Aplikasi Kriptografi pada Secure Socket Layers (SSL)

Ernestasia Siahaan
Jurusan Teknik Informatika ITB, Bandung, email: if16026@students.if.itb.ac.id

Abstraksi
Makalah ini membahas aplikasi kriptografi pada Secure Socket Layers (SSL) yang berfungsi menjamin keamanan pertukaran informasi melalui situs di internet. Kriptografi pada SSL dipakai untuk menyandi informasi yang dikirimkan oleh klien dan memastikan bahwa informasi yang diterima server benar-benar dikirim oleh klien bersangkutan.

SSL memiliki tiga protokol, yaitu protokol Handshake (jabat tangan), protokol Record dan protokol Alert. Pada protokol Handshake, dilakukan negosiasi algoritma enkripsi dan otentikasi server oleh klien. Protokol Record merupakan proses enkripsi informasi yang dikirimkan oleh klien. Protokol Alert berfungsi menangani kesalahan-kesalahan yang mungkin terjadi selama pertukaran informasi berlangsung.

Contoh penggunaan SSL adalah pada situs yang menggunakan protokol HTTPS (Secure Hypertext Transfer Protocol). HTTPS merupakan HTTP yang bekerja di atas SSL Situs-situs yang menggunakan HTTPS ini misalnya halaman login email host, situs untuk online banking, dan sebagainya.

Kata Kunci
Enkripsi: proses penyandian data

Dekripsi: proses mengembalikan data yang telah disandikan ke bentuk semula

Chiper: sepasang algoritma yang menjalankan proses enkripsi dan dekripsi

1. PENDAHULUAN

Algoritma modulo dan bilangan prima merupakan bagian dari teori bilangan bulat. Keduanya memiliki banyak penerapan dalam ilmu komputer. Salah satunya adalah pengamanan sistem komputer. Hal ini dimungkinkan dengan adanya kriptografi.

Kriptografi adalah ilmu dan praktik menjaga kerahasiaan dari pihak-pihak yang tidak dikehendaki baik saat penyampaian maupun penyimpanan informasi tersebut. Informasi yang hendak dilindungi itu disamarkan dengan menggunakan cara-cara dan kunci tertentu. Identitas pihak-pihak yang tidak berwenang atas informasi yang dienkripsi dapat dipastikan dengan kriptografi. Kriptografi tidak hanya menjaga kerahasiaan informasi, namun juga menjaga keutuhan dan keaslian informasi yang disampaikan.

Terdapat banyak penerapan kriptografi dalam kehidupan sehari-hari yang tidak disadari. Telepon seluler, kartu ATM, kartu kredit, internet merupakan sebagian contoh fasilitas yang menggunakan kriptografi.

Salah satu aplikasi kriptografi di jaringan internet adalah pengamanan situs dengan menggunakan protokol HTTPS (Secure Hypertext Transfer Protocol). HTTPS memungkinkan terjadinya akses dan transaksi melalui situs internet secara aman, misalnya dalam online banking, online shopping, login ke email host dan sebagainya.

Ketika menggunakan koneksi HTTPS, server menanggapi inisiasi koneksi oleh klien dengan menawarkan berbagai metode enkripsi yang dapat ia sokong. Klien lalu memilih metode koneksi, dan kedua belah pihak saling bertukar sertifikat untuk memastikan identitas masing-masing. Setelah itu, kedua belah pihak bertukar informasi yang telah dienkripsi. Namun sebelumnya, harus dipastikan baha keduanya menggunakan kunci yang sama dan bahwa koneksi yang digunakan tertutup. [6]

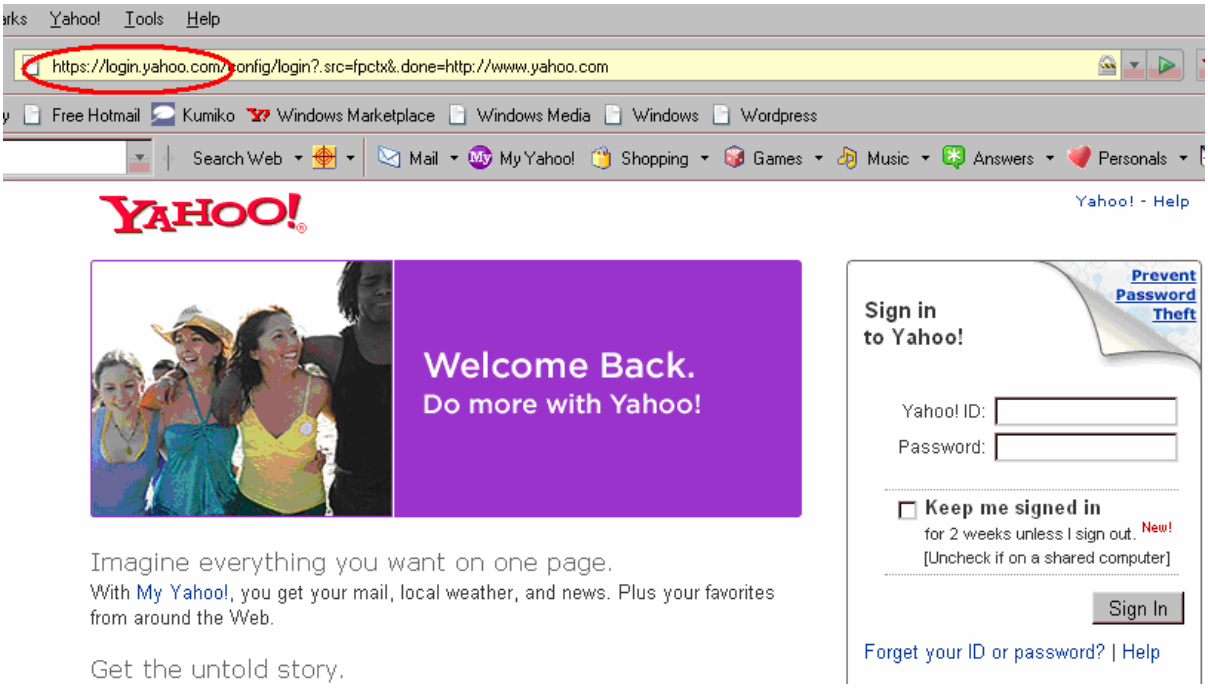
Semua hal di atas dimungkinkan karena HTTPS merupakan HTTP yang bekerja di atas SSL (Secure Socket Layer). Selanjutnya pada makalah ini akan dibahas mengenai SSL dan peran kriptografi dalam SSL.

2. BAGIAN-BAGIAN SSL

SSL berfungsi menjamin keamanan dalam pengiriman dan pengaksesan informasi lewat internet. Biasanya, hanya server yang mengalami otentikasi (untuk memastikan identitasnya). Sedangkan pengguna akhir (misalnya orang yang mengakses sebuah situs) tidak terotentikasi, namun mereka dapat mengetahui dengan jelas dengan siapa mereka berbagi informasi.

SSL menjamin kerahasiaan, kesatuan dan keaslian informasi yang terkait. Untuk menjaga kerahasiaan informasi, SSL menggunakan kriptografi. Sedangkan kesatuan informasi dimungkinkan terjadi dengan adanya digital signatures (tanda tangan digital). Keaslian informasi dijamin dengan penggunaan sertifikat.

Untuk lebih memahami SSL, akan dibahas lebih lengkap mengenai algoritma kriptografi, digital signatures dan sertifikat.



Gambar 1: Halaman login email host yang menggunakan HTTPS

2.1. Algoritma Kriptografi

Seperti telah dijelaskan pada bagian pendahuluan, kriptografi merupakan praktik penyandian informasi untuk melindunginya dari pihak-pihak yang tidak dikehendaki.

Dalam kriptografi, proses penyandian informasi disebut enkripsi Informasi yang belum disandikan disebut plainteks, sedangkan informasi yang telah melalui proses enkripsi disebut chiperteks. Proses pengembalian chiperteks ke dalam bentuk plainteks disebut dekripsi. Proses enkripsi dan dekripsi ini dilakukan oleh sepasang algoritma yang disebut chiper. Setiap operasi yang dilakukan oleh chiper ditentukan oleh algoritma tersebut dan sebuah kunci. Semakin baik algoritma yang digunakan, semakin sulit bagi orang yang tidak mengetahui kuncinya untuk memperoleh informasi yang disandikan.

Terdapat dua jenis enkripssi data: kriptografi simetis dan kriptografi asimetris.

Kriptografi simetris menggunakan kunci yang sama dalam enkripsi dan dekripsi informasi. Sedangkan pada kriptografi asimetris, kunci untuk enkripsi data berbeda dengan kunci untuk dekripsi. Karenanya, kriptografi asimetris lebih aman untuk digunakan karena pihak ketiga harus mencari tahu dua kunci yang berbeda untuk dapat memperoleh informasi yang disandikan.

Enkripsi asimetris memungkinkan kedua belah pihak yang bertukar informasi melakukan pertukaran informasi kapan saja tanpa harus bertemu satu sama lain. Hal ini dimungkinkan dengan adanya pasangan kunci publik (umum) dan kunci private (khusus).

Kunci umum dapat diketahui oleh masyarakat luas dan digunakan untuk enkripsi. Sedangkan kunci khusus digunakan untuk dekripsi dan hanya diketahui oleh pihak tertentu. Misalnya dalam online banking di internet. Setiap orang dapat mengirimkan informasi mereka kepada pihak bank melalui situs bank yang bersangkutan. Saat mengirimkan informasi tersebut, informasi itu dienkripsi dengan menggunakan kunci umum. Selanjutnya, hanya pihak bank terkait yang dapat mendekripsi informasi yang dikirimkan, karena bank tersebut memiliki kunci khusus untuk melakukan dekripsi.

Beberapa algoritma yang umumnya digunakan untuk pertukaran kunci antara lain RSA, Diffie-Hellman, DSA, SRP dan PSK.

Tabel 1: Perbandingan kriptografi simetris dengan kriptografi asimetris pada SSL [4]

Kriptografi Simetris
- Kriptografi simetris menggunakan satu kunci yang sama untuk enkripsi dan dekripsi - Kriptografi simetris mengharuskan kedua belah pihak yang bertukar informasi memiliki kunci - Distribusi kunci merupakan kelemahan kriptografi simetris - Siklus CPU yang diperlukan untuk melakukan verifikasi terhadap kunci minimal

- Chiper simetris diperkuat oleh kekuatan algoritma dan panjang kunci
- Panjang kunci SSL simetris berkisar antara 40 sampai 168 bit

Kriptografi Asimetris

- Kriptografi asimetris didesain untuk mengatasi keterbatasan kriptografi simetris
- Informasi dienkripsi dengan sebuah kunci yang berbeda dengan kunci untuk dekripsi
- Kriptografi Public Key Infrastructure (PKI / Infrastruktur Kunci Umum) 1000 kali lebih intensif pada CPU daripada kriptografi simetris
- Algoritma RSA (Rivest, Shamir, Adelman) yang menggunakan aritmatika modulo memungkinkan konsep kunci umum dan kunci khusus
- Setiap transaksi SSL dimulai dengan pertukaran kunci asimetris

2.2. Digital Signatures (Tanda Tangan Digital)

Untuk memastikan kesatuan informasi yang dikirimkan, setiap pertukaran informasi dengan SSL dilengkapi dengan sebuah digital signature.

Digital signature merupakan rangkuman informasi yang telah dienkripsi dengan kunci umum menggunakan fungsi hash.

Fungsi hash mengubah masukan menjadi sebuah untaian karakter yang panjangnya tetap dan tertentu. Keluaran dari fungsi hash disebut nilai hash. Pada contoh online banking, informasi yang hendak dikirim oleh nasabah diubah dengan sebuah fungsi hash sehingga menjadi untaian karakter yang panjangnya tertentu. Untaian karakter ini disebut message digest.

Message digest ini berfungsi untuk memastikan bahwa informasi yang dikirimkan oleh nasabah tidak diubah oleh pihak ketiga saat proses transmisi. Contohnya, saat nasabah mengirimkan informasi, bank akan menerima informasi tersebut secara utuh dan message digest dari informasi itu. Pihak bank akan mendekripsi message digest dan membandingkannya dengan informasi yang dikirim oleh nasabah.

Algoritma dalam pembuatan message digest memungkinkan terbentuknya message digest yang unik untuk masing-masing informasi yang berbeda. Dengan demikian, tidak ada dua informasi yang memiliki message digest yang sama, sehingga akan sulit untuk mengubah atau mengganti informasi yang dikirimkan oleh seseorang dengan tetap mempertahankan message digest yang sama.

Untuk mengirimkan informasi dengan aman (dalam hal ini memastikan siapa pengirim informasi tersebut), digunakan digital signature. Digital signature dibuat dengan mengenkripsi message digest dengan menggunakan kunci tertentu. Setiap digital signature terdiri atas untaian angka yang unik. Hal ini mencegah penggunaan kembali sebuah signature pada waktu lain oleh pihak yang tidak diinginkan.

Gambar 2 menunjukkan proses pertukaran informasi oleh seorang klien dengan sebuah server dengan menggunakan digital signature.

Fungsi hash yang digunakan pada SSL antara lain HMAC-MD5 atau HMAC-SHA. Versi lama dari SSL menggunakan MD2 dan MD4. [1]

Pada makalah ini, hanya akan dijelaskan tentang HMAC-MD5 dan HMAC-SHA.

MD5 merupakan fungsi hash yang memberikan nilai hash sebesar 128 bit. Biasanya hasil dari MD5 berupa 32 karakter angka heksadesimal. Pseudocode fungsi MD5 dapat diakses pada referensi [2] makalah ini. Berikut ini contoh keluaran MD5 ketika dimasukkan 43 byte ASCII: [2]

MD5("The quick brown fox jumps over the lazy dog")
= 9e107d9d372bb6826bd81d3542a419d6

Ketika satu huruf pada masukan diganti (huruf d pada ‘dog’ diubah menjadi huruf e), dihasilkan nilai hash yang benar-benar berbeda.

MD5("The quick brown fox jumps over the lazy **e**og")
= ffd93f16876049265fbaef4da268dd0e

Berikutnya ditunjukkan nilai hash yang dihasilkan bila dimasukkan sebuah string dengan panjang nol:

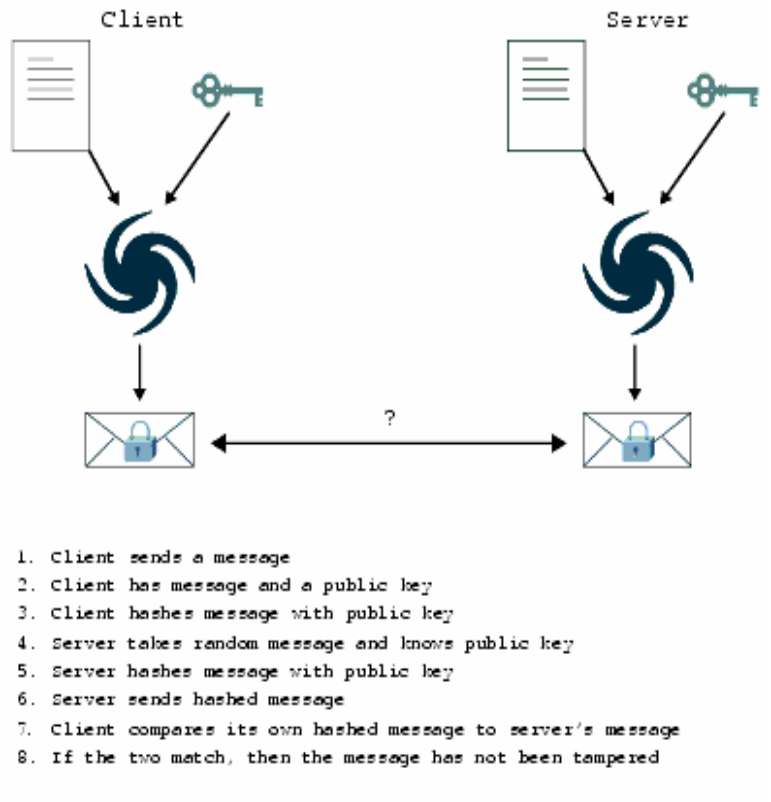
MD5("")
= d41d8cd98f00b204e9800998ecf8427e

SHA merupakan singkatan dari Secure Hash Algorithm. SHA terdiri atas lima fungsi hash yaitu SHA-1, SHA-224, SHA-256, SHA-384 dan SHA-512. Biasanya keempat SHA terakhir disebut SHA-2.

SHA-1 menghasilkan message digest yang panjangnya 160 bit. SHA lainnya menghasilkan message digest yang panjangnya sesuai dengan angka yang mengikuti namanya (SHA-224 menghasilkan message digest yang panjanganya 224 bit, dan seterusnya). Berikut ini adalah contoh hasil penggunaan SHA-1 : [3]

SHA1("The quick brown fox jumps over the lazy dog")
= 2fd4e1c6 7a2d28fc ed849ee1 bb76e739 1b93eb12

Jika satu huruf pada masukan diganti (misalnya huruf d pada kata ‘dog’ diganti dengan huruf c), dihasilkan



- Gambar 2: Pertukaran pesan dengan menggunakan digital signature [4]

sebuah nilai hash yang benar-benar berbeda dari sebelumnya:

SHA1("The quick brown fox jumps over the lazy **c**og")
= de9f2c7f d25e1b3a fad3e85a 0bd17d9b 100db4b3

2.3. Sertifikasi

Untuk memastikan siapa saja yang terlibat dalam pertukaran informasi lewat internet, SSL menggunakan sertifikat digital. Biasanya sertifikat digunakan untuk mengotentikasi (memastikan identitas) server. Otentikasi pengunjung situs tidak harus dilakukan (optional). Dengan sertifikat seperti ini, kemungkinan pihak ketiga mengaku sebagai server dengan kunci yang salah dapat dihindari.

Sebuah sertifikat memastikan identitas pihak lainnya, mengkonfirmasi kunci public dan ditandatangani oleh sebuah agen yang terpercaya. Agen seperti ini disebut Certificate Authority (Otoritas Sertifikat).

SSL menggunakan sertifikat X.509 untuk memvalidasi identitas. Sertifikat ini mengandung informasi mengenai pihak yang terkait, termasuk kunci publik dan nama. [4]

3. SECURE SOCKET LAYER (SSL)

Pada SSL, terlibat dua pihak yang saling terpisah, yaitu server dan klien. Klien merupakan pihak yang menginisiasi (memulai) transaksi, sementara server adalah pihak yang memberikan respon kepada klien

dan menegosiasi chiper yang sesuai untuk digunakan saat enkripsi. [4] Pada makalah ini, klien merujuk kepada pengunjung sebuah situs dan server merujuk pada server situs yang terkait.

Ada tiga protokol pada SSL, yaitu Handshake Protocol (Protokol Jabat Tangan), Record Protokol, dan Alert Protokol. Pada Handshake Protocol, klien mengotentikasi server (memastikan identitas server). Setelah protokol tersebut selesai, enkripsi informasi yang dikirimkan klien dilakukan pada fase Record Protocol. Apabila selama sesi terjadi peringatan-peringatan tertentu, peringatan tersebut disertakan pada paket informasi yang terkait dan ditangani dengan menggunakan Alert Protocol. [4]

3.1 SSL Handshake

Pada protokol Handshake, dilakukan langkah-

langkah penting berupa negosiasi algoritma enkripsi (chiper) dan otentikasi server bagi klien.

SSL menggunakan kriptografi simetris untuk enkripsi data selama fase transmisi. Kriptografi asimetris (yaitu PKI) digunakan untuk menegosiasi kunci yang digunakan untuk enkripsi simetris di atas. Pertukaran ini penting dalam protokol Handshake. [4]

Berikut ini diberikan contoh sederhana hubungan antara klien dan server: [1]

- Klien mengirimkan pesan ClientHello yang menyebutkan versi tertinggi protokol SSL yang dapat ia gunakan, sebuah angka yang acak, daftar chiper dan metode kompresi yang disarankan.
- Server menanggapi dengan ServerHello, yang mengandung versi protokol yang dipilih, sebuah angka yang acak, chiper dan metode kompresi yang dipilih dari yang ditawarkan oleh klien.
- Server mengirimkan sertifikatnya. Hal ini tergantung pada chiper yang digunakan. Terkadang langkah ini tidak perlu dilakukan oleh server.
- Server dapat meminta sertifikat dari klien (optional).
- Server mengirimkan pesan ServerHelloDone, yang mengindikasikan bahwa negosiasi jabat tangan (handshake) telah selesai.
- Klien menanggapi dengan pesan ClientKeyExchange, yang dapat mengandung sebuah PreMasterSecret, kunci publik, atau nihil (tergantung chiper yang digunakan).
- Klien dan server menggunakan angka-angka acak dan PreMasterSecret untuk menghasilkan sebuah rahasia bersama, yang disebut “master secret”. Semua kunci data yang lainnya diturunkan dari master secret.
- Klien mengirimkan pesan ChangeCipherSpec, yang memberitahu server bahwa semua data yang dikirimkan mulai saat itu akan dienkripsi. Langkah ini merupakan bagian dari protokol Record.
- Klien mengirimkan pesan Finished yang telah dienkripsi, yang mengandung sebuah hash dan MAC atas pesan-pesan jabat tangan (handshake) sebelumnya.
- Server akan berusaha mendekripsikan pesan Finished dari klien, melakukan verifikasi terhadap hash dan MAC. Jika dekripsi atau verifikasi gagal, maka koneksi akan diputus.
- Server mengirimkan ChangeCipherSpec dan pesan Finished yang telah dienkripsi. Klien melakukan dekripsi dan verifikasi seperti yang sebelumnya dilakukan oleh server.
- Protokol Handshake telah selesai.

3.2 SSL Record

Enkripsi untuk semua pesan pada SSL dilakukan pada protokol Record. Protokol ini menyediakan format yang umum untuk Alert, ChangeCipherSpec, Handshake dan pesan-pesan protokol aplikasi.

Message digest, digital signature, jenis, versi dan panjang pesan merupakan bagian yang direkam pada protokol Record.

3.3 SSL Alert Protocol

Protokol ini menangani paket informasi yang “meragukan”. Jika selama proses pertukaran informasi, server atau klien mendapati kesalahan atau error, pihak terkait akan mengirimkan peringatan tentang error tersebut.

Ada tiga macam pesan alert : peringatan, kritis dan fatal. Apabila pesan yang diterima berupa peringatan atau kritis, maka sesi dapat dibatasi sesuai keperluan. Namun jika pesan yang diterima berupa fatal, maka sesi dihentikan.

4. KESIMPULAN

Keamanan pertukaran informasi lewat situs di internet terjamin dengan penggunaan SSL. SSL memastikan kerahasiaan, keutuhan dan keaslian informasi yang dipertukarkan, serta melakukan otentikasi server kepada klien. Hal ini dimungkinkan dengan penggunaan kriptografi pada SSL.

Penggunaan SSL memungkinkan adanya online banking, online shopping, dan kegiatan lainnya lewat internet yang memerlukan jaminan keamanan informasi yang dipertukarkan oleh klien dengan server.

DAFTAR REFERENSI

[1] http://en.wikipedia.org/wiki/Secure_Sockets_Layer
Tanggal akses: 1 Januari 2007

[2] http://en.wikipedia.org/wiki/MD5
Tanggal akses: 2 Januari 2007

[3] http://en.wikipedia.org/wiki/SHA_hash_functions
Tanggal akses: 2 Januari 2007

[4] http://www.cisco.com/en/US/netsol/ns340/ns394/ns50/ns140/networking_solutions_white_paper09186a0080136858.shtml
Tanggal akses: 1 Januari 2007

[5]
http://httpd.apache.org/docs/2.0/ssl/ssl_intro.html
Tanggal akses: 1 Januari 2007

[6]
http://amit-badola.blogspot.com/2007/12/http-and-https.html
Tanggal akses: 1 Januari 2007

[7]
https://login.yahoo.com/config/mail?.intl=us
Tanggal akses: 1 Januari 2007