p-ISSN 2086-5805
e-ISSN 2808-2540

Pengamanan Data Menggunakan Email Terenkripsi Di Akademi Angkatan Udara

(Data Security Using Encrypted Email at The Air Force Academy)

Muhammad Fahrurozi[1*], Mavel Ridho[2], Setiyono[3]

[1,2,3] Teknik Elektronika Pertahanan, Akademi Angkatan Udara

E-mail: muhammad.fahrurozi@aau.ac.id, mavel.ridho@aau.ac.id, setiyono@aau.ac.id

Abstract— ***Confidentiality of information and communication to protect sensitive data is an absolute thing and must be fulfilled when this will not exist in the military world. Confidentiality of data in exchanging information will protect institutions from unwanted things. As a military educational institution, the Air Force Academy requires a data security system to guarantee an institution. In securing data, confidentiality and security remain, namely confidentiality, integrity and availability so that the information content is maintained. The rapid development of data security tools, one of which uses the Pretty Good Privacy method. This system uses yahoo RSA cryptographic techniques to protect data sent via email. Several AAU work units that use the PGP method in carrying out e-mail data exchange are the financial unit, the health unit and the personnel unit that manages human resources. This PGP method can protect data or information on email. This technique is expected to be the first step in data security at the Air Force Academy.***

Keywords— **AAU, data security, email, information, PGP**

Abstrak**— Kerahasiaan informasi dan komunikasi untuk melindungi data yang bersifat sensitif merupakan hal yang mutlak dan harus dipenuhi saat ini tidak terkecuali dalam dunia militer. Kerahasiaan data dalam bertukar informasi akan melindungi institusi dari hal yang tidak diinginkan. Sebagai lembaga pendidikan militer, Akademi Angkatan Udara membutuhkan suatu sistem pengamanan pertukaran data untuk menjamin kredibilitas sebuah institusi. Dalam pengamanan data tetap mengedepankan aspek kerahasiaan dan keamanan yaitu confidentiality, integrity and availability agar kandungan informasi tetap terjaga. Pesatnya perkembangan alat bantu pengamanan data, salah satunya menggunakan metode Pretty Good Privacy. Sistem ini menggunakan teknik kriptografi algoritma RSA untuk melindungi data yang dikirim melalui email. Beberapa unit kerja AAU yang menggunakan metode PGP dalam melaksanakan pertukaran data email diantaranya adalah unit keuangan, unit kesehatan dan unit personel yang mengelola sumber daya manusia. Metode PGP ini dapat melindungi data atau informasi pada email. Dengan adanya teknik ini diharapkan mampu manjadi langkah awal dalam keamanan data di Akademi Angkatan Udara.**

Kata Kunci— **AAU, email, informasi, keamanan data, PGP**

**Penulis Korespondensi (Muhammad Fahrurozi)*
E-mail: muhammad.fahrurozi@aau.ac.id

p-ISSN 2086-5805
e-ISSN 2808-2540

I. PENDAHULUAN

Akademi Angkatan Udara sebagai lembaga pendidikan bertugas mencetak calon perwira terbaik di TNI Angkatan Udara yang memiliki sifat tanggap yang berpengetahuan luas, tanggon yang berkepribadian luhur serta trengginas yang berkesehatan jasmani yang baik. AAU memiliki struktur organisasi yang memiliki kompleksitas tinggi dan load beban penuh untuk mendukung tercapainya pendidikan. Dalam pelaksanaannya unit kerja menggunakan layanan email untuk pertukaran data. Layanan email memiliki beberapa kelemahan salah satunya rentan terhadap pembajakan email. Belum adanya proteksi penggunaan email terutama dalam mengirimkan data yang bersifat sensitif, hal ini akan menjadi berbahaya. Data dan informasi dicuri tanpa sepengetahuan dan kesadaran pemilik informasi. Data dan informasi jatuh pada orang yang tidak bertanggung jawab maka dikhawatirkan data tersebut akan disalahgunakan. Kredibilitas suatu organisasi dalam hal ini Akademi Angkatan Udara akan dipertaruhkan. Oleh karena itu untuk melindungi transfer data dan informasi diperlukan suatu sistem keamanan untuk melindungi data tersebut. Dalam penelitian ini penulis menggunakan teknik *Pretty Good Privacy* (PGP). Sistem ini menggunakan teknik kriptografi algoritma RSA *(Rivest-Shamir-Adleman)* untuk melindungi data yang dikirim melalui email [1]. Penggunaan algoritma RSA adalah untuk enkripsi maupun deskripsi suatu pesan. Selain itu algoritma ini mempunyai kemampuan menandatangani serta verifikasi paket data. Keunggulan RSA yaitu terletak pada kesulitan dalam pemfaktoran bilangan prima yang besar sekali menjadi bilangan yang memiliki nilai lebih kecil. Hal tersebut dilakukan untuk mendapatkan kunci privat yang digunakan untuk keaslian pesan yang diperoleh. Algoritma RSA ini pada fungsi hash yang dihasilkan tidak ditentukan dengan menggunakan algoritma yang ditentukan, dengan demikian tingkat keamanan pada enkripsi dan tanda tangan tidak bergantung pada algoritma fungsi hash [2]. Data atau informasi tersebut akan diubah dari teks asli menjadi teks yang sulit untuk dibaca. Dengan pasangan kunci publik dan kunci privat diharapkan sistem *pretty good privacy* dapat melindungi data atau informasi pada email staf personil. Selain itu dengan adanya teknik ini diharapkan mampu manjadi langkah awal dalam mengaplikasikan keamanan data di Akademi Angkatan Udara.

II. LANDASAN TEORI

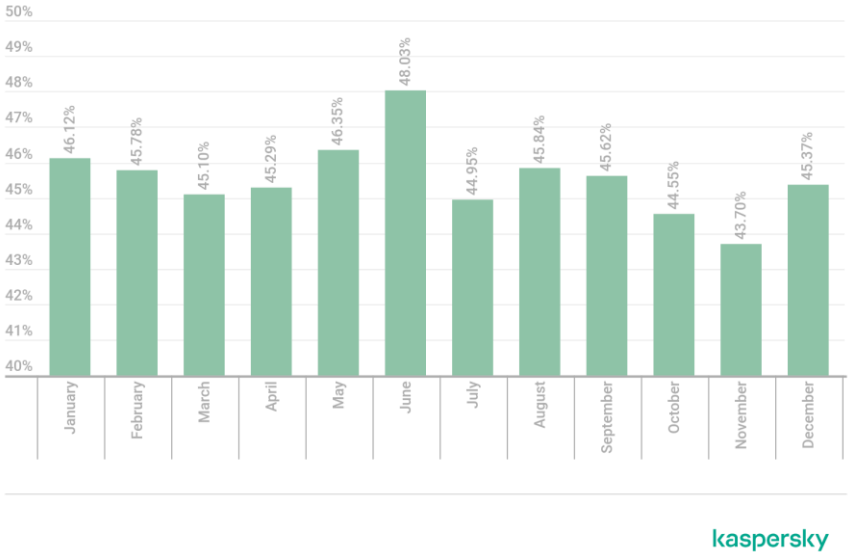
Pada bagian ini dijelaskan teori yang berkaitan dengan sistem *secure email*, kriptografi dan *Pretty Good Privacy*.

A. Secure email

Layanan pesan dan email adalah salah satu yang penting fasilitas yang sangat penting dan diperlukan dalam setiap organisasi untuk memfasilitasi komunikasi antara karyawan dan pemangku kepentingan. Saat ini penggunaan email masih mendominasi komunikasi digital dan email merupakan media pilihan yang rentan mendapatkan oleh penjahat dunia maya. Studi literatur menyebutkan bahwa beberapa jenis ancaman komunikasi pada email dan yang ancaman secara umum diuraikan di bawah ini [3].

1. Spam

Spam email adalah email yang dikirim secara massal ke banyak pengguna dengan tindakan kejahatan dari alamat yang tidak diketahui. Tindakan *spam* ini harus mendapatkan perhatian dari semua pihak. Serangan *spam* bertujuan menipu pengguna dengan cara mengklik URL, kemudian membuka lampiran yang mengandung virus. *Spammer* juga menggunakan teknik yang disebut *"snowshoe spam"* yaitu sebuah teknik dengan mengirim volume spam yang besar ke berbagai alamat IP kemudian hal tersebut akan menyumbat *bandwidth* jaringan. Sesuai *Kaspersky* pada tahun 2021 dilaporkan bahwa rata-rata, 45,56% lalu lintas email global adalah spam pada tahun 2021 [4] .



Gambar 1. Pangsa *spam* dalam lalu lintas *email* global, 2021. [4]

2. *Phising*

Penyerangan menggunakan *phishing* yaitu menipu situs web tepercaya untuk menargetkan pengguna melalui email untuk mendapatkan informasi pribadi korban yaitu nomor akun, ID email, kata sandi, kode rahasia dan lain sebagianya. Ada juga insiden, dimana dikompromikan ID email dimanipulasi tanpa sepengetahuan pengguna dan berkomunikasi atas nama pengirim dengan korban untuk transfer dana, informasi rahasia, slip gaji, dsb.

3. *Malware*

Penjahat dunia maya menggunakan banyak teknik berbeda untuk mengirim *spam* dan *malware* seperti lampiran *malware*, *hyperlink* di badan pesan, yang mengarahkan pengguna ke *hosting* situs penginstal *malware* dan PDF berbahaya dan *Microsoft Office Document* yang hampir selalu tercantum dalam "*white list"* organisasi. Sistem dengan keamanan yang tidak memadai langkah-langkah perlindungan akan dikompromikan, saat lampiran dibuka atau klik tautan. Sistem ini dapat digunakan untuk mengirim spam dan juga titik masuk untuk serangan terhadap jaringan internal organisasi.

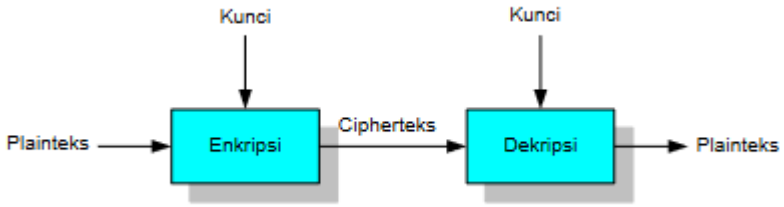
Penerapan email yang aman memiliki tujuan pada gerbang penyaringan masuk URL, spam, perlindungan *virus*, *phishing*, *email* berbahaya, mendeteksi berbagai jenis serangan termasuk pada manajemen hak akses email, isi dan lampiran.

B. Kriptografi

Kriptografi adalah suatu bidang ilmu yang mempelajari penulisan secara rahasia. Teknik ini digunakan untuk mengubah isi data kedalam kode-kode tertentu sehingga informasi yang dikirim atau ditransmisikan melalui internet tidak dapat dibaca oleh siapapun kecuali orang yang berhak. Dalam menjaga kerahasiaan data, kriptografi mentranformasikan data/informasi asli yang belum mendapat pemrosesan didalamnya disebut *plaintext* kedalam bentuk data/informasi yang dihasilkan melalui proses enkripsi disebut *ciphertext* yang tidak dapat dikenali [5]. *Cipertext* inilah yang akan dikirimkan oleh pengirim kepada penerima pesan. Setelah diterima, *ciphertex*t ini akan ditransformasikan kembali kedalam bentuk *plaintext* agar dapat dibaca kembali. Untuk membuka pesan tersebut dan menggubahnya ke bentuk *plaintex*t

p-ISSN 2086-5805
e-ISSN 2808-2540

kembali pengirim harus memiliki *public key* penerima, jika tidak maka proses deskripsi pesan akan tidak dapat diproses [6] (sesuai Gambar 2).



Gambar 2. Proses enkripsi dan deskripsi. [7]

Ada tiga faktor utama yang merupakan aspek dari keamanan informasi yaitu *Confidentiality*, *Integrity*, dan *Availability* [8]:

1. Confidentiality

Confidentiality (kerahasiaan) yaitu layanan agar isi pesan yang dikirimkan terjaga dan tidak diketahui oleh pihak lain (kecuali pihak pengirim, pihak penerima atau pihak - pihak memiliki ijin).

2. Integrity

Integrity (keutuhan). yaitu layanan yang mampu mengenali atau mendektesi adanya manipuliasi berupa peghapusan, pengubahan, atau penambahan data oleh pihak yang tidak berwenang

3. *Availability*

Availability (ketersediaan) yaitu aspek keamanan yang berfungsi memastikan sumber daya yang ada siap untuk diakases oleh siapapun, kapanpun dan sistem yang membutuhkannya.

C. Pretty Good Privacy

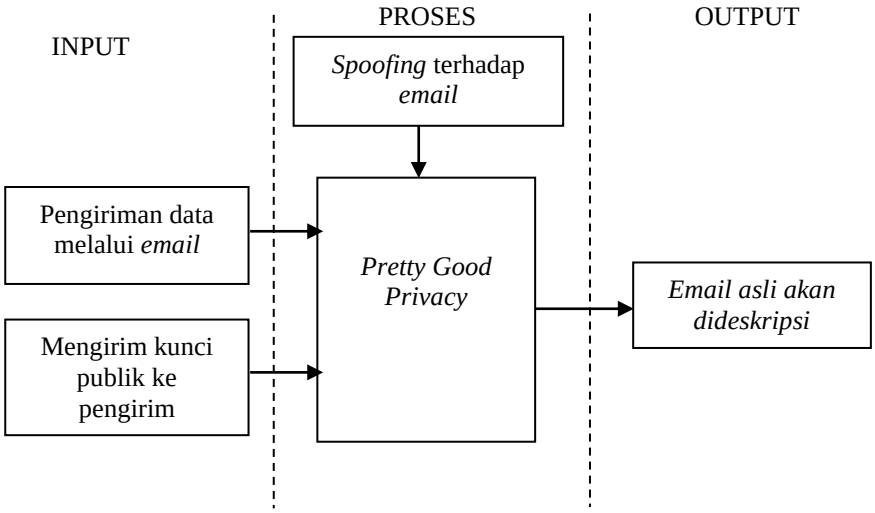
Pretty Good Privacy (PGP) dikembangkan pertama kali oleh Phil Zimmermann tepatnya akhir tahun 1980. Teknik ini digunakan untuk melindungi pesan pada *email* dengan memberikan perlindungan kerahasiaan menggunakan metode enkripsi dan deskripsi. *Pretty good privacy* menggunakan kriptografi kunci privat dan kriptografi kunci publik. Oleh karena itu, PGP mempunyai dua tingkatan kunci, yatu kunci rahasia yang disebut juga *private key* dan pasangan kunci privat-kunci publik untuk melindungi pesan. Setiap orang yang menggunakan PGP harus menerima kunci publik terlebih dahulu. Kunci publik tersebut didapatkan dengan cara membagi kunci tersebut kepada orang yang akan mengirim pesan dan berkomunikasi. Setelah kunci publik didapat proses selanjutnya adalah melakukan verifikasi kunci tersebut. Proses verifikasi tersebut juga dapat dilakukan secara tidak langsung oleh pengguna PGP [9].

Setiap orang yang menggunakan PGP harus memperoleh kunci publik. Unutk mendapatkan kunci publik, bisa diperoleh dengan mengirimkan *email* kepasa rekan yang akan saling melakukan komunikasi dengan menggunakan teknik PGP. Selain itu kunci publik bisa didapat dengan terhubung ke *server* kunci PGP yang tersebar di seluruh dunia[10]. Kunci ini dapat disimpan untuk dipublikasikan secara publik di key server. Ada beberapa *key server* PGP seperti pgp.mit.edu ataupun *key server* yang lain yang akan menyimpan kunci kunci publik. Penerima email yang terenkripsi tersebut menggunakan kunci publik dan kunci privat untuk melakukan dekripsi terhadap email tersebut. Kunci publik ini terdapat pada email yang terenkripsi tersebut dan diperoleh dengan cara mendekripsinya dengan menggunakan kunci privat. Pada proses ini pesan email asli akan muncul dan dapat dibaca oleh penerima setelah proses deskripsi email berhasil.

III. METODOLOGI PENELITIAN

Proses perancangan alat diawali dengan membuat mekanisme sistem *pretty good privacy* dan langkah kedua dengan mengaplikaskan sistem tersebut pada layanan data *email*. Lihat Gambar 3.

A. Blok Diagram Sistem



Gambar 3. Blok diagram sistem

Pada blok diagram sistem diatas menjelaskan bagaimana sistem ini dapat bekerja hingga menghasilkan output sesuai dengan yang di rancang. Adapun penjelasan pada blok diagram sistem diatas yaitu input berupa pengiriman sebuah email. Pengiriman email disini dengan diserta enkripsi data melalui PGP. Penerima email akan berbagi kunci publik kepada pengirim email. Kunci publik tersebut digunakan untuk mengenkripsi pesan yang akan dikirim. Proses berupa sistem *pretty good privacy* yang didalamnya sebagai pengolah data. PGP akan memproses email yang akan dienkripsi dengan mengubah teks asli menjadi *chipertext* yang tidak bisa dibaca oleh orang yang tidak berkepentingan. Pada sesi *spoofing* akan dilaksanakan percobaan penyerangan email yang dilengkapi dengan PGP dengan tidak dilengkapi PGP. Setelah PGP selesai mengenkripsi email, email tersebut disalurkan kepada penerima pada output sistem. Output sistem ini berupa pesan email yang terenkripsi. Kunci publik dan kunci privat akan membuka enkripsi pesan tersebut dan mengubahnya dari *chipertext* menjadi *plaintext* atau pesan asli.

B. Perancangan Sistem

Pada perancangan sistem pengamanan data melalui email menggunakan teknik *pretty good privacy* ini memerlukan beberapa *software* dan *tools* pendukung diantaranya adalah sistem operasi *ali Linux* dengan *tools Ettercap* dan virtual mesin menggunakan *VmWare Workstation Pro.*

1. Gnu Privacy Guard

Gnu Privacy Guard (GPG) merupakan implementasi dari PGP yang bersifat terbuka. Penggunaan bisa secara *GPG* versi *command line interface*, yaitu dengan mengetikkan perintah "gpg" di program terminal atau *CMD.exe* dan bisa juga menggunakan GPG program secara GUI [5].

p-ISSN 2086-5805
e-ISSN 2808-2540

2. Ettercap

Ettercap merupakan *tools packet sniffer* yang penggunaannya untuk menganalisa protokol jaringan dan mangaudit keamanan jaringan. *Ettercap* memiliki kemampuan untuk memblokir lalu lintas pada jaringan LAN, mencuri *password,* dan melakukan penyadapan aktif terhadap protokol-protokol umum, *packet sniffing* juga dapat dipakai untuk penyerangan oleh pihak yang tidak bertanggung jawab dengan tujuan mengambil data penting yang dimiliki oleh pengguna yang sedang terhubung dengan *acces point* [11][12].

3. Mailvelope

Mailvelope digunakan sebagai sarana untuk mengirim *email* dengan enkripsi dari sistem *pretty good privacy*, sehingga *email* terkirim dalam bentuk *chipertext* dan butuh pasangan kunci publik dan kunci privat untuk membukanya. *Mailvelope* berhasil terunduh di laptop/PC langkah selanjutnya adalah menambahkan kunci publik dan kunci privat baik pengirim email dan penerima email. Tujuannya adalah untuk membuat hubungan antara kunci publik dan kunci privat.

IV. PENGUJIAN DAN ANALISIS

Pada bagian ini berisi tentang pengujian email dengan *tools ettercap*. Pada tahap ini *password* dan *username email* target akan dilakukan serangkaian pengujian. Pengujian data yang dikirim melalui email baik sebelum dan sesudah diterapkan sistem *pretty good privacy.*

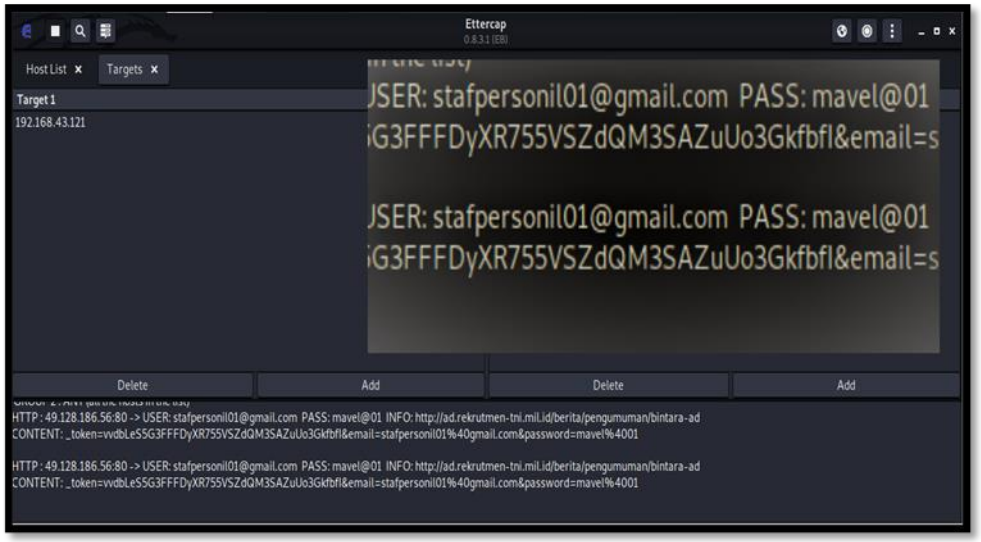
A. Pengujian Non Secure Email

1. Social Engineering

Mengidentifikasi keberadaan dan keamanan yang digunakan email target dengan menggunakan teknik *social engenering.* Teknik ini digunakan dengan segala cara agar target bersedia untuk memberitahu *IP address* komputernya dan bersedia *login* disalah satu *website* atau situs yang telah penulis inginkan. Setelah mendapatkan persetujuan target untuk *login* ke salah satu situs yang sudah dikenali *IP address*, penulis masuk untuk mendapatkan IP target.

2. Sninffing Menggunakan *Ettercap*

Percobaan ini dilakukan untuk mendapatkan informasi berakitan dengan *account username* dan *password email.* Hal ini dimaksudkan agar penyerang dalam hal ini penulis dapat melakukan akses *login* ke *account email* target.

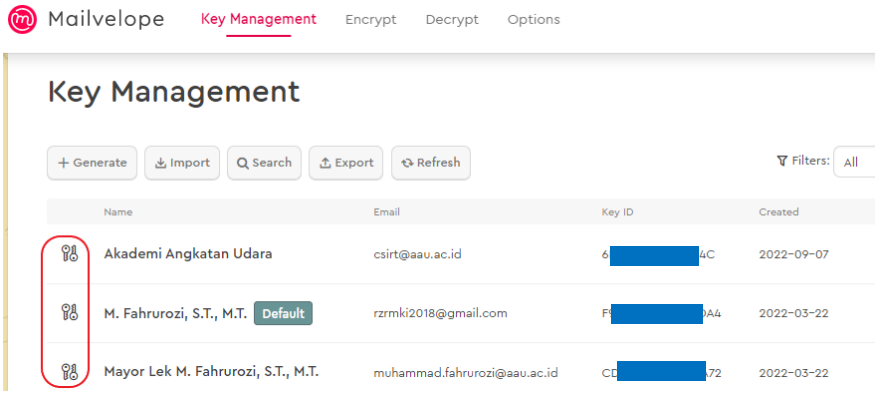


Gambar 4. Hasil serangan *sniffing*

Hasil dari s*niffing* dapat dilihat bahwa *username* dan *password* email korban dapat terlacak dan muncul di *software ettercap* saat melakukan *sniffing*. Dapat dijelaskan bahwa software ettercap dapat merekam aktivitas yang berbahaya.

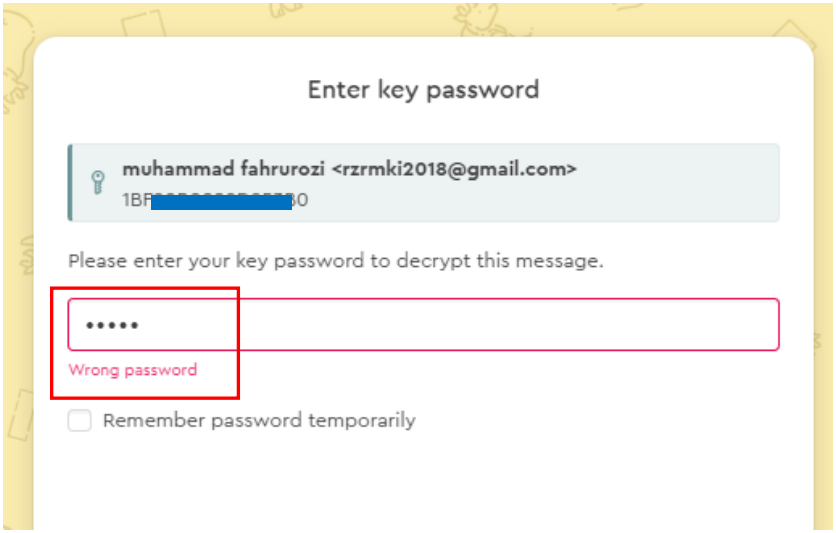
B. Pengujian Secure Email

Perancangan pengamanan email melalui teknik *pretty good privacy* ini dapat berfungsi dengan car membuat kunci publik dan kunci privat agar pesan atau dokumen yang dikirim akan diubah dari *plaintext* menjadi *chipertext.* Dapat dilihat pada Gambar 5 pasangan kunci sudah dihasilkan kedua kunci sudah saling berhubungan dengan kunci privatnya.



Gambar 5. *Key pair* dalam PGP

Pesan yang siap untuk dikirim akan diminta kunci *password* atau *paraphrase* yang dimasukan saat pembuatan kunci publik dan privat oleh penerima *email.* Pengririm *email* dan penerima *email* harus saling mengetahui kunci *paraphrase* ini. Disinilah letak kerahasiaan pesan dimana tanpa mengatahui *paraphrase* yang dibuat dan disetujui penerima *email*, *email* pesan tidak akan bisa langsung dibaca, dapat dilihat pada Gambar 6.



Gambar 6. Pesan pada *email* tidak dapat dibuka

p-ISSN 2086-5805
e-ISSN 2808-2540

C. Analisis Secure Email

Pada pengujian keamanan *email* dengan teknik *pretty good privacy* yang sudah dilaksanakan dilakukan analisis terkait percobaan pada penelitian ini sebagai berikut :

1. Hasil ketika *email* diuji dengan ARP *Poisioning* bantuan *software Ettercap* aktivitas email berhasil direkam *Ettercap*. Hasil tersebut menampilkan *username email* beserta *password email*. Hasil pengujian ini membuktikan bahwa *non secure email* tidak ada jaminan keamanannya dapat dilihat pada Tabel I.

TABEL I
HASIL PENGUJIAN *SNIFFING EMAIL* PADA LAPTOP

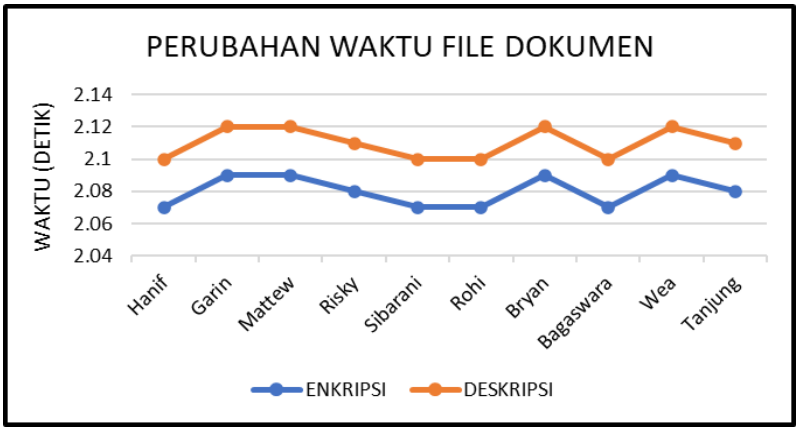
No	Jumlah Laptop	Waktu *sniffing email (second)*						
		Asusrog Strike	Asus Rog Zephyrus	HP Pavillion	HP 15 Ryzen	Asus Vivobook	Asus A409FJ	Acer Nitro-5
1	1	2,45	x	x	x	x	x	x
2	2	2,45	2,44	x	x	x	x	x
3	3	2,51	2,46	2,49	x	x	x	x
4	4	2,55	2,55	2,55	2,53	x	x	x
5	5	2,55	2,55	2,57	2,55	3,18	x	x
6	6	2,59	2,58	2,58	2,55	3,18	3,18	x
7	7	2,59	2,59	2,58	2,59	3,21	3,24	3,26

Pada Tabel I dilakukan pengujian sniffing email dengan beberapa merk laptop. Pada tujuh laptop tersebut untuk laptop dengan merk *Asus Rog Strix, Asus Rog Zephyrus, HP Pavilion* dan *HP 15 Ryzen* memiliki kapasitas RAM 16 GB sedangkan merk lainya berkapasitas sama yaitu 8 GB. Hasil pengujian menunujukan hasil bahwa dengan kapasitas RAM 16 GB performa laptop dalam melakukan *sniffing email* lebih cepat dari laptop dengan RAM 8 GB dengan rata-rata selisih 0,34s. Dari pengujian ini dapat disimpulkan bahwa waktu *sniffing email* dipengaruhi oleh kapasitas RAM laptop yang akan melakukan *sniffing email*, semakin besar RAM laptop semakin cepat laptop melakukan *sniffing email*.

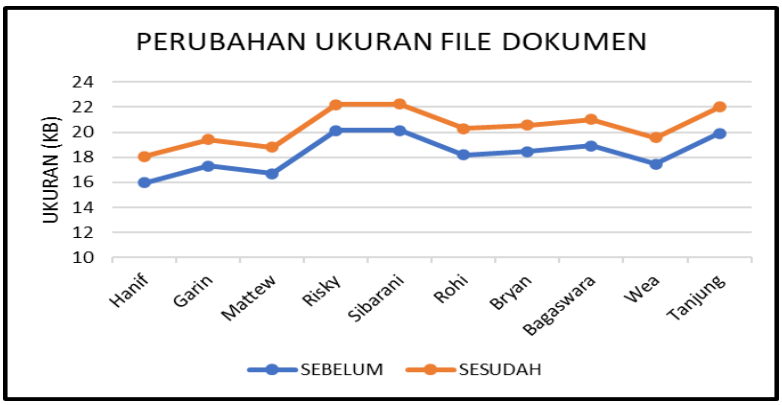
2. Pada tahap analisis selanjutnya ini akan diambil beberapa sampel email yang telah dienkripsi dengan teknik *pretty good privacy* untuk diketahui berapa waktu yang di butuhkan dalam enkripsi dan deskripsi suatu *email.* Selain itu juga akan dilakukan pengujian terhadap file yang dikirim apakah file yang dikirim dengan enkripsi *email* terjadi perubahan ukuran file atau tidak. Pengujian dibagi atas empat file yaitu file dokumen, file pdf tanpa kunci, file foto dan file video. Namun dalam naskah ini yang ditampilkan adalah pengujian pada file yang berisi dokumen, dapat dilihat pada Tabel II.

TABEL II
HASIL PENGUJIAN PENGIRIMAN DOKUMEN MELAUI SECURE EMAIL PGP

No	*Client*	Waktu *(second)*			Perubahan ukuran file (KB)		
		Enkripsi	Deskripsi	Perubahan	Sebelum	Sesudah	Perubahan
1	Hanif	2,07	2,10	0,03	15,991	18,091	21
2	Garin	2,09	2,12	0,03	17,302	19,402	21
3	Mattew	2,09	2,12	0,03	16,712	18,812	21
4	Risky	2,08	2,11	0,03	20,122	22,222	21
5	Sibarani	2,07	2,10	0,03	20,134	22,234	21
6	Rohi	2,07	2,10	0,03	18,203	20,303	21
7	Bryan	2,09	2,12	0,03	18,445	20,545	21
8	Bagaswara	2,07	2,10	0,03	18,921	21,021	21
9	Wea	2,08	2,12	0,03	17,451	19,551	21
10	Tanjung	2,09	2,11	0,03	19,921	22,021	21



Gambar 7. Hasil pengujian terhadap waktu pada pengiriman dokumen dengan email PGP



Gambar 8. Hasil pengujian terhada ukuran file pada pengiriman dokumen dengan email PGP

V. KESIMPULAN

Email dirancang untuk memudahkan pengguna email bertukar data. Email memiliki kelemahan yaitu mudah untuk diretas, hal ini dibuktikan pada percobaan dengan teknik social engineering dan tools ettercap. Username dan password email dengan mudah didapat. Semakin banyak laptop yang digunakan untuk sniffing email maka semakin besar waktu yang dibutuhkan untuk melakukan peretasan email.

Teknik pretty good privacy dalam mengenkripsi file data akan membuat file data bertambah dalam ukuran file, berdasarkan percobaan pengukuran ukuran file pada data yang dikirim dengan teknik PGP diperoleh hasil semua file percobaan menunjukan hasil peningkatan ukuran file. Hal ini disebabkan oleh saat proses enkripsi data, file data diubah dalan bentuk chipertext sehingga terdapat perubahan ukuran file. Namun perubahan ukuran file tidak merubah isi file. Isi file saat dideskripsi tidak terdapat perubahan. Sehingga PGP dapat menjamin keaslian file.

Untuk penelitian mendatang (future works) dapat dilakukan dengan membuat perbandingan efektifitas baik dari segi waktu enkripsi, ukuran pertambahan file oleh enkripsi PGP dengan teknik enkripsi lainnya.

UCAPAN TERIMA KASIH

Ucapan Terima Kasih kepada Gubernur Akademi Angkatan Udara, Marsda TNI Eko D. Indarto, S.I.P., M.Tr.(Han). yang telah memberikan izin untuk melakukan penelitian, mengakses sarana dan prasarana serta fasilitas untuk mendukung kegiatan penelitian.

p-ISSN 2086-5805
e-ISSN 2808-2540

REFERENSI

[1] A. Nitaj, “The Mathematical Cryptography of the RSA Cryptosystem,” p. 31.
[2] R. A. Azdy, “Tanda tangan Digital Menggunakan Algoritme Keccak dan RSA,” *J. Nas. Tek. Elektro Dan Teknol. Inf.*, vol. 5, no. 3, Art. no. 3, 2016.
[3] K. Om, “Secure email gateway,” in *2017 IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)*, Chennai, India, Aug. 2017, pp. 49–53. doi: 10.1109/ICSTM.2017.8089126.
[4] “Kaspersky spam and phishing report for 2021.” https://securelist.com/spam-and-phishing-in-2021/105713/ (accessed Oct. 16, 2022).
[5] B. Rahardjo, “Keamanan Informasi,” p. 47.
[6] R. I. Ananda, Fauziah, and N. Hayati, “KEAMANAN EMAIL MENGGUNAKAN METODE PRETTY GOOD PRIVACY DENGAN ALGORITMA RSA,” *J. Ilm. Inform. Komput.*, vol. 25, no. 3, pp. 213–224, 2020, doi: 10.35760/ik.2020.v25i3.3118.
[7] R. Munir, “Pengantar Kriptografi,” p. 68.
[8] B. Rahardjo, “Keamanan Perangkat Lunak,” p. 39.
[9] A. Tanoto, “Analisis Keamanan pada Pretty Good Privacy (PGP),” p. 15.
[10] N. Iriadi, “ANALISIS KEAMANAN E-MAIL MENGGUNAKAN PRETTY GOOD PRIVACY,” *Paradigma*, vol. 13, no. 1, Art. no. 1, 2011, doi: 10.31294/p.v13i1.3422.
[11] A. R. Fauzi, “MONITORING JARINGAN WIRELESS TERHADAP SERANGAN PACKET SNIFFING DENGAN MENGGUNAKAN IDS,” vol. 8, p. 7, 2018.
[12] E. Budi, D. Wira, and A. Infantono, “Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0,” *Pros. Semin. Nas. Sains Teknol. Dan Inov. Indones. SENASTINDO*, vol. 3, pp. 223–234, Dec. 2021, doi: 10.54706/senastindo.v3.2021.141.