BAB I
PENDAHULUAN

A. LATAR BELAKANG MASALAH

Perkembangan teknologi saat ini semakin hari kian meningkat dengan cepat. Hal itu tentunya dapat membawa kemudahan bagi manusia dalam melakukan kegiatan sehari-hari. Begitupun dengan jaringan komputer yang berkembang mengikuti arus teknologi yang terus berinovasi. Dalam mengikuti perkembangan teknologi, saat ini banyak bidang yang membutuhkan sebuah jaringan komputer. Jaringan komputer yang baik memberikan kemudahan pengguna untuk melakukan komunikasi data antar pengguna dan dapat dilakukan dengan mudah dan cepat. Oleh karena itu efektifitas dan efisiensi bisa dicapai dan meningkatkan produktifitas lebih tinggi.

Komunikasi data adalah proses pengiriman data atau informasi dari suatu sumber disebut *source* sedangkan ke tujuan disebut *destination*. Komunikasi data dapat dilakukan antara dua jenis komputer atau lebih yang jenisnya sama ataupun berbeda. Komunikasi data dapat berjalan dengan baik jika mengacu pada aturan atau standar yang direkomendasikan oleh badan internasional utama yang mengaturnya. Komunikasi data merupakan bagian vital dari suatu masyarakat informasi karena sistem ini menyediakan infrastruktur yang memungkinkan komputer-komputer dapat berkomunikasi satu sama lain. Data yang dimaksud disini adalah sinyal-sinyal *elektromagnetik* yang dibangkitkan oleh sumber data yang dapat ditangkap dan dikirimkan ke terminal atau *device* penerima. Agar data dapat dikomunikasikan dengan baik, maka harus terpenuhi model komunikasi. Model komunikasi dalam komunikasi data terdiri dari sumber *(source),* pemancar *(transmitter),* sistem transmisi *(transmision sistem),* penerima *(receiver),* dan tujuan *(destination)* (Handika dan Imam Riyadi, 2014,p.12).

Adanya manfaat dari perkembangan teknologi komunikasi dan informasi juga dapat dirasakan seiring dengan semakin berkembangnya sistem komunikasi dalam komputer. Komputer sebagai salah satu bukti adanya perkembangan teknologi pastinya sudah tidak asing lagi dalam kehidupan sehari-hari. Bahkan dengan berkembangnya literasi media dan komunikasi masa seperti internet yang dapat memudahkan mencari informasi juga menjadikan komputer sebagai sarana teknologi informasi dan komunikasi yang menjanjikan. Oleh sebab itu, pembahasan mengenai sistem komunikasi dalam komputer menarik untuk dibahas. Sistem komunikasi sendiri sebenarnya merupakan gabungan dari adanya perangkat keras dan perangkat lunak yang dicipatakan untuk

menyampaikan informasi atau komunikasi dari satu lokasi ke lokasi yang lainnya. Perkembangan sistem komunikasi tersebut juga berpengaruh pada perkembangan teknologi komunikasi dalam komputer. Komputer juga dianggap menjadi suatu komponen yang penting dalam sistem komunikasi. Hal ini dikarenakan komputer memiliki peran penting dalam proses perubahan data menjadi informasi. Oleh sebab itu, jenis teknologi komunikasi dalam komputer juga beragam.

Selain itu, hal yang mendasar dari teknologi komunikasi dan informasi adalah standar. Sementara itu, perkembangan jaringan amat membutuhkan sebuah standar sistem operasional. Ketika seseorang menggunakan jaringan untuk berkomunikasi dengan orang lain, maka sesungguhnya dia secara tidak langsung membutuhkan sistem yang kompatibel antara satu dengan lainnya.. Keterikatan antara standar, jaringan dan sistem ibarat perekat dalam menunjang komunikasi bersama (Amar, 2012,p141).

Virtual Private Network (VPN) adalah cara untuk mensimulasikan jaringan privat melalui jaringan publik, seperti internet. Disebut "*virtual*" karena bergantung pada penggunaan *virtual* yaitu koneksi, koneksi sementara yang tidak memiliki kehadiran fisik secara nyata, tetapi terdiri dari paket diarahkan melalui variasi mesin di internet secara *ad-hoc*. Koneksi *virtual* yang aman yang dibuat antara dua mesin, mesin dan jaringan, atau dua jaringan. Teknologi *Virtual Private Network (VPN)* memiliki kemampuan untuk melakukan autentikasi terhadap sumber pengirim data yang akan diterima. *Virtual Private Network (VPN)* akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi *source* datanya. Alamat *source* data ini akan disetujui jika proses autentikasinya berhasil. Dengan demikian, *Virtual Private Network (VPN)* menjamin semua data yang dikirim dan diterima oleh *client* berasal dari sumber yang semestinya. Tidak ada data yang dipalsukan atau dikirimkan oleh pihak-pihak lain.

Seiring dengan maraknya penggunaan internet, banyak perusahaan yang kemudian beralih menggunakan internet sebagai bagian dari jaringan mereka untuk menghemat biaya. Akan tetapi permasalahan keamanan masih menjadi faktor utama dalam *relabilitas* suatu jaringan. *Virtual Private Network (VPN)* merupakan salah satu cara yang dapat digunakan untuk membuat jaringan yang bersifat *private* dan koneksi jarak jauh (*remote access*) dengan tingkat keamanan yang tinggi diatas jaringan publik dan internet.

Layanan *VPN* didukung oleh beberapa protokol komunikasi data, yang mana tiap protokol tersebut memiliki konsep keamanan yang berbeda-beda. Berikut jenis setiap *VPN*. *Point to Point Transfer Protocol (PPTP), Layer 2*

Transfer Protocol (L2TP), Internet Protocol Security (IPSec), Internet Key Exchange (IKEv2), Secure Socket Tunneling Protocol (SSTP).

Dalam merancang dan implemntasi *VPN* pada sebuah jaringan nirkabel karyawan dapat dengan mudah memperoleh data ataupun informasi dari internet dengan tetap memastikan bahwa kerahasiaan dari data yang sensitif dapat terjaga pada saat transmisi. Sehingga dibangun sebuah sistem baru dengan mempertimbangkan beberapa aspek keamanan dan hak akses. Sistem tersebut yaitu *Virtual Private Network* (*VPN*) yang memberikan fungsi dalam menjaga kerahasiaan data (*Confidentiality)*, keutuhan data (*Data Integrity)* serta otentikasi sumber (*Origin Authentication)* (Sahari, 2008, pp.47-48).

Tunnel adalah dasar dari *VPN* untuk membangun jaringan *private* melalui jaringan internet, dan jika diterjemahkan *tunnel* artinya adalah terowongan. Sesuai dengan namanya *tunnel* merupakan sebuah terowongan khusus yang didalamnya dapat dilewati oleh data yang akan dikirim dan data tersebut dapat sampai ke tujuan tanpa terganggu oleh data lain yang dilewatinya. *tunneling* merupakan teknologi yang bertugas untuk manangani dan menyediakan koneksi *point-to-point* dari sumber ke tujuannya. Koneksi *point-to-point* tersebut sebenarnya terbentuk dengan melintasi jaringan umum, namun koneksi tersebut tidak mempedulikan paket data milik orang lain yang sama-sama melintasi pada jaringan publik, tetapi koneksi tersebut hanya melayani komunikas data dari pembuatnya. Hal ini sama dengan penggunaan jalur busway yang pada dasarnya menggunakan jalan raya, tetapi dia membuat jalur sendiri untuk dapat dilalui bus khusus. Koneksi *point-to-point* ini sesungguhnya tidak benar-benar ada, namun data yang dihantarkannya terlihat seperti benar-benar melewati koneksi pribadi yang bersifat *point-to-point* (Amar, 2012,p.188).

Gambar 1.1 Manfaat Jaringan Intranet
(Sumber : IDCloudHost)

Intranet adalah sebuah jaringan privat *(private network)* yang menggunakan protokol-protokol *internet (TCP/IP),* untuk membagi informasi rahasia perusahaan atau operasi dalam perusahaan tersebut kepada karyawannya. Terkadang istilah *intranet* hanya merujuk kepada layanan yang terlihat, yakni situs *web* internal perusahaan. Deskripsi lain yang digunakan untuk implementasi teknologi *internet* global. Perbedaan mendasar antara *internet* dan *intranet* adalah bahwa *internet* menyediakan akses tidak terbatas terhadap setiap pengguna di seluruh dunia, sedangkan akses ke *intranet* dibatasi oleh organisasi operasi itu sendiri atau dalam arti dengan jumlah *user* terbatas. *Intranet* dapat diakses oleh beberapa pemasok dan pelanggan, disamping karyawan di berbagai lokas, tapi *intranet* tidak bisa diakses oleh masyarakat umum. Dijelaskan oleh *Information Week* sebagai *"trend arguably* terpanas di *IT"*, pengembangan *intranet* adalah booming. *Intranet* menawarkan *database* yang terintegrasi dan sistem komunikasi, *e-mail* dan *transfer file.*

Beberapa ahli memprediksi *intranet* pada akhirnya akan menggantikan jaringan perusahaan. Bahkan banyak pengembang perangkat lunak, *vendor* dan konsultan sekarang memfokuskan usaha mereka membangun sistem *intranet.* Dengan *intranet* biaya yang dikeluarkan relatif murah dan cepat, dan memungkinkan semua pengguna dalam suatu perusahaan untuk mengakses informasi dalam format yang sama, terlepas dari platfrom yang digunakan untuk mengakses jaringan. Untuk membangun sebuah *intranet, maka* sebuah jaringan haruslah memiliki bebrapa komponen yang membangun *intranet,* yakni protokol *internet* (protokol *TCP/IP,* alamat *IP,* dan protokol lainnya)*, client* dan juga *server*. protokol *HTTP* dan beberapa protokol *internet* lainnya (*FTP, POP3, dan SMTP)* umumnya merupakan komponen protokol yang sering digunakan.

Umumnya sebuah intranet dpaat dipahai sebagai sebuah "versi pribadi dari jaringan *intranet*", atau sebagai sebuah versi dari *internet* yang dimiliki oleh sebuah organisasi. Perbedaan spesifik nya adalah bahwa *intranet* adalah jaringan lokal *PC to PC (host to host)* dalam satu tempat atau lokasi tertentu, sedangkan *internet* perluasan dari *intranet. Intranet* adalah konsep *LAN* yang mengadopsi teknologi *internet* (mulai tahun 1996). Atau dapat dikatakan *intranet* adalah *LAN* yang menggunakan standar komunikasi dan segala fasilitas *internet,* dengan kata lain ber*internet* dalam lingkungan lokal (Mukhamad, 2011,p.145).

Namun, semakin tingginya penggunaan teknologi informasi di era globalisasi komunikasi ini, semakin meningkat pula risiko yang dihadapi, terutama dari sisi kualitas dan keamanannya. Berbagai ancaman terhadap suatu data atau informasi yang dipertukarkan melalui jaringan internet menuntut suatu solusi keamanan salah satunya dengan menggunakan sertifikat elektronik yang dikeluarkan dan dikelola oleh pihak ketiga terpercaya *(Trusted Third Party)* atau

lazim disebut *CA (Certification Authority). CA* atau dikenal juga dengan istilah sertifikat elektronik menjamin 4 (empat) aspek dalam interaksi data, yaitu kerahasiaan *(confidentiality),* menyangkut kerahasiaan dari data atau informasi, dan perlindungan bagi informasi tersebut dari pihak yang tidak berwenang, Keotentikan *(authenticity),* menyangkut kemampuan seseorang, organisasi, atau komputer untuk membuktikan identitas dari pemilik yang sesungguhnya dari informasi tersebut, integritas *(integrity),* menyangkut perlindungan data terhadap upaya pemodifikasian oleh pihak-pihak yang tidak bertanggung jawab, baik selama data itu disimpan maupun selama data itu dikirimkan kepada pihak lain, dan Nir sangkal *(non repudiation),* menyangkut perlindungan terhadap suatu pihak yang terlibat dalam suatu transaksi (Ahmad, 2015,p.16).

Kriptografi adalah ilmu yang mempelajari teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan *(confidentiality),* integritas *(integrity),* dan otentikasi *(authenticity)*. *Kriptografi* bertujuan agar informasi yang bersifat rahasia dan dikirim melalui suatu jaringan, seperti *intranet* atau *internet* tidak dapat diketahui dan dimanfaatkan oleh orang lain atau pihak yang tidak berkepentingan. *RSA* merupakan *algoritma kriptografi* kunci publik atau sering disebut kunci asimetrik (kunci enkripsi dan kunci dekripsi berbeda) sehingga tidak membutuhkan saluran yang aman untuk distribusi kunci. *RSA* ditemukan oleh tiga peneliti dari *MIT (Massachussets Institute of Technology)*, *yaitu Ronald Linn Rivest, Adi Shamir*, dan *Len Adleman* pada tahun 1977. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima (Albert dkk, 2015,p.254).

CRT (Chinese Remainder Theorem) merupakan suatu algoritma untuk mengurangi perhitungan *aritmatika* modular dengan modulus besar untuk perhitungan yang sama untuk masing-masing faktor dari modulus. *CRT* dapat memperpendek ukuran *bit* eksponen dekripsi d (merupakan kunci publik *RSA* atau *RSA-CRT*) dengan cara menyembunyikan d pada sistem *kongruen* sehingga mempercepat waktu dekripsi serta dapat digunakan bersama *algoritma RSA* yang disebut *RSA-CRT*.

Algoritma RSA menggunakan 2 angka (e dan d) sebagai kunci publik dan kunci privat. Pada *algoritma RSA* e dan n diumumkan untuk umum sedangkan d dirahasiakan. Meskipun *RSA* dapat digunakan untuk mengenkripsi dan mendekripsi pesan, sangat lambat jika pesan tersebut panjang. Oleh karena itu, *algoritma RSA* berguna untuk pesan singkat. Sejak *algoritma* menggunakan 2 kunci untuk *enkripsi* dan *dekripsi*, *algoritma RSA* dianggap sebagai contoh kunci *asimetrik kriptografi.* Sistem *kriptografi RSA* dapat dimodifikasi dengan menggunakan *teorema CRT* disebut dengan *RSA-CRT.* Terbukti sistem *kriptografi RSA-CRT* memiliki waktu komputasi yang lebih singkat dari pada

sistem kriptografi RSA biasa, yaitu sekitar empat kali lebih cepa*t* (Ahmad, 2015,p.16).

Untuk meningkatkan keamanan jaringan intranet dari pihak yang tidak berwenang serta *generate algoritma RSA* dengan menggunakan *teorema CRT* agar dapat dibandingkan dengan algoritma RSA, perlu dibangun jaringan Virtual Private Networ (VPN) dengan mengimplementasikan algoritma kriptografi RSA untuk meningkatkan keamanan jaringan intranet.

B. RUMUSAN MASALAH

1. Identifikasi Masalah

Jaringan *intranet* pada sebuah lembaga atau perusahaan diperlukan untuk menciptakan keamanan dalam proses interaksi data sehingga informasi dan data yang dikirim tepat sasaran. Mengurangi resiko tindakan pencurian informasi dan data yang dapat merugikan lembaga atau perusahaan. Dengan teknologi *Virtual Private Network (VPN)*, dapat menghubungkan pengguna *VPN client* di lokasi yang tidak terjangkau oleh jaringan *intranet* ke dalam jaringan *intranet*. Namun dibutuhkan metode untuk mengamankan data dan informasi yang melewati jaringan komputer *intranet*.

Ketika menyediakan akses kepada *VPN client* secara global, maka faktor keamanan menjadi resiko tersendiri karena informasi sensitif lembaga atau perusahaan dapat diakses dari perangkat mana saja. Oleh karena itu perlu meningkatkan keamanan jaringan *VPN* dari segi pengaturan *user VPN client* dan perangkat *VPN client*. Dengan membangun infrastruktur dan sistem jaringan yang dapat menyesuaikan kebutuhan sebuah lembaga atau perusahan diperlukan untuk keamanan lembaga atau perusahaan.

2. Pernyataan Masalah / *Problem Statement*

Berdasarkan indentifikasi masalah dapat disimpulkan pokok permasalahan adalah lemahnya keamanan pada *VPN* dalam mengautentikasi username dan perangkat *VPN client* yang akan tersambung ke dalam jaringan *intranet*.

3. Pertanyaan Penilitian / *Research Question*

Bagaimana penerapan *Algoritma RSA* pada *VPN* untuk meningkatkan keamanan jaringan *intranet* ?

C. MAKSUD DAN TUJUAN PENGEMBANGAN

1. Maksud

Menerapkan *Algoritma RSA* pada *VPN* untuk meningkatkan keamanan jaringan *intranet*.

2. Tujuan

1. Terciptanya keamanan jaringan dalam jaringan *intranet*
2. Menghubungkan perangkat *VPN client* menggunakan *Algoritma RSA* ke dalam jaringan *intranet*
3. Membangun *Infrastruktur* dan keamanan jaringan intranet

D. SPESIFIKASI HASIL YANG DIHARAPKAN

Melalui penelitian ini diharapkan meningkatnya keamanan interaksi data dan informasi pada jaringan *intranet* dengan menerapkan metode *Algoritma RSA* pada *VPN* dengan spesifikasi sebagai berikut:

1. Menerapkan metode *Algoritma RSA* pada *VPN*.
2. Metode digunakan untuk mengamankan informasi dan data dalam jaringan *intranet*.
3. Metode yang dibuat menggunakan perangkat keras *router*.
4. Pengoperasian metode menggunakan *router* yang *support VPN*.
5. Metode yang digunakan membantu dalam pengembangan jaringan

E. PENTINGNYA PENGEMBANGAN

Dalam rangka proses tukar menukar informasi dan data maka keamanan pada jaringan intranet sangatlah dibutuhkan. Diharapkan dengan penerapan metode *Algoritma RSA* pada *VPN* keamanan pada jaringan *intranet* dapat menjamin informasi dan data tidak mudah diretas dan diakses oleh pihak yang tidak memiliki wewenang.

F. ASUMSI DAN KETERBATASAN PENGEMBANGAN

1. Asumsi

   Pada sebuah jaringan intranet yang telah memiliki jaringan yang luas membutuhkan keamanan yang baik, yang dapat menjaga keamanan dan keutuhan informasi dan data dari pihak-pihak yang tidak memiliki hak akses terhadap informasi dan data internal perusahaan.

2. Keterbatasan pengembangan

   a. Data

      Data yang terdapat pada lembaga atau perusahaan memiliki sensitif untuk dipublikasikan.

b. Alat

Router yang digunakan untuk penilitian harus bisa *multi tasking* untuk menjalankan beberapa *services* yang dibutuhkan.

G. DEFINISI ISTILAH

1. *Algoritma RSA*

   Algoritma RSA merupakan *algoritma kriptografi* kunci publik atau sering disebut kunci asimetrik (kunci enkripsi dan kunci dekripsi berbeda) sehingga tidak membutuhkan saluran yang aman untuk distribusi kunci. *RSA* ditemukan oleh tiga peneliti dari *MIT (Massachussets Institute of Technology)*, *yaitu Ronald Linn Rivest, Adi Shamir*, dan *Len Adleman* pada tahun 1977 (Ahmad, 2015,p.16).

2. *Virtual Private Network (VPN)*

   Virtual Private Network (VPN) adalah cara untuk mensimulasikan jaringan privat melalui jaringan publik, seperti internet (Sahari, 2008, pp.46-54).

3. *Local Area Network (LAN)*

   (Local Area Network (LAN) merupakan suatu jaringan komputer yang masih berada di dalam gedung atau ruangan. Dalam membuat jaringan *LAN,* minimal harus menyediakan dua buah komputer yang masing-masing memiliki kartu jaringan *Lan Card. LAN* digunakan di rumah, perkantoran, industri, akademik, rumah sakit, dan lain sebagainya (Handika dan Riyadi, 2014,p.12).

4. *Wide Area Network (WAN)*

   Wide Area Network (WAN) merupakan jaringan komputer yang mencakup area yang besar sebagai contoh yaitu jaringan komputer antar wilayah, kota atau bahkan negara, atau dapat didefinisikan juga sebagai jaringan komputer yang membutuhkan *router* dan saluran komunikasi publik. *Wide Area Network (WAN)* merupakan bentuk jaringan yang terdiri dari *Local Area Network (LAN)* (Handika dan Riyadi, 2014,p.12).

5. *Intranet*

   Intranet adalah sebuah jaringan privat *(private network)* yang menggunakan protokol-protokol *internet (TCP/IP),* untuk membagi informasi rahasia perusahaan atau operasi dalam perusahaan tersebut kepada karyawannya (Mukhamad, 2011,p.145).