KELOMPOK 5 :

1. AGHA SYARILA M. (V3920002)
2. ALEXANDRO GABRIEL P.P (V3920004)
3. FEBY VALERINA A. (V3920023)
4. INEZ LAURENSYA (V3920027)
5. KHOIRUL DIANTORO (V3920031)

PRAKTIK SISTEM KEAMANAN DATA
PERTEMUAN 13

A. JURNAL 1

Judul : Implementasi Keamanan SMS Dengan Algoritma RSA Pada Smartphone Android

LATAR BELAKANG

Kebutuhan masyarakat akan adanya pengiriman informasi dari satu tempat ke tempat yang berbeda sudah tidak dapat dipungkiri lagi. Sejak zaman tradisional pengiriman informasi atau pesan sudah dilakukan dengan menggunakan surat menyurat. Pada zaman sekarang telah dipermudah dengan adanya SMS , yang mana dapat menggantikan peran surat dalam bertukar pesan. Tidak dapat dipungkiri bahwa zaman sekarang sudah banyak para pengusaha/petinggi/pejabat pemerintahan yang menggunakan SMS untuk bertukar pesan yang sifatnya sangat rahasia.

TUJUAN PENELITIAN

Penelitian ini bertujuan untuk merancang dan membuatkan sebuah aplikasi enkripsi dan dekripsi yang akan diimplementasikan untuk aplikasi SMS pada smartphone android. Aplikasi ini digunakan untuk mengirim dan menerima pesan teks pada smartphone berbasis android dengan mengamankan atau menyembunyikan pesan asli. Sehingga, pengirim tidak perlu takut pesannya akan disadap dan diketahui orang lain yang tidak berkepentingan.

ALGORITMA YANG DIPAKAI DAN ALUR PENELITIAN

1. Algoritma Yang DIgunakan

   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. Pada penelitain ini menggunakan metode RSA yaitu

menggunakan perhitungan matematika yang rumit dan disertai dengan kunci pengaman awal sehingga amat sulit untuk ditembus oleh hacker.

2. Alur Penelitian
    - Metode Riset

        Metodologi pengembangan sistem yang digunakan sebagai tahapan riset adalah Metode prototyping. Dengan metode ini pengembang dan pelanggan dapat saling berinteraksi selama proses pembuatan sistem. Sebaliknya disisi pengembang kurang memperhatikan efisiensi Algoritma.

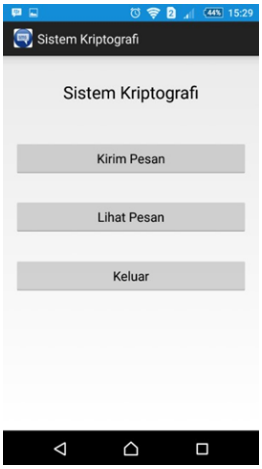
        Pada Prototyping model kadang-kadang klien hanya memberikan beberapa kebutuhan umum software atau sistem tanpa detail input, proses atau detail output dilain waktu mungkin tim pembangun tidak yakin terhadap efisiensi dari algoritma yang digunakan, tingkat adaptasi terhadap sistem operasi atau rancangan form user interface.
    - Analisis Permasalahan

        Short Message Service atau yang sering disebut SMS dewasa ini hampir semua perangkat smartphone android menggunakannya. Sehingga informasi dari fiture tersebut dapat diambil atau disadap oleh orang yang tidak berkepentingan. Khususnya dikalangan pemerintahan atau pengusaha yang memiliki rahasia akan isi dari pesan yang akan dikirim melalui SMS tersebut. Maka dari itu, diterapkan kriptografi untuk meningkatkan keamanan dalam bertukar pesan menggunakan SMS dengan metode RSA.

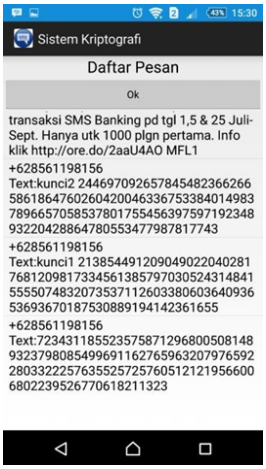
HASIL PENELITIAN

- Implementasi Sistem

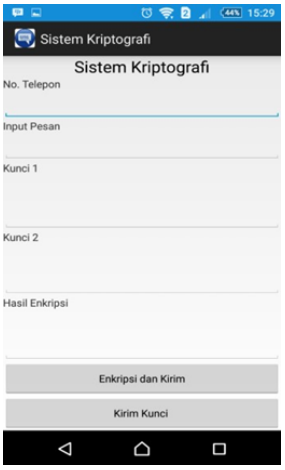
Tampilan Home



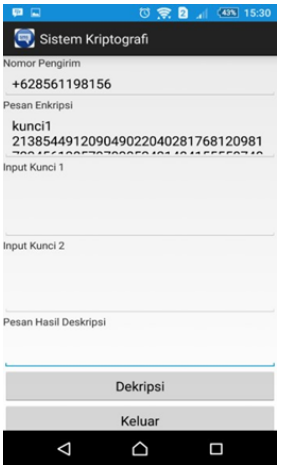
Tampilan Daftar Pesan



Tampilan Kirim Pesan (Enkripsi Pesan)



Tampilan Lihat Pesan (Dekripsi Pesan)



- Pengujian Sistem

  Dari keseluruhan proses pengujian dapat dianalisis bahwa :

  1. Aplikasi dapat terinstall dengan baik di smartphone berbasis android.
  2. Pada menu Kirim Pesan, Pesan dapat diinput, dienkripsi dan dikirim dengan baik.
  3. Pada menu Lihat Pesan, pesan dapat diterima, didekripsi dan dibaca dengan baik.
  4. Menu Keluar dapat berfungsi sebagaimana mestinya.

KESIMPULAN

Pertukaran pesan dengan menggunakan fitur SMS pada zaman modern ini memiliki kelemahan yaitu pada faktor tingkat keamanan pesan, karena pesan dapat disadap oleh orang yang tidak berkepentingan pada saat pesan tersebut dikirim. Dibutuhkannya keamanan tambahan, sehingga peneliti mengimplementasikan enkripsi dan deskripsi pada fitur SMS untuk menguatkan tingkat keamanan pesan. Dengan adanya aplikasi Sistem Kriptografi ini diharapkan dapat mengatasi masalah tersebut.

B. JURNAL 2

Judul : Implementasi Algoritma RSA Untuk Pengamanan Data Berbentuk Teks

LATAR BELAKANG

Perkembangan teknologi berdapat besar bagi perubahan cara pandang hidup manusia. Berbagai organisasi, perusahaan, atau pun pihak–pihak lain telah memanfaatkan teknologi basis data untuk menyimpan dan mengelola data organisasi atau perusahaannya. Karena itu dibutuhkan suatu cara untuk melindungi data data tersebut, salah satunya dengan kriptografi.

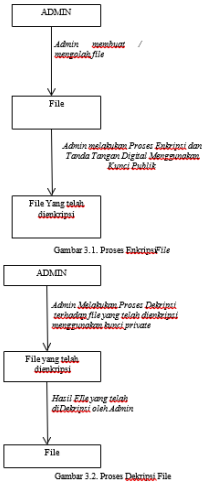
TUJUAN PENELITIAN

Tujuan penelitian untuk menerapkan keamanan file menggunakan Algoritma RSA. Aplikasi ini mempunyai dua teknik pembacaan yaitu teknik enkripsi (mengubah file asli menjadi file yang tidak dapat dibaca) dan dekripsi (mengubah file yang tidak dapat dibaca menjadi file asli). Aplikasi ini menggunakan algoritma RSA yang merupakan block cipher, dimana sebuah plaintext dan ciphertext merupakan integer antara 0 dan n-1.

ALGORITMA YANG DIPAKAI DAN ALUR PENELITIAN

1. Algoritma Yang Digunakan
   Pada penelitian ini menggunakan algoritma RSA yang digunakan pada aplikasi ini untuk mengenkripsi pesan rahasia yang berupa file agar keamanan dari pesan rahasia tadi semakin kuat. Proses dari enkripsi dilakukan sebelum file rahasia disembunyikan pada arsip ZIP
2. Alur Penelitian
   - Waktu dan Tempat Penelitian
     Waktu Penelitian ini akan dilaksanakan selama satu bulan. Tempat penelitian dan pengumpulan data tidak terikat karena didasarkan dari pengujian.
   - Metode Pengumpulan Data
     A. Studi Pustaka
        Pada metode ini, sebagai tahap awal penulis mencari data.
     B. Pengujian Lab
        Pada metode ini, penulis melakukan pembuatan aplikasi dengan menggunakan bahasa pemrogaman visual basic, setelah aplikasi berjalan selanjutnya melakukan tahap uji coba langsung terhdap data yang akan di enkripsi dan dekripsi

- Metode Perancangan Sistem



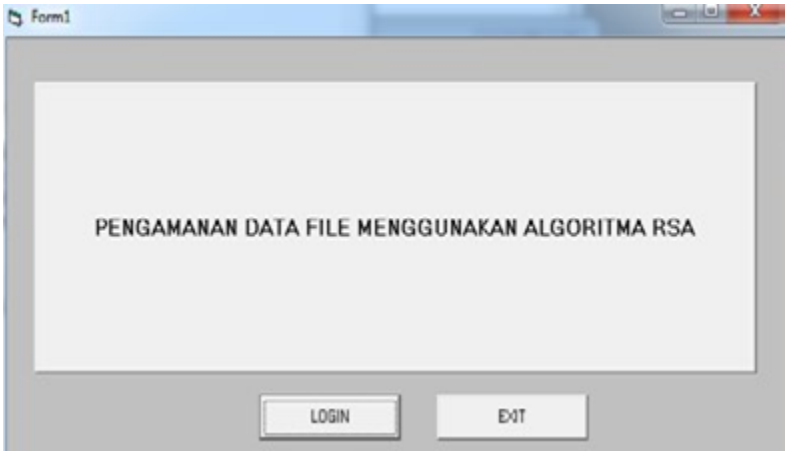
Gambar 3.1. Proses Enkripsi File

Gambar 3.2. Proses Dekripsi File

HASIL PENELITIAN

1. Menu Awal

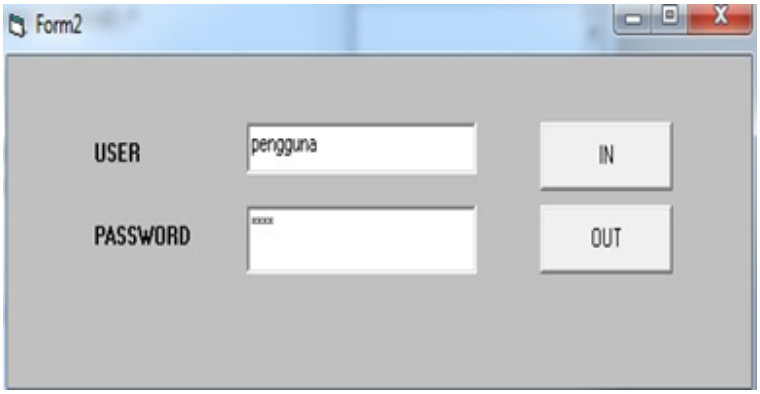
Tampilan dari Menu Awal terdiri dari Dua tombol yaitu tombol *Login* dan *Cancel*. Tombol *Login* akan menampilkan *Form Login*. Sedangkan tombol Cancel akan menyebabkan batal melanjutkna ke form selanjutnya.

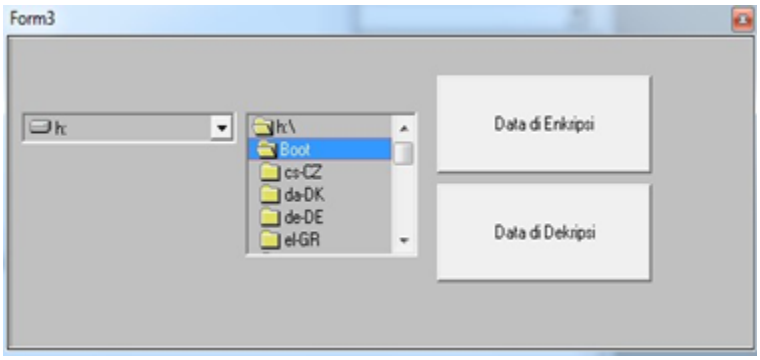


- Proses Enkripsi

Pada Form Enkripsi dan Dekripsi, terdapat tampilan Pilih Folder Data, Pilih Data Teks, Hasil dan Pilih Proses.

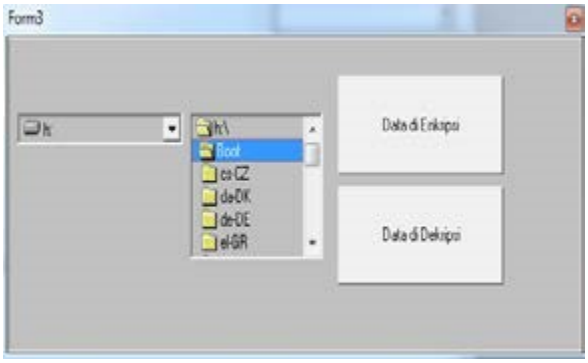
Selanjutnya akan tampil menu enkripsi dan dekripsi data atau *file*





- Proses Dekripsi

  Pada proses Dekripsi hampir Tampilan menu Dekripsi sama dengan proses Enkripsi, telah di Enkripsi dan selanjutnya menekan tombol Dekripsi.



2. Pengujian Sistem

   Pengujian yang akan dilakukan pada aplikasi ini adalah pengujian integrasi, pengujian antarmuka dan pengujian kehandalan dengan menggunakan metode *black box testing*.

   - Pengujian Form Interface

     Pengujian form interface merupakan pengujian terhadap sistem atau subsistem lengkap dengan komponen-komponen penyusunnya yang terintegrasi. Metode yang digunakan pada

pengujian ini adalah *black box*. Dengan *black box*, pengujian hanya dilakukan pada representasi sistem yang terlihat tanpa perlu mengetahui bagaimana cara kerja sistem tersebut.

KESIMPULAN

1. Aplikasi pengamanan data menggunakan algoritma RSA mempunyai dua teknik pembacaan yaitu teknik enkripsi (mengubah file asli menjadi file yang tidak dapat dibaca) dan teknik dekripsi (mengubah file yang tidak dapat dibaca menjadi file asli).
2. Aplikasi pengamanan mempunyai kalimat sandi / passphare yang harus diingat dan bersifat sensitif, maksudnya huruf besar dan kecil dibedakan,agar passphare sulit ditebak oleh siapapun.
3. Setelah melakukan uji coba, file yang telah diterapkan aplikasi pengamanan akan memiliki empat aspek keamanan, yaitu kerahasiaan, integritas data, otentikasi, dan nirpenyangkalan.

C. KELEBIHAN DAN KEKURANGAN

1) JURNAL 1 (ALEX)

Judul : Implementasi Keamanan SMS Dengan Algoritma RSA Pada Smartphone Android

- Kelebihan

  Metode yang menggunakan perhitungan matematika yang rumit dan disertai dengan kunci pengaman awal (dengan private key maupun dengan public key) sehingga amat sulit untuk ditembus oleh peretas/hacker.

- Kekurangan

  Pada faktor tingkat keamanan pesan, karena pesan dapat disadap oleh orang yang tidak berkepentingan pada saat pesan tersebut dikirim. Dibutuhkannya keamanan tambahan, sehingga peneliti mengimplementasikan enkripsi dan deskripsi pada fitur SMS untuk menguatkan tingkat keamanan pesan.

2) JURNAL 2 (AGHA)

Judul : Implementasi Algoritma RSA Untuk Pengamanan Data Berbentuk Teks

- Kelebihan

  Penulis menggunakan dasar teori dan sumber literatur yang beragam dan relevan sesuai dengan permasalahan yang diteliti dalam penelitian ini. Selain itu jurnal tersusun secara sistematis, dan bahasa yang digunakan mudah dipahami.

- Kekurangan

  Tidak adanya pemaparan maupun dokmentasi cara pengujian system menggunakan metode black bock, dalam jurnal tersebut penulis hanya menyampaikan materi.