Jurnal 1

**Penerapan Algoritma RSA Dalam Keamanan File Ms Word**

( <https://journal.fkpt.org/index.php/malda/article/view/301/197> )

1. **Latar Belakang**

Teknologi informasi telah menjadi integral dalam kehidupan sehari-hari, memicu kemajuan sistem keamanan untuk melindungi data, terutama pada file Word. Maraknya pencurian data menuntut keberadaan aplikasi keamanan dengan kriptografi untuk mengenkripsi data file Word, memperkuat keamanan dengan sistem penguncian. Berbagai metode keamanan, termasuk kriptografi, digunakan untuk mencegah kecurangan dan manipulasi data. Kriptografi modern tidak hanya berkaitan dengan penyembunyian pesan, tetapi juga dengan sejumlah teknik untuk menyediakan keamanan informasi. RSA, sebagai algoritma kunci publik, dianggap aman dan digunakan untuk mengatasi kecurangan pada data file Word dengan enkripsi dan deskripsi. Sistem keamanan diperlukan untuk menjaga kerahasiaan data dari ancaman pihak yang tidak bertanggung jawab. Pemanfaatan algoritma RSA memungkinkan pengguna mengenkripsi data asli menjadi chiperteks dengan menggunakan kunci, dan penerima dapat mendeskripsikan data menggunakan kunci yang sama, mempermudah pengiriman dan penggunaan informasi melalui keamanan algoritma RSA.

1. Tujuan Penelitian

* Menyadarkan Pentingnya Keamanan Data
* Memperkenalkan Konsep Kriptografi dan Algoritma RSA
* Mendorong Pembangunan Aplikasi Keamanan

1. Algoritma yang dipakai beserta alur penelitian

Algoritma yang dipakai adalah algoritma RSA. Untuk alur penelitiannya menggunakan metode waterfall. Perancangan pengamanan file data Word menggunakan Algoritma RSA berbasis desktop pada model air terjun memiliki tahapan sebagai berikut:

* Data Akuisisi

Metode akuisisi data meliputi pengumpulan, pengumpulan, dan persiapan data terkait desain sistem keamanan data file Word menggunakan Algoritma RSA. Referensi berasal dari jurnal, web, buku, perpustakaan, dan skripsi terkait.

* Sistem Desain

Tahap desain sistem menentukan perangkat keras (hardware) dan mendefinisikan arsitektur keseluruhan menggunakan use case. Ini membantu dalam merancang sistem secara keseluruhan.

* Sistem Implementasi

Sistem dikembangkan di unit-unit kecil yang disebut unit, yang nantinya terintegrasi dalam tahap selanjutnya. Setiap unit diuji untuk fungsionalitasnya melalui pengujian unit.

* Sistem Pengujian

Pengujian sistem dilakukan melalui Black Box Testing untuk menguji kemampuan dan keefektifannya. Kekurangan dan kelemahan sistem diidentifikasi, dan dilakukan pengkajian ulang serta perbaikan.

* Sistem Pemeliharaan

Tahap akhir dalam model air terjun ini melibatkan pengoperasian sistem yang sudah jadi dan pemeliharaan. Pemeliharaan mencakup perbaikan kesalahan yang tidak terdeteksi sebelumnya, perbaikan unit implementasi sistem, dan peningkatan sesuai kebutuhan baru.

Dengan pendekatan ini, penelitian dapat dilaksanakan secara terstruktur mulai dari akuisisi data hingga pemeliharaan sistem, memastikan pengembangan yang sistematis dan terurut.

1. Hasil penelitian

Didalam aplikasi ini terdapat beberapa halaman sebagai berikut :

1. Halaman login : Form login merupakaninterfaceprogram kriptografi, dimana untuk menggunakan aplikasi kriptografi ini dapat melaluiinterface form login
2. Halaman utama atau dashboard : Form utama merupakaninterfaceprogram kriptografi secara keseluruhan, dimana untuk menggunakan aplikasi kriptografi ini dapat melaluiinterface form utama. Dalam bentuk utama terdapat beberapa menu yaitu, menu filedan menu program
3. Halaman form data enkripsi : form enkripsi ini berfungsi untuk mengubah isi file data dalam bentuk chipretext, sehingga isi plaintext tidak dapat dikenali isi datanya dan hanya bisa dibuka dengan menggunakan kunci yang diberikan oleh pengguna terhadap sistem.
4. Halaman form deskripsi : Form data dekripsi ini berfungsi untuk mengubah isi data chipertext ke dalam bentuk plaintext, sehingga isi chipertext dapat dikenali kembali isi datanya dan dapat dibuka dengan menggunakan kunci yang diberikan oleh pengguna terhadap system
5. Halaman daftar list : Form Daftar listberfungsi untuk menampilkan data yang sudah terenkripsi
6. Kesimpulan

Kesimpulannya, penelitian ini bertujuan untuk mengamankan data file Word menggunakan Algoritma RSA berbasis desktop dengan pendekatan model air terjun. Melalui aplikasi kriptografi ini, pengguna dapat melakukan enkripsi dan deskripsi data, memastikan keamanan dan kerahasiaan informasi. Hasil penelitian meliputi halaman login, halaman utama, form enkripsi, form deskripsi, dan daftar list untuk melihat data yang sudah terenkripsi. Dengan demikian, penelitian ini memberikan kontribusi dalam pengembangan sistem keamanan data yang sistematis dan terstruktur.

Jurnal 2

**Pengimplementasian Algoritma RSA Untuk Mengamankan E-mail Menggunakan Outlook dan OpenPGP**

( <https://www.djournals.com/resolusi/article/view/589/391> )

1. Latar Belakang

Penelitian ini mengeksplorasi tantangan keamanan pada penggunaan email di era informasi dan mengusulkan solusi melalui penerapan kriptografi, terutama algoritma RSA, untuk memperkuat keamanan data. Algoritma RSA, dengan konsep bilangan prima dan aritmetika modulo, dijelaskan secara konkret untuk proses enkripsi dan dekripsi. Penggunaan Pretty Good Privacy (PGP) sebagai alternatif kriptografi juga dimaksudkan, meningkatkan keamanan email dengan kunci publik dan kunci privat.Penelitian ini tidak hanya memberikan pemahaman mendalam tentang konsep keamanan email, tetapi juga memberikan solusi konkret dengan mengimplementasikan algoritma dan metode kriptografi. Outlook digunakan sebagai contoh untuk mengilustrasikan langkah-langkah konkret dalam meningkatkan keamanan email, termasuk manajemen email, kalender, tugas, kontak, dan pencatatan. Melalui kombinasi enkripsi email menggunakan OpenPGP dan algoritma RSA, penelitian ini menyajikan solusi yang dapat diadopsi untuk menjaga keamanan pertukaran informasi elektronik. Secara keseluruhan, penelitian ini memberikan gambaran komprehensif dan solusi konkret dalam mengatasi tantangan keamanan terkait penggunaan email dalam informasi teknologi lingkungan.

1. Tujuan Penelitian

Tujuan penelitian di atas adalah untuk mengeksplorasi dan mengatasi tantangan keamanan yang terkait dengan penggunaan email sebagai alat komunikasi utama dalam era informasi. Penelitian bertujuan untuk memberikan solusi konkret dengan menerapkan metode kriptografi, terutama algoritma RSA, untuk memperkuat keamanan, kerahasiaan, dan keaslian informasi yang dikirim melalui email. Selain itu, penelitian ini bertujuan untuk memberikan pemahaman mendalam tentang konsep keamanan email dan mengilustrasikan langkah-langkah konkret dalam meningkatkan keamanan penggunaan email, termasuk manajemen email, kalender, tugas, kontak, dan pencatatan. Melalui implementasi kombinasi enkripsi email menggunakan OpenPGP dan algoritma RSA, penelitian ini bertujuan memberikan solusi yang dapat diadopsi untuk menjaga keamanan pertukaran informasi elektronik dalam lingkungan teknologi informasi.

1. Algoritma yang dipakai dan alur penelitian

Algortima yang dipakai adalaha algoritma RSA. Alur penelitian dimulai dair input,proses dan kemudian output

1. Input

* Studi Literatur:

Penelitian dimulai dengan studi literatur yang melibatkan jurnal dan penelitian terdahulu untuk memahami alur penelitian dan konsep terkait.

* Instalasi Open PGP dan Ms. Outlook:

Penginstalan dua jenis perangkat lunak, yaitu Open PGP dan Microsoft Outlook, menjadi langkah selanjutnya. Microsoft Outlook digunakan sebagai platform pertukaran pesan, sementara Open PGP merupakan alat tambahan yang terhubung dengan Outlook setelah instalasi.

1. Proses

* Membuat Akun Outlook:

Langkah ini melibatkan pembuatan akun atau login dalam Microsoft Outlook, memungkinkan pengguna untuk bertukar pesan sesuai kebutuhan.

* Konfigurasi Private Key:

Setelah login ke Outlook, langkah berikutnya adalah konfigurasi atau pembuatan private key. Private key ini digunakan untuk membuka pesan yang dikirim oleh orang lain kepada penerima.

* Menyandingkan Public Key dan Private Key:

Untuk melakukan enkripsi dan dekripsi pesan, pengirim dan penerima harus bertukar public key dan private key serta melakukan konfigurasi di akun masing-masing.

* Mengirim Pesan Enkripsi:

Setelah penyandingan antara pengirim dan penerima, langkah selanjutnya adalah mengirim pesan dengan melakukan enkripsi. Pesan awalnya berupa plaintext, dan dengan enkripsi, diubah menjadi ciphertext yang lebih aman.

1. Hasil penelitian

Penelitian ini fokus pada implementasi pengamanan pesan melalui enkripsi dan dekripsi menggunakan Outlook dan OpenPGP. Tahap awal setelah instalasi dan login pada akun email melibatkan konfigurasi privat key, yang disebut passphrase dalam OpenPGP. Proses konfigurasi ini memastikan bahwa pesan yang akan dikirimkan dan diterima dapat dienkripsi dan didekripsi dengan keamanan yang diperlukan.

Setelah konfigurasi privat key, langkah selanjutnya adalah penyandingan antara public key dan private key antara pengirim dan penerima pesan. Kedua pihak harus saling memiliki keduanya untuk memastikan bahwa proses enkripsi dan dekripsi dapat berjalan dengan lancar. Hal ini menunjukkan penerapan Algoritma RSA, di mana kedua kunci diperlukan untuk proses keamanan yang optimal.

Proses pengiriman pesan dilakukan dengan memilih opsi "New Mail," mengisi detail pesan, dan memilih fitur "encrypt." Proses ini memungkinkan pengguna untuk memasukkan private key mereka sebelum mengirimkan pesan. Hasilnya, pesan dikirimkan dalam format terenkripsi, memastikan keamanan dalam proses pertukaran informasi.

Saat penerima menerima pesan, mereka dapat melakukan pengecekan email untuk melihat isi pesan yang telah dienkripsi. Tampilan email yang dienkripsi menunjukkan pesan dalam bentuk file terlampir. Penerima perlu melakukan dekripsi dengan memilih opsi "decrypt," memasukkan privat key mereka, dan kemudian memilih "open" atau "save." Ini akan menghasilkan tampilan pesan yang telah menjadi plaintext.

1. Kesimpulan

Secara keseluruhan, penelitian ini memberikan pandangan praktis tentang langkah-langkah implementasi pengamanan pesan melalui enkripsi dan dekripsi menggunakan Outlook dan OpenPGP. Dengan penekanan pada konfigurasi kunci dan proses pertukaran antara pengirim dan penerima, penelitian ini memberikan solusi konkret untuk memastikan keamanan dalam pertukaran informasi melalui email.