Seminar Nasional Inovasi Teknologi
UN PGRI Kediri, 22 Februari 2017

ISBN : 978-602-61393-0-6
e-ISSN : 2549-7952

IMPLEMENTASI TANDA TANGAN DIGITAL DENGA PRETY GOOD PRIVACY (PGP) UNTUK KEAMANAN TRANSAKSI ELEKTRONIK

Adimas Ketut N, M.Kom[1]
[1]Teknik Informatika, Fakultas Teknik, Universitas Nusantara PGRI Kediri
E-mail: *[1]*dimasketutuchiha@gmail.com*

,

Abstrak **–** *Indonesia dengan jumlah penduduk lebih dari 200 juta orang merupakan pasar yang strategis dalam memasarkan suatu produk. Akhir-akhir ini menjadi trend pemasaran suatu produk dilakukan dengan bantuan Teknologi Informasi (TI). Sehingga dengan jumlah penduduk yang besar maka semakin besar pula jumlah transaksi elektronik yang terjadi. Dengan besarnya transaksi elektronik tidak sedikit juga orang yang memanfaatkan kelengahan seseorang seperti melakukan kejahatan elektronik mulai pencurian data, hacking, spofing sampai cracking.*
Untuk meminimalisasi kejatahan elektronik tersebut perlu adanya suatu keamanan yang dapat menjaga data dari kejahatan elektronik. Prety Good Privacy(PGP) menawarkan suatu keaman data yang terenkripsi pasangan dengan menggunakan "Private-Publik Key". Dengan metode PGP dapat membuat suatu tanda tangan digital dengan tingkat keamanan yang tinggi dalam suatu transaksi elektronik.

Kata Kunci *— Keamanan data, kejahatan elektronik, PGP, tanda tangan digital, Private-Publik Key.*

Abstract **–** *Indonesia with a population of over 200 million people is a strategic market in marketing a product. Lately the trend of marketing a product is done with the help of Information Technology (IT). So with a large population, the greater the number of electronic transactions that occur. With the amount of electronic transactions not least also the person who took advantage of someone as committed crimes ranging electronic data theft, hacking, spofing to cracking.*
To minimize electronic kejatahan the need for a security that can keep data from electronic crime. Prety Good Privacy (PGP) offers a couple Security settings encrypted data by using the "Private-Public Key". With the PGP method can create a digital signature with a high level of security in an electronic transaction.

Keywords *— Data security, electronic crime, PGP, digital signatures, Private-Public Key.*

1. PENDAHULUAN

Menurut data bps Indonesia dengan jumlah penduduk lebih dari 200 juta[6].orang merupakan pasar yang strategis dalam pemasaran suatu produk. Oleh karena itu perkembangan teknologi informasi di Indonesia begitu pesat. Peran teknologi ini adalah untuk membantu dalam proses komunikasi dan transaksi yang lebih cepat dan efisien. Perkembangan teknologi tersebut juga mempunyai beberapa kelemahan. Kelemahan tersebut apabila tidak dapat di tangani dengan baik, maka akan menjadi bomerang bagi pengguna teknologi informasi.

Dengan pesatnya perkembangan teknologi informasi di indonesia tidak sedikit juga orang yang tidak betanggung jawab memanfaatkan kelemahan dari teknologi informasi. Jenis penyalah gunaan tersebut mulai dari hacking, carding sampai cracking. Internet Security Threat Report (ISTR), melaporkan di tahun 2013, ada peningkatan 62 persen dari tahun sebelumnya mengenai jumlah pelanggaran data global, sehingga lebih dari 552 juta identitas terekspos. Menurut Symantec, sistem keamanan internet di Indonesia masih rawan akan pencurian

ISBN : 978-602-61393-0-6
e-ISSN : 2549-7952

data KemananKeamanan internet Indonesia menurun tahun lalu dan berada di peringkat ke-22 di dunia. Indikasi ini menjelaskan pejahat cyber tidak berkurang," kata Alex Lei, Direktur Security Sales ASEAN dan Korea di Hotel Intercontinetal Mid Plaza, Rabu 7 Mei 2014 [7].

Dengan disahkannya undang-undang Informasi dan Transaksi Elektronik (ITE) tidak serta merta menyelesaikan masalah tersebut. Sebenarnya dengan UU ITE ini pemerintah sudah mempunyai niat baik untuk melindungi pengguna teknologi informasi tetapi UU ITE juga mempunyai beberapa kelemahan. Seperti kasus florence di Yogyakarta yang terjerat UU ITE. Kasus Florence dapat dijerat hukum karena ada yang melaporkan tindakan florence tersebut [8]. Dengan kelemahan UU ITE tersebut mengharuskan para penggunya untuk lebih memproteksi diri sendiri untuk dapat terhindar dari segala bentuk jenis kejahatan teknologi informasi.

Kehidupan kita saat ini dilingkupi oleh kriptografi. Mulai dari transaksi di mesin ATM, percakapan melalui telpon genggam, mengakses Internet sampai mengaktifkan peluru kendalipun menggunakan kriptografi. Begitu pentingnya kriptografi untuk keaman sistem informasi (Information Security), sehingga jika berbicara mengenai masalah keamanan yang berkaitan dengan penggunaan komputer, maka tidak bisa dipisahkan dari kriptografi[5].

Untuk dapat menjaga keaaman sistem dibutuhkan tanda tangan digital untuk menjaga keaslian informasi tersebut. Menurut Arrianto Mukti Wibowo tanda tangan digital memiliki sifat otentik yang artinya tidak bisa ditiru, hanya sah untuk dokumen (pesan) itu saja dan dapat diperiksa dengan mudah[1].

Teknologi tanda tangan digital tersebut salah satunya bisa menggunakan sistem Prety Good Privacy (PGP). Prety Good Privacy(PGP) merupakan suatu sistem enkripsi yang mempunyai keamanan cukup tinggi yang bersifat rahasia dengan menggunakan “Private-Public Key”. Metode Prety Good Privacy ini pertama kali di kembangkan Phil Zimmermann[2].

2. METODE PENELITIAN

2.1. Tinjauan Pustaka

Menurut Zimmerman:1980, PGP (Pretty Good Privacy) adalah Suatu metode program enkripsi informasi yang memiliki tingkat keamanan cukup tinggi bersifat rahasia dengan menggunakan “Enkripsi dan depkripsi” sebagai dasar autentifikasinya sehingga jangan sampai dengan mudah diketahui oleh orang lain yang tidak berhak.

Pada awal mulanya, PGP digunakan untuk melindungi surat elektronik (e-mail) dengan memberikan perlindungan kerahasiaan (enkripsi). Untuk itu Phill Zimmerman membuat sebuah program yang digunakan agar dapat melindungi informasi data dengan kerahasiaan. Sehingga file atau data yang terenskripsi kemudian dikirimkan ke tujuan melalui e-mail. Jadi penerima e-mail harus menyimpan sebuah file yang terenskripsi didalam e-mail tersebut ke dalam sebuah file. File tersebut dideskripsi sehingga isi file atau data aslinya akan terlihat. Jadi, file atau data yang dikirim melalui email dalam bentuk terenkripsi sehingga tidak dapat dibaca dengan mudah oleh orang-orang yang tidak memiliki akses pembaca file atau data tersebut. [4]

Tabel 1. Proses Pelayana PGP.

Fungsi	**Algoritma yang digunakan**	**Uraian**
Penandaan Digital	RSA, MD5	Kode yang diciptakan oleh MD5. Pesan yang dibuat oleh deskripsi oleh RSA dengan kunci rahasia penerima dan termasuk dalam pesan.
Enkripsi Pesan	IDEA, RSA	Pesan yang dienkripsi menggunakan IDEA, sekali saja dibuat oleh pengirim. Sesi kunci ini dienkripsi oleh RSA

ISBN : 978-602-61393-0-6
e-ISSN : 2549-7952

		dengan kunci publik penerima pesan di dalamnya.
Pemampatan	ZIP	Pesan boleh dimampatkan untuk penyimpanan atau transmisi dengan ZIP
Kompatibilitas e-mail	Radix 64 conversion	Menyediakan transparasi untuk aplikasi e-mail yang dapat dikonversikan ke kode ASCII dengan menggunakan Radix 64 conversion.
Segementasi		Untuk mengakomodasi pesan maksimum untuk ukuran tertentu, PGP menyediakan segmentasi dan reassembly.

Tabel di ambil dari sumber referinsi [2].

2.1.1. Kunci Kode Umum

Azas pengoperasian PGP merupakan syarat agar tiap pengguna memiliki kode pribadi sebaik seperti salinan kode umum dari setiap korespondensi yang potensial. Kode-kode ini dikumpulkan dan disimpan dalam jaringan kode unum. Tiap hal berkaitan dengan jaringan, mencakup beberapa bagian sebagai berikut :

a. Kunci kode umum itu sendiri.
b. Identitas pengguna dari pernilik kode umun tersebut. khususnya si pemilik nama.
c. Kode identitas, yang merupakan pengidentifikasi yang khusus untuk kode ini.
d. Informasi lain yang berhubungan dengan kode yang patut dipercayai dari pemilik informasi.

Dikutip dari sumber referensi [2].

2.2. Kunci Kode Pribadi

Tiap-tiap kode PGP memiliki kunci kode pribadi dan mampu menerima beberapa kunci kode pribadi spesifik. Jadi, hal pertama yang harus dilakukan pengguna sebelum mengisntalasi PGP adalah mengaktifkan RSA atau pasangan kode umum. Ketika dua buah kode diaktifkan, PGP menempatkan kunci kode umum pada struktur data yang dikenal sebagai jaringan kunci kode umum. Dikutip dari sumber referensi [2].

2.3. Tertanda Digital

Langkah pertama dalam generasi dari pesan PGP adalah proses penandaan secara digital. Urutanya sebagai berikut :

a. Pengirim membuat pesan.
b. PGP menggunakan MD5 untuk mengaktifkan kode pengacak pesan 128-bit.
c. Pengirim menentukan kode umum untuk digunakan pada operasi ini dan menetapkan kombinasi karakter, memungkinkan PGP untuk menyembunyijan kunci kode umum si pengirim.
d. PGP menyamarkan kode pengacak RSA, dengan menggunakan kode pribadi pengirim dan memberikan hasilnya pada pesan.

Bagaimana pengirim PGP sampai menangani penandaan :

a. PGP mengambil lampiran kode identitas pada penandaan untuk mendapatkan kode umum yang tepat dari jaringan kode umum.
b. PGP menggunakan RSA dengan kode umum pengiriman, fungsinya untuk menyamarkan dan melindungi kode pengacak.
c. PGP menghasilkan kode pengacak yang baru untuk pesan, dan membandingkannya dengan kode pangacak yang tersembunyi. Jika keduanya sama, maka pesan diterima sebagai pesan yang asli.

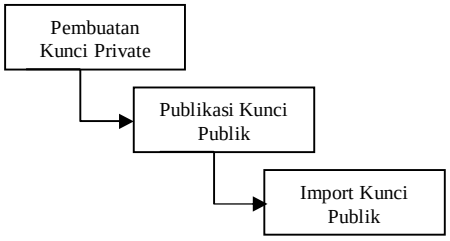
Kombinasi dari MD5 dan RSA (metode enkripsi) menyediakan rencana penandaan secara digital yang efektif. Dengan sistem enkripsi RSA, maka penerima dapat memastikan bahwa hanya prosesor dari kode pribadi yang sama dapat menghasilkan

ISBN : 978-602-61393-0-6
e-ISSN : 2549-7952

penandaan. Karena kemampuan MD5 ini, maka penerima dapat memastikan bahwa tidak ada seorangpunyang dapat menghasilkan pesan yang baru, yang cocok dengan kode pangacak, dengan penandaan pesan yang asli. Di ambil dari sumber referensi [2].

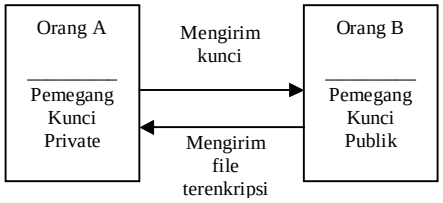
2.4. Metode Penelitian

Penelitian ini akan melakukan pengembangan dalam penggunaan tanda tangan digital. Tanda tangan digital tersebut akan di kaji dengan membuat kunci private, mempublikasikan kunci publik dan mengimport kunci publik. Software yang digunakan adalah kleopatra gpg4win yang dapat di download di alamat http://www.gpg4win.de. Software ini bersifat GNU atau General Publik Lisensi versi 2. Untuk lebih detil dapat di lihat pada diagram di bawah ini.



Gambar 1. Metode Penelitian

Untuk transaksi elektronik penulis penggambarkan transaksi dengan cara pertukaran file notepad antara orang A ke orang B. Untuk lebih jelasnya dapat dilihat pada diagram seperti di bawah ini.



Gambar 2**.** Tansaksi elektronik

2.5. Manfaat Penelitian

Manfaat yang bisa di dapat dari adanya penelitian ini adalah :

1. Memberikan manfaat yang besar terhadap para professional di bidang IT khususnya dan diberbagai bidang umumnya dalam pengiriman berkas data-data penting yang bersifat rahasia via internet.
2. Memberikan pengamanan terhadap berkas-berkas data perusahaan yang saling dikirimkan antara kantor pusat dan kantor cabang.
3. Memberikan verifikasi keabsahan data yang dikirim dari pihak penerima maupun pihak pengirim.
4. Memberikan kemudahan kepada pihak penerima untuk mengetahui tentang siapa yang mengirim data tersebut.

3. HASIL DAN PEMBAHASAN

Hal yang terpenting ketika kita membuat tanda tangan yang di tulis tangan menurut dugaan bersifat unik untuk setia orang, tanda tangan digital juga bersifat untik untuk tiap dokumen satu ke dokumen yang lain dan masih kelihatan valid. Sedangkan tanda tangan digital apabila diberitahukan hal yang sama dengan tanda tangan biasa akan mengalamami kegagalan pembuktian apabila diterapkan pada dokumen lain.

Tanda tangan digital berkaitan erat dengan sertifikat digital. Hal yang terpenting yang perlu diperhatikan dalam proses sertifikat, terutama menyangkut kunci publik yang akan menggunakan PGP antara lain :

a. Kunci publik itu sendiri
b. Kartu identitas pemakai yang meliputi nama dan alamat e-mail dari pemilik kunci.
c. Satu atau lebih tanda tangan digital untuk kunci publik dan kartu identitas pemakai.

Tanda tangan memberi kesaksian bahwa kartu identitas pemakai berhubungan dengan kunci publik dan dinyatakan valid. Hal itu dapat terjadi karena adanya kunci penanda tangan.

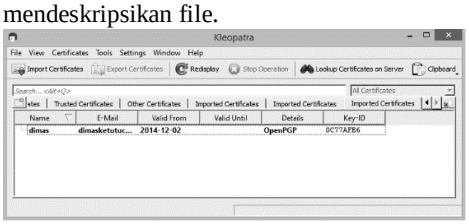
KUNCI PRIVATE

Algoritma kriptografi yang di gunakan adalah RSA dan digunakan untuk mengekrip kunci simetri untuk dikirimkan bersama pesan. Pengirim dan penerima harus mendapatkan kunci publik rekan-rekannya[4].

Fungsi kunci private ini adalah untuk membuka file yang terenkripsi dengan kunci publik. Dalam pembutan kunci private dibutuhkan key pair. Key pair seperti

ISBN : 978-602-61393-0-6
e-ISSN : 2549-7952

password yang dibutuhkan saat mendeskripsikan file.



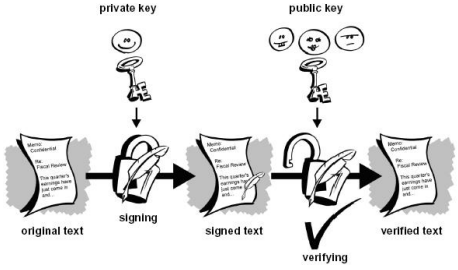
Gambar 3. Kunci Private

KUNCI PUBLIK

Kunci publik dalam PGP berfungsi sebagai enkripsi ketiga akan membuat file yang akan terinkripsi. Kunci publik terenkripsi secara asimetris. Kunci publik ini merupakan pasangan dari kunci private. Hasil enkripsi dari kunci publik tidak akan bisa di buka tanpa mempunyai kunci private. Jika pembuatan kunci publik berhasil maka pada saat kunci publik dibuka dengan bantuan aplikasi notepad akan terdapat kata "-----BEGIN PGP PUBLIC KEY BLOCK-----". Kunci publik dapat diberikan kepada orang yang dituju dengan cara di export.

Gambar 4. Importing Kunci Publik

Tanda tangan digital membutuhkan kunci pasangan yaitu kunci private dan kunci publik. Untuk dapat membuat enkripsi Prety good Privacy (PGP) dapat menggunakan software PGP4Win.



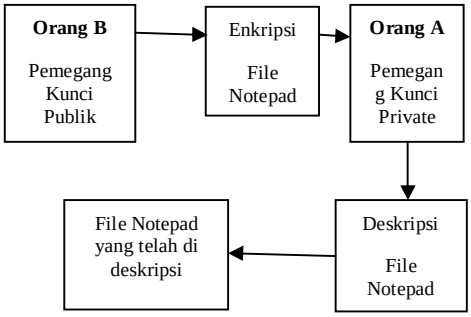
Gambar 5. Tanda tangan sederhana

Untuk penggunaan transaksi elektronik penulis menggunakan file notepad sebagai bahan. Penulis menganalogikan bahwa orang A telah mempunyai kunci private dan orang B telah mempunyai kunci publik dari orang A.

Orang B akan mengirimkan pesan pribadi di notepad yang berisi pesan "Hallo Nama saya dimas". Setelah itu Orang B melakukan enkripsi.

File hasil enkripsi dengan tipe data .pgp akan di kirimkan ke orang A untuk kemudian di decrypt dan pesan dapat di baca.

Dari penjabaran di atas dapat di gambarkan cara kerja transaksi elektronik seperti di diagram di bawah ini.



Gambar 6. Alur kerja transaksi elektronik.

Dari penjabaran transaksi elekteronik tersebut. Tanda Terlihat suatu data apabila di enkripsi lalu di kirim kepada orang lain. Maka perlu deskripsi dengan memasangkan kunci publik dan kunci private. Apabila kedua kunci tersebut tidak berpasangan maka file tersebut tidak akan bisa terbuka. Sehingga apabila data dicuri di tengah jalan tidak akan menjadi masalah. Karena pencuri data tersebut tidak memiliki kunci pasangan untuk membuka file tersebut. Penggunaan Prety Good Privacy dapat dikatakan mempunyai keamanan yang tinggi.

4. SIMPULAN

Tanda tangan digital dapat menjaga keaman data baik dari pengirim maupun penerima. Untuk membuat tanda tangan digital dapat menggunakan Prety Good Privacy (PGP) dengan bantuan software PGP4Win. PGP adalah sistem enkripsi data yang berpasangan menggunakan sistem "Private-Pulic Key". Dalam implentasinya penggunaan kunci tersebut harus berpasangan. Sehingga keamanan data lebih terjaga.

ISBN : 978-602-61393-0-6
e-ISSN : 2549-7952

5. SARAN

Karena terdapat proses pencocokan kunci dengan private dan publik key. Sehingga metode ini dapat mengurangi bahaya dari kejahatan pencurian data. Apabila data di ambil di tengah jalan. Maka pencuri data tersebut tidak akan bisa membuka file tersebut. Di karenakan untuk membuka file tersebut membutuhkan kunci pasangan. Namun apakah proses pengiriman data yang dikirim melewati email atau media internet lainya dapat menjaga kemanan data atau tidak perlu penelitian lebih lanjut.

DAFTAR PUSTAKA

[1] Wibowo, Arrianto Mukti. "Tanda tangan digital & sertifikat digital: Apa itu?."Infokomputer edisi Internet Juni (1998).
[2] Tung, Koe Yao. "KEAMANAN TRANSAKSI DENGAN PRETTY GOOD PRIVACY (PGP)." Meditek 7.19 (1999).
[3] Xenitellis, Symeon (Simos), “A guide to PKIs and Open–source Implementations”, The Open–source PKI Book Version 2.4.6 Edition.
[4]Alamsyah, Alamsyah. "IMPLEMENTASI KEAMANAN E-MAIL DENGAN MENGGUNAKAN PGPTRAY." MEKTEK 13.2 (2012).
[5] Rizal, M. Syaiful, and Idris Winarno. "Implementasi algoritma kriptografi kunci publik ElGamal untuk keamanan pengiriman Email." eepis final project (2010).
[6] http://www.bps.go.id/tab_sub/view.php?tabel=1&id_subyek=12. Diakses pada tangal 12 desember 2014.
[7]http://teknologi.news.viva.co.id/news/read/502681-mega-data-breach--ancaman-pengguna-internet-2014 diakses pada tanggal 12 Desember 2014.
[8]http://media.kompasiana.com/new-media/2014/08/31/kebebasan-berekspresi-di-media-sosial-dan-blog-tidak-lolos-dari-jerat-hukum-671833.html diakeses pada tanggal 12 Desember 2014.