TUGAS PRAKTIKUM SISTEM KEAMANAN DATA

JURNAL ALGORITMA RSA

Disusun Oleh:

(Clarissa Putri Aurellia) (V3920015)

(Farhanang Wahyu Aprian) (V3920021)

(Augesvina Seiyusanda L) (V3920011)

(Alfida Shofiya Mufti) (V3920005)

(Hildanniar Fauzi) (V3920026)

TI-D

PROGRAM STUDI INFORMATIKA

FAKULTAS SEKOLAH VOKASI

UNIVERSITAS SEBELAS MARET

SURAKARTA

2021

JURNAL I
IMPLEMENTASI ALGORITMA RSA UNTUK PENGAMANAN DATA BERBENTUK TEKS

I. Latar Belakang Masalah

Teknologi informasi telah membawa perubahan dan cara orang melihat kehidupan dan organisasi. Perkembangan pesat membawa dunia ke era baru lebih cepat dari yang dibayangkan sebelumnya. Seperti komputer, tidak hanya berfungsi sebagai mesin pengolah data, tetapi menjadi senjata sebagai mesin pengolah data tetapi menjadi senjata utama dalam kompetisi.

Banyak organisasi, bisnis atau pihak lain telah menggunakan teknologi database untuk menyimpan dan mengelola data untuk organisasi atau bisnis. Untuk mencegah hal ini terjadi, diperlukan metode enkripsi suatu ilmu sekaligus seni untuk melindungi file yang dikenal dengan cipher. Salah satu software kriptografi adalah Pretty Good Privacy (PGP) juga dapat digunakan secara online atau offline. Selain kemampuan mengamankan file, perangkat lunak ini juga dapat menyediakan tanda tangan digital yang mampu memenuhi tiga aspek keamanan, yaitu integritas data, autentikasi, dan non-repudiation.

II. Tujuan Penelitian

Tujuan penelitian ini untuk mengimplementasikan algoritma RSA ke dalam keamanan file dengan menggunakan dua teknik yaitu enkripsi (mengubah file asli menjadi file yang tidak dapat dibaca) dan deskripsi (mengubah file yang tidak dapat dibaca menjadi file asli).

III. Algoritma Yang Dipakai Beserta Alur Penelitiannya

Algoritma yang dipakai menggunakan Algoritma RSA. Algoritma RSA merupakan algoritma pertama yang sangat aman karena adanya kunci-kunci yang cukup panjang dan penerapannya yang dan up to date.

1. Admin membuat/mengolah file
2. Admin melakukan proses enkripsi dan tanda tangan digital menggunakan kunci publik
3. Admin melakukan proses dekripsi terhadap file yang telah di enkripsi menggunakan kunci private
4. Muncul hasil file yang telah didekripsi oleh admin

IV. Hasil dan Kesimpulan

Hasil

Dari perancangan yang telah dilakukan pada menu awal terdapat dua tombol yaitu login dan cancel, ketika login terdapat 2 input yaitu user dan password, lalu memilih file yang akan dienkripsi, data ditemukan ketika enkripsi ditekan maka akan muncul pesan. data berhasil dienkripsi. untuk deskripsi dari tabel yang telah disediakan hasil dari deskripsi adalah baik sehingga aplikasi siap digunakan. kemudian terdapat pengujian sistem agar sesuai antara hasil dan harapan.

Setelah itu melakukan pengujian form interface sistem lengkap dengan komponen penyusunnya secara terintegrasi. dengan metode black box.

Kesimpulan

dari hasil pembahasan dapat disimpulkan bahwa:

1. Aplikasi pengamanan data menggunakan RSA terdapat 2 pengamanan yaitu enkripsi dan deskripsi
2. Penggamanan sandi harus diingat secara detail karena huruf kapital dan kecil dibedakan
3. Aplikasi pengamanan RSA memiliki empat aspek keamanan, yaitu kerahasiaan, integritas data, otentikasi dan nir-penyangkalan

V. Kelebihan dan Kekurangan dari jurnal

Kelebihan dari jurnal tersebut adalah penggunaan bahasa yang digunakan sangat simple sehingga mudah dimengerti oleh orang awam sekalipun, selain itu isi jurnal yang ringkas memudahkan pengguna memahami informasi lebih cepat

Untuk kekurangan dari jurnal tersebut adalah pembahasan kurang spesifik dari sini pengguna tidak mengetahui bagaimana enkripsi bekerja karena hanya menampilkan sebuah proses perubahan pada file saja.

JURNAL II

Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email

I. Latar Belakang Masalah

Mengikuti perkembangan teknologi, semakin banyak cara mengubah orang berkomunikasi. Sebelum komunikasi jarak jauh selalu menggunakan metode yang sama dengan cara biasa, yaitu dengan saling berkirim surat, tapi kini komunikasi jarak jauh dapat dilakukan dengan mudah dan cepat, apalagi dengan adanya teknologi seperti email, layanan pesan singkat (SMS) dan internet adalah salah satu teknologi telekomunikasi yang paling banyak digunakan.

Dalam proses pengiriman data (pesan), ada beberapa hal yang harus diperhatikan, yaitu: kerahasiaan, integritas data, membuktikan dan tidak menolak. Oleh karena itu harus diproses dengan mengenkripsi pesan terlebih dahulu sebelum pengiriman dilakukan. Jadi pesan yang terkirim dirahasiakan dan tidak dapat dengan mudah diubah untuk menjaga keutuhan pesan. Contoh algoritma kriptografi yang terpercaya adalah RSA, dimana RSA merupakan proses enkripsi kunci asimetris. Proses membangun RSA didasarkan pada teorema euler, sehingga menghasilkan kunci publik dan kunci privat yang terkait. Jadi walaupun proses enkripsi dan dekripsi menggunakan dua kunci yang berbeda, hasilnya akan tetap benar. kunci publik dan pribadi yang digunakan adalah bilangan prima dan bilangan prima besar direkomendasikan. Hal ini digunakan untuk menggagalkan upaya untuk mendekripsi teks rahasia, semakin besar bilangan prima digunakan sebagai kunci maka semakin sulit untuk menemukan sejumlah besar bagian faktor nya.

II. Tujuan penelitian

Tujuan penelitian ini yaitu untuk merancang dan membangun purwarupa email client yang mampu melakukan enkripsi dan deskripsi dengan menerapkan ilmu kriptografi RSA sehingga dirasa aman.

III. Algoritma Yang Dipakai Beserta Alur Penelitiannya

Algoritma yang digunakan yaitu algoritma kriptografi RSA. Alur penelitiannya yang pertama yaitu dengan mengunduh email dari Google server kemudian mengenkripsi pesan tersebut. Kedua,pesan yang telah dienkripsi selanjutnya akan didekripsi untuk membuktikan pesan tersebut masih sama dengan pesan asli sebelum dienkripsi dengan menggunakan kunci yang sama dengan pesan asli sebelum dienkripsi dengan menggunakan kunci yang sama.

a. proses Enkripsi :
    1. Plaintext diubah ke dalam bentuk bilangan bulat. Untuk mengubah plaintext yang berupa huruf menjadi bilangan dapat digunakan kode ASCII dalam sistem bilangan decimal.
    2. Plaintext m dinyatakan menjadi blok-blok x1,x2,x3,...., sedemikian sehingga setiap blok merepresentasikan nilai di dalam selang [0, n-1], sehingga transformasinya menjadi satu ke satu.
    3. Setiap blok mi dienkripsikan menjadi blok Ci dengan rumus Yi = XiPK mod r.
b. Proses Deskripsi :
    1. Setiap blok ciphertext Yi dideskripsi kembali menjadi blok Xi dengan rumus Xi=YiSK mod r
    2. Kemudian blok-blok m1,m2,m3……, diubah kembali ke bentuk huruf dengan melihat kode ASCII hasil deskripsi.

IV. Hasil dan Kesimpulan

1. Aplikasi yang menerapkan algoritma kriptografi RSA ini berjalan dengan baik mampu mengirim dan menerima email, dan dapat mengenkripsi dan dekripsi kotak masuk yang diterima.

2. Dengan perangkat lunak ini, tujuan penelitian tercapai yaitu keamanan dalam menerima email terjamin. Ada pengamanan ganda untuk membuka pesan tersandi. Saat mendekripsi pesan yang telah dienkripsi harus memasukkan password terlebih dahulu, apabila masukan password salah pesan tidak akan didekripsi.

3. Perangkat lunak ini hanya mengamankan isi pesan masuk email bukan mengamankan jalur transfer email.

4. Pada aplikasi yang dikembangkan ini, satu pesan asli dapat menghasilkan ciphertext yang berbeda-beda, karena proses pembangkitan kunci RSA didasarkan oleh nilai P dan Q yang acak.

5. Pesan kesalahan akan ditampilkan apabila terjadi kesalahan saat memasukkan suatu nilai yang salah saat enkripsi atau dekripsi pesan. Saat enkripsi masukan bit bernai kosong dan saat dekripsi masukan password salah.

V. Kelebihan dan Kekurangan dari Jurnal

Kelebihan dari jurnal ini yaitu di dalam jurnalnya menjelaskan secara detail alur penelitian mengenai Algoritma Kriptografi RSA. Kekurangan dari jurnal ini menurut kami yaitu kami kurang bisa memahami jurnal tersebut karena bahasanya kurang bisa kami pahami.