BAB I
PENDAHULUAN

1.1 Latar Belakang

Pertukaran data berbasis komputer menghasilkan satu komputer saling terkait dengan komputer lainnya dalam sebuah jaringan komputer. Perkembangan teknologi jaringan komputer ini tidak hanya membuka banyak peluang dalam pengembangan aplikasi transmisi antar komputer, tetapi juga akan membuat peluang adanya ancaman terhadap pencurian, penyadapan dan pemalsuan data dan informasi. Media komunikasi sebagai alat pengiriman data atau informasi yang melintasi jaringan publik seperti internet ataupun jaringan lokal diasumsikan dapat diakses oleh siapapun termasuk orang-orang atau pihak-pihak yang memang berniat untuk mencuri, menyadap atau mengubah data. Untuk melindungi data terhadap pencurian, penyadapan dan pemalsuan yang dilakukan oleh pihak yang tidak berwenang, piranti keamanan data yang melintas di jaringan komputer harus disediakan.

Data yang ditransmisikan melalui jaringan sebagai sarana umum harus terjamin keamanannya, apalagi untuk data atau informasi penting yang bersifat sangat rahasia dan seringkali menjadi target bagi para penyerang. Tidak adanya mekanisme pengamanan dapat menyebabkan data ini diketahui dan dirusak oleh pihak yang tidak berhak. Bentuk ancaman yang dilakukan oleh penyerang dapat berupa ancaman pasif (*passive attack*), yaitu dengan sengaja mengambil, membaca dan menampilkan data, dan ancaman aktif (*active attack*), yaitu memodifikasi bahkan memalsukan data yang tersimpan dalam basis data (Meyer, 1982).

Salah satu data yang harus terjamin keamanannya adalah pajak, karena pajak menyangkut tentang transaksi keuangan dimana transaksi keuangan merupakan informasi yang sensitif untuk diketahui oleh pihak yang tidak berwenang atas data keuangan itu sendiri. Pelaporan data pajak yang ditransmisikan melalui jaringan ini rentan adanya pencurian ataupun penyadapan

oleh pihak-pihak yang tidak berhak untuk mengetahui data tersebut. Hal ini dapat terjadi dikarenakan data pajak yang ditransmisikan melewati jaringan tidak disertai mekanisme keamanan data pajak tersebut.

Untuk mengatasi masalah keamanan transmisi data pajak tersebut, maka perlu dibuat suatu metode yang dapat melakukan pengamanan data selama dalam jaringan, salah satu caranya dengan mengimplementasikan teknik kriptografi. Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (Schenier, 1996). Sistem kriptografi terdiri dari algoritma kriptografi, plainteks, chiperteks, kunci. Algoritma kriptografi adalah aturan untuk melakukan proses enkripsi yaitu proses menyandikan dari plainteks menjadi chiperteks dan proses dekripsi yang merupakan kebalikan dari enkripsi.

Algoritma kriptografi terbagi menjadi algoritma kriptografi simetri dan algoritma kriptografi asimetri. Algoritma simetri yaitu algoritma kriptografi yang setiap proses enkripsi maupun dekripsi data secara keseluruhan menggunakan kunci yang sama. Algoritma simetri memiliki kelebihan yaitu ringan dalam proses pengenkripsian, namun memiliki kelemahan dalam pendistribusian kunci.

Sedangkan algoritma kriptografi asimetri yaitu algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Skema ini disebut juga sebagai sistem kriptografi kunci publik karena kunci untuk enkripsi dibuat untuk diketahui oleh umum (*public key*), tapi untuk proses dekripsinya hanya dapat dilakukan oleh yang berwenang yang memiliki kunci rahasia untuk mendekripsinya yang disebut *private key*. Algoritma asimetri memiliki kelebihan dalam masalah keamanan pada distribusi kunci dapat lebih baik, namun memiliki kekurangan yaitu proses enkripsi dan dekripsi data umumnya lebih lambat daripada sistem simetri, karena enkripsi dan dekripsi menggunakan bilangan yang besar dan melibatkan operasi perpangkatan yang besar.

Untuk menutupi kelemahan masing-masing algoritma, maka digunakanlah metode kriptografi *hybrid.* Kriptografi *hybrid* adalah metode gabungan antara algoritma simetri dan algoritma asimetri dengan memanfaatkan kelebihan dari masing-masing algoritma yang dipilih.

Beberapa penelitian yang mengangkat topik tentang kriptografi *hybrid* yaitu penelitian tentang "Aplikasi Kriptografi Untuk Pengamanan E-Dokumen dengan Metode *Hybrid*" (Ana Wahyuni, 2011) melakukan pengkombinasikan biometrik tanda tangan dan DSA untuk mengamankan e-dokumen menggunakan tanda tangan digital. Penelitian ini menghasilkan e-dokumen, tandatangan *digital* dan kunci publik ditransmisikan lewat internet via *e-mail* pada pihak *verifier*. Kemudian pihak *verifier* memverifikasi apakah hasilnya *valid* artinya e-dokumen tersebut masih otentik/ utuh dan pengirim adalah *signer* sebenarnya dari e-dokumen tersebut. Sebaliknya jika hasilnya tidak valid artinya e-dokumen tersebut sudah tidak otentik/ utuh dan atau pengirim bukanlah *signer* sebenarnya dari e-dokumen tersebut.

Kemudian penelitian tentang "*Securing E-Mail Communication Using Hybrid Cryptosystem on Android-based Mobile Devices*" (Teddy Mantoro dan Andri Zakariya, Desember 2012) melakukan pengamanan komunikasi e-*mail* pada perangkat mobile berbasis android menggunakan *hybrid cryptosystem* dengan mengkombinasikan enkripsi simetrik, asimetrik dan fungsi *hash*. Hasil eksperimen menunjukkan bahwa metode yang diusulkan dapat memenuhi seluruh aspek keamanan informasi yang meliputi kerahasiaan, integritas data, otentikasi dan tidak dapat dilakukan penyangkalan.

Maka dalam penulisan tugas akhir ini, digunakan metode kriptografi *hybrid* dengan menggabungkan algoritma simetri *Rijndael* dan algoritma asimetri RSA. Algoritma simetri *Rijndael* dipilih karena kestabilan, ringan dan tingkat keamanannya tinggi (Afdal Yulius, 2008). Sedangkan algoritma asimetri RSA dipilih karena algoritma yang *powerful* dan cukup aman sebagai algoritma kunci publik (Munir, 2006).

Secara teknis, proses dari metode kriptografi *hybrid* adalah algoritma asimetri RSA hanya ditujukan sebagai *key exchange session* (sesi pertukaran kunci) dalam arti untuk menyepakati dan saling bertukar kunci rahasia yang akan digunakan saat berkomunikasi. Pasangan kunci publik dari algoritma asimetri RSA digunakan untuk enkripsi kunci algoritma simetri *Rijndael*, sedangkan pasangan kunci privat digunakan untuk dekripsi kunci algoritma simetri *Rijndael*. Algoritma simetri *Rinjdael* berfungsi untuk mengenkripsi plainteks pesan

menggunakan kunci *Rijndael* yang kemudian akan didekripsi dengan kunci yang sama dengan kunci pengenkripsi. Algoritma simetri *Rijndael* yang akan digunakan untuk pengamanan plainteks selama komunikasi didalam jaringan. Penerapan metode kriptografi *hybrid* dilakukan dengan membuat modul pengenkripsi dan modul pendekripsi pada sumber dan tujuan.

Diharapkan dengan mengimplementasikan metode kriptografi *hybrid* dapat meningkatkan keamanan transmisi data dari ancaman seperti tersebut diatas tanpa mengurangi performa transmisi data secara signifikan.

1.2 Rumusan Masalah

Permasalahan yang akan diselesaikan dalam tugas akhir ini adalah bagaimana mengimplementasikan metode kriptografi *hybrid* untuk pengamanan transmisi data perpajakan RSUD Bangkinang.

1.3 Batasan Masalah

Dalam pelaksanaan tugas akhir ini ditetapkan beberapa batasan yang akan dijadikan pedoman dalam pelaksanaan tugas akhir. :

1. Sistem ini hanya melakukan enkripsi dan dekripsi terhadap data pajak selama transmisi.
2. Metode yang digunakan dalam pengamanan transmisi ini yaitu metode kriptografi *hybrid* dimana algoritma simetri *Rijndael* sebagai algoritma pengenkripsian data pajak dan algoritma asimetri RSA sebagai pengenkripsian kunci *Rijndael*.
3. Sistem tidak mengatur tempat penyimpanan pasangan kunci RSA. Sistem hanya mengamankan data pajak dan data kunci *Rijndael* selama transmisi.

1.4 Tujuan Penelitian

Tujuan penulisan tugas akhir ini adalah mengimplementasikan pengamanan transmisi data pajak menggunakan metode kriptografi *hybrid*.

1.5 Sistematika Penulisan

BAB I Pendahuluan

Pada bab ini berisi penjelasan latar belakang, rumusan masalah, batasan penelitian, tujuan penelitian, dan sistematika penulisan.

BAB II Landasan Teori

Pada bab ini berisi penjelasan mengenai dasar teori teknologi yang digunakan dalam melaksanakan penelitian dalam tugas akhir ini meliputi keamanan jaringan, kriptografi, dan metode kriptografi *hybrid*.

BAB III Metodologi Penelitian

Bab ini membahas langkah-langkah yang dilaksanakan dalam proses penelitian, yaitu tahapan penelitian, studi literatur, studi lapangan, perumusan masalah, pengumpulan data, identifikasi permasalahan, perancangan perangkat lunak, implementasi, pengujian sistem.

BAB IV Analisa dan Perancangan

Bab ini berisi pembahasan mengenai kebutuhan sistem, yang terdiri dari analisa masalah, analisa aplikasi pajak RSUD Bangkinang, analisa kebutuhan, analisa input, analisa proses, analisa output, analisa kebutuhan antarmuka, analisa fungsional, analisa data, analisa penerapan metode kriptografi *hybrid*, perancangan basis data, perancangan modul perangkat lunak, dan perancangan antarmuka.

BAB V Implementasi dan Pengujian

Bab ini menjelaskan mengenai implementasi penelitian yang dilakukan dengan melakukan berbagai evaluasi dan perbaikan yang dirasa perlu berdasarkan hasil penelitian.

BAB VI Kesimpulan dan Saran

Bab ini membahas mengenai kesimpulan yang dapat diambil dari penelitian dan saran yang diperoleh untuk pengembangan lebih lanjut.