Makalah Tugas Kuliah EL6115

Operasi Keamanan dan *Incident Handling*

PENERAPAN *END TO END ENCRYPTION* UNTUK MENJAGA KEAMANAN DAN INTEGRITAS DATA PADA PROTON MAIL

Oleh :

CINDY AGUSTINA

23215117

Dosen :

Dr. Ir. Budi Rahardjo

SEKOLAH TEKNIK ELEKTRO DAN INFORMATIKA

PROGRAM MAGISTER TEKNIK ELEKTRO

INSTITUT TEKNOLOGI BANDUNG

2016

ABSTRAK

Komunikasi merupakan faktor penting dalam kehidupan. Cara untuk berkomunikasi dibagi menjadi dua verbal dan tulisan. Berbagai media untuk komunikasi secara tulisan sudah banyak digunakan. Email merupakan salah satu contoh komunikasi secara tulisan di samping surat dan sms. Keunggulan dari email yaitu tidak mengenal batasan waktu, tempat dan biaya yang amat murah ketika seseorang ingin melakukan korespondensi dengan kenalannya di seluruh dunia selama terhubung dengan internet. Email dapat digunakan untuk melakukan komunikasi secara pribadi. Kadangkala dalam penulisan Email terdapat informasi yang hanya boleh dibaca pihak tertuju saja. Akan tetapi yang terjadi sekarang banyak pihak yang menjadi penyadap informasi tersebut dan mempergunakannya untuk hal negatif seperti kriminal. Email yang sering ada sekarang masih belum memiliki tingkat keamanan yang maksimal. Di samping itu sebagian besar server email itu berada di bawah yuridiksi EU dan US. Oleh karena itu perlu dipelajari email (contohnya proton mail) yang memiliki tingkat keamanan tinggi (menggunakan *end to end encryption*) dan memiliki server yang tidak berada di bawah yuridiksi EU dan US untuk meminimalkan penyadapan informasi.

Kata kunci: keamanan, email, *end to end encryption*, proton mail

DAFTAR ISI

DAFTAR GAMBAR

BAB I PENDAHULUAN

Komunikasi merupakan faktor penting dalam kehidupan. Cara untuk berkomunikasi dibagi menjadi dua verbal dan tulisan. Berbagai media untuk komunikasi secara tulisan sudah banyak digunakan. Email merupakan salah satu contoh komunikasi secara tulisan di samping surat dan sms. Keunggulan dari email yaitu tidak mengenal batasan waktu, tempat dan biaya yang amat murah ketika seseorang ingin melakukan korespondensi dengan kenalannya di seluruh dunia selama terhubung dengan internet. Email dapat digunakan untuk melakukan komunikasi secara pribadi. Kadangkala dalam penulisan Email terdapat informasi yang hanya boleh dibaca pihak tertuju saja. Akan tetapi yang terjadi sekarang banyak pihak yang menjadi penyadap informasi tersebut dan mempergunakannya untuk hal negatif seperti kriminal. Email yang sering ada sekarang masih belum memiliki tingkat keamanan yang maksimal. Di samping itu sebagian besar server email itu berada di bawah yuridiksi EU dan US. Oleh karena itu perlu dipelajari email yang memiliki tingkat keamanan tinggi dan memiliki server yang tidak berada di bawah yuridiksi EU dan US untuk meminimalkan penyadapan informasi.

BAB II TINJAUAN PUSTAKA

Pada bab ini diberikan tinjauan pustaka mengenai penelitian yang berhubungan dengan topik makalah antara lain: model proses umum respon insiden dan forensik komputer, model umum investigasi forensik komputer, dan metodologi investigasi bertahap untuk menelusuri penggunaan komputer.

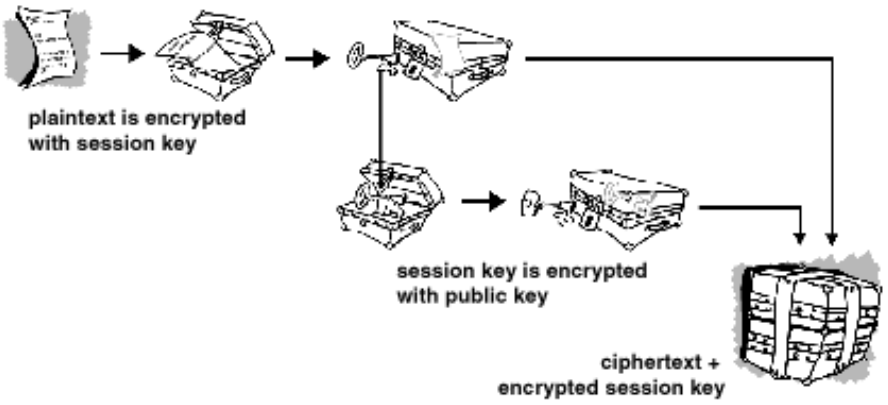
2.1 PGP (*Pretty Good Privacy*)

PGP termasuk hybrid cryptosystem yaitu kriptografi dengan kombinasi sistem sandi simetris atau dengan kunci sama dan sistem sandi asimetris atau dengan kunci publik dan private key. Penyandian dengan sistem public key yang digunakan dalam PGP ini adalah untuk mengatasi masalah distribusi kunci dalam algoritma sistem sandi simetris. Sehingga penggunaan sistem sandi simetris dan asimetris yang secara bersama-sama ini akan meningkatkan keamanan e-mail sekaligus mengatasi masalah pendistribusian kunci.

OpenPGP software menggunakan kombinasi public key dan sistem sandi simetris yang kuat untuk melindungi data dalam harddisk atau komunikasi e-mail, dengan kemampuan melindungi kerahasiaan, key management, otentikasi dan digital signature. Ketika user menggunakan aplikasi PGP untuk menyandi e-mail, yang pertama dilakukan PGP adalah kengkompres plaintext. Mengkompres plaintext ini bertujuan untuk menghemat besaran file yang akan dikirim, menghemat tempat penyimpanan dan yang lebih lebih penting, akan memperkuat kriptografinya, karena kompresi file akan menghilangkan pola-pola dalam plaintext yang dapat mengaburkan usaha-usaha kriptanalisis.

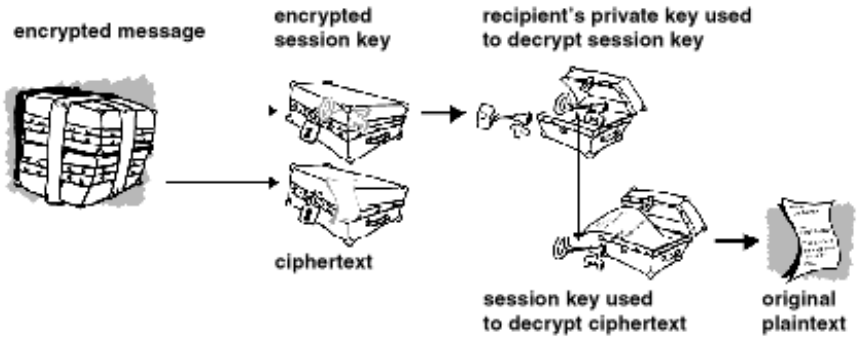
PGP kemudian membuat session key yang merupakan one-time-key system. Kunci ini terdiri dari angka acak yang dihasilkan oleh random-key-generator yang dipicu oleh gerakan mouse dan/atau ketikan tuts keyboard. Dengan sistem sandi simetris, session key digunakan untuk menyandi plaintext dan menghasilkan ciphertext. Setelah itu session key nya disandi dengan kunci publik milik si alamat (user yang

dituju). Kemudian, ciphertext dan session key yang telah disandi tersebut digabung untuk dikirimkan ke alamat. Berikut ilustrasi proses enkripsi pesan dengan PGP.



Gambar II-1 Proses Enkripsi Pesan dengan PGP [1]

Penerima e-mail (si alamat yang dituju) akan membuka e-mail dengan cara sebaliknya, menggunakan private key miliknya untuk mendapatkan session key. Setelah itu session key yang didapatkan, digunakan untuk membuka ciphertext untuk mendapatkan plaintext nya. Berikut ilustrasi proses dekripsi pesan dengan PGP.



Gambar II-1 Proses Dekripsi Pesan dengan PGP [1]

Langkah-langkah penyandian dengan PGP ini tidak perlu dilakukan sendiri oleh user, sebab software sistemnya telah otomatis melakukannya. User hanya melakukan klik mouse dan mengisi passphrase nya saja.

2.2 AES (Advanced Encryption Standard)

AES merupakan standar enkripsi simetris pengganti DES yang sudah dapat diotak – atik (di-hack). Standar ini terdiri atas 3 blok cipher, yaitu AES-128, AES-192 and AES-256, yang diadopsi dari koleksi yang lebih besar yang awalnya diterbitkan sebagai Rijndael. Proses AES terdiri dari dua yaitu enkripsi dan key schedule. Kedua proses ini berkaitan satu dengan yang lain. Di dalam proses enkripsi terdapat 4 proses yaitu subsitusi box, pergeseran baris, mix column, dan add round key yang memperoleh kunci dari key schedule.

2.3 RSA (Rivest Shamir Adleman)

RSA adalah algoritma yang melibatkan ekspresi dengan fungsi eksponensial. Plaintext dienkripsi dalam blok-blok. Setiap blok memiliki nilai biner yang kurang dari angka tertentu (n).

Proses Enkripsi

- Dalam proses enkripsi misalkan Tulus mengirimkan sebuah pesan X kepada Ariana
- Tulus haruslah menerima terlebih dahulu kunci publik dari Ariana yaitu berupa PU={e,n}. Tulus selanjutnya melakukan enkripsi pesan M dengan PU={e,n}.
    - $C = M^e \bmod n$
- Selanjutnya Tulus mengirimkan pesan C tersebut kepada Ariana

Proses Dekripsi

- Seletah ciphertext yang dikirimkan oleh Tulus diterima oleh Ariana, selanjutnya Ariana menggunakan kunci privatnya PR={d,n} untuk mendeskripsi ciphertextnya.
- Pendeskripsian pesan dilakukan dengan rumus
    - $M = C^d \bmod n$
- Didapatkan plaintext M yang merupakkan hasil dekripsi dengan PR (kunci privat).

BAB III PEMBAHASAN

3. Arsitektur Infrastuktur ProtonMail

Setelah semua langkah pada tahap praanalisis selesai dilakukan, tahap selanjutnya tahap analisis. Pada tahap ini dilakukan dua macam analisis, yaitu analisis pola penggunaan komputer dan analisis berkas pengguna.

3.1.1. *Hardware* dan *Software* ProtonMail

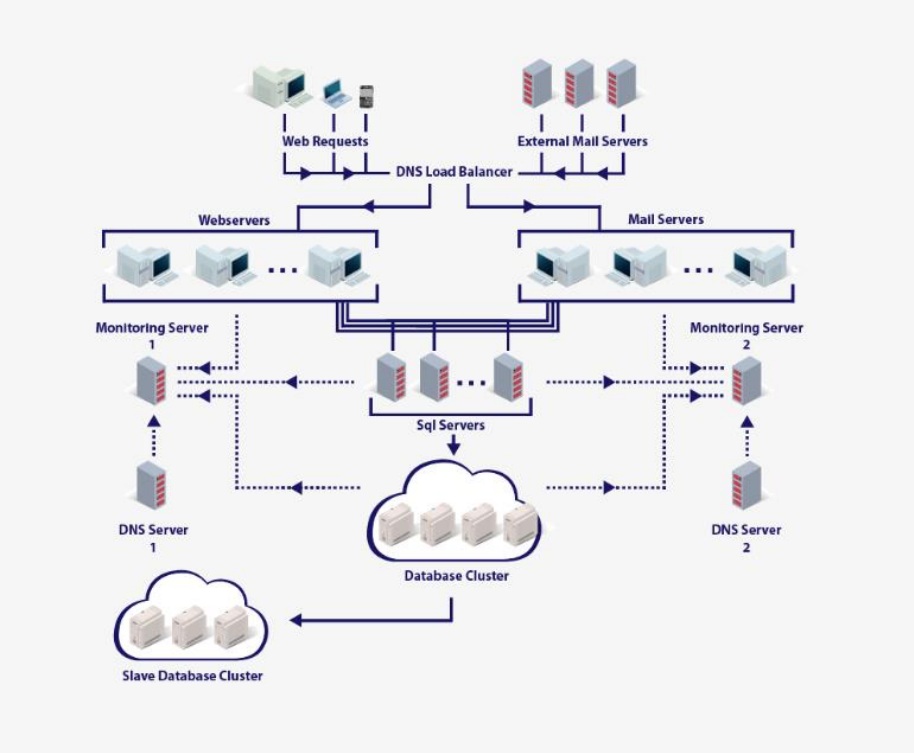
Dalam melakukan komunikasi yang aman dibutuhkan pihak ketiga (third parties). Namun saat ini pihak ketiga ini tidak dapat dipercayai untuk menjaga keamanan secara online. Oleh karena itu salah satu cara untuk menjamin tingkat keamanan yang tinggi maka dibutuhkan kontrol baik pada *server hardware* maupun pada *network*. Untuk menciptakan jaringan ini cukup sulit dan kompleks. Protonmail memiliki *server hardware* sendiri untuk menjamin keamanannya. Selain itu kontrol jaringan dilakukan dari Switzerland Host. Semua fitur yang dimiliki oleh server di enkripsi dan menggunakan RAID *arrays* yang memiliki kelebihan dalam hal penyimpanan datanya (*backup*).

3.1.2. Datacenter redundancy

Dalam tiap datacenter yang dimiliki oleh protonmail semua server terhubung pada sistem power unit yang baik. Apabila terjadi kegagalan dari upstream power maka tidak akan membuat semua server menjadi offline. Protonmail juga memiliki dua datacenter yang terpisah di Switzerland untuk menjamin apabila terjadi bencana alam pada salah satu datacenternya maka tidak akan menyebabkan adanya data yang hilang.

3.1.3. Infrastruktur Arsitektur Protonmail

Berikut ini arsitektur dari ProtonMail.



Gambar III-1 Arsitektur ProtonMail [2]

3.1.4. Load Balancing

Agar server seimbang maka dibutuhkan sistem load balancing. Pada sistem ini kapasitas single server dibuat imbang. Pada sistem ini beban dibagi antara beberapa web dan email server. Selain itu juga disediakan failover instant untuk mengatasi adanya crash. [2]

3.1.5. Web Server

Semua server ProtonMail dijalankan pada software open source berbasis Linux. Arsitektur yang dibuat memungkinkan adanya tambahan web server tanpa adanya downtime. Setiap web server dapat diambil secara offline tanpa mempengaruhi pengguna. Oleh karena itu protonmail memberikan redudansi penuh dalam hal kegagalan web server. [2]

3.1.6. Mail Server

Apabila terjadi kegagalan pada server maka tidak akan memperngaruhi emial masuk maupun keluar. Jika terjadi kegagalan dalam menyimpan database maka email server dapat menyimpan pesan masuk sampai database server kembali online. Sehingga kegagalan penyimpanan database tidak akan menyebabkan pesan masuk hilang. [2]

3.1.7. Database Layer

Pada protonmail digunakan server database cluster untuk menyimpan pesan enkripsi dari pengguna. Terdapat multiple SQL server yang akan melakukan failover secara otomatis. Apabila SQL hilang maka tidak akan membuat sistem mengalami downtime.

Sebagai lapisan tambahan keamanan dalam protonmail maka pada protonmail terdapat layer tambahan keamanan untuk melakukan backup data. Duplikat yang dilakukan adalah replikasi dari master cluster secara real time. Dimana apabila terjadi masalah atau adanya bencana maka dapat diambil data backup.

3.1.8. DNS (*Domain Name Server*)

Untuk menambah keamanan dari DNS attack dan untuk melakukan kontrol yang lebih baik pada domain maka protonmail juga menjalankan infrastruktur DNS yang didistribusikan antara dua datacenter untuk redudansi. Zona DNS diatur oleh SWITCH administer Swiss Federal Office of Communications (OFCOM).

3.1.9. *Monitoring* (Pemantauan)

ProtonMail menggunakan sistem monitoring canggih yang didistribusikan antara dua datacenter untuk memantau kondisi hardware dan juga untuk mendeteksi gangguan jaringan. Sehingga apabila suatu hari terdapat gangguan pada sistem maka penanganan dapat segera dilakukan.

3.2. Cara Kerja

Berikut adalah tahap kerja dari sistem protonmail.

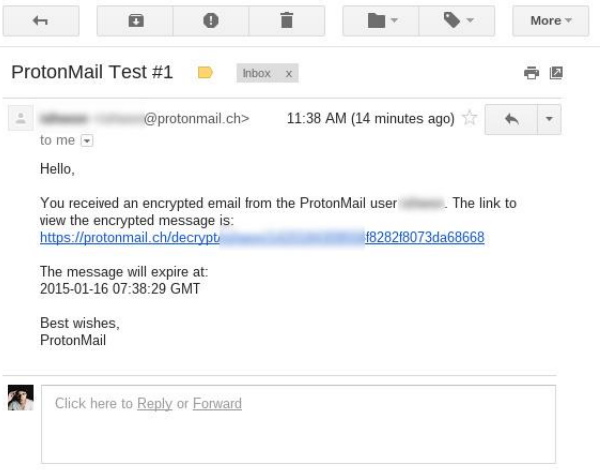
1. Ketika seorang pengguna membuat akun ProtonMail, maka browser akan menghasilkan sepasang kunci RSA publik dan privat. Kunci publik digunakan untuk mengenkripsi email pengguna dan data pengguna lainnya. Kunci privat berguna untuk mendekripsi data pengguna dan mendekripsi pesan yang masuk. Kunci privat ini dienkripsi secara simetris dengan password mailbox milik pengguna di web browser dengan menggunakan algoritma AES-256. Kunci publik dan kunci privat yang telah terenkripsi kemudian keduanya disimpan pada server ProtonMail. Jadi ProtonMail hanya menyimpan kunci dekripsi dalam bentuk terenkripsi. Oleh karena itu server tidak dapat membaca baik pesan maupun data pengguna karena semua tersimpan dalam bentuk enkripsi.
2. Proses otentikasi dan dekripsi sistem pada ProtonMail dilakukan secara terpisah yang berarti ketika masuk ke akun ProtonMail membutuhkan dua password. Password pertama digunakan untuk otentikasi pengguna dan mengambil akun yang benar. Hal ini bertujuan untuk memastikan yang melakukan login adalah benar pengguna. Setelah itu, data login terenkripsi dikirim ke pengguna sehingga pengguna dapat mengakses akun ProtonMailnya.

   Password kedua adalah MailBox Password. MailBox Password digunakan untuk mendekripsi pesan pada browser. Password dekripsi ini tidak pernah dikirim kepada pihak server ProtonMail. Oleh karena itu hanya pengguna yang dapat menggunakannya. Password ini digunakan untuk mendekripsi data pengguna di browser sehingga ProtonMail tidak pernah memiliki akses ke data didekripsi, atau password dekripsi. Untuk alasan ini, ProtonMail tidak mampu melakukan recovery password. Apabila pengguna lupa akan password dekripsinya maka pihak ProtonMail tidak dapat memulihkan datanya.
3. Pesan yang dikirim dari satu akun ProtonMail ke akun ProtonMail lain dienkripsi dengan kunci publik mailbox penerima. Ketika penerima log in, password Mailbox pengguna mendekripsi kunci privat dan membuka isi pesannya. Proses ini menggunakan implementasi PGP. Metode PGP ini

digunakan oleh Proton Mail untuk menangani pertukaran kunci dekripsi dengan menggunakan kombinasi algoritma kunci asimetris (RSA) dan algoritma kunci simetris (AES) enkripsi.

4. Pesan yang dikirim dari ProtonMail ke alamat email non-ProtonMail dapat dikirimkan dengan enkripsi atau tanpa enkripsi. Hal ini bergantung pada keinginan dari pihak pengirim pesan. Pengiriman email tanpa enkripsi berarti email dikirimkan dalam bentuk plain teks. Sedangkan pengiriman email dengan enkripsi berarti sebelum pesan dikirimkan dilakukan proses enkripsi terlebih dahulu. Enkripsi yang digunakan adalah dengan menggunakan algoritma AES. Password yang digunakan untuk mengenkripsi pesan ditentukan secara bebas oleh pihak pengirim pesan (kunci simetris). Selanjutnya pihak pengirim perlu memberikan password enkripsi pesan pada pihak penerima.

   Pihak non-ProtonMail sebagai penerima email akan menerima link. Melalui link tersebut maka pengguna dapat menuju pada situs ProtonMail. Password pre shared yang telah diberikan oleh pihak pengirim pesan digunakan untuk melakukan dekripsi pesan pada web browser.
5. Email dari alamat non-ProtonMail untuk ProtonMail dikirim dalam bentuk teks. Berikut contohnya.

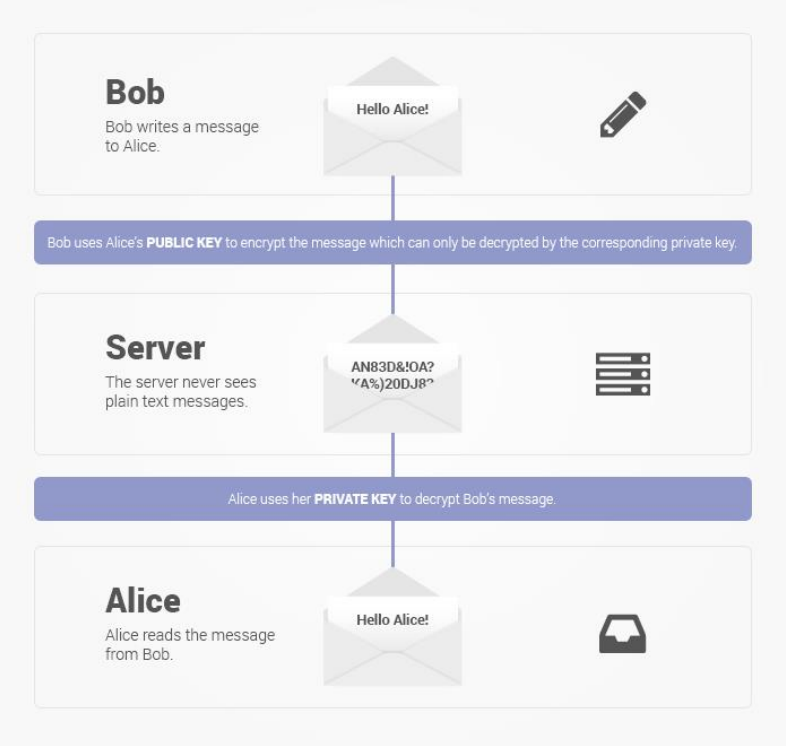


Gambar III-2 Email dari non-ProtonMail

Email yang dikirim ke penerima akan merusak diri sendiri setelah tempo waktu tertentu yang ditentukan (*Self Sensitive Destructing Message*).

3.3. Keamanan *End to End Encryption*

Pesan disimpan di server ProtonMail dalam format terenkripsi. Mereka juga ditransmisikan dalam format terenkripsi antara server dan perangkat pengguna. Pesan di antara pengguna ProtonMail juga ditransmisikan dalam bentuk terenkripsi dalam jaringan server kami yang aman. Karena data dienkripsi di semua langkah, risiko pesan intersepsi sebagian besar dihilangkan.



Gambar III-3 *End to End Encryption Proton Mail*

3.3.1 AES pada ProtonMail

AES yang digunakan pada ProtonMail adalah AES-256. AES-256 merupakan sistem enkripsi yang terkuat karena memiliki beberapa proses dalam pengenkripsiannya. Pada AES-256 terjadi pengulangan sebanyak 14 ronde. AES ini digunakan untuk enkripsi pesan yang akan dikirim baik pengiriman dari ProtonMail ke ProtonMail atau ProtonMail ke email lainnya.

3.3.2 RSA pada ProtonMail

RSA adalah sebuah algoritma enkripsi asimetrik dengan menggunakan kunci privat dan kunci publik. Protonmail menggunakan algoritma RSA ini dalam melakukan enkripsi pesan yang dikirimkan antara ProtonMail dengan ProtonMail. RSA yang digunakan dalam ProtonMail ini adalah 2048 bit. Algoritma RSA memiliki kekuatan yang baik dalam proses enkripsinya. Beberapa kekuatan yang dimiliki algoritma RSA adalah sebagai berikut.

- Dalam algoritma RSA untuk melakukan penentuan kunci tidaklah bebas, harus melalui rumus tertentu.
- Keamanan algoritma RSA terletak pada bagian matematikanya dimana sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima.
- Sulitnya untuk mencari modulo e^n akar dari sebuah bilangan komposit N yang faktor-faktornya tidak diketahui.
- Tingkat keamanan yang dimiliki algoritma RSA ini sangat bergantung pada ukuran sandinya dimana semakin besar ukuran kunci yang digunakan maka makin besar juga kemungkinan kombinasi kunci yang dapat dibobol dengan melakukan pengecekan dengan metode kombinasi satu persatu kunci (*brute force attack*). Jika misalnya digunakan panjang sandi 256 bit maka para pembobol tidak akan sanggup untuk melakukan penjebolan sandi tersebut secara satu persatu.
- Pasangan kunci privat dan kunci publik memiliki hubungan secara matematis namun tidak dapat dilihat secara komputasi untuk mendeduksi kunci yang satu ke pasangannya.

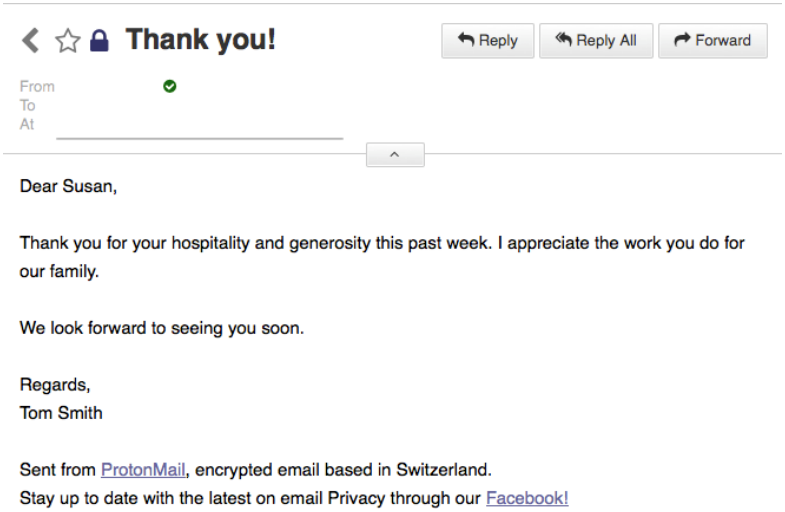
Oleh karena itu proses dekripsi dari sebuah ciphertext RSA dianggap sebagai hal yang tidak mudah karena seperti yang telah dipaparkan pada poin-poin diatas bahwa algoritma RSA ini sulit untuk di jebol. Hingga saat ini belum ada algoritma yang dapat membobol secara baik. RSA hingga saat ini adalah suatu algoritma yang sangat powerful dan cukup aman pada kriptografi kunci publik.

Secara matematika, proses yang digunakan berdasarkan fungsi-fungsi trap-door satu arah. Hal ini lah yang membuat prosedur enkripsi mudah untuk dilakukan dengan

menggunakan kunci publik oleh semua orang namun proses dekripsinya sulit dilakukan. Dimana dalam implementasinya sangat sulit untuk mendapatkan nilai p dan q untuk mendapatkan (p x q = M) haruslah sebuah bilangan yang sangat besar sehingga sulit untuk melakukan pemfaktoran bilangan prima. Pemfaktoran inilah yang dilakukan untuk memperoleh kunci privat. Sejauh pemfaktoran bilangan besar menjadi faktor-faktor prima belum ditemukan maka selama itu pula keamanan algoritma RSA dapat dipastikan terjaga.

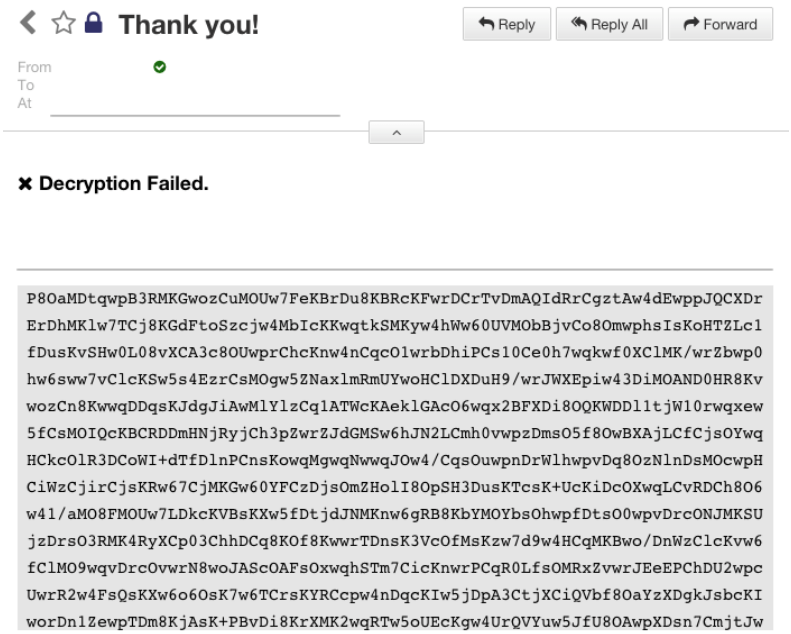
Pada tahun 2005 bilangan faktorisasi terbesar yang digunakan secara umum ialah sepanjang 663 bit, menggunakan metode distribusi mutakhir. Kunci RSA pada umumnya sepanjang 1024- 2048 bit. Beberapa pakar meyakini bahwa kunci 1024-bit ada kemungkinan dipecahkan pada waktu dekat (hal ini masih dalam perdebatan), tetapi tidak ada seorangpun yang berpendapat kunci 2048-bit akan pecah pada masa depan yang terprediksi. Oleh karena itu ProtonMail yang menggunakan algoritma RSA 2048 bit ini memiliki kekuatan enkripsi yang baik karena sulit untuk dibobol.

Pada ProtonMail ini algortitma RSA digunakan untuk mengenkripsi dan mendekripsi pesan pada browser dari pengguna. Berikut ini adalah contoh ilustrasi dari penggunaan RSA 2048 pada sisi penerima



Gambar III-4 Penggunaan RSA 2048 pada sisi penerima

Sedangkan apabila sisi browser penerima tidak menggunakan RSA 2048 maka pesan yang diterima adalah sebagai berikut ini.



Gambar III-5 Pada sisi penerima tidak menggunakan RSA 2048

3.3.3 PGP pada ProtonMail

Pada proton mail, pendistribusian kunci yang dilakukan adalah dengan menggunakan open PGP. Pada saat pertama kali melakukan pendaftaran pada ProtonMail maka pengguna akan mendapatkan sepasang kunci privat dan kunci publik. Kunci privat dibuat pada browser pada saat pertama kali membuat akun. Kunci privat ini terenkripsi oleh password mailbox dan disimpan pada server dalam bentuk terenkripsi. Sedangkan kunci publik disimpan oleh server berupa enkripsi dari kunci publik tersebut. Server tidak memiliki akses untuk mengetahui password dari mailbox. Sehingga pada dasarnya server menyimpan seluruh kunci publik dari pengguna dalam bentuk enkripsi.

Dimana PGP atau (Pretty Good Privacy) adalah sistem yang terdiri dari gabungan algoritma untuk melakukan enkripsi pesan. PGP berguna untuk mengkodekan data sehingga hanya orang tertentu saja yang bisa membukanya. E-mail yang dikirim lewat internet melalui program PGP akan diubah bentuknya sehingga menjadi tidak terbaca. Kemudian hanya orang yang berhak (penerima resmi) yang dapat mengubah kembali E-mail tersebut dari bentuk yang tak terbaca menjadi terbaca kembali seperti semula.

Biasanya hal ini disertai dengan tanda tangan digital yang membuktikan bahwa pesan yang kita kirim memang berasal dari kita.

3.3.4. Keamanan ProtonMail

Berikut ini beberapa keamanan yang diberikan PortonMail yang dimiliki oleh ProtonMail. [3]

- Protonmail memiliki tingkat keamanan yang tinggi.
- Mempersulit *hacker* untuk melakukan gangguan sistem atau pencurian data.
- Melindungi hak asazi manusia dalam melakukan komunikasi, berpendapat serta melakukan kritik secara online. Hal ini ditunjukan dengan sistem keamanannya yang tinggi serta dilindungi oleh peraturan privasi yang ada pada Swiss.
- Pesan yang dikirimkan mampu menghancurkan diri nya sendiri dalam tempo waktu tertentu yang ditentukan (*Self Sensitive Destructing Message*). Secara default pesan akan terhapus setelah 14 hari atau waktu dapat ditentukan oleh pengirim. [3]

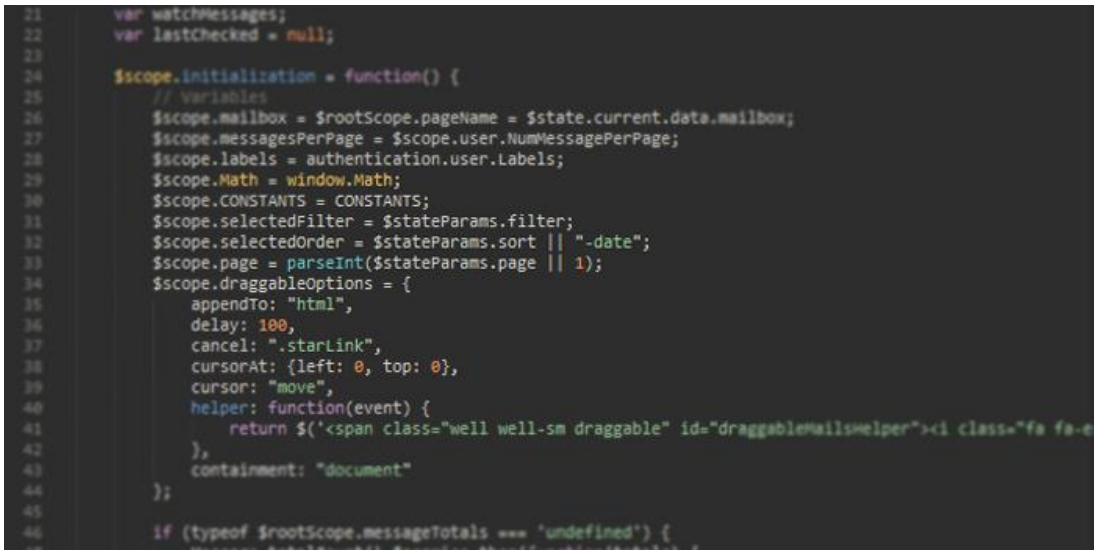
- Bersifat Zero Access dimana server tidak dapat membaca data karena semua data yang diterima telah terenkripsi terlebih dahulu pada browser client. Selain itu pada server juga di enkripsi dengan multiple password layer dan tidak seorangpun mengetahui passwordnya. Sehingga pengguna adalah satu satunya yang dapat melakukan akses pada email. [4]
- Server ditempatkan pada pegunungan Alpen di Swiss (bekas pusat komando militer) dengan hukum privasi yang tinggi.
- Bekerjasama dengan Switzerland (*Swiss based*) Dimana semua data pengguna dilindungi oleh Swiss Federal Data Protection Act (DPA) dan Swiss Federal Data Protection Ordinance (DPO) yang memberikan kekuatan keamanan yang paling baik di dunia. Hanya perintah dari pengadilan Cantonal Court of Geneva atau Swiss Federal Supreme Court yang dapat memaksa ProtonMail untuk membuka informasi mengenai pengguna. [5]

- *Hardware Level Security*. Semua data yang tersimpan pada *hardware* datacenter disimpan dalam bentuk enkripsi. ProtonMail memiliki hardware sendiri yang digunakan sebagai datacenter penyimpanan segala data dan pesan pengguna. Segala pengelolaan data dan email yang dikirimkan diatur oleh ProtonMail tanpa adanya *third parties* sehingga membuat keamanan menjadi lebih terjaga. Server yang digunakan berisikan data terenkripsi dengan beberapa lapisan password.
- Fasilitas anonimitas dimana tidak ada pelacakan alamat IP dari pengguna dan juga tak ada data log-in pengguna yang diketahui oleh server.
- Menyediakan dalam versi gratis dan juga berbayar. Untuk ProtonMail berbayar maka memiliki fitur fasilitas yang lebih banyak.
- Kapasitas yang disediakan adalah 100 MB untuk masing-masing pengguna (500 pesan/bulan)
- Terdapat dua password keamanan yang menjamin kerahasiaan lebih baik. Password yang pertama yaitu password login yang berfungsi untuk melakukan autentifikasi pengguna. Password yang kedua yaitu mailbox password yang digunakan untuk mendekripsi pesan pada browser. [1]

Gambar III-6 End to End Encryption [6]

- Bersifat End to End Encryption dimana semua data yang ada pada jaringan berupa chipertext sehingga data yang dikirimkan tidak mungkin dicegat atau diuraikan oleh *intruder*. Pesan yang disimpan pada server ProtonMail dalam format terenkripsi. Pesan tersebut ditransmisikan dalam format terenkrisi antara server dengan browser pengguna.
- *Open Source Cryptography*. ProtonMail mengimplementasikan algoritma AES 256, RSA 2048 dan juga Open PGP. Seluruh *library* yang digunakan untuk memberikan keamanan pada ProtonMail adalah bersifat open source dan tidak ada

yang disembunyikan. Dengan menggunakan ketiga kombinasi algoritma kriptografi tersebut maka ProtonMail dapat dipercaya memberikan perlindungan yang cukup aman. [2]



```
var watchMessages;
var lastChecked = null;

$scope.initialization = function() {
    // variables
    $scope.mailbox = $rootScope.pageName = $state.current.data.mailbox;
    $scope.messagesPerPage = $scope.user.NumMessagePerPage;
    $scope.labels = authentication.user.Labels;
    $scope.Math = window.Math;
    $scope.CONSTANTS = CONSTANTS;
    $scope.selectedFilter = $stateParams.filter;
    $scope.selectedOrder = $stateParams.sort || "-date";
    $scope.page = parseInt($stateParams.page || 1);
    $scope.draggableOptions = {
        appendTo: "html",
        delay: 100,
        cancel: ".starLink",
        cursorAt: {left: 0, top: 0},
        cursor: "move",
        helper: function(event) {
            return $('<span class="well well-sm draggable" id="draggableMailsHelper"><i class="fa fa-e
        },
        containment: "document"
    };

    if (typeof $rootScope.messageTotals === 'undefined') {
```

Gambar III-7 Open Source Cryptography [7]

- Sistem otentifikasi dan enkripsi terpisah sehingga sistem lebih aman.
- Proses enkripsi yang dilakukan bersifat invisible dari pengguna dimana pada saat melakukan proses enkripsi dan dekripsi pesannya maka tidak perlu menginstal aplikasi dan tidak ada kunci yang perlu di generate. Hal ini membuat ProtonMail menjadi mudah untuk digunakan.
- *No Advertisers, No Governments, No Third Parties*. Hanya pengguna yang dapat melakukan akses pada inbox pesan. Hal ini bererti bahwa tidak ada iklan, campur tangan pemerintah maupun pihak ketiga yang mendapatkan akses data pengguna. Dengan menggunakan ProtonMail maka dapat dipastikan komunikasi pribadi tetap terjaga dengan baik. [4]
- Protonmail didesain agar mudah digunakan oleh pengguna dan untuk melakukan produktifitas yang tinggi. Tampilan ProtonMail dirancang untuk mempermudah pengguna melakukan pekerjaan lebih cepat dan menyenangkan untuk digunakan. Setiap detail dari desain toolbar dan tombol dioptimalkan untuk mempermudah pengguna dalam membaca dan mengirimkan email.

- Digunakan SSL Swiss untuk mengamankan koneksi antara server dengan client. Data pesan antara server dengan client telah terenkripsi dan ditambahkan SSL untuk lapisan perlindungan dan untuk memastikan bahwa halaman web browser yang dibuka oleh pengguna tidak diganggu oleh pihak ketiga yang mengganggu (*man in the middle attack*). *Certivicate Authority* (CA) yang diguanakan adalah SwissSign yang merupakan anak perusahaan dari SwissPost (lembaga publik yang dimiliki oleh Swiss Convederation dan bukan dibawah kendali AS atau lembaga pemerintahan Uni Eropa). Sekarang telah dirilis kunci hash SHA1 untuk kunci publik dari SSL ini.
- Memungkinkan berkomunikasi secara aman dengan pengguna Non-ProtonMail. ProtonMail ini mendukung pengiriman komunikasi terenkripsi untuk pengguna Non-ProtonMail. Pihak Non-ProtonMail akan menerima enkripsi simetris. Pada saat pengirim (ProtonMail) mengirim pesan yang dienkripsi untuk pengguna non-ProtonMail maka penerima (Non-ProtonMail) akan menerima link yang memuat pesan terenkripsi pada browsernya. Selanjutnya pihak penerima melakukan dekripsi dengan menggunakan passphrase yang telah dibagikan dari pihak pengirim pesan. [8]

BAB IV KESIMPULAN

Dari hasil pembahasan mengenai ProtonMail ini maka dapat ditarik beberapa kesimpulan sebagai berikut ini.

1. Protonmail adalah layanan email yang server protonmail ini terletak di Swiss dimana pada negara ini keamanan privasi sangat dijaga.
2. Layanan email ini diklaim paling aman dan kebal dari penyadapan.
3. ProtonMail menggunakan end-to-end encryption yang artinya pesan yang dikirimkan berupa enkripsi data dari server hingga tiba pada clientnya sehingga data sulit untuk dicegat ataupun dicuri ditengah perjalanan.
4. Untuk pengiriman email antar protonmail tingkat keamanan yang digunakan tinggi karena mengkombinasikan algoritma enkripsi simetri AES-256 dan asimetri RSA-2048. Sedangkan untuk pengiriman email protonmail ke non-protonmail menggunakan algoritma enkripsi simetri AES-256.
5. Dalam pendistribusian kuncinya, ProtonMail menggunakan metode pertukaran kunci openPGP yaitu dengan menggunakan kunci public yang disimpan secara terenkripsi
6. Memiliki kemampuan *self sensitive-destructing message* yaitu fitur email yang bisa "rusak" dalam jangka waktu tertentu.

DAFTAR PUSTAKA

[1] "How PGP works," [Online]. Available: https://users.ece.cmu.edu/~adrian/630-f04/PGP-intro.html. [Accessed 18 May 2016].

[2] A. Yen, "Infrastructure Upgrades," Protonmail Technologies AG, 17 December 2014. [Online]. Available: https://protonmail.com/blog/infrastructure-upgrades/. [Accessed 18 May 2016].

[3] A. Yen, "Security Details," ProtonMail Technologies AG, [Online]. Available: https://protonmail.com/security-details. [Accessed 20 May 2016].

[4] A. Yen, "Why ProtonMail," Protonmail Technologies AG, [Online]. Available: https://protonmail.com/why-protonmail. [Accessed 18 May 2016].

[5] A. Yen, "Why Switzerland?," Proton Technologies AG, 19 May 2014. [Online]. Available: https://protonmail.com/blog/switzerland/. [Accessed 18 May 2016].

[6] A. Yen, "What is End-to-End Encryption?," Proton Technologies AG, 4 May 2015. [Online]. Available: https://protonmail.com/blog/what-is-end-to-end-encryption/. [Accessed 18 May 2016].

[7] A. Yen, "ProtonMail Open Source Cryptography," Proton Technologies AG, 13 June 2015. [Online]. Available: https://protonmail.com/blog/protonmail-open-source-crytography/. [Accessed 18 May 2016].

[8] A. Yen, "ProtonMail," [Online]. Available: https://www.indiegogo.com/projects/protonmail#/story. [Accessed 18 May 2016].