BAB 1
PENDAHULUAN

Dalam bab ini akan dibahas latar belakang dilaksanakannya penelitian, rumusan masalah, tujuan penelitian, batasan masalah, metodologi penelitian dan sistematika penulisan.

1.1 Latar Belakang

Electronic Commerce (*e-commerce*) atau Perdagangan elektronik, adalah penggunaan jaringan komunikasi dan komputer untuk melaksanakan proses bisnis. Pengertian lain dari *e-commerce* adalah menggunakan *internet* dan komputer dengan *browser web* untuk mengenalkan, menawarkan, membeli dan menjual produk. Manfaat dengan penerapan *e-commerce* sebuah perusahaan dapat memiliki sebuah pasar internasional. Bisnis dapat dijalankan tanpa harus terbentur pada batas negara dengan adanya teknologi digital. Biaya operasional dapat ditekan sedikit mungkin. Mempercepat waktu pemrosesan dan mengurangi resiko human error. Mengurangi penggunaan kertas dalam berbagai aktifitas pengerjaan mulai dari mendesain, memproduksi, pengiriman, pendistribusian hingga marketing (McLeod, 2008) .

Menurut IdEA Asosiasi E-commerce Indonesia, Indonesia adalah salah satu pasar e-commerce terbesar di Asia Tenggara, dengan jumlah penduduk kurang lebih 248 juta jiwa, dengan 39 juta jiwa yang menggunkan internet, dan yang melakukan transaksi di e-commerce sebesar 5 juta jiwa. Menurut riset yang dilakukan BMI (BMI, 2015). di 10 kota dengan 1.213 responden berusia 18 hingga 45 tahun tersebut, industri belanja online di Indonesia akan mengalami pertumbuhan yang semakin kuat di masa depan. BMI Research mencatat bahwa rata-rata pengeluaran belanja online orang Indonesia dalam setahun mencapai Rp 825.000 per orang. Tahun lalu saja, nilai transaksi belanja online orang Indonesia mencapai Rp 21 triliun. Angka ini diproyeksi akan

meningkat signifikan di tahun 2015, yakni hingga mencapai Rp 50 triliun atau meningkat lebih dari dua kali lipat.

Live Chat merupakan salah satu bentuk layanan komunikasi di internet yang menawarkan transmisi instant berbasis teks dari pengirim ke penerima, maka keterlambatan akses visual terhadap pesan yang dikirim tidak akan menghambat arus komunikasi dalam arah apapun. Minat *live customer service chat* dalam *e-commerce* telah berkembang secara signifikan di beberapa tahun terakhir. *Live Chat* membantu komunikasi antara penjual dan pembeli yang memungkinkan penggunanya untuk mengirimkan pesan secara *real time* melalui jaringan internet (Elmorshidy, Applying The Technology Acceptance And Service Quality Models To Live Customer Support Chat For E-Commerce Websites, 2013). Beberapa contohnya *e-commerce* yang sudah menerapkan *Live Chat* adalah Lazada, Bhineka.com, Blanja.com, dan lain sebagainya. Penggunaan layanan *Live chat* ini sangat berguna, untuk menjembatani antara penjual dan pembeli. obrolan yang dilakukan melalui fitur *live chat* ini ialah obrolan yang bersifat informasi mengenai produk yang hendak dibeli pelanggan, komplain mengenai produk, dan lain sebagainya.

Minat *Live chat* untuk penggunaan di situs e-commerce telah berkembang secara signifikan dalam beberapa tahun terakhir. *Live chat* memiliki banyak keuntungan bagi *e-commerce* diantaranya, *live chat* memberikan ruang untuk *customer* bertanya kepada *customer service* secara *real time* untuk meningkatkan tingkat kepuasan *customer*, menghemat uang yang sebelumnya harus menghubungi *customer service* lewat nomor, waktu yang digunakan lebih efisien, dan kemampuannya untuk memberikan hasil kerja manusia dalam website anda (Elmorshidy, 2011). Data yang dimaksud berisi data customer, maupun data yang bersifat penting bagi *e-commerce.* Biasanya didalam obrolan live chat *customer service* atau penjual akan menanyai alamat email, dan id transaksi guna untuk memverifikasi produk yang dibeli oleh pelanggan. Data tersebut merupakan data pelanggan yang harus dilindungi dan bersifat rahasia, resiko yang akan terjadi salah satunya adalah Sniffing yang akan berujung pencurian informasi rahasia terjadi dan akan mengakibatkan

kerugian yang besar bagi customer (Santoso, 2015). Resiko lainnya adalah data yang disimpan di dalam *database* rentan terhadap pencurian data. Untuk memberikan jaminan bahwa data yang bersangkutan akan aman maka teknik yang dilakukan *develop* adalah meningkatkan dan mempromosikan keamanan *live chat*, seperti *firewall* dan teknologi enkripsi (Elmorshidy, M. Mostafa, El-Moughrabi, & Al-Mezen, 2015). Hal tersebut umum terjadi pada saluran publik yang tidak aman. Sang pengendus dapat merekam pembicaraan yang terjadi. Salah satu penyalahgunaan data yang berhasil dicuri yaitu, penyalahgunaan *email.* Pihak yang tidak bertanggung jawab akan melakukan penipuan kepada *email* yang berhasil dicuri dan akan berujung kerugian bagi pemilik *email*. Akses *Chatting* tidak hanya harus terlihat pada saat dibutuhkan, tetapi juga harus menyampaikan kepercayaan kepada pengguna (Arrazola, Hererra, Mothias, & Marcos, 2013). Beberapa faktor dapat dikurangi dengan adanya interaksi antar pengguna *Live chat,* seperti pemilihan produk, proses *checkout* yang membingungkan, mengatasi *customer* yang ingin berkomunikasi langsung dengan *customer service,* dan meningkatkan pembelian dari *e-commerce* tersebut (D. C. Andrews & Haworth, 2010).

Antisipasi yang akan dilakukan adalah membuat sebah protokol keamanan alternatif *live chat* dengan menggunakan algoritma kriptografi. Dari beberapa tujuan kriptografi, yang dibutuhkan oleh *live chat* adalah (*Confidentiality*) dan integrasi data (*Data Integrity*) yaitu dengan enkripsi dan fungsi hash. enkripsi data teks dilakukan agar tidak ada penyadap mencuri data teks dan fungsi hash dilakukan agar tidak ada yang merubah data teks tersebut. Enkripsi pada data teks dilakukan sebelum data dikirimkan, sehingga pihak lain yang tidak berhak, tidak dapat memahami data yang dikirimkan meskipun data berhasil diakses. Fungsi Hash digunakan saat mengirim pesan dan menerima pesan, jika nilai hash nya sama maka data plaintext tidak ada perubahan pada saat pengiriman pesan. Kriptografi yang dipakai adalah kriptografi *hybrid* yaitu menggabungkan kriptografi kunci simetri dan asimetri. Kriptografi kunci Simetris, yang akan dibahas pada tugas akhir ini adalah algoritma Rijndael (Daeman & Rijmen, 2002) dan Kriptografi kunci Asimetri yang akan dibahas

adalah Kriptografi RSA. Kedua algoritma ini di kombinasikan karena kunci simetri harus dikirim lewat saluran yang sangat aman agar sampai kepada penerima, inilah salah satu kelemahan dari algoritma simetri. Maka dari itu, untuk menutupi kelemahan dari algoritma Rijindael diperlukan algoritma untuk mengamankan kunci simetri yaitu dengan algoritma kunci public atau RSA. Jadi, kunci simetri dienkripsi menggunakan RSA dan penerima hanya mengirimkan kunci *public* untuk mengenkripsi kunci simetri oleh pengirim, dan penerima mendeskripsi kunci simetri menggunakan kunci *private* nya, dengan begitu kunci simetri aman untuk dikirimkan.

Komunikasi dan Kriptografi adalah dua hal yang sangat berkaitan erat di bidang telekomunikasi. Komunikasi adalah proses pertukaran data dan pesan. Dengan demikian, istilah komunikasi dapat menunjukkan kerjasama, keterbukaan dan lain lain. Namun, komunikasi memang memiliki sifat kompetitif karena banyak persyaratan yang harus ada dalam system komunikasi, yaitu dari bentuk keamanannya, privasi, dan kepercayaan (Blahut, 2014).

Menurut Kalyani dan Prof. Vaishali dalam penelitiannya (Kadam & Khairnar, 2015) mengemukakan Algoritma RSA tidak bisa dipakai untuk data yang berukuran besar, dan AES mempunyai kekhawatiran dalam mengirimkan kunci. Maka dari itu dalam penelitiannya dalam merancang *web service*, harus mempertimbangkan solusi keamanan yang akan mengatasi keterbatasan AES dan RSA. Dan juga untuk menjaga integritas data maka solusinya adalah kombinasi dari algoritma AES dan RSA dengan hasing SHA256. *Hybrid* enkripsi dan deskripsi terjadi antara pengirim dan penerima untuk memastikan bahwa hanya data yang sah akan ditukar dan pada waktu yang sama data tidak dapat dirusak.

Menurut Willy dalam penelitiannya pada tahun 2011 (Setiawan, 2011) mengemukakkan bahwa hasil dari peneletiannya adalah menganalisa perbandingan algoritma Twofish dan algoritma Rijndael, dengan plainteks dan kunci yang sama, telah terbukti bahwa algoritma Twofish lebih cepat yaitu 0.015 detik, dan algoritma Rijndael 0.016 detik. Tetapi pada perbedaan memori

terlihat bahwa Rijndael menggunakan memori yang lebih sedikit dibandingkan dengan Twofish yaitu Rijndael 385.488 byte sedangkan Twofish 480.896 byte. Perbedaan itu cukup terlihat ketika menggunakan mesin dengan memori dengan ukuran yang rendah. Sehingga, dapat disimpulkan bahwa Rijndael merupakan algoritma yang lebih baik untuk digunakan dalam melakukan enkripsi.

Pada tahun 2011 beberapa peneliti mengemukakan bahwa menemukan adanya celah pada enkripsi AES yang memungkinkan memecahkan kunci rahasia lebih cepat dari sebelumnya. Walaupun AES dinyatakan telah melalui berbagai macam tes seperti yang dikemukakan Daeman dan Rijndael. Peneliti akan melakukan modifikasi pada Rijndael yang sudah ada. Dan panjang kunci yang dipilih adalah Rijndael 256 *bits*, karena Rijndael 256 *bits* mempunyai ekspansi 14 putaran dan memiliki kompleksitas lebih tinggi dibandingkan yang lainnya. Untuk menambahkan kompeksitas peneliti akan memodifikasi Rijndael yang mengacu pada prinsip Shannon yaitu *Confusion* dan *Diffusion*. Untuk *Confusion* yang akan dimodifikasi adalah S-Box, dan *Diffusion* yang akan dimodifikasi *ShiftRow*, menurut penelitian yang sudah dilakukan tahun 2015 (Prasetyo, Judhie Putra, & Ramadhan, 2016). Karena menurut Claude Shanon (Shannon, 1949), algoritma enkripsi yang baik harus memiliki dua sifat operasi yaitu *Confusion* dan *Diffusion.*

Berdasarkan masalah dan studi literatur diatas maka penulis akan membuat sebuah protokol keamanan alternatif pada aplikasi *Live chat* berbasis web, dengan mengimplementasikan algoritma Rijndael termodifikasi untuk mengenkripsi dan deskripsi pesan teks dengan menggunakan algoritma RSA untuk pertukaran kunci simetri agar kunci simetri dapat dikirimkan dengan aman. Proses enkripsi dilakukan sebelum pesan dikirim, dan deskripsi dilakukan setelah pesan diterima. Kunci untuk mengenkripsi dan deskripsi pesan di enkripsi lagi menggunakan algoritma RSA untuk mengamankan pengriman kunci. Untuk fungsi hash dilakukan sebelum pesan dikirim, dan setelah pesan diterima, lalu dibandingkan jika hasil hash sama maka tidak terjadi perubahan data jika tidak sama maka pesan telah terjadi perubahan.

Dengan demikian, menyulitkan pihak ketiga mencuri dan mengubah informasi yang terdapat pada pesan teks tersebut.

Dengan menerapkan algoritma Rijndael termodifikasi, RSA dan SHA256, maka diharapkan akan membuat keamanan data untuk data teks di aplikasi *Live chat* berbasis web dapat berjalan dengan baik dan bisa mengatasi masalah yang ada.

1.2 Rumusan Masalah

Berdasarkan permasalahan-permasalahan yang muncul, maka dirumuskan beberapa masalah yang ingin diselesaikan, yaitu :

1. Bagaimana melakukan proses modifikasi algoritma Rijndael untuk enkripsi deskripsi terhadap pesan teks ?
2. Bagaimana mengimplementasikan algoritma Rijndael, RSA, dan fungsi hash ke dalam aplikasi *Live Chat* berbasis Web?
3. Bagaimana menguji keamanan pesan yang telah terenkripsi oleh aplikasi *Live Chat* tersebut ?
4. Bagaimana membuktikan keaslian pesan yang dikirimkan melalui aplikasi *Live Chat?*

1.3 Tujuan

Beberapa tujuan yang ingin dicapai pada penelitian ini sebegai berikut :

1. Memahami Algoritma Rijndael, RSA dan SHA256.
2. Mendapatkan proses modifikasi algoritma Rijndael.
3. Melakukan pengujian terhadap modifikasi algoritma Rijndael.
4. Memberikan cara pengimplementasian algoritma Rijndael, RSA, dan fungsi hash ke dalam aplikasi *Live Chat* berbasis Web.
5. Melakukan pengujian keamanan aplikasi *Live Chat* yang sudah dibuat menggunakan *Man-in-the-Middle-Attack.*

1.4 Batasan Masalah

Beberapa batasan masalah yang dilakukan dalam penelitian ini :

1. Algoritma kriptografi yang digunakan adalah Algoritma Rijndael, RSA, dan SHA256.
2. Modifikasi algoritma Rijndael hanya dalam *S-Box* dan *ShiftRow*.
3. Proses enkripsi dilakukan sebelum data dikirimkan.
4. Kunci simetri di enkripsi menggunakan Algoritma RSA.
5. Fungsi hash digunakan sebelum pesan dikirim dan sebelum pesan diterima, guna untuk memvalidasi keaslian data.
6. Proses deskripsi dilakukan sesudah data diterima.
7. Data yang di enkripsi merupakan pesan *Live chat* sebagai layanan *customer service* di *e-commerce*.
8. Aplikasi chat berbasis web dibuat dengan Bahasa pemograman PHP.
9. Pengujian modifikasi algoritma Rijndael berupa pengujian *Avalanche effect, Randomness test.*
10. Pengujian keseluruhan aplikasi menggunakan teknik *Man-in-the-middle-attack.*

1.5 Struktur Organisasi Skripsi

Adapun sistematika penulisan skripsi ini adalah sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian yang akan dilakukan, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi penjelasan tentang teori-teori dan konsep algoritma yang digunakan dalam penelitian.

BAB III METODOLOGI PENELITIAN

Bab ini berisi penjelasan langkah-langkah yang akan dilakukan dalam penelitian.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Bab ini berisi uraian tentang hasil penelitian dan pembahasan terhadap hasil penelitian yang dilakukan.

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.