Aplikasi Secure Hypertext Transfer Protocol dengan Algoritma RSA

Yomanovian 13510067[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]yomanovian@std.itb.ac.id

HTTP *(Hypertext Transfer Protocol)* adalah suatu protokol jaringan yang merupakan basis dari *World Wide Web (WWW)*. Fungsi utama HTTP adalah menangani permintaan dan memberikan respon dalam model jaringan *client-server*. Saat kita menjelajah WWW, kita menggunakan suatu perangkat lunak yang berfungsi dan berperan sebagai Client yaitu Web Browser. Web Browser akan melakukan komunikasi dengan Server, dengan mengajukan permintaan kepada Server dan Server akan memberikan respon berupa informasi kepada Web Browser.

Isi dari permintaan dan informasi yang dilakukan saat transaksi antara client dan server ini umumnya transparan, tidak terenkripsi, sehingga dapat dilihat oleh pihak ketiga (selain client dan server). Terkadang kita tidak menginginkan komunikasi antara client dan server ini dapat dilihat oleh pihak ketiga, oleh karena itu, komunikasi ini harus ter-enkripsi, dan salah satu algoritma pengenkripsian yang dapat digunakan adalah Algoritma RSA.

Kata kunci : HTTP, WWW, RSA, Client, Server, Public-Key, Private-Key.

I. PENDAHULUAN

Semakin meningkatnya penerimaan masyarakat akan perkembangan teknologi informasi membuat hamper semua kegiatan bisa dilakukan secara virtual. Tidak heran menjamurnya *website* dan layanan turunnya menjadi hal yang biasa terjadi di seluruh penjuru dunia. *World Wide Web* (atau yang lebih dikenal dengan singkatannya WWW) merupakan bagian utama yang membangun sebuah *website*. Komponen ini adalah suatu sistem yang terdiri dari dokumen *hypertext* yang saling terhubung dan dapat diakses melalui jaringan Internet.

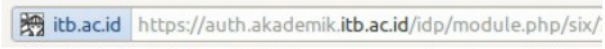
WWW bukan merupakan istilah yang terlalu asing di era internet sekarang ini. Karena aksesnya yang mudah, WWW berperan penting dalam penyampaian informasi saat ini. Hanya dengan mengetikkan alamat dari suatu *Web Page*, dalam hitungan detik dapat diperoleh informasi yang kita inginkan, salah satu contohya dengan mengetikkan https://ol.akademik.itb.ac.id/, lalu login, maka akan ditampilkan status dan berbagai hal berkaitan dengan akademik selama berkuliah di ITB. Selain itu WWW juga merupakan sarana komunikasi yang efisien saat ini yang memberikan kemudahan dalam berkomunikasi dengan keluarga dan kerabat melalui *Social Network*.

Melihat kompleksitas dan kemudahan sistem tersebut, terkadang timbul pertanyaan, “Apakah informasi akademik dari ol.akademik.itb.ac.id yang diperoleh dapat dilihat oleh orang lain?”, atau “Apakah *password social network* yang dimasukkan dapat terlihat oleh orang ketiga?”. Tanpa fitur keamanan berupa pengenkripsian data, jawabannya adalah “Ya”, Sedangkan jika data yang dikirim atau diterima terenkripsi terlebih dahulu, jawabannya bisa “Ya” atau “Tidak”, tergantung tingkat keampuhan algoritma kriptografi yang digunakan.

Pengenkripsian semakin penting dilakukan jika hendak menyampaikan atau menerima informasi yang penting dan sensitif, misalnya *username* dan *password* untuk login ke portal informasi akademik selama berkuliah di ITB, atau bahkan nomor kartu kredit untuk melakukan pembayaran melalui WWW. Pengenkripsian tidak selalu menjamin keamanan dalam penyampaian atau penerimaan informasi. Jika pengenkripsian informasi tersebut lemah, informasi “rahasia” yang terenkripsi itu dapat dengan mudah didekripsi oleh pihak ketiga, atau lebih disebut dengan “penyerang”. Oleh karena itu, dalam pengenkripsian informasi harus menggunakan suatu algoritma yang ampuh, yang tidak dengan mudah dapat didekripsi oleh “penyerang”.

WWW sendiri memerlukan suatu protokol jaringan yang dikenal dengan HTTP *(Hypertext Transfer Protocol)*, protokol jaringan inilah yang bertanggung jawab menangani transaksi (permintaan dan respon) informasi dalam WWW. Oleh karena itu, suatu alamat WWW memiliki *prefix* http:// yang menandakan penggunaan protokol HTTP. Semua urusan penyampaian informasi berjalan di protokol ini, sehingga pengenkripsian informasi juga dilakukan disini juga. Untuk membedakan WWW mana yang terenkripsi atau

tidak, maka pada WWW yang terenkripsi diberikan prefix https:// yang menandakan penggunaan protokol *Secure* HTTP.



II. DASAR TEORI

2.1. Kriptografi

Kriptografi adalah ilmu sekaligus seni untuk menjaga keamanan informasi. Keamanan informasi diperolah dengan menyandikan (mengenkripsi) informasi tersebut menjadi informasi yang tidak memiliki makna. Informasi yang ingin dirahasiakan dinamakan plainteks (Informasi yang masih dimengerti), hasil dari penyandian informasi tersebut dinamakan cipherteks (Informasi sudah tidak dapat dimengerti). Proses ini disebut dengan proses enkripsi, sedangkan proses kebalikannya, yaitu mengubah informasi yang telah dienkripsi (cipherteks) menjadi informasi yang dapat dimengerti (plainteks) disebut dekripsi. Gambar 2. Proses enkripsi dan dekripsi Contoh, informasi rahasia yang belum dienkripsi sebagai berikut:

UAS Struktur Diskrit Hari Senin

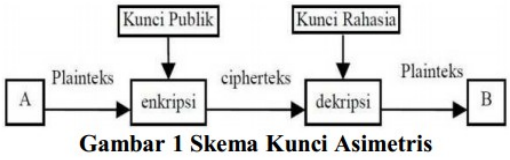
Dienkripsi menjadi cipherteks sebagai berikut:

WCU"Uvtwmvwt"Fkumvtkv

Terlihat cipherteks sudah tidak memiliki makna sama sekali dengan informasi awal sebelum dienkripsi. Informasi rahasia yang telah menjadi cipherteks-lah yang akan diberikan ke pihak penerima, sehingga jika ada pihak ketiga yang memperoleh informasi tersebut, pihak ketiga tersebut tidak dapat memaknakan pesan rahasia tersebut. Penerima informasi telah diberitahu algortima untuk mendekripsi pesan tersebut terlebih dahulu.

2.2. Algortima RSA

RSA merupakan algoritma kriptografi asimetris. Ditemukan pertama kali pada tahun 1977 oleh Ron Rivest, Adi Shamir, dan Leonard Adleman. Nama RSA sendiri diambil dari inisial nama depan ketiga penemunya tersebut. Sebagai algoritma kunci publik, RSA mempunyai dua kunci, yaitu kunci publik dan kunci pribadi. Kunci publik boleh diketahui oleh siapa saja, dan digunakan untuk proses enkripsi. Sedangkan kunci pribadi hanya pihak - pihak tertentu saja yang boleh mengetahuinya, dan digunakan untuk proses dekripsi. Algoritma RSA masih digunakan hingga pada saat ini seperti yang diuraikan M. Zaki Riyanto dan Ardhi Ardhian: Keamanan sandi RSA terletak pada sulitnya memfaktorkan bilangan yang besar. Sampai saat ini RSA masih dipercaya dan digunakan secara luas di internet. (Kriptografi Kunci Publik: Sandi RSA, 2008).



Gambar 1 Skema Kunci Asimetris

Gambar 1 Skema Kunci Asimetris

Skema algoritma kunci publik Sandi RSA terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Sebelumnya diberikan terlebih dahulu beberapa konsep perhitungan matematis yang digunakan RSA.

Algoritma Pembentukan Kunci:

1. Tentukan p dan q bernilai dua bilangan Prima besar, acak dan dirahasiakan. $p \neq q$, p dan q memiliki ukuran sama.
2. Hitung $n = pq$, dan hitung $(n) = (p-1)(q-1)$. Bilangan integer n disebut (RSA) modulus.
3. Tentukan e bilangan prima acak, yang memiliki syarat: $1 < e < (n)$
   GCD(e, (n)) = 1, disebut e relatif prima terhadap (n),

   Bilangan integer e disebut enciphering exponent.
4. Dengan menggunakan *Extended Eucledian Algorithm,* dihitung bilangan khusus d.
   Syarat $1 < d < (n)$
   $d \equiv e^{-1} \mod (n)$
   $ed \equiv 1 \pmod{(n)}$
   $ed \equiv 1 + k\{(n)$ untuk nilai k integer. $\}$

   Bilangan integer d disebut deciphering exponent.
5. Nilai (n, e) adalah nilai yang boleh dipublikasi. Nilai $d, p, q, (n)$ adalah nilai yang harus dirahasiakan.
   Pasangan (n, e) merupakan kunci publik.
   Pasangan (n, d) merupakan kunci rahasia.

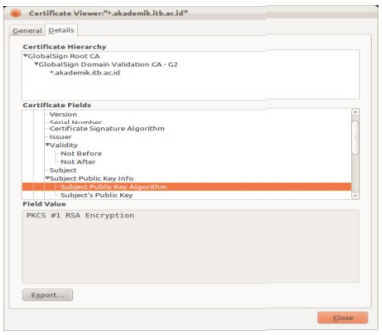
2.3. HTTP (Hypertext Transfer Protocol)

Hypertext Transfer Protocol (HTTP) adalah suatu protokol jaringan pada lapisan aplikasi yang digunakan untuk sistem informasi terdistribusi. HTTP merupakan fondasi dari World Wide Web (WWW). Fungsi utama HTTP adalah menangani permintaan dan memberikan respon dalam WWW, bertanggung jawab pada proses pertukaran informasi dalam WWW. Protokol jaringan HTTP adalah salah satu jaringan bersistem client-server.

Client memberikan beberapa informasi kepada server (disebut permintaan), lalu server memberikan respon informasi yang diminita oleh client. Pada

kasus membuka
https://ol.akademik.itb.ac.id/
(ol.akademik.itb.ac.id adalah server), client, meminta kepada server, mengirimkan informasi berupa identitas dan URL (Unified Resource Locator) untuk melihat status akademik, sehingga server memroses dan merespon apa yang diminta client yaitu informasi status akademik untuk user dengan identitas yang diberikan kepada server.

Tentunya informasi yang kita inginkan ini sifatnya pribadi, kita tidak ingin ada pihak ketiga yang dapat melihat informasi tersebut. Alamat ol.akademik.itb.ac.id memiliki prefiks https:// yang berarti server ol.akademik.itb.ac.id menggunakan Secure HTTP, yaitu protokol yang telah diamankan karena informasi yang disampaikan telak dienkripsi terlebih dahulu.

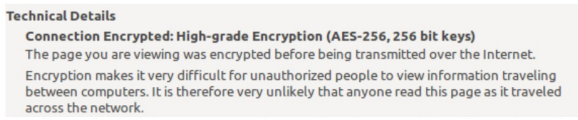


III. PENGAPLIKASIAN DALAM SECURE HYPERTEXT TRANSFER PROTOCOL

Mekanisme pada aplikasi *secure hypertext transfer protocol* adalah sebagai berikut, saat *Web Browser (client)* berinteraksi dengan *server Secure HTTP (HTTPS)*, pertama-tama, browser meminta terlebih dahulu kunci publik dari server yang bersangkutan.

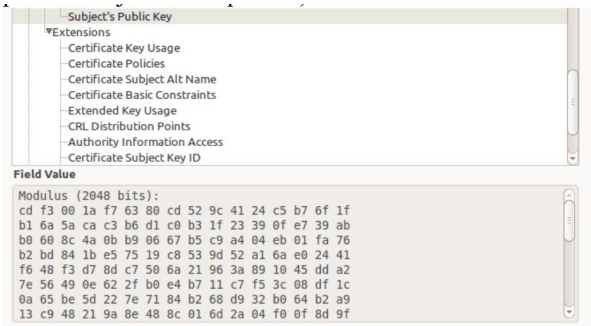
Secara umum, di WWW ada beberapa lembaga sertifikasi yang mengeluarkan sertifikat keabsahan dari kunci publik suatu server (contohnya yang cukup terkenal adalah *Verisign*, dan *Thawte*). Browser kemudian perlu memeriksa kunci publik yang didapat dari server tersebut sah atau tidak, karena bisa jadi ada pihak ketiga (atau penyerang) yang mengirimkan kunci publik palsu sehingga pesan terenkripsi itu dapat dilihat oleh penyerang tersebut. Jika tidak sah, web browser akan memperingati pengguna untuk berhati-hati dengan server HTTPS tersebut.

Kunci publik digunakan untuk pengenkripsian jalur client ke server. Setelah mendapatkan kunci publik tersebut, browser akan mengirimkan sebuah sandi kepada server (sandi yang dikirimkan dienkripsi menggunakan kunci publik) untuk pengenkripsian dari jalur server ke client. Pengenkripsian jalur server ke client dapat menggunakan algoritma seperti AES atau RC4 (*non-Public-key*).



Gambar 4.

Selain menggunakan Algoritma RSA, digunakan juga Algoritma AES-256.Kunci publik RSA yang digunakan haruslah bilangan non-prima yang sangat besar, paling tidak jumlah (dalam satuan bit) bilangan tersebut harus lebih dari atau sama dengan 2048 untuk saat sekarang ini, dan besaran ini akan semakin bertambah seiring perkembangan teknologi (semakin cepatnya komputer, atau semakin mangkusnya algoritma pemecahan / pemfaktoran kunci publik menjadi kunci pribadi).



Gambar 5.

Kunci publik yang diberikan oleh *.akdemik.itb.ac.id. Kunci publik harus merupakan bilangan non-prima yang besar.Penggunaan Algoritma RSA dalam Secure HTTP ini sangat bermanfaat dalam pengrahasiaan pesan. Electronic Frontier Foundation mengatakan bahwa idealnya komunikasi saat kita menjelajah WWW adalah terenkripsi. Akan tetapi tetap ada sisi kelemahan dalam penggunaan Algoritma RSA ini, sehingga tidak digunakan secara umum (untuk hal-hal khusus yang menyangkut informasi sensitif saja.

Kekurangan tersebut antara lain, komputer memerlukan kerja yang lebih banyak untuk mengenkripsi informasi dan mendekripsikan cipherteks. Dan tentu saja, tidak semua server di dunia mampu menangani semua permintaan dan respon secara terenkripsi, oleh karena itu, pengenkripsian lebih sering dilakukan hanya pada bagian yang berisi informasi sensitif untuk menghemat sumber daya yang ada pada komputer.

Kunci publik juga perlu disertifikasi oleh suatu lembaga yang dipercaya supaya kunci publik terserbut terbukti keabsahannya, dan untuk mencegah adanya serangan “man-in-the-middle”.

IV. KESIMPULAN

Kesimpulan yang dapat diambil dari Pengaplikasian Algoritma RSA dalam Secure Hypertext Transfer Protocol, antara lain:

1. Algoritma RSA sangat efektif dalam pengamanan penyampaian informasi di WWW.
2. Pengenkripsian dapat mencegah adanya pihak ketiga yang dapat melihat suatu informasi rahasia.
3. Kunci publik haruslah bilangan non-prima yang sangat besar sehingga sulit untuk difaktorkan.
4. Standar besaran bilangan kunci publik terus membesar seiring perkembangan teknologi.
5. Perlu suatu status keabsahan pada kunci publik untuk menghindari adanya kunci publik palsu dari penyerang.
6. Pengenkripsian memang menjamin penyampaian informasi secara rahasia, tetapi membutuhkan sumber daya komputer yang lebih besar.

V. REFERENSI

1. Rinaldi Munir, – Diktat Kuliah IF2091, Struktur Diskrit, Program Studi Teknik Informatika, STEI, ITB, 2008.
2. Iqbal, Muhammad.. Studi Teknis Metode nkripsi RSA dalam Perhitungannya. Bandung:
   Institut Teknologi Bandung, 2006
3. Rivest, R.; A. Shamir; L. Adleman (1978). “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”
4. https://tools.ietf.org/html/rfc2818
5. https://tools.ietf.org/html/draft-ietf-tls-ssl-version3-00

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 18 Desember 2012

Yomanovian 13510067