Pendekatan Kriptografi Hybrid pada Keamanan Dokumen Elektronik dan HypertextTransfer Protocol Secure (HTTPS) (Analisis Potensi Implementasi Pada Sistem Keamanan)

Basri

Program Studi Teknik Informatika Fakultas Ilmu Komputer
Universitas Al Asyariah Mandar

Abstract

Security issue always to be challenge for the development of information technology. As the security aspects of information systems, both of electronic and document data in hypertext data communications, must be able to meet safety standards. The implementation of security systems calssified as two methods, Symmetric and Asymmetric. Implementation of these methods certainly have their advantages and disadvantages of each, so it is necessary to apply a method to merge some types of the methods. This project was analyzed using a hybrid approach of cryptographic methods that are implemented on the security of electronic documents and Hypertext Transfer Protocol Secure (HTTPS). In the implementation of electronic document used of biometric signatures and DSA (Digital Signature Algorithm) and implementation on HTTPS used a combination of asymmetric cryptography and symmetric cryptography. The analysis of this research translated into the implementation of hybrid method on electronic documents and Hypertext Transfer Protocol Secure. From the analysis shows that the hybrid method is able to combine the advantages of symmetric and asymmetric methods, although of course the constraints in implementation complexity of the system will be even greater.

Keywords*: Hybrid Cryptography; Electronic Documents; HTTPS*

1. Pendahuluan

Pada saat ini perkembangan teknologi sistem informasi sangat cepat. Banyak perusahaan dalam berbagai sektor industri, dalam skala yang kecil, menengah maupun dalam skala yang lebih besar, sudah menggunakan fasilitas sistem informasi ini. Salah satu bagian dari perkembangan ini adalah dengan adanya internet. Teknologi ini membuat banyak kemudahan yang dapat dirasakan oleh manusia secara umum. Namun pemanfaatan layanan di internet yang meluas untuk suatu kepraktisan dan kecepatan dalam era teknologi informasi ini, memungkinkan kerawanan terhadap keamanan informasi dan privasi dapat terjadi (Munandar, dkk).

Dalam kejahatan di bidang Teknologi Informasi, para hacker dan cracker selalu mengintai celah dari sebuah sistem. Anomali yang terjadi adalah sangat sulit memisahkan terminologi *hacker* dan *cracker*, karena perbedaan diantara keduanya sangat sulit sekali untuk dikategorikan, ada yang mengatakan bahwa hacker merupakan sisi terang dari pecandu komputer sedangkan cracker adalah sisi gelap para pecandu komputer tersebut (Mantra, IGN., 2008).

Namun apapun istilahnya, celah keamanan sistem informasi yang berpotensi dimanfaatkan merupakan hal yang sangat berbahaya. Kerawanan data akan mengundang para penyusup lainnya untuk berusaha menyerang. Banyaknya penyusup yang dapat melihat bahkan merusak data merupakan hal yang harus diperhatikan. Sehingga diperlukan sistem informasi dengan tingkat keamanan yang dapat terjamin dan bisa terhindar dari serangan (attack), walaupun pada akhirnya akan terjadi trade off antara tingkat keamanan dan kemudahan akses (kurniawan, Ashadi., dkk).

Pada akhirnya diperlukan suatu metode pengamanan yang efektif dan efisien untuk menunjang hal tersebut. Ada banyak metode yang telah diteliti dan diimplementasikan dengan baik. Namun pada dasarnya terbagi atas dua jenis yaitu metode Simetris dan Metode Asimetris. Kedua metode dengan berbagai varian ini banyak digunakan untuk mengamankan data, namun penggabungan kedua metode ini masih sangat jarang dilakukan. Dari hasil analisis kedua metode, sangat mungkin diterapkan penggabungan kelebihan kedua metode tersebut yang biasa disebut dengan metode *hybrid*.

Penelitian terkait yang menggunakan metode Hybrid diantaranya yang dilakukan oleh Ana Wahyuni (2011), yang melakukan penelitian untuk pengamanan e-dokumen dengan menggabungkan Biometrik dan DSA (Digital Signature Algorithm), dan Aris Munandar, dkk. yang meneliti keamanan pada Hypertext Transfer Protocol Secure dengan menggunakan metode *hybrid*. Kedua penelitian terkait ini kemudian akan dianalisis untuk diambil kesimpulan berupa kelebihan dari hasil implementasi metode hybrid untuk kasus dokumen elektronik dan pada *Hypertext Transfer Protocol Secure* sebagaimana studi kasus pada penelitian terkait.

2. Kerangka Teori

2.1. Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu cryptós yang artinya “secret” (yang tersembunyi) dan gráphein yang artinya “writting” (tulisan). Jadi, kriptografi berarti ”secret writting” (tulisan rahasia). Definisi yang dikemukakan oleh Bruce Schneier (1996), kriptografi

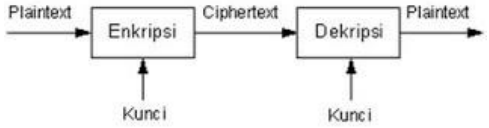
- *basri05@gmail.com*

adalah ilmu dan seni untuk menjaga keamanan pesan (*Cryptography is the art and science of keeping messages secure*).

Kriptografi merupakan ilmu sekaligus seni untuk menjaga keamanan pesan (message). Algoritma kriptografi adalah :

- Aturan untuk enkripsi (enciphering) dan dekripsi (deciphering).
- Fungsi matematika yang digunakan untuk enkripsi dan dekripsi.

Suatu pesan yang tidak disandikan disebut sebagai *plaintext* ataupun dapat disebut juga sebagai *cleartext*. Proses yang dilakukan untuk mengubah plaintext ke dalam ciphertext disebut *encryption* atau *encipherment*. Sedangkan proses untuk mengubah ciphertext kembali ke plaintext disebut *decryption* atau *decipherment*. Secara sederhana istilah-istilah di atas dapat digambarkan sebagai berikut :

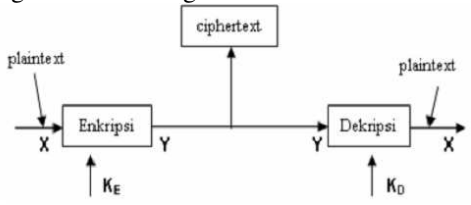


Gambar 2.1. Proses Enkripsi/Dekripsi Sederhana

Algoritma kriptografi berkembang terus dan terbagi atas dua bagian yaitu algoritma kriptografi klasik dan modern. Pada kriptografi klasik, kriptografer menggunakan algoritma sederhana, yang memungkinkan cipherteks dapat dipecahkan dengan mudah (melalui penggunaan statistik, terkaan, intuisi, dan sebagainya). Algoritma kriptografi modern dibuat sedemikian kompleks sehingga kriptanalis sangat sulit untuk memecahkan cipherteks tanpa mengetahui kunci. Pengelompokan algoritma juga dilakukan berdasarkan kunci enkripsi – dekripsi yang digunakan, yaitu *symmetric cryptosystem* atau simetris (menggunakan kunci yang sama untuk proses enkripsi – dekripsi) dan *Assymmetric cryptosystem* atau asimetris (menggunakan kunci yang berbeda untuk proses enkripsi – dekripsi). Serta penggabungkan dua buah metode kriptografi yang disebut *hybrid*.

2.2. Enkripsi dan Dekripsi

Proses penyandian pesan dari *plaintext* ke *ciphertext* dinamakan *enkripsi / enchipering*. Sedangkan proses mengembalikan pesan dari *chipertext* ke *plaintext* dinamakan *deskripsi /dechipering*. Proses enkripsi dan deskripsi ini dapat diterapkan pada pesan yang dikirim ataupun pesan yang disimpan. Algoritma Kriptografi dari setiap kriptografi klasik selalu terdiri dari dua bagian yaitu enkripsi dan dekripsi. Secara sederhana proses kriptografi dapat digambarkan sebagai berikut :



Gambar 2.2. Kriptografi secara umum.

Operasi enkripsi dan dekripsi dijelaskan secara umum sebagai berikut :

EK (M) = C (Proses Enkripsi)
DK (C) = M (Proses Dekripsi)

Ada dua cara yang paling dasar pada kriptografi klasik. yaitu adalah Transposisi dan Subsitusi :

a. Transposisi adalah mengubah susunan huruf pada plaintext sehingga urutannya berubah. Contoh yang paling sederhana adalah mengubah suatu kalimat dengan menuliskan setiap kata secara terbalik.
b. Substitusi yaitu setiap huruf pada plaintext akan digantikan dengan huruf lain berdasarkan suatu cara atau rumus tertentu.

2.3. Hybrid Cryptosystem

Hybrid cryptosystem atau *hybrid key*, secara umumnya memiliki konsep keamanan terhadap komunikasi client dan server dalam suatu jaringan internet dengan menggunakan kriptografi simetris. Peranan kriptografi asimetris, hanya ditujukan dalam *share session key* atau *key exchange* (pertukaran kunci) dalam arti untuk menyepakati dan saling bertukar kunci rahasia yang akan dipakai saat berkomunikasi. Jadi pertukaran kunci rahasia dilakukan dalam keadaan ter-enkripsi dengan kriptografi asimetris namun saat komunikasi menggunakan kriptografi simetris.

Kriptografi Simetris efisien dalam proses enkripsi-dekripsi namun memiliki kelemahan pada proses pendistribusian kunci sedangkan kriptografi asimetris kurang efisien pada saat proses enkripsi-dekripsi dikarenakan membutuhkan waktu yang lebih lama dibandingkan pada *sysmmetric cryptosystem*. Namun demikian, kriptografi asimetris memiliki keuntugan dimana tidak diperlukan proses distribusi kunci dikarenakan kunci yang digunakan untuk proses enkripsi-dekripsi ditempatkan pada *public directory*, oleh karena itu pada saat ini kriptografi hybrid digunakan secara luas dikarenakan menggabungkan keuntungan yang terdapat kepada kedua cryptosystem tersebut (Soohyun, et al., 2003).

2.4. Tandatangan Digital dengan Metode Hybrid : Biometrik Tandatangan dan DSA (Digital Signature Algorithm)

Pada metode hybrid : biometrik tandatangan dan DSA, biometrik yang digunakan yaitu tandatangan offline. Kunci privat dan publik dapat dihitung sebagai berikut (Wahyuni, Ana. 2011):

1. Perhitungan p, q dan g
   a. p = 512 sampai 1.024 bit bilangan prima
   b. q = 160 bit faktor prima dari p-1
   c. g = $h^{(p-1)/q}$ mod p, dimana h<(p-1) dan $h^{(p-1)/q}$ mod p > 1
2. Pembangkit kunci privat
   Hitung kode string tandatangan offline yang ditentukan. Ambil nilai kode sting tandatangan offline sebagai nilai SEED untuk membangkitkan kunci privat x.
3. Pembangkit kunci public
   Hitung y = gx mod p. Nilai y adalah p-bit kunci publik.

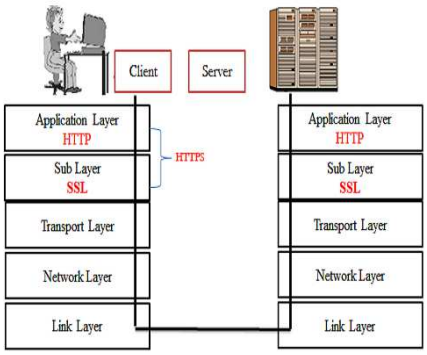
2.5. Hypertext Transfer Protocol Secure (HTTPS)

Berdasarkan RFC 2660, HTTPS adalah protokol yang berorientasi terhadap keamanan *message* (pesan) dalam suatu komunikasi. HTTPS dirancang agar dapat berdampingan dengan model pesan HTTP dan mudah diintergrasikan dengan HTTP dalam suatu jaringan.

HTTPS menyediakan layanan keamanan yang dapat digunakan dengan bebas untuk *transaction confidentiality* (kerahasiaan bertransaksi), *authenticity/ integrity and non-repudiability of origin* (otentikasi dan keaslian maupun anti penyangkalan) (Munandar, Aris., Purnama, Sigit).

Dalam impementasinya, HTTPS digunakan sebagai layanan keamanan pada suatu website yang memiliki data atau informasi yang bersifat rahasia baik yang dimiliki user maupun admin dari website tersebut. Suatu website yang menggunakan layanan HTTPS, dapat diketahui dengan adanya indikator ikon gembok pada browser, dan dapat terlihat pada address bar di browser dengan URL "https://".

HTTPS merupakan protocol HTTP yang menggunakan Secure Socket Layer (SSL) yang merupakan sublayer dibawah HTTP aplication layer. Pendekatan HTTPS dapat dikatakan sederhana, karena saat client membuat koneksi ke server, melakukan negosiasi koneksi SSL, kemudian mengirim HTTP tersebut melalui aplikasi SSL. Dari gambar 3 berikut diketahui bahwa protokol SSL beroperasi antara transport layer dan aplication layer.



Gambar 2.3. Koneksi pada HTTPS

2.6. Protokol Secure Socket Layer (SSL)

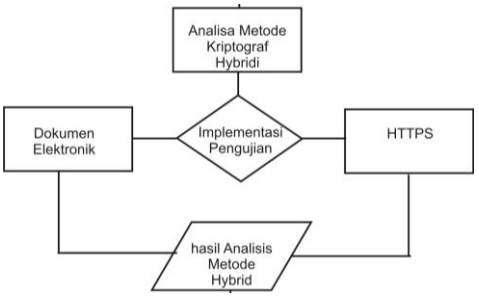
Protokol SSL adalah sebuah protokol keamanan yang digunakan untuk menjaga pengiriman data web server dan pengguna situs website tersebut, yang secara de facto saat ini merupakan standar untuk mengamankan komunikasi dan transaksi di Internet. SSL sudah diterapkan di semua browser dan Web server.

Oleh karena itu, SSL memainkan peran utama dalam e-commerce dan kegiatan e-bisnis pada website. Dengan pengimplementasian SSL pada aplikasi e-commerce, data user dan data admin akan terjaga kerahasiaannya (Rosmala, Dewi, 2012).

Dalam perkembangannya, suatu protokol SSL belum ditunjukan terhadap UDP (User Datagram Protocol) namun masih berupa protokol kriptografi yang menawarkan enkripsi, otentikasi dan integritas kontrol untuk TCP. Dalam arti SSL merupakan protokol connection-oriented dan hanya bekerja dengan koneksi TCP yang berorientasi sama (bersifat connection-oriented), tidak dengan UDP yang bersifat connectionless. SSL menggunakan peranan sistem kriptografi dalam penerapannya. Sistem kriptografi ini digunakan dalam suatu key exchange (pertukaran kunci) maupun sesi komunikasi antara client dan server. Peranan sistem kriptografi yang digunakan SSL, khususnya dalam sesi *key exchange* adalah kriptografi Hybrid.

3. Metode Penelitian

Pada analisis ini menggunakan pendekatan studi pustaka dengan beberapa hasil penelitian sebelumnya. Analisis pertama dengan menggunakan data pada implementasi kriptografi hybrid pada dokumen elektronik dan analisis berikutnya menggunakan data pada implementasi kriptografi hybrid pada HTTPS. Dalam analisis ini selanjutnya akan mengumpulkan informasi bagaimana implementasi kriptografi hybrid pada kedua data tersebut, bagaimana tingkat keamanan, serta kekurangan penerapanya. Dalam proses analisis akan dimulai dengna analisa dan pengambilan kesimpulan, sebagaimana ditunjukkan pada gambar berikut.



Gambar 3.1. Analisis Kriptografi Hybrid

Proses implementasi yang dilakukan pada data elektronik sebagai masukan (generator kunci) adalah tandatangan *offline* satu atau lebih pengguna menghasilkan satu atau lebih tandatangan digital untuk satu dokumen elektronik (e-dokumen). Selanjutnya e-dokumen, tandatangan digital dan kunci publik ditransmisikan lewat internet via e-mail pada fihak verifier. Kemudian pihak verifier memverifikasi apakah hasilnya valid artinya e-dokumen tersebut masih otentik/ utuh dan pengirim adalah signer sebenarnya dari e-dokumen tersebut. Sebaliknya jika hasilnya tidak valid artinya e-dokumen tersebut sudah tidak otentik/ utuh dan atau pengirim bukanlah signer sebenarnya dari e-dokumen tersebut (Ana Wahyuni, 2011).

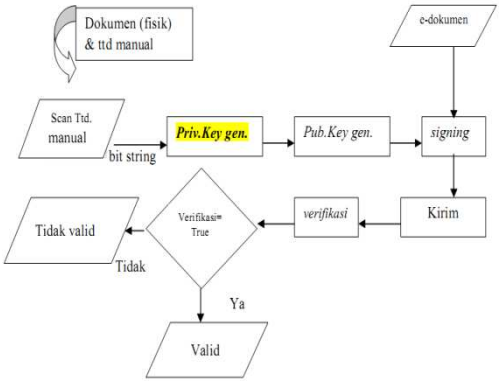
Sementara itu implementasi pada HTTP menggunakan kunci hybrid sebagai *Key Exchange.* Dalam implementasinya ada berbagai macam teknik key exchange, namun dalam analisis kedua ini lebih dikhususkan terhadap key exchange dengan sistem kriptografi simetris dan key exchange dengan sistem kriptografi asimetris (Munandar, Aris., Purnama, Sigit).

4. Hasil Implementasi Kriptografi Hybrid

4.1. Implementasi pada pengamanan e-dokumen

Implementasi metode hybrid : biometrik tandatangan dan DSA dapat dilihat pada gambar 4.1. Pada gambar

dapat dijelaskan bahwa pada hasil print out dokumen (dokumen fisik) yang telah diberi tandatangan oleh signer, dengan proses scanning, diambil tanda tangan manual tersebut untuk diproses menjadi kode string. Dari kode string tersebut digunakan sebagai nilai SEED untuk membangkitkan (Key generation) parameter dan sepasang kunci yaitu kunci privat dan kunci publik. Kunci publik diturunkan dari kunci privat yang didapat. Sepasang kunci tersebut digunakan pada pembangkitan tandatangan digital (signing). E-dokumen, kunci publik dan tandatangan digital selanjutnya dikirim via internet yaitu sebagai file lampiran dalam e-mail. Setelah e-mail diterima pihak verifer, kemudian dilakukan proses verifikasi terhadap file lampiran tersebut. Pada hasil proses verifikasi akan menampilkan hasil verifikasi valid berarti pesan masih asli dan e-dokumen dikirim oleh pengirim/ signer sebenarnya atau tidak valid.



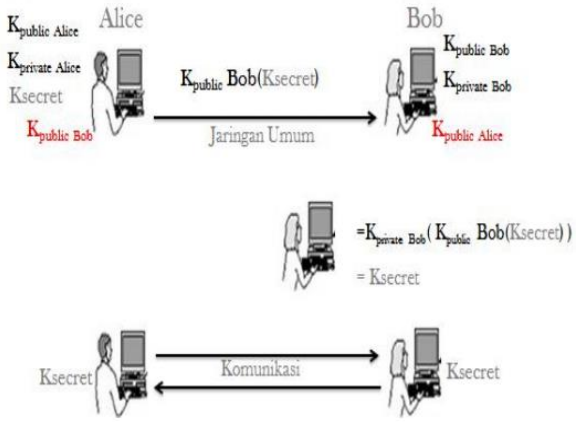
Gambar 4.1. Alur Proses Tandatangan Digital dengan Metode Hybrid : Biometrik Tandatangan dan DSA (Wahyuni, Ana. 2011)

4.2. Implementasi pada HTTPS

HTTPS memadukan kedua jenis cryptosystem (sistem kriptografi), yang dikenal dengan istilah hybrid key atau hybrid cryptosystem dan menggunakan peranan pihak ke-3. Secara analoginya, Alice ingin berkomunikasi dengan Bob dalam keadaan pesan terenkripsi, namun diasumsikan tidak menggunakan peranan pihak ke-3 dan kedua belah pihak telah memiliki public key dan private key masing-masing maupun public key setiap pihak yang tergabung dalam suatu komunikasi. Contohnya, Alice telah memiliki public key Bob maupun sebaliknya, dalam prosesnya:

1. Bila Alice ingin berkomunikasi dengan Bob, sebelumnya Alice telah memiliki public key Bob
2. Alice mengirimkan pesan berisi secret key (kunci rahasia) yang akan digunakan dalam proses komunikasi dengan dienkripsi terlebih dahulu dengan public key Bob
3. Bob mendapatkan secret key tersebut dengan cara mendekripsi pesan menggunakan private key miliknya
4. Alice dan Bob telah sama-sama memiliki secret key yang akan digunakan dalam proses komunikasi rahasia

Proseskey exchange sebagaimana ditunjukkan pada gambar berikut.



Gambar 4.2. Key exchange dengan hybrid key (Munandar, Aris., Purnama, Sigit)

Dalam penerapannya di HTTPS, hybrid key digunakan pada keamanan terhadap key exchange dan komunikasi client-server. Client atau dapat juga sebagai web browser saat melakukan koneksi terhadap server atau mengakses suatu website untuk layanan yang bersifat finansial tentunya memerlukan keamanan dan perlu memastikan bahwa website yang sedang diakses adalah benar sebagai pemilik yang sah, bukan suatu teknik phising atau sejenis *fake website* (website palsu).

Dari gambar 4.2 mengenai *key exchange* dengan *hybrid key*, adanya penjelasan bahwa diasumsikan tidak melibatkan pihak ketiga atau pihak terpercaya, namun dalam penerapan terhadap suatu proses HTTPS di jaringan internet, keterlibatan pihak ketiga sangat diperlukan. Hal ini karena, harus adanya suatu pihak yang dapat menjamin terhadap keaslian suatu web-server dalam arti bahwa website yang sedang diakses oleh client merupakan website yang sah atau dalam kriptografi dikenal dengan istilah *authentication* (otentikasi) baik terhadap *entity authentication* (identitas dari pihak yang berkomunikasi), data, public key dll. Pihak ketiga/ pihak terpercaya, dalam kasus ini adalah certification authority (CA), memiliki tugas, diantaranya: "Mengeluarkan certificate (sertifikat), menyediakan dan menjamin otentikasi public key suatu pihak. Dalam sistem berbasis sertifikasi hal ini termasuk mengikat public key pada nama-nama yang berlainan melalui sertifikat yang telah disahkan, mengelola nomor-nomor seri sertifikat dan penarikan/pembatalan sertifikat".

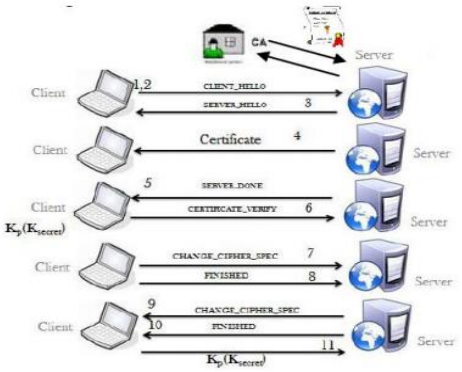
Mekanisme Kerja perananan hybrid key dan keterlibatan certification authority (CA) dalam penerapannya terhadap proses HTTPS di era teknologi internet ini, dijelaskan sebagai berikut:

1. Client mengakses layanan finansial dari suatu website, maka client menuliskan alamat di address bar dengan awalan URL: *https*://
2. Client mengirimkan perintah CLIENT_HELLO ke server
3. Server merespon dengan mengirim perintah SERVER_HELLO
4. Server mengirim perintah CERTIFICATE. Perintah ini termasuk sertifikat server dan rantai sertifikat sebagai opsional dimulai dengan sertifikat dari certification authority (CA) yang mengeluarkan

sertifikat server yang berisi data public key server,data-data server dll.
Catatan: Daftar CA yang dipercaya telah terdaftar di dalam web browser. Jika sertifikat digital ditandatangi oleh salah satu CA di dalam daftar tersebut, maka client dapat memverifikasi public key server.

5. Server mengirim perintah SERVER_DONE yang mengindikasi bahwa server telah menyelesaikan tahap *handshake*.
6. CERTIFICATE_VERIFY, client menginformasikan server bahwa sertifikat server telah diverifikasi mulai dari identitas server, masa berlaku public key-nya, tanda tangan/ pengesahan dari CA, dll.
7. Client mengirimkan perintah CHANGE_CIPHER_SPEC, adanya proses menyepakati Cipher (algoritma enkripsi).
8. Client mengirimkan perintah FINISHED, Perintah ini dikirim untuk memvalidasi bahwa tidak ada perintah yang dikirim sebelumnya.
9. Server mengirim perintah CHANGE_CIPHER_SPEC. Perintah ini menunjukkan bahwa semua data berikutnya yang dikirim oleh server selama sesi komunikasi akan dienkripsi.
10. Server mengirim perintah FINISHED, Perintah ini termasuk digest untuk menvalidasi dari semua perintah handshake SSL yang mengalir antara server dan klien.
11. Pada tahap terakhir ini, klien dapat mengirim secret key (kunci rahasia simetris) yang telah disepakati ke server setelah menyandikannya dengan public key (kunci public) yang diterima dalam sertifikat server SSL. secret key yang dienkripsi hanya dapat didekripsi dengan menggunakan private key server. Jadi, hanya server yang dapat mendekripsi pesan.

Proses penerapan Hybrid key pada proses HTTPS ditunjukkan melalui gambar berikut.



Gambar 4.3 Penerapan Hybrid key pada Proses HTTPS
(Munandar, Aris., Purnama, Sigit)

Dari proses diatas saat ini client dapat menggunakan layanan finansial yang disediakan suatu website dalam proses transaksi yang ter-enkripsi dengan tidak meninggalkan faktor kecepatan. Hal tersebut dikarenakan, dalam proses transaksi/ komunikasi menggunakan sistem kriptografi simetris dan asimetris hanya pada sesi *key exchange* (pertukaran kunci) *secret key* (kunci rahasia/simetris) tersebut.

4.3. Analisis Kriptografi Hybrid

Dari implementasi yang dijelaskan sebelumnya aplikasi kriptografi untuk pengamanan e-dokumen dengan metode hybrid : Biometrik tandatangan dan DSA (Digital Signature Algorithm), maka hasil analisi menunjukkan bahwa:

1. Biometrik tandatangan manual offline pengguna dapat digunakan untuk membuat kunci privat. Kunci privat yang dihasilkan, digunakan untuk membuat kunci publik pasangannya. Panjang kunci antara 512 sampai 1024 bit sesuai standar keamanan yang dikeluarkan oleh FIPS *(Federal Information Processing Standard)*. Dari masukan satu tandatangan offline dapat menghasilkan lebih dari satu pasang kunci. Hal ini menunjukkan pembangkitan kunci secara dinamis sebagai konsep baru pada penggunaan kunci untuk satu kali pakai.
2. Tandatangan digital dapat memenuhi kebutuhan ketidaktunggalan *signer*. Hal ini sebagai konsep baru pada penerapan tandatangan digital yang memenuhi kebutuhan otorisasi satu e-dokumen dengan lebih dari satu signer.
3. Keamanan implementasi Biometrik tandatangan dan DSA pada penelitian ini didasarkan atas satu e-dokumen jika ditandatangani oleh *n signer* maka harus diverifikasi sebanyak n kali. Jika semua *n* verifikasi bernilai valid berarti telah menembus *n* lapis keamanan.
4. Pada implementasi tandatangan digital dengan metode hybrid : Biometrik tandatangan dan DSA terpenuhi kebutuhan keamanan e-dokumen dalam hal :
   a. Kerahasiaan (confidentiality) signature hanya dapat didekrip oleh verifier dengan kunci publik pasangan kunci privat pada pihak signer.
   b. Keutuhan atau keotentikan (integrity) e-dokumen yang ditransmisi, dijamin dengan hash SHA-1 dari e-dokumen tersebut.
   c. Jaminan atas identitas dan keabsahan (authenticity) *n signer* dengan *n signature* yang dihasilkan serta hasil verifikasinya, dimana n = 1,2,3,....

Analisis hasil implementasi kriptografi hybrid pada HTTPS khususnya terhadap interaksi antara client/web browser dan server digunakan sebagai solusi keamanan yang menggabungkan keuntungan yang terdapat kepada kedua kriptografi antara Simetris dan Asimetris. Public key dan *private key* pada *publickey cryptosystem* hanya digunakan untuk proses *handshaking* dan *key exchange*. Hal ini dilakukan untuk dua alasan:

1. Kriptografi Asimetris berbasis komputasi sangat mahal sehingga penggunaannya harus diminimalkan.
2. Mekanisme kunci rahasia yang dibutuhkan untuk komunikasi client server.

Sedangkan kriptografi simetris digunakan sebagai keamanan saat proses komunikasi antara client dan server berlangsung setelah proses *handshaking* dan *key exchange* selesai.

5. Kesimpulan

5.1 Kontribusi Penelitian

Dari data hasil analisis dapat disimpulkan bahwa implementasi metode *hybrid* memiliki tingkat keamanan dan waktu komputasi yang lebih baik dibanding hanya menggunakan metode kriptografi simetris ataupun hanya kriptografi asimetris. Hasil implementasi menunjukkan tingkat kerahasiaan, keutuhan atau keotentikan, jaminan atas identitas dan keabsahan yang lebih baik, baik pada implementasi pada e-dokumen maupun pada HTTPS. Selain itu metode hybrid mampu mengkombinasikan kelebihan dari tiap jenis kriptografi simetris dan asimetris sehingga dapat mengatasi masalah kerentanan keamanan yang terdapat pada kriptografi simetris dan masalah kompleksitas waktu yang terdapat pada kriptografi asimetris.

5.2 Usulan Pengembangan Penelitian

Kriptografi hybrid pada faktanya memiliki kelebihan yang menggabungkan antara kriptografi simetris dan asimetris. Kelebihan ini haruslah diimplementasikan dalam berbagai sistem keamanan, karena pada perkembangannya saat ini dan kedepannya, sistem informasi akan mengarah pada sistem terdistribusi. Hal ini menjadikan sistem yang dibangun akan sangat beresiko dalam hal keamanan data. Pengamana data yang baik adalah ketika memiliki tingkat kompleksitas pemecahan kunci yang rumit dan proses kriptografi dengan waktu yang relatif singkat. Tentunya metode *hybrid* yang dijelaskan pada analisis ini hanya mengambil masing-masing satu sampel dari tiap metode kriptografi. Sehingga kedepannya perlu dilakukan analisis lebih jauh dengan mengkombinasikan berbagai jenis kriptografi simetris dan asimetris agar dapat meningkatkan kompleksitas kunci dan waktu komputasi yang lebih cepat.

Daftar Pustaka

Bruce Schneier, 1996. *Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C (cloth)*. John Wiley & Sons, Inc.

Kurniawan, Ashadi., Yuliana, Mike., Hadi, M.Zen Samsono. *Analisa dan Implementasi Sistem Keamanan Data dengan menggunakan Metode Enkripsi Algoritma RC-5*. Karya tidak diterbitkan. Surabaya : Institut Teknologi Sepuluh Nopember.

Mantra, IGN. 2008. *Desain Intruder Detection System (IDS) Sebagai Antisipasi Hacker dan Cracker di Dunia*. KOMMIT. 637-645.

Munandar, Aris., Purnama, Sigit. *Analisis hybrid Cryptosystem pada Hypertext Transfer Protocol Secure (HTTPS)*. Karya tidak diterbitkan. Bogor : Sekolah Tinggi Sandi Negara.

Munawar. 2012. *Perancangan Algoritma Sistem Keamanan Data Menggunakan Metode Kriptografi Asimetris*. KOMPUTA. Vol I : 11-17.

Rosmala, Dewi. 2012. *Implementasi Aplikasi Website E-Commerce Batik Sunda dengan Menggunakan Protokol Secure Socket Layer (SSL)*. JURNAL INFORMATIKA. No. 3. Vol. 3.

Soohyun, oh., Kwak, Jin., Won, Dongho. 2003. *An Efficient Hybrid Cryptosystem Providing Authentication for Sender's Identity*. ICOIN 20013, LNCS 2662. Pp. 737-747.

Wahyuni, Ana. 2011. *Aplikasi Kriptografi untuk Pengamanan e-Dokumen dengan Metode Hybrid* : Biometrik Tandatangan dan DSA (Digital Signature Algorithm). Karya tidak diterbitkan. Semarang : Universitas Diponegoro.