Penerapan Enkripsi dan Dekripsi Data dengan Algoritma RSA

Marlina

Fakultas Teknik UPI Y.A.I
Jakarta
linabahar@ymail.com

Abstrak

Penelitian ini membahas mengenai proses pengiriman data secara acak (enkripsi) sehingga tidak dapat dibaca oleh pihak lain, pengiriman data tersebut haruslah menyertakan kunci sehingga data yang yang dinamakan deskripsi, agar tidak bocor kepada pihak yang tidak bertanggung jawab maka dibuatlah user id dan password dengan menggunakna algoritma RSA, Tujuan penelitian ini adalah menjaga keamanan data agar tidak digunakan oleh pihak yang tidak berkepentingan, metode penelitian ini adalah studi literature, dengan hasil penelitian ini adalah data yang dikirimkan terlebih dahulu di enkripsikan dan data yang telah di enkripsikan maka menyediakan kunci sebagai deskripsi sehingga informasi tersebut tidak terlihat oleh pihak lain.

Kata Kunci : pengiriman data, enkripsi, deskripsi, algoritma RSA, menjaga keamanan data

Pendahuluan

Latar Belakang

Pengiriman data yang sering dilakukan kepada penerima data menjadi hal yang sering terjadi, namun kegiatan tersebut sering sekali terjadi pencurian data dan informasi yang sering dilakukan oleh para hecker. Para pengirim maupun penerima data menjadi khawatir terhadap data yang dimiliki, sehingga dibutuhkan teknologi untuk pelindungan data dan informasi yang dimiliki pengirim dan penerima data. Salah satu cara yang dapat digunakan adalah dengan diterapkannya suatu kriptografi untuk melakukan enkripsi . Dengan enkripsi, data tidak dapat terbaca oleh orang lain yang tidak berkepentingan. Karena teks asli atau plaintext telah diubah ke teks yang tidak bias terbaca atau disebut chipertext. sehingga informasi akan sampai ketujuan tanpa adanya kebocoran atau pencurian data teks. Ilmu yang mempelajari mengenai cara pengamanan data dikenal dengan istilah kriptografi, sedangkan langkah-langkah kriptografi dinamakan dengan algoritma kriptografi. Berdasarkan dari kkunci yang digunakan algoritma kriptografi dapat dibagi menjadi dua, yaitu algoritma simetri dan algoritma assimetri. Algiritma kriptografi menggnakan kunci simetri adalah DES, RC2, RC4, RC6, IDEA, AES, OTP, A5 dan sebagainya. Proses penyadian biasanya dipakai adalah RSA coding, RSA coding merupakan proses penyadian kunci asisimetris, proses ini didasarkan pada teorema euler, sehingga menghasilkan kunci umum dan kunci pribadi yang saling berkaitaitan sehingga prorses enkripsi dan deskpris dapat menggunakan dua kunci yaitu bilangan prima. Algoritma RSA memiliki mekanisme kerja yang cukup sederhana dan mudah dimengerti namun tetap kokoh dalam tugasnya mengamankan data. Panjang kunci dalam bit dapat diatur,dengan semakin panjang bit maka semakin sukar untuk dipecahkan karena sulitnya memfaktorkan dua bilangan yang sangat besar tersebut, tetapi juga semakin lama pada proses. Dan dalam menenkripsi dan mendekripsi nya memiliki kunci yang berbeda.

Masalah dan batasannya

Berdasarkan latar belakang di atas maka akan dibahas mengenai bagaimana cara menerapkan algoritma RSA ke dalam aplikasi enkripsi dan dekripsi?. Batasan penelitian ini menggunakan algoritma RSA dan penerapannya

Tujuan Penelitian

Untuk keamanan dalam berkomunikasi agar tidak ada pihak ketiga yang tidak berkepentingan mengetahui informasi dalam komunikasi .

Manfaat penelitian

Penelitian ini diharapkan memberikan manfaat antara lain : a. Bagi mahasiswa Sebagai bahan dasar mempelajari mata kuliah kriptografi b. Bagi dosen Sebagai media pendukung pembelajaran yang disampaikan oleh dosen sehingga dosen dengan mudah menyampaikan materi mata kuliah

State of the art penelitian

Penelitian dengan topik sejenis ini adalah:

a. Penelitian yang membahas mengenai pengiriman file yang telah di deskripsi merupakan isi file dari sumber sehingga apabila akan dilakukan proses dekripsi maka akan kembali seperti ke sumber semula. [1]

b. Penelitian yang membahas mengenai pengiriman data yang diamankan (dekripsi) ketika hendak dikirim melalui media internet, proses enrkipsi dan dekripsi file maupun teks, pada prinsipnya memiliki mekanisme proses yang sama.[2]

Tinjauan Pustaka

Kriptografi

Kriptografi adalah suatu seni ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Menurut Bruce Scheiner [4], kriptografi adalah ilmu pengetahuan dan seni menjaga message-message agar tetap aman (secure).

Konsep kriptografi sendiri telah lama digunakan oleh manusia misalnya pada peradaban Romawi walau masih sangat sederhana. Prinsip-prinsip yang mendasari kriptografi yakni:

a. Confidelity (kerahasiaan) yaitu layanan agar isi pesan yang dikirimkan tetap rahasia dan tidak diketahui oleh pihak lain (kecuali pihak pengirim, pihak penerima / pihak-pihak memiliki ijin). Umumnya hal ini dilakukan dengan cara membuat suatu algoritma matematis yang mampu mengubah data hingga menjadi sulit untuk dibaca dan dipahami.

b. Data integrity (keutuhan data) yaitu layanan yang mampu mengenali/mendeteksi adanya manipulasi (penghapusan, pengubahan atau penambahan) data yang tidak sah (oleh pihak lain).

c. Authentication (keotentikan) yaitu layanan yang berhubungan dengan identifikasi. Baik otentikasi pihak-pihak yang terlibat dalam pengiriman data maupun otentikasi keaslian data/informasi.

d. Non-repudiation (anti-penyangkalan) yaitu layanan yang dapat mencegah suatu pihak untuk menyangkal aksi yang dilakukan sebelumnya (menyangkal bahwa pesan tersebut berasal dirinya).

Berbeda dengan kriptografi klasik yang menitikberatkan kekuatan pada kerahasiaan algoritma yang digunakan (yang artinya apabila algoritma yang digunakan telah diketahui maka pesan sudah jelas "bocor" dan dapat diketahui isinya oleh siapa saja yang mengetahui algoritma tersebut), kriptografi modern lebih menitikberatkan pada kerahasiaan kunci yang digunakan pada algoritma tersebut (oleh pemakainya) sehingga algoritma tersebut dapat saja disebarkan ke kalangan masyarakat tanpa takut kehilangan kerahasiaan bagi para pemakainya.

Berikut adalah istilah-istilah yang digunakan dalam bidang kriptografi :

a. Plaintext (M) adalah pesan yang hendak dikirimkan (berisi data asli).

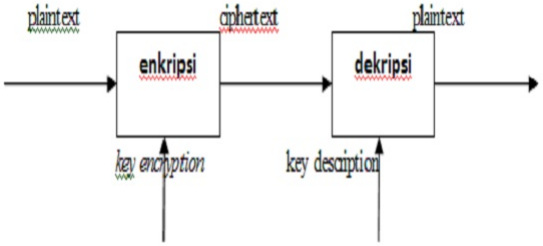
b. Ciphertext (C) adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.

c. Enkripsi (fungsi E) adalah proses pengubahan plaintext menjadi ciphertext.

d. Dekripsi (fungsi D) adalah kebalikan dari enkripsi yakni mengubah ciphertext menjadi plaintext, sehingga berupa data awal/asli.

e. Kunci adalah suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi.

Kriptografi itu sendiri terdiri dari dua proses utama yakni proses enkripsi dan proses dekripsi. Seperti yang telah dijelaskan di atas, proses enkripsi mengubah plaintext menjadi ciphertext (dengan menggunakan kunci tertentu) sehingga isi informasi pada pesan tersebut sukar dimengerti.



Gambar 1: Diagram proses enkripsi dan dekripsi

Peranan kunci sangatlah penting dalam proses enkripsi dan dekripsi (disamping pula algoritma yang digunakan) sehingga kerahasiaannya sangatlah penting, apabila kerahasiaannya terbongkar, maka isi dari pesan dapat diketahui. Secara matematis, proses enkripsi merupakan pengoperasian fungsi E (enkripsi) menggunakan e (kunci enkripsi) pada M (plaintext) sehingga dihasilkan C (ciphertext), notasinya :

Ee(M) – C

Sedangkan untuk proses dekripsi, merupakan pengoperasian fungsi D (dekripsi) menggunakan d (kunci dekripsi) pada C (ciphertext) sehingga dihasilkan M (plaintext), notasinya :

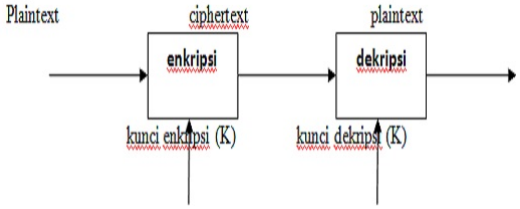
Dd(C) = M 2

Algoritma Simetris dan Asimetris Menurut Thomas H. Cormen [5] mengatakan bahwa algoritma adalah prosedur komputasi yang mengambil beberapa nilai atau kumpulan nilai sebagai input kemudian diproses sebagai output sehingga algoritma merupakan urutan langkah komputasi yang mengubah input menjadi output. Secara terminology algoritma memiliki langkah-langkah logis untuk menyelesaikan masalah yang disusun secara sistematis.

Menurut Ariyus [3] mengatakan bahwa algoritma kriptografi merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut dengan melakukan pembangkitan kunci, enkripsi dan deskripsi. Menurut Ariyus [3] mengatakan bahwa algoritma kriptografi terbagi menjadi tiga bagian berdasarkan kunci yang dipakainya yaitu : algoritma simetris, algoritma asimetri dan fungsi Hash.

a. Algoritma Simetris

Algoritma simetris (symmetric algorithm) adalah suatu algoritma dimana kunci enkripsi yang digunakan sama dengan kunci dekripsi sehingga algoritma ini disebut juga sebagai single-key algorithm.



Gambar 2: Diagram proses enkripsi dan dekripsi algoritma simetris

Sebelum melakukan pengiriman pesan, pengirim dan penerima harus memilih suatu kunci tertentu yang sama untuk dipakai bersama, dan kunci ini haruslah rahasia bagi pihak yang tidak berkepentingan sehingga algoritma ini disebut juga algoritma kunci rahasia (secret-key algorithm). Kelebihan :

1) Kecepatan operasi lebih tinggi bila dibandingkan dengan algoritma asimetrik.

2) Karena kecepatannya yang cukup tinggi, maka dapat digunakan pada sistem real time

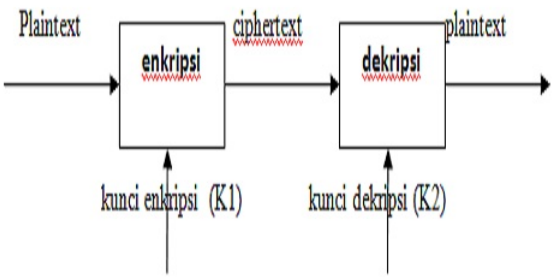
Kelemahan :

1) Untuk tiap pengiriman pesan dengan pengguna yang berbeda dibutuhkan kunci yang berbeda juga, sehingga akan terjadi kesulitan dalam manajemen kunci tersebut.

2) Permasalahan dalam pengiriman kunci itu sendiri yang disebut “key distribution problem” Contoh algoritma : TwoFish, Rijndael, Camellia

b. Algoritma Asimetris

Algoritma asimetris (asymmetric algorithm) adalah suatu algoritma dimana kunci enkripsi yang digunakan tidak sama dengan kunci dekripsi. Pada algoritma ini menggunakan dua kunci yakni kunci publik (public key) dan kunci privat (private key). Kunci publik disebarkan secara umum sedangkan kunci privat disimpan secara rahasia oleh si pengguna. Walau kunci publik telah diketahui namun akan sangat sukar mengetahui kunci privat yang digunakan.



Gambar 3: Diagram proses enkripsi dan dekripsi algoritma asimetris

Pada umumnya kunci publik (public key) digunakan sebagai kunci enkripsi sementara kunci privat (private key) digunakan sebagai kunci dekripsi. Kelebihan :

1) Masalah keamanan pada distribusi kunci dapat lebih baik

2) Masalah manajemen kunci yang lebih baik karena jumlah kunci yang lebih sedikit

Kelemahan :

1) Kecepatan yang lebih rendah bila dibandingkan dengan algoritma simetris

2) Untuk tingkat keamanan sama, kunci yang digunakan lebih panjang dibandingkan dengan algoritma simetris. Contoh algoritma : RSA, DSA, ElGamal

c. Fungsi Hash

Fungsi hash merupakan suatu fungsi dimana pesan yang sudah diubah menjadi message dapat tidak dapat dikembalikan lagi menjadi pesan semula. Dua pesan berbeda akan menghasilkan nilai kasih yang berbeda pula.

3. Algoritma RSA Algoritma RSA merupakan salah satu algoritma kriptografi kunci publik yang saat ini masih populer digunakan. Algoritma RSA diperkenalkan pada tahun 1978 oleh tiga orang profesor MIT (Massachussets Institute of Technology) yaitu Ron Rivest, Adi Shamir, dan Leonard Adleman. Nama RSA pun diambil dari inisial penemunya yaitu Rivest, Shamir dan Adleman. Secara garis besar, proses kriptografi pada algoritma RSA terdiri dari 3 tahapan yaitu :

a. Pembangkitan Kunci Untuk membangkitkan kedua kunci, dipilih dua buah bilangan prima yang sangat besar, p dan q. Untuk mendapatkan keamanan yang maksimum, dipilih dua bilangan p dan q yang besar. Kemudian dihitung : n = pq

Kemudian dihitung : $\varphi = (p-1)\ (q-1)$

Lalu dipilih kunci enkripsi e secara acak, sedemikian sehingga e dan (p-1)(q-1) relatif prima.

Kemudian dengan algoritma Euclidean yang diperluas, dihitung kunci dekripsi d, sedemikian sehingga :

$ed = 1 \bmod (p-1)(q-1)$

atau

$ed - 1 = k\ (p-1)(q-1)$

di mana k merupakan konstanta integer. Perhatikan bahwa d dan n juga relatif prima. Bilangan e dan n merupakan kunci publik, sedangkan d kunci privat.

b. Proses Enkripsi Rumus enkripsinya adalah :

$ci = mie \bmod n$

c. Proses Dekripsi Setelah menerima pesan yang sudah terenkripsi maka penerima pesan akan melakukan proses dekripsi pesan dengan cara :

$mi = cid \bmod n$

Metode Penelitian

Metodologi yang digunakan adalah :

a. Tempat Penelitian ini di lakukan di universitas persada Indonesia Y.A.I di jakarta

b. Waktu Waktu penelitian ini dari bulan maret 2014 sampai dengan juli 2014

c. Cara memperoleh Cara memperoleh data yang dilakukan oleh penulis adalah metode studi literature, yang terlebih dahulu penulis menjabarkan materi-materi dasar yang berkaitan dengan kriptografi dan aljabar khususnya tentang teori bilangan seperti kriptografi, Algoritma Simetris dan Asimetris, dan algoritma RSA.

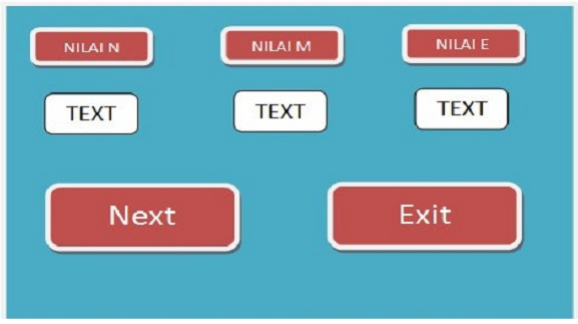
Hasil dan Pembahasan

Proses yang dilakukan pada sistem ini melakukan subsistem enkripsi dan subsistem dekripsi.

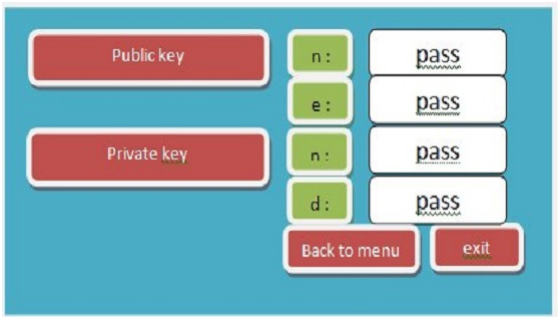
1. Subsistem enkripsi

Enkripsi ini diminta pengguna untuk memasukkan password yang akan dienkripsi, masukan bilangan prima (P) dan bilangan prima (Q) pada gambar 4, kemudian klik submit dan masukan nilai N, nilai M dan nilia E dan klik next lihat gambar 5, langkah selanjutnya next maka tampil hasil key dapat dilihat pada gambar 6, selanjutnya next proses enkripsi maka akan terlihat hasil proses enkripsinya yang dapat disimpan dalam file dengan mengklik tombol simpan.

Gambar 4: Memasukan bilangan



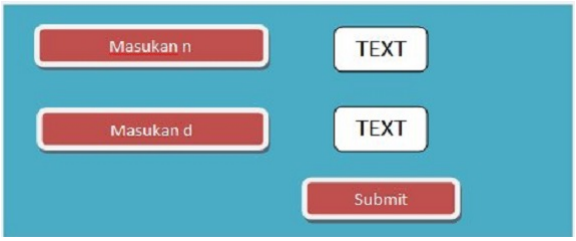
Gambar 5: menentukan nilai N, M dan E



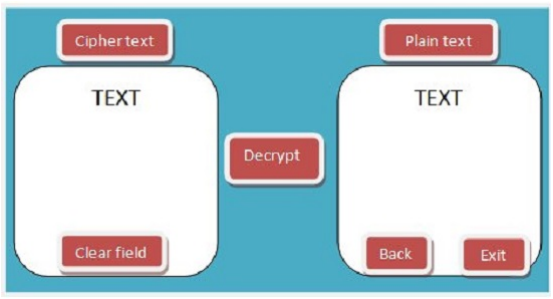
Gambar 6: Tampilan hasil key

2. Subsistem Dekripsi

Tampilan awal deskripsi dengan memasukan n, dan d kemudian submit-kan tampilan dapat dilihat pada gambar 7, langkah selanjutnya akan tampil hasil decrypt



Gambar 7: tampilan awal dekripsi



Gambar 8: Tampilan hasil decrypt

Penutup

Kesimpulan

Berdasarkan pembahasan diatas, maka disimpulkan bahwa :

a. Kriptografi bertujuan untuk menjaga kerahasiaan data dengan melakukan perubahan kode (chipper) sehingga menjadi tidak dapat terbaca secara langsung

b. Sistem pengkodean menggunakan kamus data yang didefinisikan dan melakukan pergantian karakter dari suatu informasi dengan tujuan melindungi informasi agar tidak terlihat oleh pihak yang tidak diotorisasi

c. Masukan kunci yang akan dikirim dan data tersebut di enkripsi dan deskripsi

d. Nilai bilangan yang dimasukan bilangan P dan Q, kedua data tersebut dilakukan enkripsi.

Saran

Penelitian ini sangatlah sederhana dikarenakan aplikasi ini dibangun sebagai media pendukung kegiatan belajar mengajar sehingga mahasiswa dapat memahami kegiatan proses kriptografi enkripsi dan deskpsi. Penelitian ini dapat dikembangkan lebih dalam lagi sehingga aplikasi ini menjadi media pendukung pembelajaran kriptografi bagi dosen-dosen yang mengampu mata kuliah kriptografi.

Daftar Pustaka

[1] Voni Yuniati, dkk, "Enkripsi dan deskripsi algoritma AES 256 untuk semua jenis file",Jurnal Informatika, Volume 5 Nomor 1 april 2009.

[2] Rifkie Primattha, "Penerapan enkripsi dan deskripsi file menggunakan algoritma data enkripsi standar (DES)", Jurnal Sistem Informasi (JSI) vol.3 No.2 oktober 2011

[3] Ariyus, D., "Kriptografi keamanan data dan komunikasi", Graha Ilmu. Yogyakarta, 2006

[4] Bruce Schneider, "Applied Cryptography", john wiley & sons 1996

[5] Cormen, Thomas H. dkk "Introduction to algorithms", 3rd edition, The MT Press, 2009

[6] Komputer, W.. The Best Encryption toolsi. Jakarta: PT Elex Media Komputindo, 2010.

[7] Rinaldi Munir, Kriptografi. Penerbit informatika, Bandung, 2006 .

[8] Sadikin, R. , Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java, Yogyakarta: Andi, 2012.

[9] Yusuf Kurniawan, M. Kriptografi Keamanan Internet dan Jaringan Komunikasi. Bandung: Informatika, 2004