PENGAMANAN DATA PASIEN MENGGUNAKAN METODE RC-4 BERBASIS WEB PADA RSIA PKU MUHAMMADIYAH CIPONDOH

Fefi Casio[1*], Dewi Kusumaningsih[2]

[1,2] Fakultas Teknologi Informasi, Teknik Informatika, Universitas Budi Luhur, Jakarta, Indonesia

Email: [1]*eficasio011@gmail.com, [2]dewi.kusumaningsih@budiluhur.ac.id
(* : corresponding author)

Abstrak- Pada RSIA PKU Muhammadiyah Cipondoh banyak melakukan kegiatan penyimpanan dan pengolahan data pasien. Data tersebut berisi informasi pasien yang disimpan pada komputer. Pada hal ini terdapat peluang bagi pihak yang tidak bertanggung jawab misalnya dari pihak lain mengakses atau mengubah informasi data tanpa diketahui. Tentunya hal ini sangat merugikan bagi pihak RSIA PKU Muhammadiyah Cipondoh. Untuk membuat dokumen tersebut lebih aman maka akan dibuat sebuah aplikasi keamanan data dengan metode kriptografi**.** Kriptografi RC4 (*Rivest Code 4*) merupakan algoritma kriptografi modern yang termasuk ke dalam Algoritma Simetris yang menggunakan kunci yang sama saat proses enkripsi (proses penyandian pesan) dan proses dekripsi (proses pengembalian pesan asli). Algoritma RC4 termasuk *Stream Cipher* (*Cipher* aliran). yang mengenkripsi antara kombinasi plainteks dengan menggunakan bit-wise Xor (*Exclusive-or*). Data yang akan digunakan dalam penelitian ini adalah data rawat jalan yang dimana berkasnya berupa *File* (dokumen) yang akan tersimpan di rumah sakit. Aplikasi ini dibuat dengan menggunakan bahasa pemrograman yaitu PHP. Dengan aplikasi kriptografi ini, data akan lebih aman dan tidak dapat diakses oleh pihak yang tidak bertanggung jawab. Pada aplikasi ini, data yang terenkripsi berupa data dokumen yang hanya pihak yang bertanggung jawab pada RSIA PKU Muhammadiyah Cipondoh yang dapat menggunakan aplikasi ini. Berdasarkan implementasi dan pengujian enkripsi pada dokumen dengan ukuran 830 mb dan dengan kecepatan 8,712 detik.

Kata Kunci: Kriptografi, Enkripsi, Dekripsi, RC4

SECURITY OF PATIENT DATA USING WEB-BASED RC-4 METHOD AT RSIA PKU MUHAMMADIYAH CIPONDOH

Abstract- *At RSIA PKU Muhammadiyah Cipondoh, many activities are carried out in storing and processing patient data. The data contains patient information stored on the computer. In this case, there are opportunities for irresponsible parties, for example from other parties to access or change data information without being known. Of course this is very detrimental to the RSIA PKU Muhammadiyah Cipondoh. To make the document more secure, a data security application using the cryptographic method will be created. Cryptography RC4 (Rivest Code 4) is a modern cryptographic algorithm that belongs to the Symmetric Algorithm that uses the same key during the encryption process (message encoding process) and decryption process (returning the original message). The RC4 algorithm includes a Stream Cipher. which encrypts plaintext combinations using bit-wise Xor (Exclusive-or). The data that will be used in this study is outpatient data where the file is a file (document) that will be stored in the hospital. This application is made using the programming language, namely PHP. With this cryptographic application, data will be more secure and cannot be accessed by irresponsible parties. In this application, the encrypted data is in the form of document data that only the party responsible for the RSIA PKU Muhammadiyah Cipondoh can use this application. Based on the implementation and testing of encryption on documents with a size of 830 mb and a speed of 8.712 seconds.*

Keywords*: Cryptography, Encryption, Decryption, RC4*

1. PENDAHULUAN

Dokumen adalah media informasi yang sangat penting dalam suatu perusahaan,badan usaha maupun bentuk organisasi yang lain, baik itu untuk berkomunikasi dengan pihak di luar organisasi (eksternal) dan pihak di dalam organisasi (Internal). Semua hal yang berhubungan dengan kegiatan organisasi yang bersifat resmi selalu diterapkan dalam bentuk dokumen [1]. Contohnya dokumen rawat jalan.

RSIA PKU Muhammadiyah Cipondoh banyak melakukan kegiatan penyimpanan dan pengolahan data pasien. Pada proses ini pasien mempunyai data yang masing – masing berbeda, *admin* bertugas untuk mengelola dan menyimpan data tersebut agar tidak disalahgunakan. Data tersebut berisi informasi pasien yang akan disimpan kedalam komputer. Tentu saja hal ini merupakan kesempatan peluang bagi pihak yang tidak berhak misalnya dari pihak lain mengakses atau mengubah informasi data tanpa diketahui. Tentunya hal ini sangat merugikan bagi pihak RSIA PKU Muhammadiyah Cipondoh.

Keamanan ini akan lebih berfokus kepada keamanan informasi menggunakan teknik kriptografi RC 4 (*Rivest Code 4*) untuk pengamanan dokumen di RSIA PKU Muhammadiyah Cipondoh. Tujuan menggunakan kriptografi RC 4 (*Rivest Code 4*) meningkatkan keamanan data RSIA PKU Muhammadiyah Cipondoh dengan menggunakan metode kriptografi.

Algoritma RC4 **(*Rivest Code 4*)** merupakan kriptografi *modern* yang disebut Algoritma Simetris yang merupakan algoritma kriptografi yang memakai kunci sama saat proses enkripsi data(proses penyandian pesan) dan proses dekripsi (proses pengembalian pesan asli).

2. METODE PENELITIAN

2.1 Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu *kryptos* dan *graphein*. *Kryptos* itu tersembunyi / rahasia, *graphein* ialah menulis. Makna kriptografi ialah menulis secara rahasia untuk menyampaikan pesan yang dijaga kerahasiaannya [2].

Saat ini kriptografi banyak diketahui secara luas, sebab dapat digunakan suatu alat untuk menjaga kerahasiaan data. Sejarah kriptografi disebut klasik, yaitu metode enkripsi yang menggunakan alat seperti kertas dan pensil atau bantuan alat mekanik yang lainnya. Secara umum algoritma kriptografi klasik dibagi menjadi dua kategori, yaitu :

a. Algoritma *Cipher* Transposisi
b. Algoritma *Cipher* Substitusi

Kedua kategori algoritma kriptografi ini karena dari sejarah kriptografi klasik mencatat bahwa penggunaan algoritma *cipher* transposisi oleh tentara Sparta di Yunani pada awal tahun 400 SM saat menggunakan sebuah alat yang disebut *scytale*.

Gambar 1. *Scytale* [3]

Tujuan Kriptografi

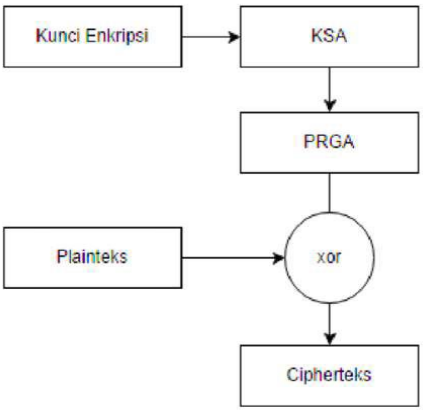
a. Kerahasiaan (*Confidentiality*) adalah menjaga agar pesan tidak dapat dibaca oleh pihak yang tidak bertanggung jawab.
b. Integritas data (*Data Integrity*) adalah menjamin data atau pesan yang dikirimkan masih asli atau sama dengan yang dikirim oleh pengirim pesan dengan yang diterima oleh penerima pesan.
c. Otentikasi (*Authentication*) adalah suatu kemampuan penerima pesan yang akan dikirim merupakan benar yang diinginkan, karena seorang penyamar untuk menjadi pengirim dan mengirimkan pesan yang salah.
d. Ketiadaan penyangkalan (*Non-Repudiation*) adalah dimana pengirim pesan tidak bisa menyangkal dan mengelak bahwa dia telah mengirim pesan [4].

2.2 RC4 (Rivest Code 4)

Algoritma RC4 disebut *Stream Cipher*. yang mengenkripsi antara plainteks dengan ciphertext. RC4 mempunyai panjang kunci mulai dari 1 - 256 *byte.* yang digunakan untuk menginisialisasikan tabel sepanjang 256 *byte*. Tabel ini digunakan untuk generasi dari *pseudo random* yang menggunakan metode XOR dengan *plaintext* untuk menghasilkan *ciphertext* [5].

2.2.1 Algoritma Enkripsi RC4

RC4 mempunyai sebuah S-Box, dari S0 - S255, yang berisi permutasi dari bilangan 0 sampai 255, Dalam algoritma enkripsi metode ini akan membangkitkan *pseudo random byte* dari *key* yang akan dikenakan operasi XOR terhadap *plaintext* untuk menghasilkan *ciphertext*, Algoritma enkripsi dapat dilihat pada Gambar 2.

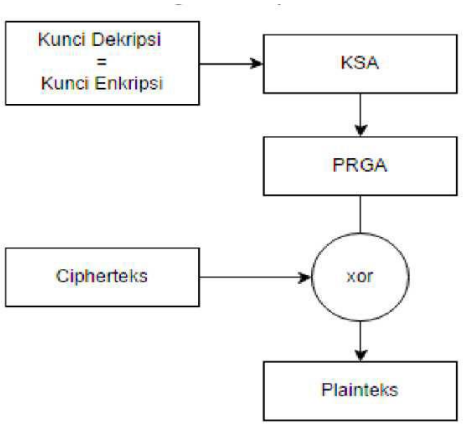


Gambar 2. Arsitektur Enkripsi RC4

2.2.2 Algoritma Dekripsi RC4

Algoritma dekripsi RC4 serupa dengan penjelasan algoritma enkripsi, perbedaannya hanya pada saat *stream generation*, yaitu untuk menghasilkan plainteks menjadi semula, maka *ciphertext* nya akan dikenakan operasi XOR terhadap *pseudo random* bytenya [6].

Algoritma *key* setup pada proses dekripsi serupa dengan algoritma enkripsinya yang akan diproses dengan inisialisasi S-Box, Untuk itu proses dekripsi dan enkripsi akan menghasilkan *key stream* yang sama. Perbedaannya hanya pada *stream generation*, yaitu yang akan dioperasikan dengan *key stream* adalah *ciphertext* untuk menghasilkan kembali *plaintext* [7], Algoritma dekripsi dapat dilihat pada Gambar 3.



Gambar 3. Arsitektur Dekripsi RC4 [7]

3. HASIL DAN PEMBAHASAN

Pada bagian akan berisi analisa, hasil dari penelitian, Bagian ini menjelaskan berupa , gambar, table, flowchart dan lainnya.

3.1 Analisa Penerapan Algoritma

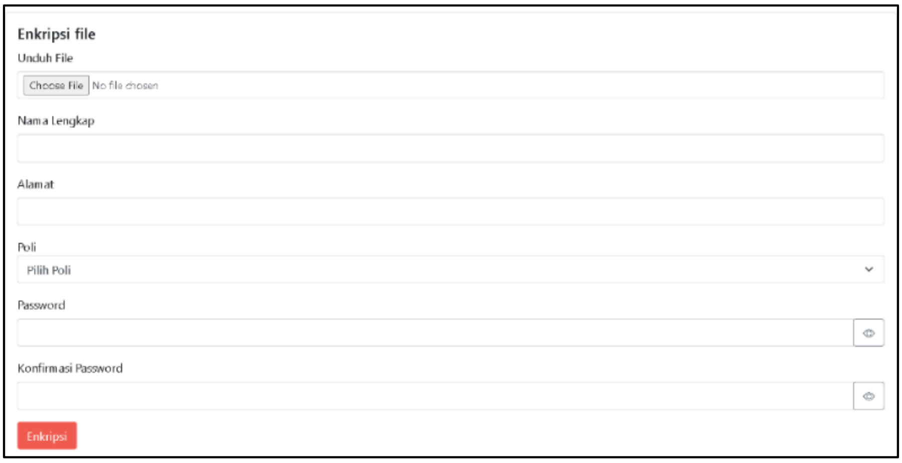
Setelah tahap pengumpulanan data, maka dapat menganalisa penerapan algoritma. Analisa penerapan algoritma menjelaskan tahapan untuk menerapkan yaitu metode kriptografi *Rivest Code 4*. Pada tahapan ini dilakukan:

a. Menentukan kunci (*key*) yang digunakan untuk proses enkripsi dan dekripsi *File* dokumen.
b. Proses enkripsi *File* dokumen menggunakan kunci yang akan enkripsi, yaitu proses menginput data *File* yang akan dienkripsi menjadi *ciphertext*.
c. Proses dekripsi menggunakan kunci dekripsi *ciphertext* yang sama dengan kunci enkripsi sebelumnya, yaitu suatu proses untuk mengubah data *file ciphertext* menjadi data *File* yang dapat dibaca kembali (*plaintext*).

3.2 Menu Enkripsi

a. Tampilan Form Enkripsi

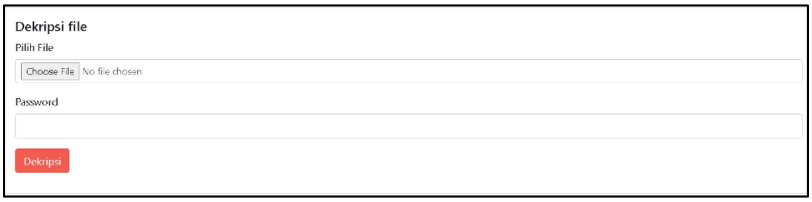
Bagian atas halaman, terdapat *input* data pasien yang digunakan untuk mengenkripsi data tersebut. Menu tampilan form enkripsi dapat dilihat pada Gambar 4.



Gambar 4. Tampilan Form Enkripsi

b. Tampilan Form Dekripsi

Di atas halaman, terdapat tombol yang digunakan untuk mendekripsi data pasien tersebut. Menu tampilan form dekripsidapat dilihat pada Gambar 5.



Gambar 5. Tampilan Form Dekripsi

3.3 Pengujian Dan Analisis

Pengujian ini dilakukan untuk menguji aplikasi apakah berhasil melakukan proses enkripsi-dekripsi menggunakan metode *Rivest Code* 4 (RC4). Dengan dilakukannya uji coba, Semoga aplikasi yang dibuat berjalan dengan baik juga dapat digunakan. Tabel data hasil uji coba enkripsi-dekripsi *Rivest Code* 4 (RC4) bisa dilihat pada tabel 1 dan tabel 2.

Tabel 1. Hasil Pengujian Enkripsi

Isi File	Ukuran	*Ciphertext*	Waktu
Data Rawat Jalan Wildan Hafizul	830 Kb	žG#MeÝ‡œ¼.'43	8.711 *second*
Data Rawat Jalan Aang Koenaefi	215 Kb	‰AÓ™X¦$êÄ¶<&üì	4.564 *second*
Data Rawat Jalan Dedy Setiawan	173 Kb	뎉 墺□騒秣ἣἰ鑽蠏 렁 鍾央ʒ	3.152 *second*

Tabel 2. Hasil Pengujian Dekripsi

Plaintext	*Ciphertext*	Ukuran	Waktu
Enkrip_Wildan_Hafizul.pdf	žG#MeÝ‡œ¼.'43	830 Kb	8.711 *second*
Enkrip_Aang_Koenaefi.pdf	.‰AÓ™X¦$êÄ¶<	215 Kb	4.564 *second*
Enkrip_Dedy_Setiawan.jgp	뎉墂□騹秼η̈ῐ鑹蠏렁鍾	173 Kb	3.152 *second*

3.4 Hasil Pengujian *Black Box*

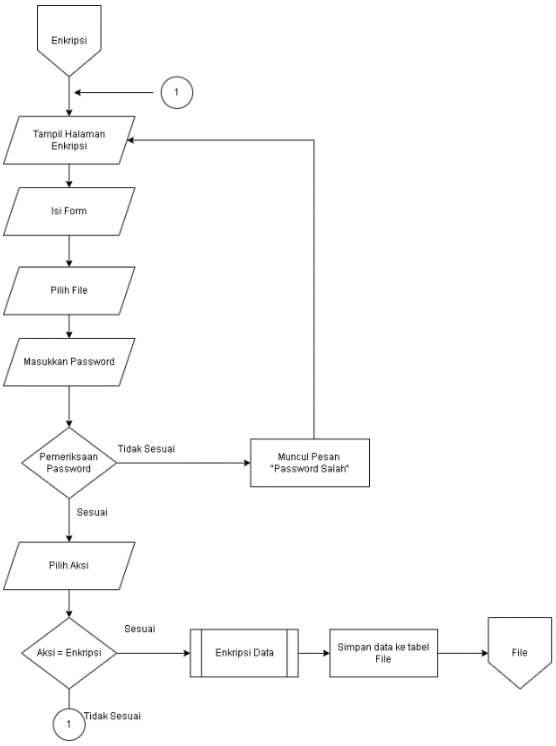
Pengujian *Black Box* merupakan cara untuk menguji sebuah *software* dengan melakukan test fungsionalitas dari aplikasi tanpa memeriksa rangkaian atau proses dalamannya. Studi kasus dibuat sesuai dengan spesifikasi dan ketentuan yang ada. Tabel 3 Menunjukkan hasil dari pengujian *Black Box*.

Tabel 3. Tabel *Black Box*

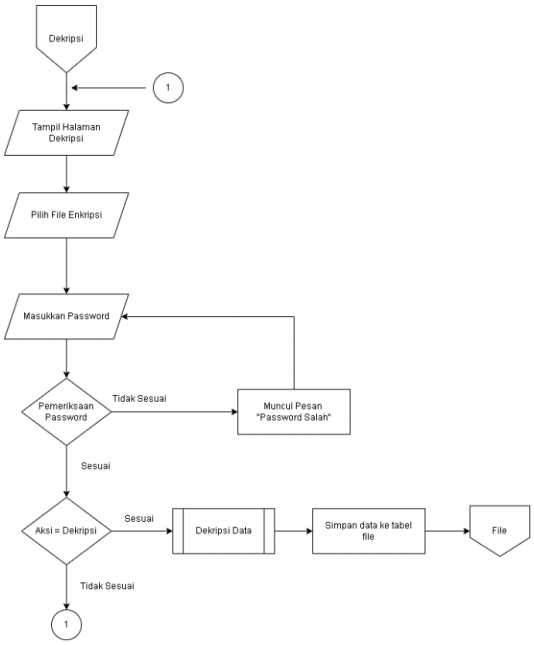
Skenario Pengujian	***Test Case***	**Hasil Pengujian**	**Kesimpulan**
Nama pengguna atau kata sandi salah	Nama pengguna atau kata sandi salah ketika melakukan *login*	Tampil Notifikasi "Username atau Password salah!"	*Valid*
Kata sandi kurang dari 8 atau kosong saat mengenkripsi file	Admin memasukkan kata sandi kurang dari 8 saat mengenkripsi	Tampil Notifikasi "Password kosong atau kurang dari 8"	*Valid*
Kata sandi kurang dari 8 atau kosong saat mendekripsi file	Admin memasukkan kata sandi kurang dari 8 saat mendekripsi file	Tampil Notifikasi "Password kurang dari 8 atau password kosong"	*Valid*
Tidak ada file yang diunggah	Admin tidak mengunggah file ketika mengenkripsi dan mendekripsi	Tampil Notifikasi "Tidak ada file yang diupload!"	*Valid*
File yang diunggah bukan file .txt, .docx, .xls, .pdf atau .pptx saat ingin mengenkripsi file	Admin mengunggah file format selain .txt, docx, .xls, .pdf dan .pptx	Tampil Notifikasi "format file tidak didukung"	*Valid*
File yang diunggah bukan dari hasil enkripsi saat akan mendekripsi file	Admin mengunggah file bernama selain "Enkrip_namafile"	Tampil Notifikasi "File yang dimasukan bukan hasil enkripsi"	*Valid*

3.5 *Flowchart*

Flowchart digunakan untuk menggambarkan alur dari sebuah program yang dibuat. Setiap alur tersebut dijelaskan kedalam model diagram yang dihubungkan dengan menggunakan garis. *Flowchart* Enkripsi bisa dilihat pada Gambar 6 dan *flowchart* Dekripsi dapat dilihat pada Gambar 7.



Gambar 6. *Flowchart* Enkripsi



Gambar 7. *Flowchart* Dekripsi

4. KESIMPULAN

Setelah melewati tahap-tahap rancangan dan pengujian aplikasi enkripsi dan dekripsi dokumen dengan menggunakan algoritme RC4, Terdapat beberapa kesimpulan yang didapat. Dan juga dalam menjalankan aplikasi ini dapat membantu dengan memberi saran dari masalah yang ada sebagai berikut :

a. Algoritme RC4 dapat berfungsi untuk melakukan enkripsi dan dekripsi data dokumen dengan memakai kunci yang sama atau sesuai.
b. Pengamanan data dokumen menggunakan algoritme RC4 dapat berfungsi untuk mengamankan sesuatu yang bersifat rahasia dari data dokumen tersebut.
c. Hasil dari Enkripsi data lebih panjang dari data aslinya .

Berdasarkan kesimpulan yang ditarik dari hasil studi yang telah dilakukan, penulis menawarkan beberapa saran sebagai literatur tambahan atau untuk dipertimbangkan dalam pengembangan sistem yang lebih relevan, yaitu:

a. Dikembangkan menggunakan algoritme yang lebih baik dari sebelumnya sehingga kualitas dalam proses enkripsi dan dekripsi data dokumen menjadi lebih aman, lebih cepat dan lebih efisien.
b. Diharapkan dapat dibuat menjadi lebih baik lagi, sehingga dapat melakukan enkripsi semua jenis dokumen.

DAFTAR PUSTAKA

[1] D. R. Saragi, J. M. Gultom, J. A. Tampubolon and I. Gunawan, “Pengamanan Data File Teks (Word) Menggunakan Algoritma RC4,” *JSON: Jurnal Sistem Komputer dan Informatika*, vol. 1, no. 2, pp. 114-119, 2020.

[2] F. Yusuf and Akbar, “Teori Bilangan Dalam Ilmu Kriptografi,” Makalah IF2120 Matematika Diskrit ITB Bandung, Sem. 1 pp.1-5, 2020.

[3] K. A. Seputra and G. A. Jude Saskara, “Kriptografi Simetris Rc4 Pada Transaksi,” *Jurnal Pendidikan Teknologi dan Kejuruan*, vol. 17, no.2, pp. 286-295, 2020.

[4] D. Irwansyah, “Pengamanan Data Teks Dengan Algoritme Modifikasi RC4,” *Jurnal Pelita Informatika*, vol.6, no.3, pp. 309-312, 2018.

[5] G. G. Putri, W. Styorini and R. D. Rahayani, “Analisis Kriptografi Simetris AES Dan Kriptografi Asimetris RSA Pada Enkripsi Citra Digital,” *ETHOS: Jurnal Penelitian dan Pengabdian Masyarakat*, vol 6, no. 2, pp. 197-207, 2018.

[6] “Mengenal Kriptografi : Definisi, Tujuan dan Jenis-jenisnya,” 26 April 2022. [Online]. Available: https://lp2m.uma.ac.id/2022/04/26/mengenal-kriptografi-definisi-tujuan-dan-jenis-jenisnya/.

[7] R. Munir, “Kriptofrafi,” in Edisi Kedua, Bandung, Institut Teknologi Bandung, 2019.

[8] 2019 Komputerkata. [Online]. Available: https://komputerkata.com/algoritma-rc4-contoh-perhitungan-lengkap/.

[9] D. Seftian and Mufti, “Aplikasi Keamanan Google Mail Berbasis Web Menggunakan Algoritma,” *SKANIKA*, vol. 1, no. 3, pp. 1039-1044, 2018.

[10] H. Kusniyati, S. Diansyah and R. Yusuf, “Penerapan Algoritma Rivert Code 4 (Rc 4) Pada Aplikasi Kriptografi Dokumen,” *PETIR*, vol. 11, no.1, pp. 38-47, 2018.