian tentang hasil penelitian secara keseluruhan dan, analisis hasil penelitian yang dihasilkan dari proses pengujian menggunakan Avalanche Effect, Randomness Test dan serangan Brute Force.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari keseluruhan penelitian yang telah dilakukan, serta saran dari penulis untuk kegiatan penelitian selanjutnya terkait dengan topik yang sedang dibahas.