Pengaplikasian Algoritma RSA dalam *Secure Hypertext Transfer Protocol*

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

World Wide Web (atau yang lebih dikenal dengan singkatannya *WWW)* 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 masa ini. Hanya dengan mengetikkan alamat dari suatu Web Page, dalam hitungan detik dapat kita peroleh informasi yang kita inginkan, contohya dengan mengetikkan https://ol.akademik.itb.ac.id/, lalu *login*, kita dapat melihat status akademik kita selama berkuliah di ITB. *WWW* juga merupakan sarana komunikasi yang efisien saat ini. Kita dapat berbagi informasi dengan teman-teman kita melalui *Social Network*, melakukan *chatting*, dsb. Terkadang timbul pertanyaan, misalnya, "Apakah informasi akademik dari ol.akademik.itb.ac.id yang saya peroleh dapat dilihat oleh orang lain?", atau "Apakah *password social network* yang saya masukkan dapat terlihat oleh orang ketiga?". Tanpa fitur keamanan berupa pengenkripsian data, jawabannya adalah "Ya", 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 kita hendak menyampaikan atau menerima informasi yang sensitif, misalnya *username* dan *password* untuk *login* ke suatu portal, informasi akademik selama berkuliah di ITB, atau bahkan nomor *credit card* 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 di protokol ini. Untuk membedakan *WWW* mana yang terenkripsi atau tidak, maka pada WWW yang terenkripsi diberikan prefix https:// yang menandakan penggunaan protokol *Secure HTTP*.

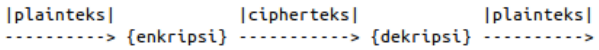
Gambar 1. Contoh alamat WWW yang menggunakan Secure HTTP.

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

Algortima kriptografi ini diperkenalkan oleh tiga orang peneliti dari *MIT*, yaitu Ron Rivest, Adi Shamir, dan Adleman pada tahun 1976. RSA merupakan kependekan dari nama ketiga orang peneliti tersebut (Rivest-Shamir-Adleman). Algoritma kriptografi RSA mendasarkan prosesnya pada konsep bilangan prima dan aritmetika modulo. Algoritma kriptografi RSA termasuk jenis *Public-Key cryptography* yang membutuhkan kunci publik (*public-key*) untuk mengenkripsi informasi menjadi cipherteks, dan kunci pribadi (*private-key*) untuk mengembalikan cipherteks menjadi informasi semula yang memiliki makna. Baik kunci publik dan pribadi keduanya merupakan bilangan bulat. Kunci publik tidak dirahasiakan, namun kunci pribadi harus dirahasiakan. Kunci pribadi dibangkitkan dari beberapa buah bilangan prima bersama-sama dengan kunci publik. Untuk menemukan (membongkar) kunci pribadi, harus difaktorkan terlebih dahulu suatu bilangan non-prima menjadi faktor primanya. Semakin besar bilangan non-prima tersebut, semakin susah juga memfaktorkannya, sehingga membuat pengenkripsian menjadi sangat kuat.

Berikut penjelasan secara ringkas proses dari Algortitma RSA:

i. Pembangkitan Pasangan Kunci

1. Pilih dua buah bilangan prima sembarang, sebut A dan B. A dan B bersifat rahasia.
2. Hitung N = AB. N tidak bersifat rahasia.
3. Hitung M = (A – 1)(B -1). Setelah M terhitung, A dan B dapat dilupakan,
4. Pilih sebuah bilangan bulat untuk kunci publik, sebut E, yang relatif prima terhadap M.
5. Hitung kunci pribadi, D, dengan kekongruenan :

$$ED \equiv 1 \pmod{M}$$

ii. Enkripsi

1. Nyatakan informasi menjadi blok-blok plainteks: p_1, p_2, p_3, …
2. Hitung blok cipherteks ci, untuk blok plainteks pi, dengan persamaan:

$$c_i = p_i^e \bmod n$$

yang dalam hal ini, e adalah kunci publik.

iii. Dekripsi

1. Proses dekripsi dilakukan dengan menggunakan persamaan:

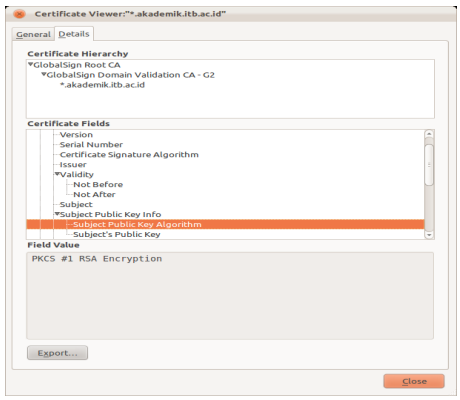
$$p_i = c_i^d \bmod n$$

yang dalam hal ini, d adalah kunci pribadi.

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 diminta 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*.

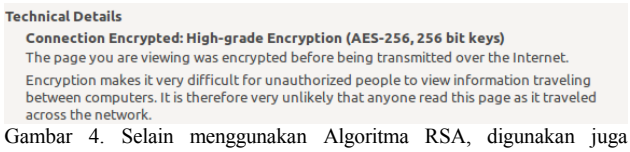
Tentunya informasi yang kita inginkan ini sifatnya pribadi, kita tidak ingin ada pihak ketiga yang dapat melihat informasi tersebut. Alamat ol.akademik.itb.ac.id memiliki prefiks https:// yang berarti server ol.akademik.itb.ac.id menggunakan *Secure HTTP*, yaitu protokol yang telah diamankan karena informasi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



Gambar 3. *.akademik.itb.ac.id dienkripsi menggunakan Algoritma RSA.

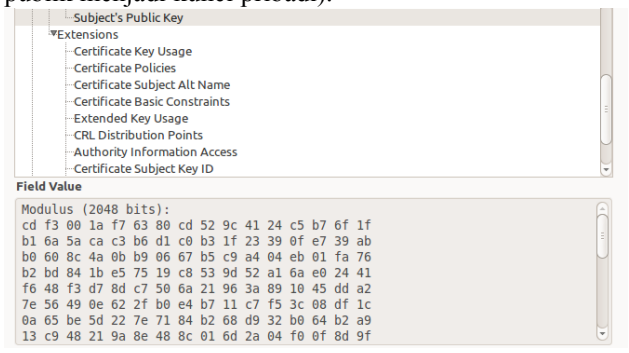
III. Pengaplikasian dalam Secure Hypertext Transfer Protocol

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, b*rowser* 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.

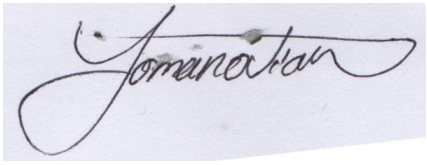
Referensi

[1] Rinaldi Munir, — Diktat Kuliah IF2091, Struktur Diskrit, Program Studi Teknik Informatika, STEI, ITB, 2008.
[2] http://en.wikipedia.org/wiki/Public-key_cryptography
[3] http://en.wikipedia.org/wiki/RSA_%28algorithm%29
[4] http://en.wikipedia.org/wiki/HTTP
[5] http://en.wikipedia.org/wiki/HTTP_Secure
[6] http://en.wikipedia.org/wiki/Transport_Layer_Security
[7] http://en.wikipedia.org/wiki/WWW

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, 29 April 2010



Yomanovian 13510067