ANALISIS KEAMANAN JARINGAN KOMPUTER DENGAN IMPLEMENTASI ENKRIPSI DAN DESKRIPSI

Audi Muhammad Jardillah, Sastya Hendri Wibowo 1, Yulia Darmi 2, Walad Mahfuzhi,
Teknik Informatika, Teknik, Universitas Muhammadiyah Bengkulu
Jl. Bali, Kp. Bali, Kec. Tlk. Segara, Kota Bengkulu, Bengkulu 38119, Indonesia
Email: audijbr@gmail.com

ABSTRAK

Kriptografi adalah menyembunyikan dan menulis. Menulis dengan menyembunyikan informasi adalah inti dari kriptografi. Dengan menggunakan kriprografi, suatu informasi seperti data dan pesan dapat terjadi aman dan kerahasiaanya. Dengan adanya kemajuan tentang ilmu yang menjelaskan bagaimana tahap-tahap keamanan suatu sistem data merupakan suatu sisi positif serta mampu menyediakan suatu aplikasi keamanan data yang tujuannya untuk melindungi data yang di *transfer* atau dikirimkan lewat jaringan telekomunikasi. Nama RSA sendiri diambil dari inisial ketiga peneliti tersebut. Algoritma ini berdasarkan konsep bilangan prima dan aritmatika modulo dalam proses enkripsi dan dekripsi, dengan kedua kunci, baik kunci enkripsi maupun kunci dekripsi, merupakan bilangan bulat. Bagaimana mengimplementasikan enkripsi dengan algoritma RSA (*Rivest-Shamir-Adleman*) yang efisien dan efektif. Untuk mengetahui cara kerja dari kriptografi dengan algoritma RSA (*Rivest-Shamir-Adleman*). Diharapkan pengembangan aplikasi keamanan jaringan komputer dengan enkripsi dapat dimodifikasi menjadi berbasis android dengan file *end-to-end*.

Kata Kunci : Aplikasi, Kriptografi, Pesan, RSA.

I. PENDAHULUAN

Kriptografi merupakan salah satu teknik keamanan yang sering digunakan pada komputer saat ini. Kata “kryptós” yang berarti menyembunyikan, dan “graphein” yang berarti menulis, digabungkan menjadi kata kriptografi. Kriptografi adalah penulisan dengan menyembunyikan informasi. Informasi seperti data dan pesan dapat dijaga kerahasiaannya dan aman dengan penggunaan kriptografi. Enkripsi adalah salah satu komponen kunci dalam kriptografi yang diperlukan untuk melindungi suatu pesan. Enkripsi pesan dapat menghentikan pihak yang tidak berkepentingan membaca komunikasi rahasia. Jika setiap orang memiliki akses ke komunikasi rahasia, maka hal ini menimbulkan kerentanan yang dapat dimanfaatkan oleh beberapa pihak, termasuk penyerang. Banyak penelitian telah dilakukan untuk menggunakan metode kriptografi untuk mengamankan pesan. (Fajrin, dkk. 2023)

Aplikasi yang dapat melindungi data dari ancaman atau kebocoran keamanan sangat banyak diminati sebagai dampak dari perkembangan dalam melindungi informasi atau data sensitif dan memfasilitasi aliran informasi penting. Salah satu manfaat yang dapat diperoleh dari penerapan keamanan data adalah kemajuan ilmu pengetahuan yang memperjelas pendekatan keamanan sistem data. Tujuannya adalah untuk menjaga informasi yang dipindahkan atau dikirim melalui jaringan telekomunikasi.(Dairi,dkk. 2023)

Salah satu metode untuk mengubah pesan tidak terenkripsi (plaintext) menjadi pesan terenkripsi (ciphertext) adalah kriptografi. Enkripsi adalah proses melakukan modifikasi tersebut, sedangkan dekripsi adalah proses mengembalikan ciphertext menjadi plaintext. Kunci kriptografi digunakan dalam proses enkripsi dan dekripsi.Teknik ini melibatkan pengacakan huruf pada kata terang atau *plaintext* menggunakan penggantian huruf atau substitusi dan pengacakan posisi huruf atau transposisi ifat pembagian yang terdapat pada bilangan bulat menghasilkan konsep seperti bilangan prima dan konsep aritmetika modulo. Aritmetika modulo berfokus pada peran penting dalam komputasi bilangan bulat khususnya dalam pengaplikasiannya pada kriptografi.(Zachary, dkk. 2023)

Algoritma RSA pertama kali diperkenalkan pada tahun 1976 oleh Ron Rivest, Adi Shamir, dan Len Adleman, tiga peneliti Institut Teknologi Massachusetts. Inisial ketiga peneliti tersebut menjadi sumber moniker RSA. Proses

enkripsi dan dekripsi teknik ini mengandalkan prinsip bilangan prima dan aritmatika modulo, dengan bilangan bulat berfungsi sebagai kunci enkripsi dan dekripsi. Kunci dekripsi perlu dirahasiakan, sedangkan kunci enkripsi dapat dipublikasikan. Kunci enkripsi dan beberapa bilangan prima digabungkan untuk membentuk kunci dekripsi. Seseorang harus memfaktorkan suatu bilangan non-prima sampai faktor prima penyusunnya ditemukan untuk mendapatkan kunci enkripsi. Sebenarnya merupakan tugas yang menantang untuk memfaktorkan bilangan non-prima ke dalam faktor primanya. Saat ini tidak ada algoritma efektif yang tersedia untuk melakukan faktorisasi ini.(Zachary, dkk. 2023)

TINJAUAN PUSTAKA

A. Kriptografi

Seni dan ilmu mengamankan pesan dikenal sebagai kriptografi. Selain itu, ilmu kriptografi digambarkan sebagai studi tentang metode matematika yang berkaitan dengan integritas data, kerahasiaan, dan otentikasi, di antara aspek keamanan informasi lainnya. Menurut definisinya, "seni" adalah metode khusus untuk menyembunyikan pesan. Sementara itu, istilah “grafi” dalam “kriptografi” sudah mengisyaratkan suatu media artistik tersendiri.

B. Algoritma RSA (Rivest-Shamir-Adleman)

Kunci publik dan kunci privat adalah dua kunci yang digunakan oleh RSA. Teknik kriptografi kunci publik diimplementasikan melalui algoritma RSA. Modulus yang dianggap sangat besar inilah yang memberikan keamanan pada proses enkripsi dan dekripsi algoritma RSA. Metode RSA mengenkripsi pesan dengan cara berikut: Alice memberikan kunci publiknya kepada Bob, n & e, sambil menjaga rahasia kunci privatnya. Bob kemudian mengirimkan pesan M kepada Alice. Bob membagi pesan M menjadi beberapa bagian (m < n) dan menghitung c sebagai *ciphertext* sambil mengenkripsinya. Bob memberikan Alice hasil perhitungan *enkripsi* setelah menerimanya dari C.

C. PHP

PHP adalah bahasa komputer populer yang dapat digunakan bersama dengan HTML untuk merancang dan membuat situs web. Akronim PHP adalah singkatan dari "PHP: *Hypertext Preprocessor*," dan merupakan bahasa pemrograman sisi *server* yang dimasukkan ke dalam teks HTML. Dengan kata lain, skrip disembunyikan dari *klien*, yang dapat dengan mudah mengakses database, dengan memiliki sintaks dan perintah di *server* tetapi disertakan dalam halaman HTML standar.

D. SQL

Yahya (2015) menyatakan bahwa SQL merupakan *Relational Database Management System* (RDBMS) yang tersedia secara bebas untuk digunakan di bawah ketentuan *General Public License* (GPL) (Biasta, 2011). Siapa pun dapat menggunakan MySQL. Sebenarnya MySQL adalah variasi dari SQL (*Structured Query Language*), ide dasar dibalik database yang sudah ada sejak lama. Pengoptimal sistem manajemen basis data (DBMS) dapat digunakan untuk menentukan seberapa tangguh suatu sistem ketika menangani permintaan SQL dari pengguna atau aplikasi.

II. METODOLOGI PENELITIAN

A. Tempat dan Waktu Penelitian

Penelitian dilaksanakan secara mandiri, waktu penelitian dilaksanakan pada tanggal 15 Mei s/d 15 Juni 2024

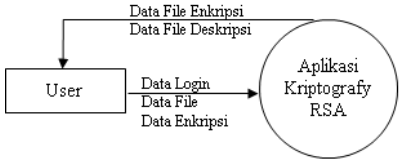
B. Teknik Pengumpulan Data

Metode pengumpulan data merupakan metode yang digunakan dalam penelitian pengumpulan data, meliputi observasi dan kajian pustaka.

C. Desain

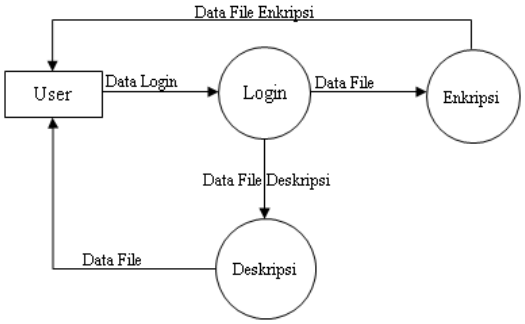
Adapun desain yang digunakan dalam penelitian ini terdapat 3 desain perancangan sistem, yaitu :

1. Diagram Konteks



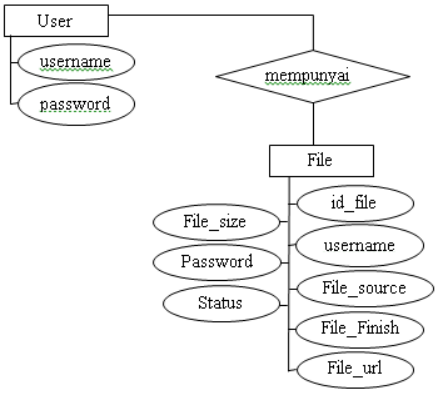
Gambar 3.1 Diagram Konteks

2. Data Flow Diagram Level 0



Gambar 3.2 Data Flow Diagram Level 0

3. ERD



Gambar 3.3 ERD

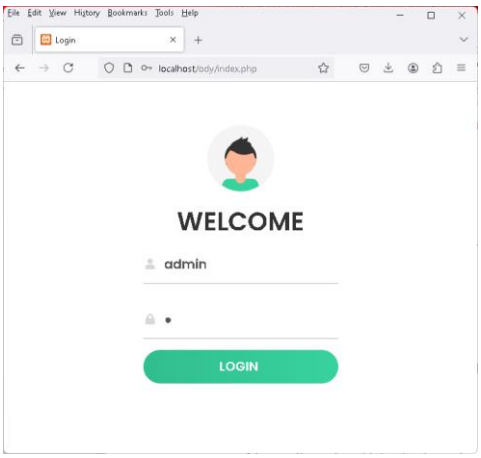
III. HASIL DAN PEMBAHASAN

A. Implementasi Perancangan Sistem

Adapun hasil analisis keamanan jaringan komputer dengan enkripsi ini dapat membangun system pengamanan file dengan menggunakan algoritma RSA dalam melakukan enkripsi dan dekripsi

1. Tampilan Menu Login

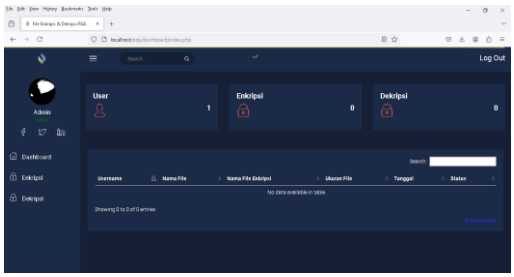
   Pada tampilan menu login merupakan system keamanan standar dalam aplikasi, dengan kondisi *username* dan *password* benar akan tampil pada halaman dashboard.



Gambar 4.1 Tampilan Menu Login

2. Tampilan Menu Utama

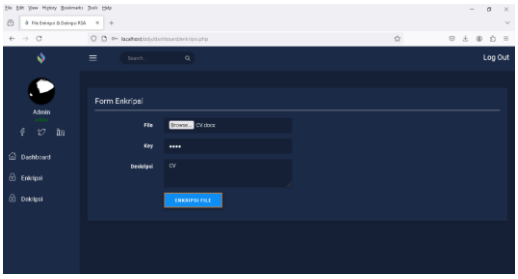
   Pada menu dashboard terdiri 4 menu, dimana 1 menu memiliki submenu yaitu enkripsi dan deskripsi.



Gambar 4.2 Tampilan Menu Utama

3. Tampilan Menu Enkripsi

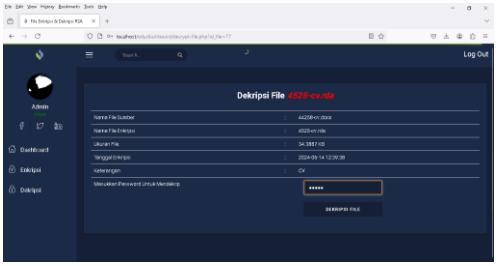
   Pada menu enkripsi terdapat *form input* yang terdiri dari tanggal, browse file, password, dan deskripsi



Gambar 4.3 Tampilan Menu Enkripsi

4. Tampilan Menu Deskripsi

   Pada menu deskripsi terdapat informasi yang terdiri dari nama file sumber, ukuran file, dan tanggal enkripsi. Namun terdapat perbedaan pada deskripsi, harus memasukkan *password* untuk melakukan deskripsi file.



Gambar 4.4 Tampilan Menu Deskripsi

B. Testing

Skenario	Hasil Yang Diharapkan	Hasil Pengujian
Tampilan Menu Login	Pada tampilan menu login merupakan system keamanan standar dalam aplikasi, dengan kondisi *username* dan *password* benar akan muncul pada dashboard	Sesuai yang diharapkan
Tampilan Menu Dashboard	Pada menu dashboard terdiri 4 menu, dimana 1 menu memiliki submenu yaitu enkripsi dan deskripsi	Sesuai yang diharapkan
Tampilan Menu Enkripsi	Pada menu enkripsi terdapat *form input* yang terdiri dari tanggal, browse file, password, dan deskripsi	Sesuai yang diharapkan
Tampilan Menu Deskripsi	Pada menu deskripsi terdapat informasi yang terdiri dari nama file sumber, ukuran file, dan tanggal enkripsi. Namun terdapat perbedaan pada deskripsi, harus memasukkan *password* untuk melakukan deskripsi file	Sesuai yang diharapkan

IV. KESIMPULAN

Berdasarkan pembahasan analisis keamanan jaringan komputer dengan enkripsi, maka dapat diambil kesimpulan sebagai berikut :

1. Dapat mengembangkan kriptografy dengan metode RSA yang lebih efektif
2. Dapat mengamankan file dengan menggunakan enkripsi dan dekripsi algoritma RSA.
3. Dapat membangun system pengamanan file dengan menggunakan algoritma RSA dalam melakukan enkripsi dan dekripsi

V. SARAN

Pada penelitian yang telah dilakukan, tentu terdapat banyak kekurangan dan kelebihan. Oleh sebab itu, ada beberapa hal yang harus diperhatikan untuk ditinjau kembali dalam pengembangan sistem ke depan antara lain sebagai berikut :

1. Diharapkan pengembangan aplikasi ini dapat menjadi referensi bukan hanya dunia kriptografi dengan metode RSA melainkan juga untuk semua pelajaran sebagai perkembangan informasi teknologi.
2. Diharapkan pengembangan aplikasi keamanan jaringan komputer dengan enkripsi dapat dimodifikasi menjadi berbasis android dengan file *end-to-end*.
3. Diharapkan metode RSA dilakukan perbandingan yang spesifik dengan metode enkripsi lainnya.

DAFTAR PUSTAKA

[1] Azhari, M., Mulyana, D.I., Perwitosari, F.J. dan Ali, F., Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES), *Jurnal Pendidikan Sains dan Komputer*, vol. 2, no. 01, hal. 163–171, 2022.

[2] Fathurrahmad, F. dan Ester, E., Development and Implementation of The Rijndael Algorithm and Base-64 Advanced Encryption Standard (AES) for Website Data Security, *International Journal of Computer Applications*, vol. 9, no. 11, hal. 9–12, 2020.

[3] Vivi Wahdini, S., Hartama, D., Okta Kirana, I., Poningsih dan Sumarno, Pengamanan Data Pelanggan dan Penjualan Menggunakan Implementasi Algoritma Kriptografi, *Journal of Informatics Management and Information Technology*, vol. 1, no. 3, hal. 101–107, 2021.

[4] Panjaitan, A.W., Zufria, I. dan Nasution, Y.R., Implementation of Data Encryption Standard (DES) Algorithm for Data Security on PDF Documents, vol. 6, no. 2, hal. 231–236, 2022.

[5] Priatama, A.D. dan painem, Pengamanan Data Anggota Polri Dengan Aes-128 Dan Base64 Pada Puslitbang Polri Bogor Security of Polri Member Data File S Using Aes-128 and Base64 Method , Puslitbang Polri Bogor ., *SENAFTI*, vol. 2, no. September, hal. 55–62, 2023.

[6] Sahid, M., Hambatan Komunikasi pada Proses Pembelajaran Menggunakan Media Whatsapp Group, *JISIP (Jurnal Ilmu Sosial dan Pendidikan)*, vol. 5, no. 1, hal. 299–308, 2021.

[7] HASANAH, M.F., Efektivitas Penggunaan Whatsapp Group (Wag) Pada Pembelajaran Jarak Jauh (Pjj) Di Masa Pandemi Covid-19, *EDUTECH : Jurnal Inovasi Pendidikan Berbantuan Teknologi*, vol. 1, no. 2, hal. 82–87, 2021.

[8] Rahman, A., Ningsih, A.K. dan Ilyas, R., PENGGUNAAN QR CODE BERBASIS KRIPTOGRAFI ALGORITMA ADVANCED ENCRYPTION STANDARD DAN SHA-512 UNTUK APLIKASI PENCATATAN BIAYA PENDIDIKAN BERBASIS WEB DI SMK PUSDIKHUBAD, *SCIENTICA*, vol. 2, hal. 205–217, 2024.

[9] Wachid Hidayatulloh, N., Tahir, M., Amalia, H., Afdlolul Basyar, N., Faizal Prianggara, A. dan Yasin, M., Mengenal Advance Encrytion Standard (AES) Sebagai Algoritma Kriptografi Dalam Mengamankan Data, *Digital Transformation Technology (Digitech)*, vol. Vol.03, no. No.1, hal. 1–10, 2023.

[10] Rahmawati, A. dan Rahman, A., Sistem Pengamanan Keaslian Ijasah Menggunakan QR-Code dan Algoritma, *Seminar*, vol. 1, no. 2, hal. 105–112, 2011