Journal of Machine Learning and Data Analytics (MALDA)
Volume 01, No. 02, Agustus 2022 Page: 95-100
ISSN 2828-3465 (media online)

Penerapan Algoritma RSA Dalam Keamanan File Ms Word

Ulfah Indriani[1], Ommi Alfina[2], Nita Syahputri[3]

[1]Teknik Dan Ilmu Komputer, Sistem Informasi S1, Universitas Potensi Utama, Medan, Indonesia
[2]Teknik Dan Ilmu Komputer, Informatika, Universitas Potensi Utama, Medan, Indonesia
[3]Teknik Dan Ilmu Komputer, Sistem Informasi D3, Universitas Potensi Utama, Medan, Indonesia
[1]ulfahindriani90@gmail.com, [2]ny.aroen@gmail.com, [3]nieta20d@gmail.com

Abstrak−Perkembangan sistem keamanan sangat cepat dan pesat, hal ini yang menyebabkan munculnya kemajuan teknologi informasi. Secara langsung atau tidak, teknologi informasi telah menjadi bagian penting dari berbagai bidang kehidupan. Teknologi juga memberikan kemudahan untuk bertukar informasi sehingga keamanan data tidak dapat lepas dari berbagai aspek kegiatan manusia yang memungkinkan dapat menjaga kerahasiaan informasi tersebut, namun dalam implementasinya masih terdapat kecurangan dan ancaman terhadap data khususnya pada data file word (isi file).Oleh karena itu dibutuhkan suatu sistem keamanan yang mampu menjaga kerahasiaan data dari ancaman lain yang dilakukan oleh pihak yang tidak bertanggung jawab. Dengan memanfaatkan algoritma RSA ini sistem akan mengenkripsi data asli yang diinputkan pengguna menjadi chipertkes dengan menggunakan key, kemudian mengirimkan kepada orang lain ataupun rekannya.

Kata Kunci: RSA, File Word, Web

Abstract− The development of security systems is very fast and rapid, this has led to the emergence of advances in information technology. Directly or indirectly, information technology has become an important part of various fields of life. Technology also makes it easy to exchange information so that data security cannot be separated from various aspects of human activities that allow it to maintain the confidentiality of the information, but in its implementation there are still frauds and threats to data, especially in word file data (file contents). a security system that is able to maintain the confidentiality of data from other threats carried out by irresponsible parties. By utilizing the RSA algorithm, the system will encrypt the original data entered by the user into a health certificate using a key, then send it to someone else.

Keywords: RSA, File Word, Web

1. PENDAHULUAN

Perkembangan sistem keamanan sangat cepat dan pesat, hal ini yang menyebabkan munculnya kemajuan teknologi informasi. Secara langsung atau tidak, teknologi informasi telah menjadi bagian penting dari berbagai bidang kehidupan. [1] Teknologi juga memberikan kemudahan untuk bertukar informasi sehingga keamanan data tidak dapat lepas dari berbagai aspek kegiatan manusia yang memungkinkan dapat menjaga kerahasiaan informasi tersebut, namun dalam implementasinya masih terdapat kecurangan dan ancaman terhadap data khususnya pada data file word.[2] Akibat dari maraknya pencurian data, maka diperlukan aplikasi keamanan data file Word (isi file) yang memberikan kerahasiaan data lebih terjaga dan kurangnya keamanan kerahasiaan data file Word (isi file) maka diperlukan sebuah aplikasi kriptografi.[3] untuk melakukan enkripsi pada data file Word (isi file) yang penyembunyiannya dapat diperkuat dengan sistem penguncian.[4]

Terdapat banyak metode pengamanan data yang bisa dimanfaatkan untuk mencegah adanya kecurangan ataupun manipulasi data salah satunya menggunakan kriptografi atau teknik penyamaran lainnya.[5] Kriptografi adalah ilmu yang berdasarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas.[6] Jadi pengertian kriptografi modern adalah tidak saja berurusan hanya dengan penyembunyian pesan namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi.[7]

RSA (Rivest Shamir Adleman) merupakan salah satu algoritma public key yang populer dipakai dan bahkan hingga saat ini Algoritma RSA masih dianggap aman adalah perluasan dari caesar cipher, yang menggalikan plainteks dengan sebuah nilai dan menambahkannya dengan sebuah pergeseran.[8]

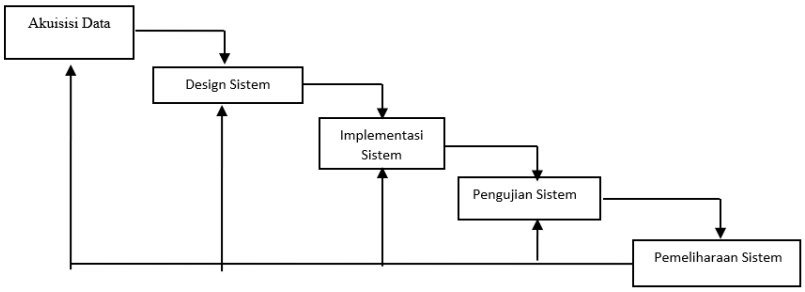
Kecurangan data file word (isi file) tersebut dapat diatasi dengan memanfaatkan metode RSA secara enkrip dan deskrip.[9] Oleh karena itu dibutuhkan suatu sistem keamanan yang mampu menjaga kerahasiaan data dari ancaman lain yang dilakukan oleh pihak yang tidak bertanggung jawab. Dengan memanfaatkan algoritma RSA ini sistem akan mengenkripsi data asli yang diinputkan pengguna menjadi chipertkes dengan menggunakan key, kemudian mengirimkan kepada orang lain ataupun rekannya.[10] Untuk penerimaan data asli dideskripsi menjadi plainteks menggunakan key juga oleh penerima sehingga pengiriman informasi atau pemanfaatan informasi melalui keamanan algoritma RSA menjadi lebih muda dipahami oleh penerima ataupun pengguna file word tersebut.[11]

2. METODOLOGI PENELITIAN

Journal of Machine Learning and Data Analytics (MALDA)
Volume 01, No. 02, Agustus 2022 Page: 95-100
ISSN 2828-3465 (media online)

2.1 Tahapan Penelitian

Dalam pengembangan suatu sistem ini peneliti menggunakan model *waterfall* kerena pengaplikasian menggunakan model ini mudah diimplementasikan dimana hal ini menggambarkan pendekatan yang sistematis dan juga berurutan pada pengembangan perangkat lunak.[12] Tahapan metode *waterfall* dapat dilihat pada gambar 1. di bawah ini.



Gambar 1. Model Waterfall

Penjelasan gambar 1 Perancangan pengamanan data file word menggunakan Algoritma *RSA* berbasis desktop pada model *waterfall:*

a. Akusisi Data
   Akuisisi data merupakan metode yang dilakukan penulis dengan mengambil, mengumpulkan dan menyiapkan data yang berisi tentang Perancangan pengamanan data file word menggunakan Algoritma *RSA* berbasis web. Pada penelitian ini penulis memilih referensi dari jurnal, web, buku, perpustakaan dan skripsi yang berkaitan dengan penelitian ini.
b. Design Sistem
   Pada tahapan ini, design sistem membantu dalam menentukan perangkat keras *(hardware)* dan mendefinisikan arsitektur sistem secara keseluruhan dengan menggunakan *use case* pada sistem yang akan dibangun.
c. Implementasi Sistem
   Pada tahap ini, sistem pertama kali dikembangkan di program kecil yang disebut *unit*, yang terintegrasi dalam tahap selanjutnya. Setiap *unit* dikembangkan dan diuji untuk fungsionalitas yang disebut sebagai *unit testing*.
d. Pengujian Sistem
   Dalam tahapan ini, sistem yang dirancang diuji kemampuan dan keefektifan nya dalam suatu *BlackBox Testing*. Sehingga didapatkan kekurangan dan kelemahan sistem yang kemudian dilakukan pengkajian ulang dan perbaikan terhadap aplikasi.
e. Pemeliharaan Sistem
   Tahap akhir dalam model *waterfall* ini perangkat lunak yang sudah jadi, dijalankan serta dilakukan pemeliharaan. Pemeliharaan termasuk dalam memperbaiki kesalahan yang tidak ditemukan pada langkah sebelumnya. Perbaikan implementasi *unit* sistem dan peningkatan jasa sistem sebagai kebutuhan baru.

2.2 Metode Algoritma RSA (Rivest Shamir Adleman)

RSA merupakan salah satu dari Public Key Cryptosystem yang sangat sering digunakan untuk memberikan kerahasiaan terhadap keaslian suatu data digital. Keamanan enkripsi dan dekripsi data model ini terletak pada kesulitan untuk memfaktorkan modulus n yang sangat besar.[13] Dalam kriptografi, RSA adalah algoritma untuk enkripsi kunci publik. Algoritma ini adalah algoritma pertama yang diketahui paling cocok untuk menandai (signing) dan untuk enkripsi dan salah satu penemuan besar pertama dalam kriptografi kunci publik.[14] RSA masih digunakan secara luas dalam protokol-protokol perdagangan elektronik dan dipercayai sangat aman karena diberikan kunci-kunci yang cukup panjang dan penerapan-penerapannya yang sangat mutakhir. [15]

Algoritma pembentukan kunci :

1. Tentukan p dan q bernilai dua bilangan prima besar, acak dan dirahasiakan, $p \neq q$, p dan q memiliki ukuran yang sama.
2. Hitung $n = p \times q$, dan hitung $\phi(n) = (p - 1) \times (q - 1)$, bilangan integer n disebut (RSA) modulus. Tentukan e bilangan prima acak yang memiliki syarat : $1 < e < 1(n)$, GCD(e, i(n)) = 1, disebut e relatif prima terhadap i(n), bilangan integer n disebut (RSA) enciphering component, sehingga menghasilkan Dd (Ee(m)) = Ee(Dd(c)) ≡ md mod n. (Indra Gunawan, 2018;125).[16]

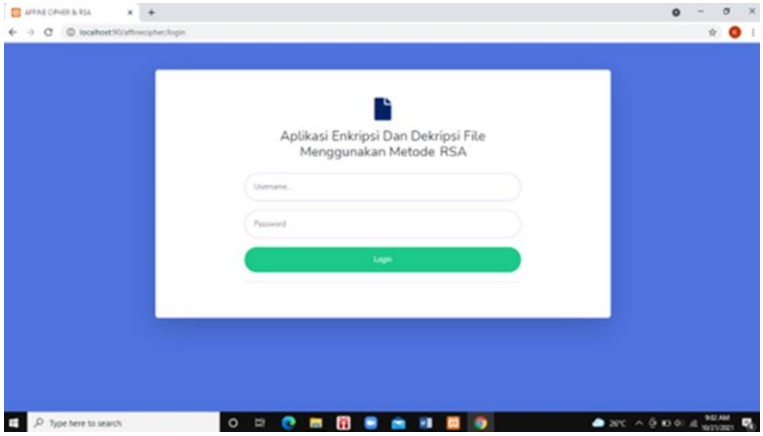
Journal of Machine Learning and Data Analytics (MALDA)
Volume 01, No. 02, Agustus 2022 Page: 95-100
ISSN 2828-3465 (media online)

3. HASIL DAN PEMBAHASAN

Aplikasi Penerapan Algoritma RSA dalam Keamanan File MS Word dalam mengamankan sebuah data *file*.

3.1.2. Tampilan *Form* Login

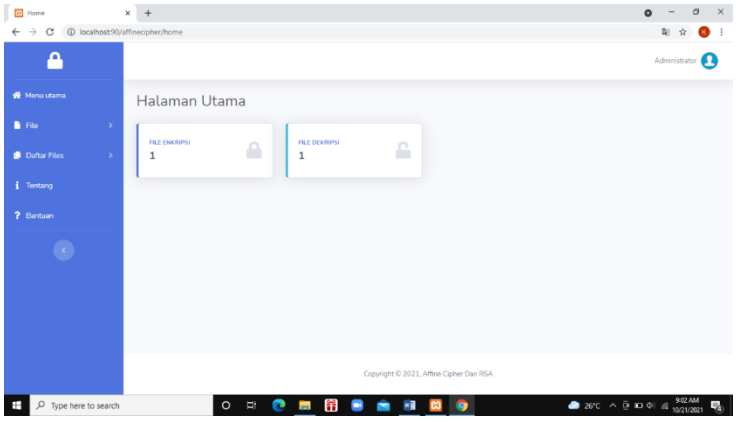
Form login merupakan *interface* program kriptografi, dimana untuk menggunakan aplikasi kriptografi ini dapat melalui *interface form* login. dapat dilihat dibawah ini.



Gambar.2. Tampilan *Form* Login

3.1.3. Tampilan *Form* Utama

Form utama merupakan *interface* program kriptografi secara keseluruhan, dimana untuk menggunakan aplikasi kriptografi ini dapat melalui *interface form* utama. Dalam *form* utama terdapat beberapa menu yaitu, menu *file* dan menu program. Untuk lebih jelasnya tampilan *form* utama dapat dilihat dibawah ini.

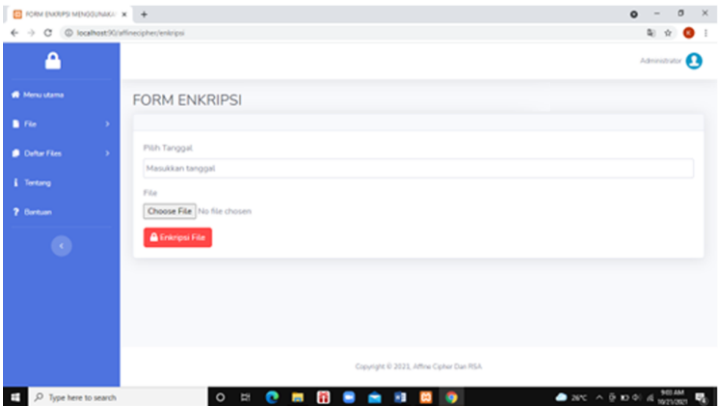


Gambar 3. Tampilan *Form* Utama

3.1.4. Tampilan *Form* Data Enkripsi

Form enkripsi ini berfungsi untuk merubah isi data *file* dalam bentuk *chipretext*, sehingga isi *plaintext* tidak dapat dikenali isi datanya dan hanya bisa dibuka dengan menggunakan kunci yang diberikan oleh *user* terhadap sistem. Ada beberapa hal yang bisa dilakukan didalam *form* data enkripsi seperti memasukkan data *file doc*, menyimpan hasil enkripsi (*chipertext*), dan keluar dari *form* data enkripsi. Berikut ini tampilan *form* data enkripsi dapat dilihat pada gambar berikut ini:

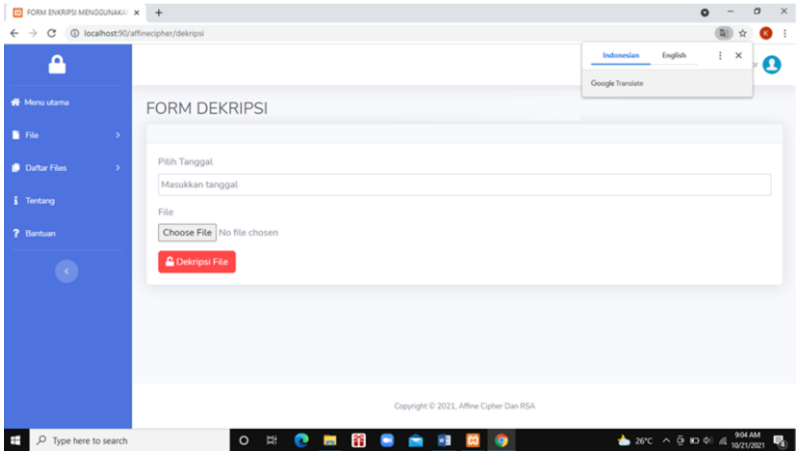
Journal of Machine Learning and Data Analytics (MALDA)
Volume 01, No. 02, Agustus 2022 Page: 95-100
ISSN 2828-3465 (media online)



Gambar 4. Tampilan *Form* Data Enkripsi

3.1.4. Tampilan *Form* Dekripsi

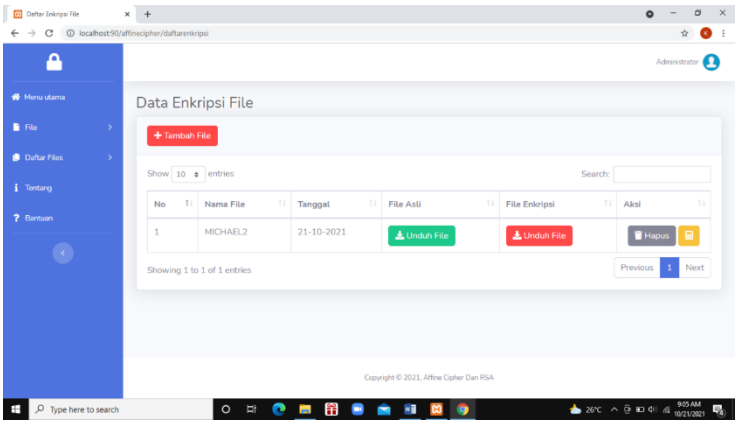
Form data dekripsi ini berfungsi untuk merubah isi data *chipertext* dalam bentuk *plaintext*, sehingga isi *chipertext* dapat dikenali kembali isi datanya dan bisa dibuka dengan menggunakan kunci yang diberikan oleh *user* terhadap sistem. Ada beberapa hal yang bisa dilakukan didalam *form* data dekripsi, seperti memasukkan atau membuka data teks (*chipertext*), menyimpan hasil dekripsi (*plaintext*), dan keluardari *form* dekripsi.



Gambar 5. Tampilan *Form* Dekripsi

3.1.5. Tampilan *Form* Daftar List

Form Daftar list berfungsi untuk menampilkan data yang sudah terenkripsi pesan asli menjadi plainteks, dapat dilihat sebagai berikut ini:



Gambar 6. Tampilan *Form* Daftar List

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan selama sistem pendukung keputusan pemilihan *berbasis web* untuk pengamanan file (isi file) dengan menggunakan algoritma affine cipher dan rsa dapat ditarik kesimpulan sebagai berikut:

1. Algoritma rsa dapat membantu meningkatkan data, menggunakan perhitungan menggunakan memfaktoran bilangan prima dapat meningkatkan sistem keamanan data, sehingga data yang tersimpan akan semakin terjaga
2. Dalam proses pembuatan aplikasi berbasis web yang baru dapat diketahui bahwa untuk pengamanan file (isi file) yang baik, tahap-tahap yang perlu dilakukan adalah dengan mempelajari sistem yang ada, kemudian mendesain sistem dan melakukan perhitungan dengan kriteria-kriteria pemilihan.
3. Dengan adanya sistem ini maka akan sangat membantu untuk pengamanan file (isi file) dalam pengamanan suatu file.

REFERENCES

[1] D. I. G. H. Wirhan Fahrozi, Samsir, "Penerapan E-Commerce Pada Toko Bunga Underwear," *J. Tek. Inform.*, vol. 04, no. 01, pp. 1–6, 2020.

[2] Samsir, "Klasifikasi Penyakit Tenggorokan Hidung Telinga (THT) Menggunakan Jaringan Syaraf Tiruan Dengan Metode Learning Vektor Quantization (THT) Di RSUD Rantauprapat Labuhanbatu Klasifikasi penyakit Tenggorokan Hidung Telinga (THT) Menggunakan," vol. 05, no. 01, pp. 38–47, 2019.

[3] M. Siddik and S. Samsir, "Rancang Bangun Sistem Informasi Pos (Point of Sale) Untuk Kasir Menggunakan Konsep Bahasa Pemrograman Orientasi Objek," *JOISIE (Journal Inf. Syst. Informatics Eng.*, vol. 4, no. 1, p. 43, 2020, doi: 10.35145/joisie.v4i1.607.

[4] Samsir and Syaiful Zuhri Harahap, "Application Design Resume Medical By Using Microsoft Visual Basic. Net 2010 At the Health Center Appointments," *Int. J. Sci. Technol. Manag.*, vol. 1, no. 1, pp. 14–20, 2020, doi: 10.46729/ijstm.v1i1.5.

[5] B. Siswa and S. Dasar, "Pengembangan media pembelajaran multimedia interaktif dalam peningkatan kemampuan melaksanakan shalat bagi siswa sekolah dasar," vol. 13, no. 1, pp. 39–47, 2021.

[6] A. H. Dalimunthe, R. Aditiya, and R. Watrianthos, "Implementation Naïve Bayes Classification for Sentiment Analysis on Internet Movie Database," vol. 4, no. 1, pp. 4–9, 2022, doi: 10.47065/bits.v4i1.1468.

[7] U. Verawardina, F. Edi, and R. Watrianthos, "Analisis Sentimen Pembelajaran Daring Pada Twitter di Masa Pandemi COVID-19 Menggunakan Metode Naïve Bayes," vol. 5, pp. 157–163, 2021, doi: 10.30865/mib.v5i1.2604.

[8] Firman Edi, A. Ambiyar, U. Verawardina, S. Samsir, and R. Watrianthos, "Improving Lesson Plan Models Using Online-Based in the New Normal Era," *EDUTEC J. Educ. Technol.*, vol. 4, no. 3, pp. 527–535, 2021, doi: 10.29062/edu.v4i3.109.

[9] J. H. P. Sitorus *et al.*, "Perancangan pengontrol lampu rumah miniatur dengan menggunakan micro controler arduino berbasis android 1," vol. 4, no. 1, pp. 1–11, 2020.

[10] A. Syahputra, D. I. G. Hts, and Samsir, "Perancangan Aplikasi Media Pembelajaran Jarimatika Penjumlahan Dan Pengurangan Berbasis Multimedia," *U-NET J. Tek. Inform.*, vol. 3, no. 1, pp. 35–42, 2019, doi: 10.52332/u-net.v3i1.20.

[11] S. P. Sitorus and S. Samsir, "Perancangan Aplikasi Game Tetris Batu Bara," *U-NET J. Tek. Inform.*, vol. 3, no. 2, pp. 35–41, 2019, doi: 10.52332/u-net.v3i2.290.

[12] E. S. Budi, E. Hariska, and G. L. Ginting, "Implementation of the Simple Additive Weighting Method in Determining Recipients of Subsidized Food Materials for Poor Families," vol. 3, no. 3, pp. 384–392, 2021, doi: 10.47065/bits.v3i3.1097.

[13] "OVERVIEW OF EDUCATION ON THE PHILOSOPHY OF PANCASILA AND OVERVIEW OF EDUCATION ON THE PHILOSOPHY OF PANCASILA AND INDONESIAN EDUCATION SYSTEM," no. September, 2020.

[14] S. Samsir, J. H. P. Sitorus, Z. Ritonga, and F. Aini, "Comparison of machine learning algorithms for chest X-ray image COVID-19 classification Comparison of machine learning algorithms for chest X-ray image COVID-19 classification," doi: 10.1088/1742-6596/1933/1/012040.

[15] S. M. Oriented, "Edge Detection to Make Drawing Sketch using Laplacian Operator and Gabor Wavelet for

Learning Devices (GJH ’ HWHFWLRQ WR 0DNH ’ UDZLQJ 6NHWFK XVLQJ / DSODFLDQ 2SHUDWRU DQG * DERU : DYHOHW IRU / HDUQLQJ ’ HYLFHV,” doi: 10.1088/1742-6596/1764/1/012070.

[16] O. Access, “The optimalization of backpropagation neural networks to simplify decision making The optimalization of backpropagation neural networks to simplify decision making,” 2020, doi: 10.1088/1757-899X/830/2/022091.