ANALISA PROTEKSI SERANGAN ENKRIPSI DATA MELALUI KEAMANAN MODEL KRIPTOGRAFI KOMUNIKASI JARINGAN KOMPUTER

Herlan Sutisna
Teknik Informatika, Universitas BSI
herlan.her@bsi.ac.id

Abstract - Security in the use of information technology system is growing. and it should be examined how security system of data transmission mechanism, especially using cryptographic encryption methods can be established with one other. the problem of data transmission email or message has become an important issue in this information technology era. Sometimes these data should be confidential, not to be a public secret, if the data was exposed by another, it can be abuse for any crime without any responsibility. data transmission which increasingly global. and open system concept of networking, allow someone to get into the network. this matter make the data transmission process unsafe and possible to be abuse by someone in the middle of data transmission. in this paper, there is a theoritical analysis of the description security hole using theoritical review methods, for example of adaptive chosen plaintext attack as a special case of a choose the example of plaintext dynamically, and change their plaintext base on the results of the previous encryption. also discussed how to evercome the attack, and also the advance tages of encryption chryptography models such as public key cryptosystem which has two primary uses, encryption and digital signature. in the system, rach person gets a pair of keys, the first called as public key and second called as private key, it means there is a security hole and the ways to evercome it by autoteknis or manually, and also the advantages of criptography performance through the analysis of the mechanism of sending and receiving data.
Key Word : encryption, crypthography, security, information system

Abstrak - *Keamanan dalam menggunakan teknologi sistem informasi semakin berkembang dan perlu dicermati bagaimana suatu System Security dari mekanisme pengiriman data khususnya menggunakan metode enkripsi kriptografi dapat terjalin dengan baik satu sama lain. Masalah pengiriman data email ataupun pesan telah menjadi masalah penting pada era teknologi informasi seperti sekarang ini. Terkadang data-data ini harus bersifat rahasia agar tidak diketahui secara umum. Apabila data tersebut diketahui, maka data tersebut dapat disalahgunakan untuk kejahatan oleh orang lain Lalu lintas pengiriman data dan informasi yang semakin global, serta konsep open system dari suatu jaringan memudahkan seseorang untuk masuk ke dalam jaringan tersebut. Hal tersebut dapat membuat proses pengiriman data menjadi tidak aman dan dapat saja dimanfaatkan oleh pihak lain yang tidak bertanggungjawab, yang mengambil informasi atau data yang dikirimkan tersebut di tengah perjalanan. Dalam jurnal ini diberikan suatu analisa teoritik mengenai gambaran analisa lubang keamanan dengan metode Theoritical Review, contoh dari Serangan Adaptive-chosen-plaintext yaitu kasus khusus dari serangan chosen-plaintext dimana penyerang dapat memilih contoh plaintext secara dinamis, dan mengubah pilihannya berdasar dari hasil enkripsi sebelumnya dan dibahas juga cara mengatasi dari serangan, keunggulan yang diciptakan oleh model enkripsi kriptografi seperti Public-key CryptoSystems yang memiliki dua kegunaan primer, enkripsi dan tanda tangan digital. Pada sistemnya, setiap orang mendapatkan sepasang kunci, satu disebut kunci Public dan yang lain disebut kunci privat, menjelaskan bahwasannya terdapat suatu celah keamanan dan terdapat cara mengatasi secara autoteknis maupun dari sisi pengguna secara manual, dan menjelaskan bagaimana keunggulan dari kinerja kriptografi melalui analisa mekanisme pengiriman dan penerimaan data.*
Kata Kunci : ***enkripsi, kriptografi, keamanan, sistem informasi***

I. PENDAHULUAN

Keamanan dalam menggunakan teknologi informasi dirasakan merupakan suatu hal yang sangat penting dan vital. Seiring kemajuan, banyak ditemui celah yang dapat merusak komunikasi. Saat komunikasi diserang, maka sejumlah data dapat rusak atau bahkan hilang begitu saja. Kasus penyadapan telah ada sekitar 100 tahun yang lalu. Salah satu contoh kasus penyadapan yang terkenal yaitu perkara yang dilaporkan pada tahun 1867 oleh sebuah makelar saham Wall Street bekerjasama dengan Western Union untuk melakukan penyadapan ke operator telegrap yang dikirim ke koran yang ada di Timur Tengah kemudian pesan telegrap tersebut diganti dengan yang palsu. Beberapa kasus menyangkut keamanan jaringan komputer saat ini menjadi suatu pekerjaan yang membutuhkan biaya penanganan dan pengamanan yang sedemikian besar. Sistem-sistem vital, seperti sistem pertahanan, sistem perbankan, sistem bandara udara dan sistem-sistem lain yang setingkatnya, membutuhkan tingkat keamanan yang sedemikian tinggi Hal tersebut tentunya, membuat penulis perlu mencermati bagaimana suatu *System Security* dari mekanisme pengiriman data dapat terjalin dengan baik satu sama lain.

Perkembangan komputer dan sistem komunikasi berdampak pada permintaan dari sektor-sektor privat sebagai sarana untuk melindungi informasi dalam bentuk digital dan untuk menyediakan layanan keamanan. *Cryptography* atau kriptografi lebih populer ketika pertama dikenalkan sebagai keamanan dalam tanda tangan digital. Salah satu kontribusi penting dari kriptografi kunci publik adalah tanda tangan digital. Ini bermula pada 1991 standar internasional pertama untuk tanda tangan digital (ISO/IEC 9796) diadopsi. Standar ini berdasar pada rancangan kunci publik RSA. Pada 1994 pemerintah US mengadopsi Digital Signature Standard, sebuah mekanisme yang berdasar pada rancangan kunci publik ElGamal.

Namun, seiring kemajuan teknologi kriptografi hampir dipastikan sebagai suatu andalan dalam penyimpanan dan rahasia data oleh user privat. Keamanan menggunakan kriptografi, sebab dalam kriptografi dibutuhkan mekanisme-mekanisme yang merupakan bentuk enkripsi dan dekripsi dari suatu data, sehingga untuk memecahkan tanpa suatu ketentuan atau alat khusus akan dirasakan sangat sulit.

Dalam suatu perusahaan, maka kriptografi akan digunakan dalam proses komunikasi data. Melihat dari lingkup besarnya suatu perusahaan bergerak, maka sumber dayanya baik sumber daya manusia maupun infrastruktur TI dan biaya, ada beberapa aplikasi kriptografi yang mungkin diterapkan dalam lingkungan perusahaan itu sendiri. Untuk setiap perusahaan yang telah memiliki divisi TI sendiri, penerapan aplikasi kriptografi ini akan lebih murah dan mudah. Aplikasi-aplikasi kriptografi yang dapat diterapkan antara lain enkripsi pada password, file, dan email. Pengguna diberikan ID dan password untuk mengakses sistem yang ada. Password dienkripsi untuk mencegah terjadinya akses ilegal terhadap sistem misalnya pencurian data-data penting oleh mereka yang tidak berhak. Demikian juga enkripsi pada file-file penting dapat dilakukan (misalnya file yang berisi data keuangan). Metode enkripsi yang digunakan dapat berbentuk enkripsi kunci simetris, misalnya menggunakan algoritma DES, RSA, dll. Untuk mendapatkan algoritma enkripsi ini tidak dibutuhkan biaya karena telah dipublikasikan secara umum. Biaya yang dibutuhkan hanyalah biaya pengembangan dan biasanya biaya ini tidak terlalu besar jika pengembangannya dilakukan sendiri oleh divisi TI yang dimiliki perusahaan itu sendiri. (*in house development*). Karenanya untuk menunjang bagaimana kriptografi berjalan dalam prosesnya saat penyimpanan data di dalam perusahaan, maka penulis akan melakukan analisa terhadap proses tersebut.

II. KAJIAN PUSTAKA

Pada penelitian sebelumnya Kastawan, I K. (2003). “Pembuatan Perangkat Lunak Pengaman Pengiriman Pesan Via Email dengan Algoritma RSA”.mengenai algoritma RSA yang digunakan terkait tentang pengamanan pesan via email. Pengamanan pesan yang dilakukan untuk mengenkripsi email agar terjaga kerahasiaannya saat sampai ke penerima pesan yang dituju. Hasilnya ketika pengiriman E-mail dengan

menggunakan algoritma RSA lebih aman dari serangan dan pencurian data.

Pada Penelitian sebelumnya Arief Muhammad, Fitriyani, Nurul Ikhsan Yang Berjudul" Kriptografi RSA Pada Aplikasi *File Transfer Client- Server Based"* Dalam penelitian tersebut, Enkripsi RSA pada file akan diimplementasikan dalam sebuah aplikasi FTP *client* dengan mengorbankan waktu *upload* tetapi menghasilkan keamanan yang lebih baik. Selain itu terjadi peningkatan ukuran *file* karena mekanisme base64 dan enkripsi RSA yang diaplikasikan ke setiap *byte* pada *file* yang akan dienkripsi.. Saat proses *upload, file* akan dienkripsi sehingga *file* tersebut tidak bisa dibaca sembarang orang. Hanya yang memiliki kunci yang dapat membacanya. Dengan ini dihasilkan mekanisme berbagi *file* yang lebih aman walaupun menggunakan sebuah jaringan publik.

Dari beberapa percobaan, dihasilkan bahwa algoritma RSA dapat digunakan untuk enkripsi dan dekripsi sebuah *file* untuk meningkatkan keamanan pada suatu jaringan publik. Namun dikarenakan penggunaan JVM yang terbatas, ukuran *file* yang dapat dienkripsi juga terbatas.

Menurut Florensia (2005) "Kriptografi merupakan seni dan ilmu menyembunyikan informasi dari penerima yang tidak berhak. Kata *Cryptography* berasal dari kata Yunani *kryptos* (tersembunyi) dan *graphein* (menulis)". Sedangkan menurut William (2006) "*Cryptography* berasal dari kata *Crypto* yang berarti "*hidden, secret*" dan pada bidang studi informatika dapat diartikan dengan studi mengenai menyembunyikan informasi atau informasi yang disembunyikan (*hiding information*)". Pada saat ini, ilmu ini berkembang dan dapat dikategorikan menjadi tiga kelompok utama, yaitu:

1. Penggunaan operasi matematika yang mengubah *plaintext* (sumber informasi atau informasi aslinya) ke dalam bentuk *ciphertext* (informasi yang sudah dikodekan) menggunakan kunci enkripsi.
2. Apakah dibentuk sebuah *block* atau sebuah *stream cipher*.
3. Penggunaan satu atau dua kunci sistem.

Kriptografi dapat dibagi atas 4 jenis, yaitu: (1) *Symmetric Cipher*s, (2) *Public-key* Enkripsi and *Hash Function*, (3) *Network Security Applications*, dan (4) *System Security*. Pada *Symmetric Chiphers*, ada 5 teknik utama yang dapat dilakukan, yaitu *Symmetric cipher models*, *substitution techniques*, *transposition techniques, rotor machines*, dan *steganography*.

Kriptografi akan berbeda dengan Steganografi, sebab Steganografi adalah seni menyembunyikan keberadaan pesan. Kata "*steganography*" berasal dari kata Yunani "*steganos*" yang berarti "terlindungi", dan "*graphein*" yang berarti "menulis". Sebuah contohnya adalah *Microdot*, yang mengkompresi pesan kedalam ukuran *period* atau *dot*. Steganografi dapat digunakan untuk membuat "watermark" digital untuk mendeteksi penyalinan image digital secara ilegal.

Merujuk pada keamanan data yang telah menggunakan kriptografi dengan melakukan enskripsi adalah, bahwa pengertian *Encryption* adalah transformasi data kedalam bentuk yang tidak dapat terbaca tanpa sebuah kunci tertentu. Tujuannya adalah untuk meyakinkan privasi dengan menyembunyikan informasi dari orang-orang yang tidak ditujukan, bahkan mereka mereka yang memiliki akses ke data terenkripsi. Setiap bentuk enkripsi pastinya akan membutuhkan suatu dekripsi, di mana dekripsi merupakan kebalikan dari enkripsi, yaitu transformasi data terenkripsi kembali ke bentuknya semula (Florensia, 2005).

Keamanan Jaringan Komputer Masalah keamanan jaringan komputer secara umum dibagi menjadi empat kategori yang saling berkaitan:

1. *Secrecy*/*confidentiality*
   Informasi yang dikirim melalui jaringan komputer harus dijaga sedemikian rupa kerahasiaannya sehingga tidak dapat diketahui oleh pihak yang tidak berhak mengetahui informasi tersebut.
2. *Authentication*:
   identifikasi terhadap pihak-pihak yang sedang melakukan komunikasi melalui jaringan harus dapat dilakukan. Pihak yang berkomunikasi melalui jaringan harus dapat memastikan bahwa pihak lain yang diajak berkomunikasi adalah benar-benar pihak yang dikehendaki.
3. *Nonrepudiation*:
   Pembuktian korespondensi antara pihak yang mengirimkan informasi dengan informasi yang dikirimkan juga

perlu dilakukan dalam komunikasi melalui jaringan komputer. Dengan pembuktian tersebut, identitas pengirim informasi dapat dipastikan dan penyangkalan pihak tersebut atas informasi yang telah dikirimnya tidak dapat dilakukan.

4. *Integrity control*:
   informasi yang diterima oleh pihak penerima harus sama dengan informasi yang dikirim oleh pengirim. Informasi yang telah mengalami perubahan dalam proses pengiriman, misalnya diubah oleh pihak lain, harus dapat diketahui oleh pihak penerima.

Komunikasi adalah proses jalur informasi dan pengertian dari seseorang ke orang lain. (davis, 2010)

Menurut Gollmann dalam Ariyus ("Keamanan komputer adalah berhubungan dengan pencegahan dini dan deteksi terhadap tindakan pengganggu yang tidak dikenali dalam sistem komputer." Ariyus 2005).

III. PEMBAHASAN

A. Analisa Lubang Keamanan: Kajian Serangan Pada Enkripsi melalui Model Kelemahan Kriptografi

Sesungguhnya hakikat kriptografi adalah, suatu proses yang bertujuan untuk *Deter* (menghalangi), *Prevent* (mencegah), *Detect* (menemukan), *Correct* (membetulkan) atas pelanggaran keamanan, termasuk pada saat melakukan pengiriman (*transmission*) informasi. Kriptografi dalam keamanan komputer tidak hanya akan selamanya tidak dapat ditembus oleh serangan *attacker*, namun suatu celah dari sistem juga dapat diwujudkan dan mampu ditembus, sehingga dalam hal ini, penulis mencermati bagaimana membuat suatu proteksi data dalam keamanan komputer.

Kriptografi saat ini lebih dari enkripsi dan dekripsi saja. Otentikasi menjadi bagian dari kehidupan kita sama seperti privasi. Kita menggunakan otentikasi dalam kehidupan sehari-hari, sebagai contoh saat kita menandatangani sejumlah dokumen dan saat kita berpindah ke dunia dimana keputusan dan persetujuan kita dikomunikasikan secara elektronis, kita membutuhkan teknik-teknik untuk otentikasi. Kriptografi menyediakan mekanisme untuk prosedur semacam itu. *Digital signature* (tanda tangan digital) mengikat dokumen dengan kepemilikan kunci tertentu, sedangkan *digital timestamp* mengikat dokumen dengan pembuatnya pada saat tertentu.

Enkripsi dan dekripsi pada umumnya membutuhkan penggunaan sejumlah informasi rahasia, disebut sebagai kunci. Untuk beberapa mekanisme enkripsi, kunci yang sama digunakan baik untuk enkripsi dan dekripsi; untuk mekanisme yang lain, kunci yang digunakan untuk enkripsi dan dekripsi berbeda. Dua tipe dasar dari teknologi kriptografi adalah *Symmetric key (secret/private key) Cryptography* dan *aSymmetric (Public key) Cryptography*. Pada *Symmetric key Cryptography*, baik pengirim maupun penerima memiliki kunci rahasia yang umum. Pada *asymmetric key Cryptography*, pengirim dan penerima masing-masing berbagi kunci publik dan privat.

Keamanan dalam penggunaan kriptografi, umumnya juga dapat didasari pada beberapa modus untuk mengambil atau merusak data yang dikirim. Oleh karena itu, maka pada dasarnya serangan terhadap primitif dan protokol kriptografi dapat dibedakan menjadi dua jenis yaitu:

1. Serangan pasif adalah serangan dimana penyerang hanya memonitor saluran komunikasi. Penyerang pasif hanya mengancam kerahasiaan data.
2. Serangan aktif adalah serangan dimana penyerang mencoba untuk menghapus, menambahkan, atau dengan cara yang lain mengubah transmisi pada saluran. Penyerang aktif mengancam integritas data dan otentikasi, juga kerahasiaan.

Serangan pada enkripsi data adalah hal yang menjadi titik bagaimana penulis akan melakukan analisa proteksi keamanannya. Serangan-serangan primitif akan menekankan pada kelemahan kriptografi dalam melakukan enkripsi, karenanya dalam hal ini, penulis memahami bahwa, serangan ini secara umum diklasifikasikan dalam enam kategori. Tujuan dari penyerang dalam semua kasus adalah untuk dapat mendekrip sebuah *ciphertext* baru tanpa informasi tambahan. Yang menjadi idaman bagi penyerang adalah untuk mengekstrak kunci rahasia.

1. Serangan *Ciphertext-only* adalah salah satu serangan dimana penyerang mendapatkan contoh dari *ciphertext*, tanpa *plaintext* yang berhubungan dengannya. Data ini relatif mudah

didapatkan dalam banyak skenario, tetapi serangan yang berhasil biasanya sulit, dan membutuhkan contoh *ciphertext* yang sangat besar.
2. Serangan *Known-plaintext* adalah salah satu serangan dimana penyerang mendapatkan contoh *ciphertext* dan juga *plaintext* yang berhubungan.
3. Serangan *Chosen-plaintext* adalah salah satu serangan dimana penyerang dapat memilih kuantitas *plaintext* dan kemudian mendapatkan *ciphertext* terenkripsi yang berhubungan.
4. Serangan *Adaptive-chosen-plaintext* adalah kasus khusus dari serangan chosen-*plaintext* dimana penyerang dapat memilih contoh *plaintext* secara dinamis, dan mengubah pilihannya berdasra dari hasil enkripsi sebelumnya.
5. Serangan *Chosen-ciphertext* adalah salah satu serangan dimana penyerang dapat memilih sebuah *ciphertext* dan mencoba mendapatkan *plaintext* terdekripsi yang berhubungan. Tipe serangan ini biasanya banyak dilakukan pada *Public-key CryptoSystem*s.
6. *Adaptive-chosen-ciphertext* adalah versi adaptif dari serangan diatas. Penyerang dapat memuat serangan dari tipe ini dalam skenario dimana ia memiliki penggunaan bebas dari sebuah *hardware* dekripsi, tetapi tidak dapat mengekstrak kunci dekripsi darinya.

B. Analisa Proteksi Pada *Public Key CryptoSystem* guna Menentukkan *Secret Key Cryptography* Sebuah Data

Setelah mempelajari bagaimana analisa lubang keamanan pada proses enkripsi dan dekripsi data dalam model kriptografi ini, selanjutnya dalam analisa kelemahan kriptografi, umumnya akan terletak pada proses yang melibatkan enkripsi dan dekripsi. Proses ini tidak akan lepas dengan *Cryptographic System* atau *CryptoSystem* adalah suatu fasilitas untuk mengkonversikan *plaintext* ke *ciphertext* dan sebaliknya. Dalam sistem ini, seperangkat parameter yang menentukan transformasi pen-*cipher*-an tertentu disebut suatu set kunci. Proses enkripsi dan dekripsi diatur oleh satu atau beberapa kunci kriptografi. Secara umum, kunci-kunci yang digunakan untuk proses pengenkripsian dan pendekripsian tidak perlu identik, tergantung pada sistem yang digunakan.

Problem utama pada *single-key Cryptography* adalah problem distribusi kunci. Problem ini merupakan problem dasar karena di antara pengirim dan penerima harus menyalin (ada proses pengiriman) kuncinya, sementara mereka harus mencegah orang lain menyalin (mengetahui) kuncinya, Penyembunyian informasi yang dilakukan oleh pengirim (*sender*) terkadang harus pula menyertakan kuncinya dalam pengiriman tersebut (mesipun tidak harus bersamaan waktunya). Hal ini dibutuhkan penerima (*receiver*) untuk membuka informasi yang disembunyikan itu. Problem terjadi di sini, karena bisa saja kunci tersebut diambil oleh orang yang tidak berhak.

Penulis menganalisa bagaimana untuk mengatasi permasalahan di atas akibat lubang keamanan dari kriptografi adalah dengan menggunakan teknik enkripsi asimetris kriptografi. Kunci asimetris adalah pasangan kunci-kunci kriptografi yang salah satunya dipergunakan untuk proses enkripsi dan yang satu lagi untuk dekripsi. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsikan suatu pesan, sedangkan hanya satu orang saja yang memiliki rahasia tertentu – dalam hal ini kunci privat – untuk melakukan pembongkaran terhadap sandi yang dikirim untuknya.

Secara umum operasi enkripsi dan dekripsi dapat diterangkan secara matematis sebagai berikut :

EK(M) = C (Proses Enkripsi)

DK(C) = M (Proses Dekripsi)

Pada saat proses enkripsi disandikan pesan M dengan suatu kunci K lalu dihasilkan pesan C. Sedangkan pada proses dekripsi, pesan C tersebut diuraikan dengan menggunakan kunci K sehingga dihasilkan pesan M yang sama seperti pesan sebelumnya. Dengan demikian keamanan suatu pesan tergantung pada kunci ataupun kunci-kunci yang digunakan, dan tidak tergantung pada algoritma yang digunakan. Sehingga algoritma-algoritma yang digunakan tersebut dapat dipublikasikan dan dianalisis, serta produk-produk yang menggunakan algoritma tersebut dapat diproduksi massal. Tidaklah menjadi masalah apabila

seseorang mengetahui algoritma yang kita gunakan. Selama ia tidak mengetahui kunci yang dipakai, ia tetap tidak dapat membaca pesan.

Teknik enkripsi asimetris ini jauh lebih lambat ketimbang enkripsi dengan kunci simetris. Oleh karena itu, biasanya bukanlah pesan itu sendiri yang disandikan dengan kunci asimetris, namun hanya kunci simetrislah yang disandikan dengan kunci asimetris. Sedangkan pesannya dikirim setelah disandikan dengan kunci simetris tadi.

*Public-key CryptoSystem*s memiliki dua kegunaan primer, enkripsi dan tanda tangan digital. Pada sistemnya, setiap orang mendapatkan sepasang kunci, satu disebut kunci *Public* dan yang lain disebut kunci privat. Kunci publik dipublikasikan, sedangkan kunci privat disimpan rahasia. Kunci privat atau lebih dikenal dengan *Secret-key Cryptography. Secret-key Cryptography* juga kadang disebut sebagai *Symmetric Cryptography* merupakan bentuk kryptografi yang lebih tradisional, dimana sebuah kunci tunggal dapat digunakan untuk mengenkrip dan mendekrip pesan. *Secret-key Cryptography* tidak hanya berkaitan dengan enkirpsi tetapi juga berkaitan dengan otentikasi. Salah satu teknik semacam ini disebut *message authentication codes*.

Masalah utama yang dihadapi secret-*key CryptoSystem*s adalah membuat pengirim dan penerima menyetujui kunci rahasia tanpa ada orang lain yang mengetahuinya. Ini membutuhkan metode dimana dua pihak dapat berkomunikasi tanpa takut akan disadap. Kelebihan *secret-key Cryptography* dari *Public-key Cryptography* adalah lebih cepat. Teknik yang paling umum dalam *secret-key Cryptography* adalah *block ciphers*, *stream ciphers*, dan *message authentication codes*.

Selanjutnya pada *Public key*, maka kebutuhan pengirim dan penerima untuk berbagi informasi rahasia dieliminasi; semua komunikasi hanya mencakup kunci publik, kunci privat tidak pernah ditransmisikan atau dipakai bersama. Pada sistem ini, tidak perlu lagi untuk mempercayai keamanan beberapa peralatan komunikasi. Kebutuhannya hanya kunci publik diasosiasikan dengan penggunanya dengan cara yang dapat dipercaya (diotentikasi) (sebagai contoh, dalam direktori yang dipercaya). Setiap orang dapat mengirimkan pesan rahasia hanya dengan menggunakan informasi publik, tetapi pesan hanya dapat didekripsi dengan kunci privat, yang merupakan milik penerima yang dituju. Lebih jauh lagi, *Public-key Cryptography* dapat digunakan tidak hanya untuk kerahasiaan (enkripsi), tetapi juga untuk otentikasi (tanda tangan digital) dan teknik-teknik lainnya.

C. Sistem Sertifikasi Kunci Publik Pada Penggunaan Keamanan data Dalam Kriptografi

Pada *Public-key CryptoSystem*, kunci privat selalu dihubungkan secara matematis dengan kunci publik. Karena itu, dimungkinkan untuk menyerang sistem *Public-key* dengan menurunkan kunci privat dari kunci publik. Pada umumnya, antisipasi atas masalah ini adalah dengan membuat masalah penurunan kunci privat sesulit mungkin. Sebagai contoh, beberapa *Public-key CryptoSystem*s dirancang sedemikian rupa sehingga penurunan kunci privat dari kunci publik membutuhkan penyerang untuk memfaktorkan angka yang besar, dalam kasus ini tidak mungkin secara komputasi untuk melakukan penurunan ini. Ini adalah ide dibalik RSA *Public-key CryptoSystem*.

RSA *CryptoSystem* adalah *Public-key CryptoSystem* yang menawarkan baik enkripsi dan tanda tangan digital (otentikasi). *Public-key CryptoSystem*s berdasar pada (dianggap) *trapdoor one-way Function*s. Kunci publik memberikan informasi tentang instans tertentu dari fungsi, kunci privat memberikan informasi tentang *trapdoor*. Siapapun yang mengetahui *trapdoor* dapat menghitung fungsi dengan mudah dalam dua arah, tetapi siapapun yang tidak memiliki *trapdoor* hanya dapat menjalankan fungsi dengan mudah pada arah maju. Arah maju digunakan untuk enkripsi dan verifikasi tandatangan, arah invers digunakan untuk dekripsi dan pembuatan tandatangan.

Permasalahan akan kekhawatiran menyadap dan mengubah seluruh informasi atau *man-in-the-middle attack* dapat diselesaikan dengan sertifikasi digital, sebagaimana pada penggunaan kriptografi, maka akan dibutuhkan suatu otentikasi dan authorisasi, di mana didapatkan data yang dikirim nantinya

akan terintegrasi dengan baik dan tidak bisa ditembus oleh attacker yang ingin memanfaatkan data lain. *Certificate Authority* (CA) bertindak sebagai notaris dengan memverifikasi identitas seseorang dan memberikan sertifikat yang menjamin kunci publik dari individu tertentu. Agen sertifikasi ini menandai sertifikat dengan kunci privatnya sendiri. Karena itu, individu diverifikasi sebagai pengirim jika kunci publik orang tersebut dapat membuka data. Sertifikat terdiri dari nama subyek, kunci publik subyek, nama dari otoritas sertifikat, dan periode dimana sertifikat masih valid. Untuk memverifikasi tanda tangan CA, kunci publiknya harus di sertifikasi silang dengan CA yang lain. Sertifikat ini kemudian dikirim ke repositori, yang menyimpan sertifikat dan *Certificate Revocation Lists* (CRL) yang menunjukkan sertifikat yang ditarik.

Sebenarnya dalam sertifikat tersebut tak hanya berisi kunci publik, namun dapat berisi pula informasi penting lainnya mengenai jati diri pemilik kunci publik, seperti misalnya nama, alamat, pekerjaan, jabatan, perusahaan dan bahkan *Hash* dari suatu informasi rahasia. Serangan terhadap sistem yang memiliki pengamanan dengan sertifikat digital sulit dilakukan. Sehingga penulis merasa bahwa proses kriptografi saat dilakukan dengan benar sampai pada bagaimana memberikan sertifikat authorisasi akan membuat suatu perusahaan dapat meminimalisir kesalahan dalam kerusakan data dan terjamin kerahasiaan datanya.

Secara teoritis keunggulan dari tanda tangan digital adalah kemampuan untuk melakukan proses otentikasi secara *off-line*. Pemeriksa cukup memiliki kunci publik dari OS utama untuk mengetahui sah-tidaknya kunci publik dari lawan bicaranya. Selain itu untuk meningkatkan keamanan, kunci publik OS utama bisa saja diintegrasikan dalam program aplikasi. Namun kenyataannya, karena ada kemungkinan sertifikat digital tersebut hilang, tercuri atau identitas pemilik sertifikat berubah (perubahan alamat surat elektronik atau nomor KTP misalnya), maka sertifikat digital perlu diperiksa keabsahannya dengan melihat daftar sertifikat terbatalkan (*Certificate revocation list*) yang disimpan oleh OS.

Secara garis besar perlu ditekankan bagaimana sistem kriptografi dikarakteristikkan dalam tiga dimensi independen, *pertama* Tipe dari operasi digunakan untuk mengubah *plaintext* ke *ciphertext*. Semua algoritma enkripsi didasarkan pada dua prinsip umum: *substitution*, yang setiap elemen di *plaintext* (bit, huruf, kelompok bit atau huruf) dipetakan ke elemen lain, dan transposisi adalah setiap elemen di *plaintext* dibentuk ulang (*rearranged*). Fundamental requirement adalah tidak boleh ada informasi yang hilang (semua operasi bersifat *reversible*). *Kedua,* Banyaknya kunci yang digunakan. Jika di antara Pengirim dan Penerima menggunakan kunci yang sama, sistem akan mengacu pada simetris, kunci tunggal, kunci rahasia, atau enkripsi konvensional. Jika Pengirim dan Penerima menggunakan kunci yang berbeda, sistem akan mengacu pada asimetris, dua kunci, atau enkripsi kunci publik. *Dan ketiga adalah*, Dengan cara pemrosesan *plaintext*. Sebuah blok *cipher* memproses sebuah blok elemen input pada satuan waktu, menghasilkan sebuah blok output dari setiap blok input. Sebuah *stream cipher* memproses elemen-elemen input secara kontinu untuk menghasilkan sebuah elemen output pada satuan waktu.

D. Analisa Generalisasi Standar Keamanan Data pada Kriptografi

Standar dalam kriptografi dibutuhkan untuk menciptakan interoperabilitas dalam dunia keamanan informasi. Pada dasarnya standar merupakan kondisi dan protokol yang dibuat untuk memungkinkan keseragaman dalam komunikasi, transaksi dan semua aktivitas secara virtual. Evolusi teknologi informasi yang terus berlanjut memotivasi pengembangan lebih banyak lagi standar, yang membantu memandu evolusi ini. Motivasi utama dibalik standar adalah untuk memungkinkan teknologi dari pabrik yang berbeda untuk "*berbicara bahasa yang sama*", untuk berinteraksi secara efektif.

Dalam kriptografi, standarisasi memiliki tujuan tambahan, yaitu sebagai landasan dari teknik-teknik kriptografi karena protokol yang rumit cenderung memiliki cacat dalam rancangan. Dengan menerapkan standar yang telah diuji dengan baik, industri dapat memproduksi produk yang lebih terpercaya. Bahkan protokol yang amanpun dapat lebih dipercaya pelanggan setelah menjadi standar, karena telah melalui proses pengesahan.

Pemerintah, industri privat, dan organisasi lain berkontribusi dalam pengumpulan luas standar-standar kriptografi. Beberapa dari standar-standar ini adalah ISO, ANSI, IEEE, NIST, dan IETF. Ada banyak tipe standar, beberapa digunakan dalam industri perbankan, beberapa digunakan secara internasional, dan yang lain dalam pemerintahan. Standarisasi membantu pengembang merancang standar baru, mereka dapat mengikuti standar yang telah ada dalam proses pengembangan. Dengan proses ini pelanggan memiliki kesempatan untuk memilih diantara produk atau layanan yang berkompetisi.

Dalam suatu perusahaan, maka harus disadari akan kebutuhan mekanisme enkripsi password lain yang lebih aman sesuai dengan kebutuhan keamanan data yang lebih tinggi dalam perusahaan yang mana dapat digunakan mekanisme *One Time Password* untuk menggantikan mekanisme password statis.

Keunggulan dari mekanisme *One Time Password* dimana password hanya digunakan satu kali saja setiap pengguna akan *log on* ke dalam sistem ini, walaupun penyerang berhasil mendapatkan password namun ia tidak dapat menggunakannya lagi untuk melakukan akses terhadap sistem. Teknik enkripsi yang dapat digunakan untuk mekanisme ini adalah teknik-teknik enkripsi simetris / kunci rahasia.

Banyak algoritma yang dapat digunakan untuk mengenkripsi password misalnya DES, AES, Blowfish, RC6, dll. Sekali lagi yang dibutuhkan disini adalah sumber daya manusia yang mampu untuk mengimplementasikan algoritma ini, salah satunya melalui PEM. PEM mendukung enkripsi dan otentikasi Internet email. Penggunaan piranti baru, disinyalir adalah untuk meminimalisir lubang keamanan yang dapat dijadikan celah untuk mendapatkan data sekalipun kriptografi sudah berjalan dalam proses pengiriman data tersebut. Untuk enkripsi pesan, PEM menggunakan Triple DES-EDE menggunakan sepasang kunci simetris. Algoritma *Hash* RSA MD2 atau MD5 digunakan untuk menghasilkan message digest, dan enkripsi kunci publik TSA mengimplementasi tanda tangan digital dan distribusi kunci rahasia. PEM menggunakan sertifikat yang berdasar pada standar X.509 dan dihasilkan oleh CA formal.

Membahas suatu permasalahan yang dapat menyerang data email, maka penulis perlu menambahkan bahwasannya aplikasi kriptografi lain yang dapat diimplementasikan dalam suatu perusahaan adalah enkripsi email. Enkripsi email dibutuhkan untuk melindungi surat-surat penting yang akan dikirim dari maupun keluar dari perusahaan. Misalnya saja pengiriman data-data laporan rugi laba suatu perusahaan kepada pihak penagih pajak maupun pengiriman surat-surat berharga lainnya. Untuk mengimplementasikan enkripsi email ini perusahaan harus sudah terko*one*ksi Internet. Aplikasi enkripsi email yang dapat diadopsi misalnya *Pretty Good Privacy* (PGP) yang dapat diperoleh secara gratis. Selain mengenkripsi email, PGP juga dapat digunakan untuk tanda tangan digital jika dibutuhkan level keamanan yang lebih tinggi.

IV. PENUTUP

A. Kesimpulan

Sebagai suatu simpulan bahwa enskripsi memiliki lubang kemanan dan juga sekaligus menjadi suatu senjata ampuh untuk suatu sistem keamanan. Maka, rekomendasi penulis merujuk dengan seiring kemajuan teknologi seperti penggunaan data yang vital misal email yang membutuhkan sandi / password yang menjadi sasaran dari para *attacker*, meskipun sudah dilakukan model kriptografi dengan enkripsinya, maka user juga butuh untuk menggunakan piranti-piranti yang terbaru dan *update*, di mana penggunaan PEM (*Privacy Enhanched Email*) adalah standar yang diusulkan oleh IETF untuk menjadi compliant dengan standar kriptografi kunci publik (PKCS), yang dikembangkan oleh konsorsium yang terdiri dari *Micro*soft, Novell, dan Sun *MicroSystem*s.

Secara umum mekanisme kriptografi dapat diterapkan pada suatu perusahaan tanpa banyak membutuhkan modifikasi karena biasanya algoritma-algoritma enkripsi dapat diperoleh secara gratis dan mudah sehingga dapat dikembangkan/diimplementasikan sendiri sesuai dengan lingkungan dan kebutuhan perusahaan. Pengembangan ini dapat dilakukan secara *in house* (jika perusahaan telah memiliki divisi TI sendiri) maupun *outsource*. Penerapan enkripsi ini

tentunya memperhatikan aspek urgensi dari kerahasiaan data yang akan dienkripsi. Pemilihan teknik enkripsi dan apa yang akan dienkripsi disesuaikan dengan kebutuhan keamanan perusahaan tersebut.

B. Saran

Saran yang dapat diambil dari penelitian yang telah dilakukan yaitu:

1. Menambahkan Teori-teori pendukung yang lebih lengkap lagi dikarenakan pada penelitian ini hanya mengunakan metode Teoretical Review,
2. Menambahkan Anilisa lubang keamanan dari setiap Metode enkripsi yang ada saat ini, yang mungkin terlewatkan dan menambah hasil kajian dari setiap kajian yang dibahas agar penelitian ini bisa dikembangkan lebih baik lagi.

DAFTAR PUSTAKA

[1] Arifin, Zainal. (2009). *Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman.* Jurnal Publikasi FMIPA Universitas Mulawarman.

[2] Arief Muhammad, Fitriyani, Nurul Ikhsan. (2015). Kriptografi Rsa Pada Aplikasi *File Transfer Client- Server Based".* Jurnal Ilmiah Teknolog informasi Terapan Volume I, No 3. 10 Agustus 2015 ISSN : 2407 – 3911.

[3] Ariyus, Dony. (2005), Computer Security,Yogyakarta: Penerbit Andi

[4] Dony, Ariyus. (2006). *Pengantar Ilmu Kriptografi*. Bandung: Penerbit Informatika.

[5] Davis, Keit. (1972). Human Relation at Work. US: McGraw-Hill Inc. 4th edition

[6] Kranakis, E. (2010). *Probabilistic Encryption.* Jurnal of Computer and System Science Cambridge.

[7] Kurniawan, Yusuf MT.(2014). *Kriptografi: Keamanan Internet dan Jaringan Komunikasi*. Bandung: Informatika.

[8] Kristanto, Andi. (2004). *Memahami Model Enkripsi dan Keamanan Data*. Yogyakarta: Andi Offset Yogyakarta.

[9] Rahardjo B., 2001, *Aspek Teknologi dan Keamanan dalam Internet Banking*. Jakarta: INDOCISC.

[10] Rahayu, Florensia. (2005). *Cryptography*: *Suplemen Bahan Ajar Mata Kuliah Proteksi dan Teknik Keamanan Sistem Informasi*. Depok: Universitas Indonesia Press.

[11] Rinaldi, Munir. (2008). *Belajar Ilmu Kriptografi*. Yogyakarta : Andi.

[12] Scheneier, Bruce. (2006). *Applied Cryptography Second Edition*: New Jersey: John Wiley & Sons, Inc.

[13] Susanto, Phil Astrid S. (1974). Komunikasi dalam Teori & Praktek. Bandung: Binacipta

[14] William, Stallings. (2006). *Cryptography and Network Security*, *Principles and Practices*. Journal of Pearson Education, Inc.

[15] Kastawan, I K. (2003). "Pembuatan Perangkat Lunak Pengaman Pengiriman Pesan Via Email dengan Algoritma RSA". Jurnal Sains Dan Seni ITS Vol. 4, No.1, (2015) ISSN 2337-3520