PENERAPAN KEAMANAN EMAIL DENGAN SISTEM PRETTY GOOD PRIVACY MENGGUNAKAN METODE NDLC (STUDI KASUS : POLRES MAJALENGKA)

Suhendri[1], Deffy Susanti[2], Dede Dicky[3]
[1,2,3]Program Studi Informatika, Fakultas Teknik, Universitas Majalengka
Email: [1]suhendri@unma.ac.id, [2]deffysusanti@gmail.com, [3]anandadeky88@gmail.com

ABSTRAK
Aplikasi email merupakan salah satu aplikasi di internet yang berfungsi untuk mengirimkan data baik untuk pribadi maupun perusahaan / institusi. Mengirim email dapat menggunakan teknik lampiran file. Keamanan data dalam proses pengiriman e-mail juga dapat diantisipasi atau diterapkan dengan topologi jaringan yang mempunyai sistem keamanan jaringan dengan metode otentikasi pada jaringan, seperti menggunakan fasilitas keamanan login di hotspot kantor atau instansi. Berdasarkan observasi dan wawancara dengan pihak Polres Majalengka ditemukan bahwa pengiriman data menggunakan e-mail masih menggunakan jaringan dengan topologi jaringan star dan akses internet yang digunakan masih bawaan dari ISP seperti menggunakan produk speedy. Untuk keamanan data yang dikirim menggunakan e-mail dengan teknik file attachment belum menggunakan sistem pengamanan data (enkripsi) yang dimiliki oleh aparat maupun aparat kepolisian.

Kata Kunci: Keamanan, Email, Sistem Pretty Good Privacy, NDLC, Polres Majalengka.

1. PENDAHULUAN

1.1. Latar Belakang

Pada masa era globalisasi dan era teknologi informasi dan komunikasi seperti sekarang ini perkembangan teknologi telekomunikasi dan penyimpanan data yang menggunakan komputer memungkinkan pengiriman data jarak jauh, dan merupakan salah satu metode cepat dan relatif murah. Namun pengiriman data jarak jauh seperti ini yang bisa menggunakan sarana internet melalui jaringan internet seperti fiber optik, gelombang radio, satelit dan media koneksi lainnya, tidak menjamin keamanan pada data pada jaringan tersebut, akan sangat memungkinkan adanya pihak lain yang dapat menyadap dan mengubah data. Sehingga data yang diterima akan merubah atau bahkan akan hilang, tidak diterima oleh penerima.

Aplikasi e-mail adalah salah satu aplikasi di internet yang memiliki fungsi untuk mengirim data baik untuk personal maupun perusahaan/ institusi. Pengirian email bisa menggunakan teknik *file attachment*.Keamanan data pada proses pengiriman email dapat juga diantisipasi atau diterapkan dengan tapologi jaringan yang memiliki sistem keamanan jaringan dengan metode autentikasi pada jaringan tersebut, seperti menggunakan fasilitas keamanan login diarea hotspot kantor atau institusi (Kuswanto, 2017).

Berdasarkan hasil observasi dan wawancara dengan pihak kantor POLRES Majalengka didapat bahwa pengiriman data mengunakan email masih menggunakan jaringan dengan tapologi jarngan star dan akses internet yang digunakan masih bawaan dari ISP seperti menggunakan produk *speedy*. Untuk keamanan data yang dikirim menggunakan email dengan teknik *file atachment*, petugas atau staf kepolisian belum menggunakan sistem keamanan data (*enkripsi)*. Untuk menyelesaikan permasalah di atas maka penulis mendesign tapologi jaringan dengan tambahan mikrotik sebagai lapisan keamanan, dan akan dibatasi pada pengiriman file menggunakan Sistem PGP. Metode NDLC digunakan untuk membantu mengembangan jaringan hotspot di POLRES Majalengka.

Memasuki era teknologi informasi dan komunikasi sekarang ini, berbagai ilmuan dalam bidang ilmu teknologi informasi dan komunikasi ini telah mengembangkan berbagai cara dalam mengatasi permasalahan sistem keamananpada suatu data dan jaringan. Mereka mengembangkan berbagai cara untuk menangkal serangan – serangan yang bisa mengancam keamanan data. Salah satu cara yang ditempuh untuk mengatasi permasalahan diatas adalah dengan menggunakan metode penyandian email/pesan yang disebut sebagai ilmu kriptografi yang menggunakan transformasi data sehingga data yang dihasilkan tidak dapat dimengerti oleh pihak ketiga, dan *autentikasi* pada sistem keamanan jaringannya.

Transformasi ini memberikan solusi pada dua masalah keamanan data, yaitu masalah privasi (*privacy*) dan keautentikan (*authentication*).Privasi mengandung arti bahwa data yang dikirim hanya dapat dimengerti oleh penerima yang sah.Sedangkan keautentikan mencegah pihak ketiga untuk mengirimkan data yang salah atau mengubah data yang dikirimkan. Sehingga pengiriman data akan menjadi lebih aman terhadap serangan dari pihak ketiga yang tidak berhak merubah semua informasi pada data – data tersebut.

1.2. Identifikasi Masalah

Berdasarkan latar belakang diatas maka dapat diidentifikasi beberapa masalah yaitu :

1. Pengiriman data melalui email belum menggunakan sistem keamanan data dengan metode enkripsi.
2. Belum memiliki sistem autentikasi pengguna jaringan untuk pengamanan pada jaringan kantor.

1.3. Rumusan Masalah

Berdasarkan latar belakang di atas, maka rumusan masalah yang akan di bahas adalah sebagai berikut:

1. Bagaimana proses keamanan data pada proses pengiriman email menggunakan media internet?
2. Bagaimana membuat sistem keamanan jaringan pada proses pengiriman email melalui media internet?

1.4. Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut :

1. Memberikan suatu pengamanan data melalui jalur internet sehingga akan dapat mempermudah dan memberikan kenyamanan dalam menggunakan fasilitas internet.
2. Merancang suatu mekanisme untuk melakukan pengamanan data melalui metode *Pretty Good Privacy* (PGP) mengenai masalah Privacy dan Keauntentikan data.

2. TINJAUAN PUSTAKA

2.1. Kajian Pustaka

Tinjauan pustaka merupakan peninjauan kembali pustaka-pustaka yang terkait. Ada beberapa penelitian yang penulis jadikan dasar penelitian saat ini, yaitu:

1. Alamsyah (2011) dalam penelitian yang berjudul "IMPLEMENTASI KEAMANAN E-MAIL DENGAN MENGGUNAKAN PGPTRAY" yang berisi tentang menjaga keamanan data/email dari penyadapan pihak ketiga dengan metode enkripsi.
2. Nahot Frastian (2017) dalam penelitian yang berjudul "IMPLEMENTASI PROTOKOL S/MIME PADA LAYANAN E-MAIL PENINGKATAN JAMINAN KEAMANAN SECARA ONLINE PADA KANTOR PT. TAMMAR FRASTI" yang berisi tentang Penerapan teknik kriptografi berupa tanda tangan digital dan/atau enkripsi yang terbukti dapat memenuhi aspek keamanan informasi dengan metode protokol S/MIME.
3. Nandang Iriandi (2011) dalam penelitan yang berjudul "ANALISIS KEAMANAN EMAIL MENGGUNAKAN PRETTY GOOD PRIVACY" yang berisi tentang Keamanan data/email dari pihak ketiga menggunakan metode Spoofing.
4. Dandy Pramana Hostiadi dan Ida Bagus Suradarma (2017) dalam penelitian yang berjudul "Implementasi Pengamanan PGP pada Platform Zimbra Mail Server" yang berisi tentang Pengamanan komunikasi email, difokuskan pada isi email dengan mengenkripsi teks mail beserta *attachment file* dengan metode enkripsi.
5. Muh Masruri Mustofa dan Eko Aribowo (2013) dalam penelitian yang berjudul "PENERAPAN SISTEM KEAMANAN HONEYPOT DAN IDS PADA JARINGAN NIRKABEL (HOTSPOT)" yang berisi tentang Penerapan sistem keamanan jaringan nirkabel hotspot dengan metode sistem keamanan jaringan hotspot berbasis honeypot dan snort.

2.2. Kriptografi

Kriptografi merupakan seni dan ilmu menyembunyikan informasi daripenerima yang tidak berhak. Kata *cryptography* berasal dari kata Yunani *kryptos* (tersembunyi) dan *graphein* (menulis).Enkripsi dan dekripsi pada umumnya membutuhkan penggunaan sejumlahinformasi rahasia, disebut sebagai kunci. Untuk beberapa mekanisme enkripsi,kunci yang sama digunakan baik untuk enkripsi dan dekripsi, untuk mekanismeyang lain, kunci yang digunakan untuk enkripsi dan dekripsi berbeda. Dua tipedasar dari teknologi kriptografi adalah *symmetric key* (*secret/private key*) *cryptography* dan *asymmetric* (*public key*) *cryptography*. Pada symmetric keycryptography, baik pengirim maupun penerima memiliki kunci rahasia yangumum. Pada asymmetric key cryptography, pengirim dan penerima masingmasingberbagi kunci publik dan privat. (Septy, 2015).

2.3. Konsep Dasar Pretty Good Privacy (PGP)

PGP (*Pretty Good Privacy*) adalah Suatu metode program enkripsi informasi yang memiliki tingkat keamanan cukup tinggi bersifat rahasia dengan menggunakan "Private-Public Key" sebagai dasar autentifikasinya sehingga jangan sampai dengan mudah diketahui oleh orang lain yang tidak berhak.

Pada dasarnya, PGP merupakan program yang digunakan untuk mengenkripsi satu atau lebih dokumen. Dengan PGP tersebut, hanya orang – orang tertentu saja yang bisa membaca file – file enkripsi tersebut. Bagaimana PGP sebagai program enkripsi dokumen bisa digunakan untuk pengiriman e-mail? Sebenarnya, program PGP mengenkripsi isi mail yang kita tulis menjadi sebuah file. File tersebut dibaca oleh program mail yang kemudian dikirimkan ke tujuan. Penerima e-mail harus menyimpan mail tersebut ke dalam sebuah file. File tersebut dideskripsi sehingga isi mail aslinya akan terlihat. Jadi, mail yang dikirimkan adalah dalam bentuk terenkripsi sehingga tidak dapat dibaca

dengan mudah oleh orang – orang yang tidak memiliki akses membaca mail tersebut.

PGP (*Pretty Good Privacy*) dibuat dengan berdasarkan konsep Private Key Cryptography sebagai dasar otorisasinya. *Private Key Cryptography* ini digunakan untuk mengenkripsi dalam suatu hubungan komunikasi antara dua mesin. Dalam menjaga kerahasiaan data, kriptografi mentransformasikan data jelas (plaintext) ke dalam bentuk data sandi (*ciphertext*) yang tidak dapat dikenali. *Ciphertext* inilah yang kemudian dikirimkan oleh pengirim (*sender*) kepada penerima (*receiver*). Setelah sampai di penerima, *ciphertext* tersebut ditranformasikan kembali ke dalam bentuk plaintext agar dapat dikenali. Sehingga dalam penulisannya lebih dikenal dalam bentuk enkripsi (*encryption*) dan deskripsi (*descryption*).

Enkripsi (*encryption*) merupakan suatu proses di mana sebuah pesan (*plaintext*) ditranformasikan atau diubah menjadi bentuk pesan lain (*chipertext*) menggunakan suatu fungsi matematis dan enkripsi password khusus yang lebih dikenal sebagai key. Sementara Deskripsi (*descryption*) merupakan proses kebalikan, dari *chiphertext* dirubah kembali ke plaintext dengan menggunakan fungsi matematis dan key. Pada saat kita membuat kunci, PGP akan menciptakan duah buah kunci yaitu *private key* dan *public key* yang merupakan sebuah pasangan bersesuaian. *Private Key* adalah kunci yang hanya diketahui oleh kita sendiri sedangkan *Public Key* adalah kunci yang kita beritahukan kepada orang – orang yang kita percaya. Public key digunakan sebagai dasar proses pengenkripsian dokumen – dokumen yang hanya bisa dibuka oleh orang yang memiliki private key yang bersesuaian (Raka Yusuf, 2010).

2.4. Prinsip Kerja PGP

PGP bekerja dengan menggabungkan beberapa bagian yang terbaik dari key konvensional dan public key cryptography, jadi PGP ini adalah sebuah a hybrid cryptosystem. Ketika seorang pengguna mengenkrip sebuah plaintext dengan menggunakan PGP, maka awal PGP akan mengkompress plaintet ini. Data yang dikompress menghebat waktu dan media transmisi dan lebih penting adalah keamanan kriptograpik yang kuat. Kebanyakan teknik analisis sandi mengeksplotasi pola yang ditemukab dalam plaintext untuk men-crack chipernya. Kompressi mengurangi pola-pola ini dalam plaintext, dengan cara demikian perbaikan yang lebih baik untuk menghambat analisa kode-kode.

PGP membuat sebuah session key, dimana sebuah kunci rahasia pada saat itu. Kunci adalah sebuah bilangan acak yang dihasilkan dari gerakan acak dari mouse dan tombol yang anda tekan. Session Key ini berkerja dengan sangat aman, algoritma enkripsi konvesional yang cepat untuk meng-enkrip plaintext. Hasilnya adalah berupah chiper text. Sekali data dienkripsi, lalu session key ini dienkripsi lagi menggunakan kunci publik penerima. session key yang terenkripsi kunci publik key penerima dikirim dengn chipertext ke penerima (Nandang, 2011)

2.5. Definisi *SMS Gateway*

Menurut Mulyani (2012:07), SMS gateway merupakan sistem aplikasi untuk mengirim dan atau menerima SMS, terutama digunakan dalam aplikasi bisnis, baik untuk kepentingan promosi, service kepada customer, pengadaan content produk atau jasa, dan seterusnya. Karena merupakan sebuah aplikasi, maka fitur-fitur yang terdapat didalam SMS gateway dapat dimodifikasi sesuai dengan kebutuhan, beberapa fitur yang umum dikembangkan dalam aplikasi SMS gateway.

Menurut Ibrahim (2011:86), SMS Gateway adalah sebuah perangkat lunak yang menggunakan bantuan komputer dan memanfaatkan teknologi seluler yang diintegrasikan untuk mendistribusikan pesan-pesan yang di generate lewat sistem informasi melalui media SMS yang ditangani oleh jaringan seluler.

Dari defini di atas, maka dapat disimpulkan bahwa sms gateway adalah sebuah system aplikasi untuk mengirim atau meneima sms dengan menggunakan bantuan komputer untuk mendistribusikan pesan-pesan yang di generate lewat sistem informasi melalui media SMS yang ditangani oleh jaringan seluler.

2.6. Electronic Mail (E-mail)

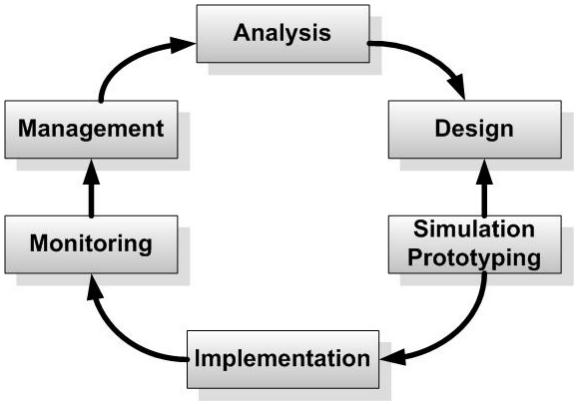
Electronic Mail (*E-mail*) adalah aplikasi yang paling banyak digunakan di internet. Hal ini karena e-mail merupakan alat komunikasi yang paling murah dan cepat. Dengan e-mail kita dapat berhubungan dengan siapasaja yang terhubung ke internet di seluruh dunia dengan biaya relatif terjangkau. Menurut Djoko Purwanto (2008: 170) "Surat elektronik atau *electronic mail* (e-mail) adalah salah satu bentuk atau cara pengiriman surat, informasi, atau pesan (bisnis dan nonbisnis) yang dilakukan secara elektronik, tanpa kertas, dan tanpa jasa pengirim." Sedangkan menurut John J. Stallord (1990: 118) "Surat elektronik didefinisikan sebagai komunikasi pesan nonverbal dari seseorang ke orang lain dengan memakai media penyampaian (*transmission*) elektronik."

Konsep e-mail adalah seperti kita mengirim surat dengan pos biasa, di mana kitamengirimkan ke pos dengan beralamatkan tempat yang kita tuju. Dari pos tersebutakan disampaikan ke pos yang terdekat dengan alamat yang dituju dan akhirnyasampai ke alamat tersebut. Penerima hanya membuka kotak posnya saja yang adadi depan rumah sedangkan pengirim tidak tahu apakah orang yang dituju

tersebutsudah menerima surat tersebut, sampai surat itu dibalas. Dengan e-mail datadikirim secara elektronik sehingga sampai di tujuan dengan sangat cepat. Kitajuga dapat mengirim file-file seperti program, gambar, grafik dan sebagainya, dandapat mengirim ke lebih dari satu orang sekaligus dalam satu masa (Raka Yusuf, 2010).

2.7. *Network Development Life Cycle* (NDLC)

Menurut Goldman dan Rawles (2004:470) *Network Development Life Cycle* (NDLC) adalah metode yang dapat digunakan untuk mengembangkan suatu jaringan komputer. Adapun tahapan yang terdapat dalam metode NDLC adalah sebagai



Gambar 1. Network Development Life Cycle (James E. Goldman,Philips T. Rawles,2004:470)

1. *Analysis*

Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan user, dan analisa topologi / jaringan yang sudah ada saat ini. Metode yang biasa digunakan pada tahap ini adalah.

a. Wawancara, dilakukan dengan pihak terkait melibatkan dari struktur manajemen atas sampai ke level bawah / operator agar mendapatkan data yang konkrit dan lengkap.
b. Observasi, pada tahap analisis juga biasanya dilakukan survei langsung kelapangan untuk mendapatkan hasil sesungguhnya dan gambaran seutuhnya sebelum masuk ke tahap design.
c. Membaca manual atau blueprint dokumentasi, pada analisis awal ini juga dilakukan dengan mencari informasi dari manual-manual atau blueprint dokumentasi yang mungkin pernah dibuat sebelumnya.

2. *Design*

Design dapat berupa design struktur topologi jaringan, design akses data, design tata layout perkabelan, dan sebagainya yang akan memberikan gambaran jelas tentang project yang akan dibangun. Biasanya hasil dari design berupa.

a. Gambar-gambar topologi (server farm, firewall, datacenter, storages, lastmiles, perkabelan, titik akses)
b. Gambar-gambar detil estimasi kebutuhan yang ada.

3. *Simulation / Prototype*

Pada tahap ini beberapa pengembang jaringan akan membuat rancangan dalam bentuk simulasi dengan bantuan tools khusus di bidang network seperti visio, boson, packet tracert, netsim. Hal ini dimaksudkan untuk melihat kinerja awal dari network yang akan dibangun dan sebagai bahan presentasi dan sharing dengan team work lainnya.

4. *Implementation*

Dalam fase implementasi, pengembang jaringan akan menerapkan semua yang telah direncanakan pada tahap design. Implementasi merupakan tahapan yang sangat menentukan berhasil / gagalnya suatu project yang akan dibangun.

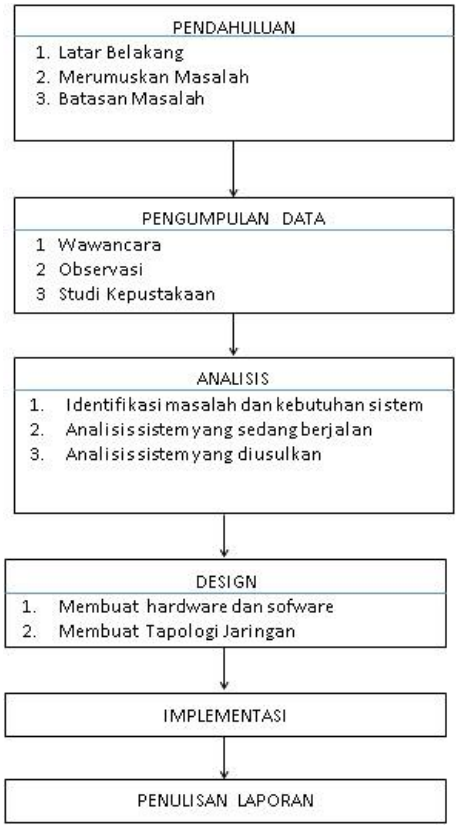
5. *Monitoring*

Monitoring merupakan tahapan yang penting, agar jaringan komputer dan komunikasi dapat berjalan sesuai dengan keinginan dan tujuan awal dari user pada tahap awal analisis, maka perlu dilakukan kegiatan monitoring.

3. METODOLOGI PENELITIAN

3.1. Kerangka Penelitian

Kerangka penelitian dapat dilihat pada gambar 2.



Gambar 2. Kerangka Penelitian

3.2. Tahapan Penelitian

1. *Analysis* : Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan pengguna dalam proses keamanan dalam pengiriman data melalui e-mail, dan analisa topologi / jaringan yang sudah ada saat ini. Metode yang biasa digunakan pada tahap ini diantaranya ;
   a. Wawancara, dilakukan dengan pihak terkait melibatkan dari struktur manajemen atas sampai ke level bawah / operator agar mendapatkan data yang konkrit dan lengkap. pada kasus di *Computer Engineering* biasanya juga melakukan *brainstorming* juga dari pihak vendor untuk solusi yang ditawarkan dari vendor tersebut karena setiap mempunyai karakteristik yang berbeda.
   b. Survey langsung kelapangan, pada tahap analisis juga biasanya dilakukan survey langsung kelapangan untuk mendapatkan hasil sesungguhnya dan gambaran seutuhnya sebelum masuk ke tahap design, survey biasa dilengkapi dengan alat ukur tingkat keamanan data pada proses pengiriman data melaui e-mail dan alat lain sesuai kebutuhan untuk mengetahui detail yang dilakukan.
   c. Membaca manual atau *blueprint* dokumentasi, pada analysis awal ini juga dilakukan dengan mencari informasi dari manual-manual atau blueprint dokumentasi yang mungkin pernah dibuat sebelumnya. Sudah menjadi keharusan dalam setiap pengembangan suatu sistem dokumentasi menjadi pendukung akhir dari pengembangan tersebut, begitu juga pada *project network*, dokumentasi menjadi syarat mutlak setelah sistem selesai dibangun.
   d. Menelaah setiap data yang didapat dari data-data sebelumnya, maka perlu dilakukan analisa data tersebut untuk masuk ke tahap berikutnya. Adapun yang bisa menjadi pedoman dalam mencari data pada tahap analysis ini adalah ;
      1) User / people : jumlah user, kegiatan yang sering dilakukan, peta politik yang ada, level teknis user
      2) Media H/W & S/W : peralatan yang ada, status jaringan, ketersedian data yang dapat diakses dari peralatan, aplikasi s/w yang digunakan
      3) Data : jumlah pelanggan, jumlah inventaris sistem, sistem keamanan yang sudah ada dalam mengamankan data.
      4) Network : konfigurasi jaringan, volume trafik jaringan, protocol, monitoring network yang ada saat ini, harapan dan rencana pengembangan kedepan
      5) Perencanaan fisik : masalah listrik, tata letak, ruang khusus, sistem keamanan yang ada, dan kemungkinan akan pengembangan kedepan.
2. *Design* : Dari data-data yang didapatkan sebelumnya, tahap Design ini akan membuat gambar design topology jaringan interkoneksi yang akan dibangun dan rancangan proses keamanan data melalui e-mail, diharapkan dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan yang ada. Design bisa berupa design struktur topology, design akses data, dan sebagainya yang akan memberikan gambaran jelas tentang sistem keamaman yang akan dibangun. Biasanya hasil dari design berupa ;
   a. Gambar-gambar topology (server, data center, storages, lastmiles, titik akses dan sebagainya)
   b. Gambar-gambar detailed estimasi kebutuhan yang ada
3. *Simulation Prototype* : beberapa pengguna akan membuat dalam bentuk simulasi dengan bantuan Tools khusus di bidang network seperti boson, packet tracert, netsim, dan sebagainya, hal ini dimaksudkan untuk melihat kinerja awal dari network yang akan dibangun dan sebagai bahan presentasi dan sharing dengan team work lainnya. Namun karena keterbatasan perangkat lunak simulasi ini, banyak para networker's yang hanya menggunakan alat Bantu tools VISIO untuk membangun topologi yang akan di design.
4. *Implementation* : di tahapan ini akan memakan waktu lebih lama dari tahapan sebelumnya. Dalam implementasi pengguna akan menerapkan semua yang telah direncanakan dan di design sebelumnya. Implementasi merupakan tahapan yang sangat menentukan dari berhasil / gagalnya project yang akan dibangun dan ditahap inilah Team Work akan diuji dilapangan untuk menyelesaikan masalah teknis dan non teknis.

Ada beberapa Masalah-masalah yang sering muncul pada tahapan ini, diantaranya ;

a jadwal yang tidak tepat karena faktor-faktor penghambat,
b masalah dana / anggaran dan perubahan kebijakan
c team work yang tidak solid
d peralatan pendukung dari vendor makanya dibutuhkan manajemen project dan manajemen resiko untuk menimalkan sekecil mungkin hambatan-hambatan yang ada.

3.3. Analisis Sistem Keamanan

Analisis sistem keamanan data dan jaringan yang berjalan di polres majalengka yaitu masih dapat disusupi karena Tapologi jaringan akses internetnya masih bawaan dari ISPnya, dan sistem keamanan data pada proses pengiriman email belum

menggunakan enkripsi. Sehingga masih lemah dan ancaman pihak ketiga pada jaringan internal polres majalengka masih ada, karena masih ada celah yang harus diperbaiki dan di optimalkan.

Topologi Jaringan akses internet yang sedang digunakan juga masih menggunakan fasilitas dari ISP yaitu Telkom dengan produk Speedy, sehingga masalah keamanan jaringanpun masih riskan dan mudah di susupi oleh pihak ketiga.

Keamanan data yang dikirim melalui file attacment juga belum menggunakan metode enkripsi, sehingga ada ancaman yang perlu diantisipasi.

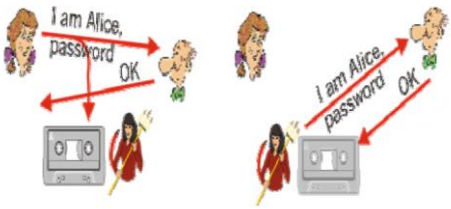
Analisis permasalahan merupakan asumsi permasalahan yang akan di uraikan dalam prosedur sistem keamanan email menggunakan PGP pada penerapan Jaringan Internet POLRES Majalengka, yaitu:

1. Privasi,
2. Autentikasi.

3.4. Analisis Sistem Keamanan data dan Jaringan yang berjalan

Analisis sistem keamanan data di POLRES Majalengka, berdasarkan observasi dan wawancara yang dilakukan penulis adalah masih menggunakan fasilitas autentikasi yang disediakan oleh provider emailnya masing masing sehingga ada kelemahan yang harus diantisifasi oleh user tersebut, karena data yang akan dikirim melalui teknik file attachment juga tidak di enkripsi sehingga terlalu riskan terhadap penyadaan, perhatikan gambar 3.

Sistem keamanan jaringan pada Kantor POLRES Majalengka masih mengunakan autentikasi umum yang disediakan oleh modem, dan ini sangat standar untuk keamanan jaringan pada lembaga kepolisian setinggkat POLRES.

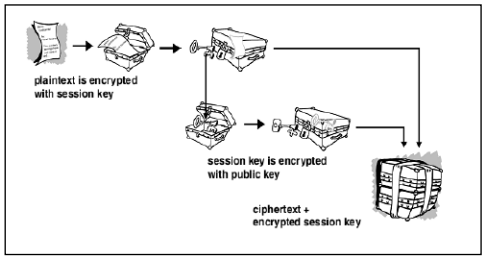


Gambar 3. Proses keamanan masih menggunakan fasilitas autentikasi

3.5. Analisis Sistem Keamanan Jaringan yang diiusulkan

Berdasarkan analisis sistem keamanan yang sedang berjalan pada POLRES Majalengka, maka sistem keamanan yang diusulkan oleh penulis dapat dilihat pada gambar 4.

Gambar 4. Sistem keamanan yang diusulkan



Gambar 5. Alur sistem engkripsi pada data yang akan dikirim

3.6. Objek Penelitian

POLRES Majalengka adalah tempat penelitian penulis yang beralamat di Jl. KH. Abdul Halim No. 518, Kecamatan Majalengka, Tonjong, Kec. Majalengka, Kabupaten Majalengka, Jawa Barat 45414. Berikut ini profil POLRES Majalengka :

Batas wilayah Administratif Polres Majalengka :
Sebelah Utara : Kab. Indramayu
Polres : Indramayu
Sebelah Selatan : Kab. Ciamis dan Garut
Polres : Ciamis dan Garut
Sebelah Barat : Kab. Sumedang
Polres : Sumedang
Sebelah Timur : Kab. Cirebon dan Kuningan
Polres : Cirebon dan Kuningan
Jumlah Polsek : 25
Jumlah Personel Polsek : 545 Personel
Jumlah Polsubsektor : Tidak Ada
Jumlah Personil Polsubsektor : Tidak Ada
Jumlah Personil Sat Polair +ABK : Tidak Ada
Jml unit Lantas Polsek Rural/Prarural : 1 (Satu) Polsek Jatitujuh
Jumlah penduduk Kab/Kota : 1.274.295 Jiwa
Luas wilayah Kab/Kota : 1.204,24 Km2
Kepadatan rata-rata per Km2 : 1058 jiwa/km²
Jumlah Kecamatan : 26 Kecamatan
Jumlah desa/kelurahan : 330 desa , kelurahan 13
Panjang Pantai : - Km2 (yang ada

pantainya).
Jumlah asrama Polri : 14 lokasi
Alamat asrama Polri : Terlampir
Penghuni berapa pintu/KK : 85 Pintu
Status tanah asrama Polri : Dimiliki dan Dikuasai Polres

4. PEMBAHASAN

4.1. PGP

PGP dapat diperoleh secara gratis untuk penggunaan pribadi. Kita dapat mendownload softwarenya pada saat kita terhubung dengan internet. Semua kunci pribadi dapat kita peroleh dan tidak ada biaya tambahan yang dibebankan untuk pembuatan sertifikat maupun tanda tangan digital yang disertakan. Pada PGP untuk melakukan proses enkripsi digunakan kunci rahasia yang berbeda dengan kunci rahasia yang digunakan pada proses deskripsi. Jadi terdapat dua buiah kunci rahasia, satu untuk deskripsi, satu untuk enkripsi. Hal inilah yang dikenal dengan kriptografi asimertrik. Selain asimterik ada juga kriptografi simetrik yang hanya menggunakan 1 buah kunci rahasia. Dengan demikian, siapa saja yang ingin menggunakan PGP akan membutuhkan 2 buah kunci. Pertama, kunci untuk proses enkripsi (kunci publik). Disebut kunci publik karena kunci yang digunakan untuk enkripsi ini akan diberitahukan kepada umum. Orang yang akan mengirimkan e-mail rahasia kepada kita harus mengetahui kunci publik ini. Kedua, kunci untuk proses deskripsi (kunci pribadi). Disebut kunci pribadi karena kunci ini hanya diketahui oleh kita sendiri.

Ilustrasi Pemakaian PGP

1. *Public-key* sangat lambat bila dibandingkan dengan konvensional, jadi PGP akan mengkombinasikan dua algoritma, yaitu RSA and IDEA, untuk melakukan enkripsi plaintext kita.
2. Sebagai contoh, Asep (pemilik PGP) ingin mengenkripsi suatu file yang diberi nama plain.txt sedemikian sehingga hanya si Matangin yang dapat mendekripsi-nya. Maka Asep mengirimkan PGP perintah (*command line*) untuk melakukan enkripsi :

   pgp -e plain.txt Matangin

   Pada command line ini, pgp adalah file executable, -e berarti memberitahukan PGP untuk meng-**e**ncrypt file, plain.txt adalah nama plaintext, dan dul merepresentasikan public key suatu tujuan (Matangin) yang diinginkan Asep untuk mengenkripsi message-nya. PGP menggunakan suatu *random number generator*, dalam file randseed.bin untuk menghasilkan suatu kunci (session key) temporary IDEA. Session key itu sendiri di-enkripsi dengan kunci RSA public yang direpresentasikan oleh Matangin yang disematkan pada plaintext.
3. Kemudian, PGP menggunakan session key untuk mengenkripsi message, ASCII-armors dan menyimpan seluruhnya sebagai cipher.asc. Bila Matangin ingin membaca pesannya, ia mengetikkan command:

   pgp cipher.asc
4. PGP menggunakan *secret key milik Matangin*, yang merupakan kunci RSA, untuk men-dekripsi sessi kunci yang mana, yang jika dipanggil oleh Badrun akan dienkripsi oleh public key. kemudian, conventional crypto digunakan dalam bentuk session key untuk mendekripsi sisa dari message. Alasan prinsip ini adalah sebagai pengganti/kompensasi dari RSA karena "RSA is too slow, it's not stronger, and it may even be weaker." (-PGP Documentation, pgpdoc2.txt).

4.2. Enkripsi PGP

Usaha-usaha penyadapan proses penyampain e-mail melalui Internet semakin hari semakin meluas. Terlebih setelah masuknya transaksi dunia bisnis ke dunia Internet yang tentunya memerlukan tingkat kerahasiaan tertentu. Ambil contoh, Anda ingin membeli sebuah barang melalui e-mail ke sebuah toko. Anda menuliskan nomor kartu kredit sebagai jaminan pembayaran pada e-mail yang Anda kirimkan. Pada akhir bulan, tiba-tiba Anda dikejutkan dengan melonjaknya nilai tagihan pada kartu kredit Anda yang disebabkan oleh pembelian-pembelian barang yang tentunya tidak pernah Anda lakukan. Hal ini sangat mungkin terjadi akibat penyadapan isi e-mail yang Anda kirimkan ke toko tersebut. Setelah sang penyadap telah mengetahui identitas kartu kredit Anda, dengan leluasa dia melakukan transaksi menggunakan kartu kredit Anda sebagai jaminan.

Jika Anda ingin menghindari kejadian di atas atau Anda menginginkan privacy saat mengirimkan e-mail, proses enkripsi menjadi salah satu solusi utama! Selain itu, jika Anda ingin file-file yang Anda miliki tidak bisa dibaca oleh orang lain kecuali oleh Anda sendiri dan orang-orang yang Anda percaya maka proses enkripsi menjadi perlu.

Enkripsi dilakukan dengan mengacak pesan plaintext secara sistematis sehingga tidak dapat terbaca tanpa alat khusus. Dalam teknologi enkripsi yang umum saat ini, digunakan sepasang kunci untuk mengenkripsi dan mendeenkripsi (menguraikan sandi) pesan yang hendak disampaikan. Sepasang kunci ini dinamakan kunci publik dan kunci privat. Dua kunci ini dibangkitkan secara simultan oleh komputer dan digunakan berpasangan. Untuk dapat mengenkripsi pesan, orang yang menulis pesan memerlukan kunci publik (public key). Kunci publik ini disebarkan

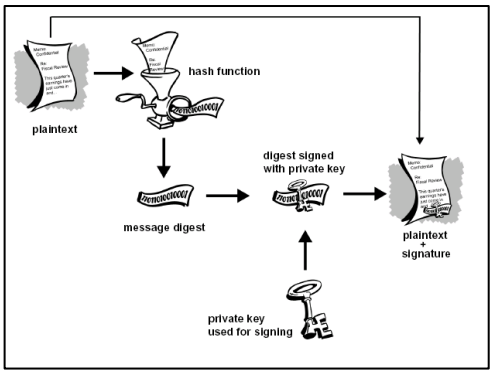
oleh pemiliknya agar orang yang ingin menulis pesan padanya bisa mengenkripsi pesan menggunakan kunci publik tersebut. Setelah dienkripsi, pesan tersebut tidak bisa diuraikan lagi, kecuali memakai kunci privat. Kunci privat disimpan dan harus dirahasiakan oleh pemiliknya. Kunci ini digunakan untuk menguraikan pesan yang dienkripsi dengan menggunakan kunci publik. Karena hanya satu orang (pemilik kunci) yang menyimpan kunci privat tersebut, maka hanya dia yang bisa membaca pesan tersebut.

4.3. Fungsi Hash

Hash adalah algoritma yang menghasilkan output yang bersifat unik dari sebuah input tertentu seperti pesan. Fungsi hash menambahkan suatu fungsi dalam prosesnya dari skema proses diatas. Fungsi ini akan membuat suatu panjang variabel output yang sama walau pun berbeda panjang pesan. Tetapi perubahan satu bit saja akan merubah nilai dari variabel fix tersebut.

PGP menggunakan kekuatan fungsi hash ini secara kriptografi pada text biasa yang pengguna menandatanganinya. Ini akan menghasilkan suatu panjang data yang tetap yang disebut dengan suatu message digest (pesan singkat), Sekali lagi perubahan sedikit saja pada data akan merubah nilai dari pesan ini. Lalu PGP menggunakan pesan singkat dan kunci privat untuk membuat "signature". PGP mengirimkan signature dan text biasa ini bersama-sama. Pada sisi penerima pesan, penerima menggunakan PGP untuk melakukan komputasi ulang digest, lalu membuktikan signaturenya. PGP dapat mengenkripsi tulisan biasa atau tidak. Menandatangani tulisan biasa akan berguna jika sebagian penerima tidak tertarik akan atau mempu untuk membuktikan *signature*.

Sepanjang suatu jaminan fungsi hash digunakan, tidak ada cara lain untuk mengambil tanda tangan seseorang dari dokumen yang satu ke dokumen yang lain atau merubahnya dalam cara apa pun. Perubhan paling kecil saja dari dokumen akan menghasilkan proses pembuktian keabsahan menjadi gagal.



Gambar 6. Fungsi Hash

4.4. Konfigurasi PGP pada Komputer

Instalisasi PGP

Dalam melakukan instalisasi PGP pada komputer kita adalah mengambil progrmnya terebih dahulu melalui situs – situs yang menyediakan software PGP seperti diatas dan melalui FTP ke salah satu FTP Server di atas.

Adapun langkah – langkah yang dilakukan jika melalui FTP server adalah :

1. Penulis mengambil program PGP dengan platform MS-Dos yang bernama *pgp263i.zip* dan kemudian mengekstraknya dengan menggunakan program Unzip atau Winzip. Pada saat proses ekstraksi berlangsung, tentukan letak direktori yang akan ditempati oleh program PGP tersebut. Dalam contoh kali ini, penulis menggunakan direktori *C:\pgp* sebagai tempat penyimpanan program PGP. Setelah diekstrak, pada direktori c:\pgp akan muncul 5 buah file yaitu : *readme.1st ; readme.usa ; setup.doc; pgp263ii.zip; pgp263ii.asc*. File *pgp263ii.zip* diekstrak dengan menggunakan program Unzip atau Winzip dengan direktori yang sama yaitu C:\pgp. Nah, setelah ekstraksi di atas, program PGP siap dikonfigurasi.
2. Langkah selanjutnya adalah kita mengkonfigurasi program PGP tersebut melalui file *config.txt*.
3. Setelah file *config.txt* selesai diedit dan disimpan, maka selanjutnya kita mengkonfigurasikan parameter TZ dan path untuk program PGP. TZ ini kependekan dari Time Zone dan untuk WIB digunakan nilai GMT-7. Jika parameter TZ tidak diset maka PGP tidak akan beroperasi. Ada dua cara untuk mengkonfigurasi parameter tersebut.

1. Cara pertama, kita langsug ketikan perintah "set TZ=GMT-7" dan "set path=c:\pgp;%path%" pada prompt DOS.

   C:\>SET TZ=GMT-7 [Enter]

   C:\>SET PATH=C:\PGP;%PATH% [Enter]
2. Cara kedua, kita tambahkan kedua perintah di atas pada file AUTOEXEC.BAT sehingga setiap kali booting, komputer akan otomatis mengkonfigurasi parameter di atas.

Jika langkah-langkah di atas telah selesai dilakukan, maka instalasi program PGP telah selesai dan siap digunakan.

5. KESIMPULAN

Dari uraian yang terdapat pada penelitian ini, maka penulis menarik beberapa kesimpulan sebagai berikut :

1. Dalam sistem pertukaran informasi, antara pengirim dan penerima masing – masing memiliki 2 kunci yaitu kunci publik (*public*) dan kunci pribadi (*private*). Kedua kunci tersebut digunakan untuk membuat sistem keamanan data. Data yang dikirimkan terlebih dahulu akan dienkrip dengan menggunakan kunci publik si penerima dan akan dibuka atau didekrip oleh kunci pribadi si penerima itu sendiri.
2. PGP merupakan aplikasi pengamanan komunikasi data yang dapat mengizinkan pengirim utnuk menandai pesan – pesan mereka dengan di buktikan pada pesan yang belum ada perubahan selama perjalanan. PGP memberikan pengamanan yang berlapis dalam beberapa tingkat. Saat ini PGP merupakan suatu aplikasi yang baik untuk keamanan e-mail juga file – file. Orang – orang banyak menggunakan aplikasi ini selain keamanan yang baik juga fleksibel yang dapat berjalan pada semua sistem operasi dan mudah didapatkan dengan gratis di internet.

PUSTAKA

Alamsyah, 2011, *Implementasi keamanan email menggunakan PGPtray . Mektek*, 121.

Ibrahim, Ali., 2011, *Pengembangan Sistem Informasi Monitoring Tugas Akhir Berbasis Short Message Service (SMS) Gateway di Fasilkom Unsri, Yogyakarta: Jurnal Sistem Informasi Indonesia.1 (2). 2087-8737.*

James E. Goldman, Philips T. Rawles, 2011, *Applied Data Communications, A business-oriented approach, Third Edition, John Willey & Sons :470.*

Kuswanto, H., 2017, *Sistem Autentikasi Hotspot Menggunakan Radius Server Mikrotik Router. INFORMATICS FOR EDUCATORS AND PROFESSIONALS*, 43–50.

Mulyani, I., Satria, E. dan Supriatna, AD., 2012, Pengembangan Short Message Service(SMS) GatewayLayanan Informasi Akademikdi SMK YPPT Garut, Jurnal Algoritma Sekolah tinggi Teknologi Garut. Vol. 9(11).

Nandang, I., 2011, *Analisis Keamanan email menggunakan PGP. Paradigma Vol VIII No. 1* , 30.

Raka Yusuf, A. W., 2010, *Aplikasi Enkripsi E-Mail dengan PGP Menggunakan PHP Menggunakan PHP. Seminar Nasional Pengaplikasian Telematika SINAPTIKA 2010 – ISSN 2086-8251*, 385-390.

Septy, R. F., 2015, *Kriptograpy.* Jakarta: MTI Fakultas Ilmu Komputer.

Sommerville, I., 2003, *Software Engeneering (Rekayasa Perangkat Lunak) jilid 2.* Jakarta: Erlangga.

Stallord, John J., dkk., 1990), *Perkantoran Elektronik*. Jakarta: Rineka Cipta.

Tera, M., 2009, *Q Tera Mandiri*. Dipetik Desember Senin, 2019, dari Q Tera Mandiri: http://www.qtera.co.id/

Umar, H., 2005, *Metode Penelitian Untuk Skripsi dan Tesis Bisnis.* Jakarta: Salemba Empat.

Wibowo, A., 2014, *Penyelesaian Problem Gaussian Elimination Menggunakan Posix Thread, OpenMP Dan Intel TBB. Jurnal Integrasi, VI, 166-170.*