APLIKASI PENGAMANAN DOKUMEN MENGGUNAKAN METODE *RIVEST CODE* 4 *(*RC4) BERBASIS WEB PADA YAYASAN BERKEMBANG MANDIRI INDONESIA

Muhammad Farhansyah[1*], Utomo Budiyanto[2]

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

Email: [1*]mfarhansyah1412@gmail.com, [2]utomo.budiyanto@budiluhur.ac.id
(* : corresponding author)

Abstrak- Perkembangan bidang teknologi di era ini memberikan pengaruh yang cukup besar pada bagian keamanan dari suatu data dan informasi yang memiliki sifat penting dan rahasia. Keamanan data dalam penyimpanan merupakan suatu hal yang perlu diperhatikan pada saat ini. Tetapi kemudahan dalam memperoleh akses pada informasi oleh semua orang mempengaruhi keamanan suatu data informasi. Memungkinkan data menjadi rentan untuk dicuri, diubah dan dimanipulasi pihak-pihak tidak berhak atas akses data informasi tersebut. Yayasan Berkembang Mandiri Indonesia memiliki banyak dokumen penting seperti dokumen keuangan. Karena itu, dibuatlah sebuah aplikasi keamanan data yang mampu menjaga dan memberikan keamanan pada data tersebut. Pada perancangan aplikasi pengamanan data dokumen ini, penulis menggunakan sistem dengan suatu metode enkripsi dan dekripsi. Pada perancangan aplikasi, penulis menggunakan salah satu algoritme kriptografi yaitu *Rivest Code* 4 (RC4), Kriptografi RC4 adalah sebuah algoritme kriptografi yang bisa berfungsi untuk melakukan enkripsi pada data yang akhirnya data asli tersebut hanya bisa dibaca oleh seseorang yang mengetahui kunci enkripsi tersebut. Aplikasi pengamanan dokumen dibuat menggunakan bahasa pemrograman PHP. Dengan aplikasi pengamanan dokumen ini, data menjadi lebih aman dan tidak dapat diakses oleh pihak yang tidak berhak atas akses data informasi tersebut. Pada aplikasi ini, data yang terenkripsi berupa data dokumen yang hanya pihak yang bertanggung jawab pada Yayasan Berkembang Mandiri Indonesia yang memiliki akses pada aplikasi. Menurut implementasi dan uji coba program yang telah dilakukan, disimpulkan maka aplikasi ini mampu mengamankan dan merahasiakan data dokumen.

Kata Kunci: kriptografi, enkripsi, dekripsi, RC4

DOCUMENT SECURITY WEB-BASED APPLICATION USING THE RIVEST CODE 4 (RC4) METHOD AT YAYASAN BERKEMBANG MANDIRI INDONESIA

Abstract- Technological advances in today's global era have a great influence on the security of important and confidential data and information. Data security in storage is very important in modern times. However, the ease of accessing communication media by everyone, has an impact on data information security. Data becomes particularly vulnerable to being stolen, tampered with and manipulated by irresponsible parties. Yayasan Berkembang Mandiri Indonesia has many important documents such as financial documents. Therefore, a data security application was created that can maintain and secure the data. In designing a document data security application, the author created a system with a method of encryption and decryption process. The author will use a cryptographic algorithm, namely *Rivest Code* 4 (RC4), RC 4 cryptography is one of the algorithms that can be used to encrypt data so that the original data can only be read by someone who has the Encryption key. This application was created using the PHP programming language. With this cryptographic application, the 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, only the party responsible for the Yayasan Berkembang Mandiri Indonesia can use this application. Based on the implementation and testing of the program, it can be concluded that this application is able to maintain and protect the confidentiality of document data.

Keywords*: cryptography, encryption, decryption, RC4*

1. PENDAHULUAN

Dokumen merupakan hal yang tertulis atau tercetak yang mengandung informasi khususnya dalam suatu perusahaan, badan usaha atau bentuk instansi lainnya, yang digunakan untuk bertukar informasi dengan pihak di luar maupun di dalam organisasi. Segala hal yang berkaitan dengan kepentingan instansi selalu tercatat dalam bentuk dokumen. Contoh dokumen penting yang perlu diamankan seperti dokumen keuangan.

Yayasan Berkembang Mandiri Indonesia memiki dokumen penting seperti dokumen keuangan dan sebagainya yang terdapat di dalam ataupun di luar yayasan. Menurut dari pihak Yayasan Berkembang Mandiri Indonesia

beberapa kali terjadi dokumen hilang atau mudah terakses oleh beberapa pihak yang tidak diinginkan menyebabkan kerahasiaan dokumen tersebut diketahui karena banyaknya dokumen dan pengelolaannya yang kurang baik. Masalah yang dihadapi untuk keamanan suatu dokumen merupakan aspek penting. Maka dari itu perlunya dibuat sebuah pengamanan yang baik sehingga dokumen tersebut menjadi aman dan terjaga kerahasiaannya.

Keamanan informasi memiliki beberapa macam teknik untuk pengamanannya antara lain seperti Kriptografi, Steganografi, *Secure Socket Layer*, dan masih banyak yang lainnya. Pada masalah ini akan lebih berfokus kepada keamanan informasi menggunakan teknik kriptografi untuk pengamanan dokumen di Yayasan Berkembang Mandiri Indonesia.

Algoritme RC 4 **(*Rivest Code 4*)** adalah sebuah algoritme pada kriptografi *modern* yang termasuk dalam Algoritme Simetris. Algoritme Simetris merupakan algoritme dalam kriptografi yang menggunakan kunci sama sebagai syarat untuk proses enkripsi (proses pengubahan pesan) dan proses dekripsi (pengembalian menjadi pesan asli).

Keamanan ini akan berfokus kepada keamanan dokumen menggunakan teknik kriptografi RC 4 (*Rivest Code 4*) untuk pengamanan dokumen di Yayasan Berkembang Mandiri Indonesia yang bertujuan meningkatkan keamanan data dokumen.

2. METODE PENELITIAN

2.1 Kriptografi

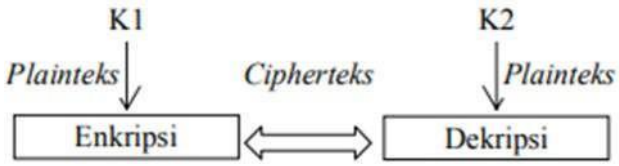
Kriptografi adalah sebuah ilmu yang menggunakan persamaan yang bersifat matematis untuk pengerjaan proses Enkripsi (*Encrypt*) dan dekripsi (*Decrypt*) data. Metode tersebut dipakai untuk mengubah data menjadi kode simbol tertentu sehingga data informasi yang terkirim membuat data informasi tidak mampu dibaca oleh pihak yang tidak berhak atas akses data informasi tersebut [1].

Beberapa tujuan dari Kriptografi adalah sebagai berikut [2]:

a. Kerahasiaan (*Confidentiality*) merupakan sebuah sifat yang bertujuan untuk membatasi hak atas data informasi tersebut.
b. Integritas data (*Data Integrity*) merupakan kemampuan seorang penerima suatu informasi untuk memvalidasi pesan tersebut, untuk memastikan jika informasi tersbut tidak dimanipulasi dalam pengiriman.
c. Penyangkalan (*Non-Repudiation*) merupakan kondisi seorang pengirim data informasi tidak dapat mengelak atau menyangkal bahwa dia telah mengirim suatu informasi.
d. Otentikasi (*Authentication*) merupakan mampunya penerimaan suatu informasi untuk membuktikan bahwa informasi yang terkirim tersebut asli.

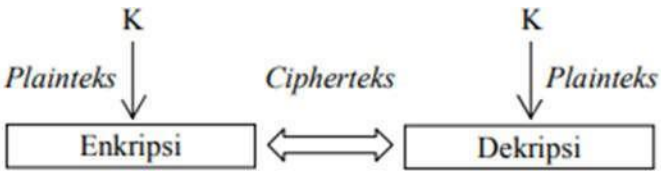
Berdasarkan pada *key* enkripsi dan juga dekripsi algoritme pada kriptografi dibagi menjadi 2 jenis yaitu [3]:

a. Kriptografi Kunci Asimetris (Kriptografi Kunci Publik) : Kriptografi ini terdapat dua key yang berbeda pada proses enkripsi dan proses dekripsi. key yang digunakan untuk enkripsi ini tidak bersifat rahasia. Pengirim melakukan enkripsi dengan menggunakan kunci publik, lalu penerima mendekrip kunci privat. Skema Kriptografi Asimetris ini bisa dilihat pada Gambar 1:



Gambar 1. Skema Kriptografi Asimetris

b. Kriptografi Kunci Simetris : Merupakan Kriptografi yang menggunakan key yang sama untuk melakukan proses enkripsi dan dekripsi data. Kriptografi tersebut menganggap bahwa penerima data dan pengirim data telah melakukan berbagi kunci sebelum data dikirim yang menjadikan keamanan terdapat pada key tersebut. Cipher pada kriptografi bekerja dalam bentuk blok, menjadikannya setiap proses enkripsi dan dekripsi dilakukan pada sebuah blok data, atau bekerja dalam mode aliran, yaitu setiap kali enkripsi atau dekripsi diproses kepada sebuah bit data. Skema Kriptografi Simetris ini bisa dilihat pada Gambar 2:



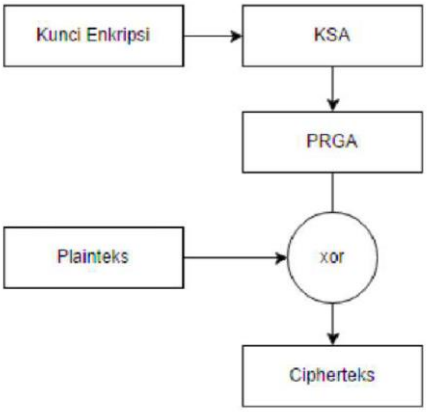
Gambar 2. Skema Kriptografi Simetris

2.2 RC 4 (Rivest Code 4)

RC 4 adalah sebuah arus kode yang bertujuan untuk enkripsinya diproses per 1 *byte* dalam sebuah pengoperasian. Algoritme *Rivest Code* 4 adalah algoritme kunci simetris yang dibentuk oleh RSA Data Security Inc *(RSADSI)* berbentuk *stream chiper*. Algoritme RC4 merupakan jenis *Stream Cipher* yang melekukan enkripsi diantara kombinasi dari plainteks yang terdapat *bit-wise* Xor (*Exclusive-or*). RC4 menjalankan dari panjang kunci dari 1 hingga 256 bit berfungsi untuk melakukan inisialisasi tabel yang memiliki panjang 256 bit. Tabel tersebut berguna untuk generasi selanjutnya dari *pseudo random* utnuk proses XOR dengan menggunakan plainteks untuk menciptakan cipherteks [4].

2.2.1 Algoritme Enkripsi RC4

RC4 adalah sebuah *stream cipher* yang terdapat suatu S-Box, S0,S1 sampai dengan S255 yang mengandung mutasi dari 0 sampai dengan 255, permutasi adalah kegunaan dari *key* dengan sifat panjang yang variabel. Metode tersebut membangunkan *pseudo random byte* berasal dari kunci untuk proses XOR kepada plainteks yang menciptakan chiperteks [5]. Arsitektur proses enkripsi dari algoritme RC4 bisa dilihat pada Gambar 3

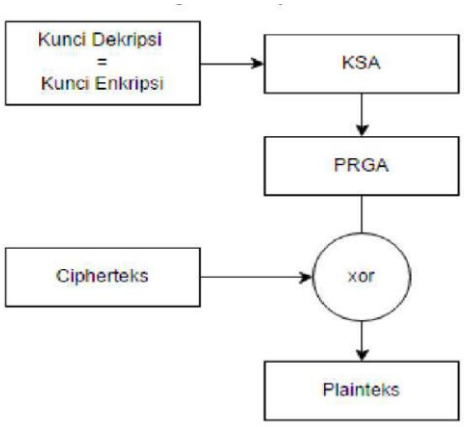


Gambar 3. Arsitektur Enkripsi RC4

2.2.2 Algoritme Dekripsi RC4

Algoritme dekripsi pada RC4 memiliki bentuk seperti algoritme enkripsinya, perbedaan yang terpadat diantaranya adalah pada *stream generation*, untuk menciptakan plainteks kembali, maka cipherteksnya akan dilakukan pengoperasian XOR kepada *pseudo randombyte*-nya.

Algoritme kunci pada prosesnya seperti dengan algoritme enkripsi yang memproses inisialisasi pada *S-Box*, pencadangan *key* kepada *key byte array* sehingga proses tersebut mengacu kepada *key byte array* nya. Maka proses enkripsi dan dekripsi akan menciptakan *key stream* sesuai. Perbedaan terdapat di *stream generation*-nya, yaitu yang dijalankan dengan *key stream* merupakan cipherteks untuk menciptakan plainteks *kembali* [5]. Arsitektur proses dekripsi dari algoritme RC4 bisa dilihat pada Gambar 4



Gambar 4. Arsitektur Dekripsi RC4

3. HASIL DAN PEMBAHASAN

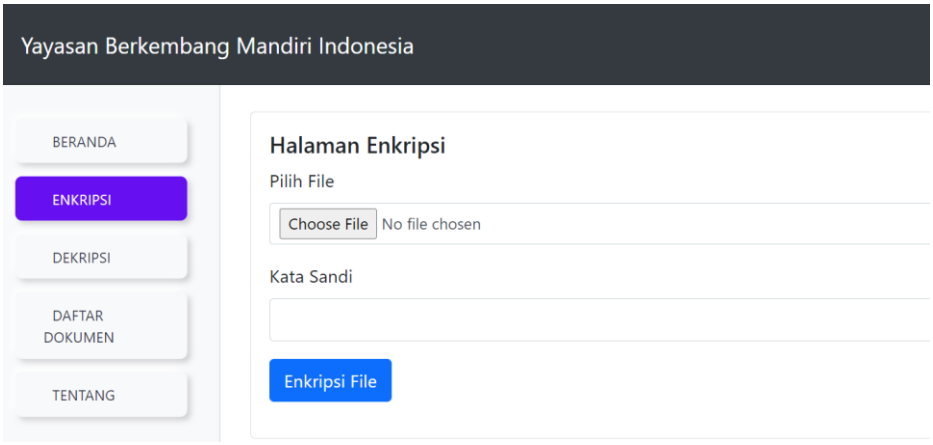
3.1 Penerapan Sistem

Implementasi untuk pengamanan informasi pada suatu sistem adalah proses enkripsi data dokumen untuk disimpan dalam *database*. Metode enkripsi berguna sebagai pelindung informasi untuk disimpan ke dalam *database*. Oleh sebab itu, ketika menyimpan data ke dalam database, diperlukan modul untuk mengenkripsi data tersebut. Enkripsi ditempatkan pada aplikasi yang akan dipanggil ketika pengguna ingin menyimpan data. Modul dekripsi dipanggil ketika pengguna ingin melihat data.

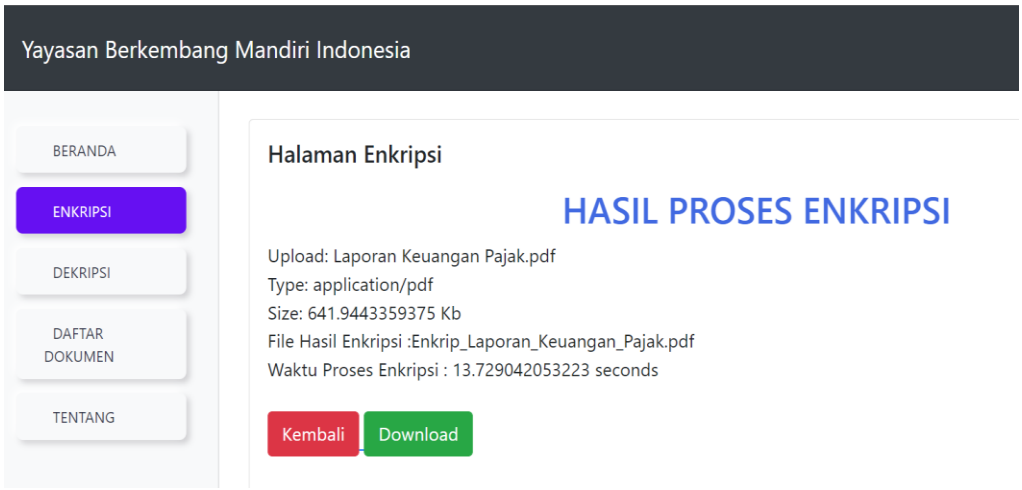
3.2 Tampilan Halaman Menu Enkripsi & Dekripsi

a. Menu Enkripsi dan Hasil Enkripsi

Pada menu enkripsi berisi kolom untuk memilih dokumen yang ingin dienkripsi serta kolom untuk memberikan kata sandi untuk dokumen yang akan di enkripsi. Lalu akan muncul hasil proses enkripsi yang terdapat nama dokumen, tipe dan ukuran dokumen hasil enkripsi, dan waktu proses enkripsi. Pengguna juga dapat mengunduh dokumen hasil proses enkripsi ke dalam komputer pengguna. Tampilan Halaman Menu Enkripsi dapat dilihat pada Gambar 5 dan Tampilan Halaman Menu Hasil Enkripsi dapat dilihat pada Gambar 6.



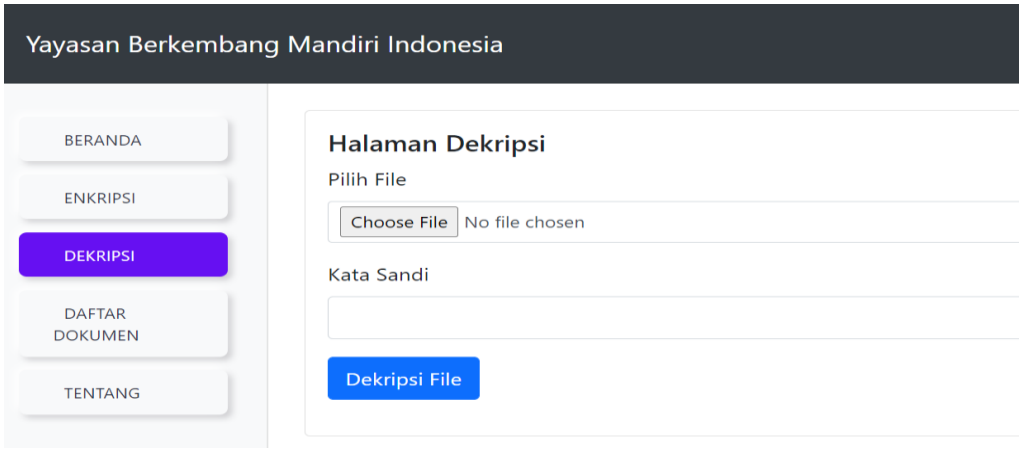
Gambar 5. Tampilan Halaman Menu Enkripsi



Gambar 6. Tampilan Halaman Menu Hasil Enkripsi

b. Menu Dekripsi dan Hasil Dekripsi

Pada menu dekripsi berisi kolom untuk memilih dokumen beserta kolom kata sandi untuk melakukan input kata sandi, kata sandi harus sesuai atau sama persis dengan kata sandi dokumen yang sudah dienkripsi. Lalu akan muncul hasil proses dekripsi yang terdapat nama dokumen, tipe dan ukuran dokumen hasil enkripsi, dan waktu proses enkripsi. Pengguna juga dapat mengunduh dokumen hasil proses dekripsi ke dalam komputer pengguna. Tampilan Halaman Menu Dekripsi bisa dilihat pada Gambar 7 dan Tampilan Halaman Menu Hasil Dekripsi bisa dilihat pada Gambar 8.



Gambar 7. Tampilan Halaman Menu Dekripsi

Gambar 8 Tampilan Halaman Menu Hasil Dekripsi

3.3 Pengujian Dan Analisa

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 Uji Coba Enkripsi

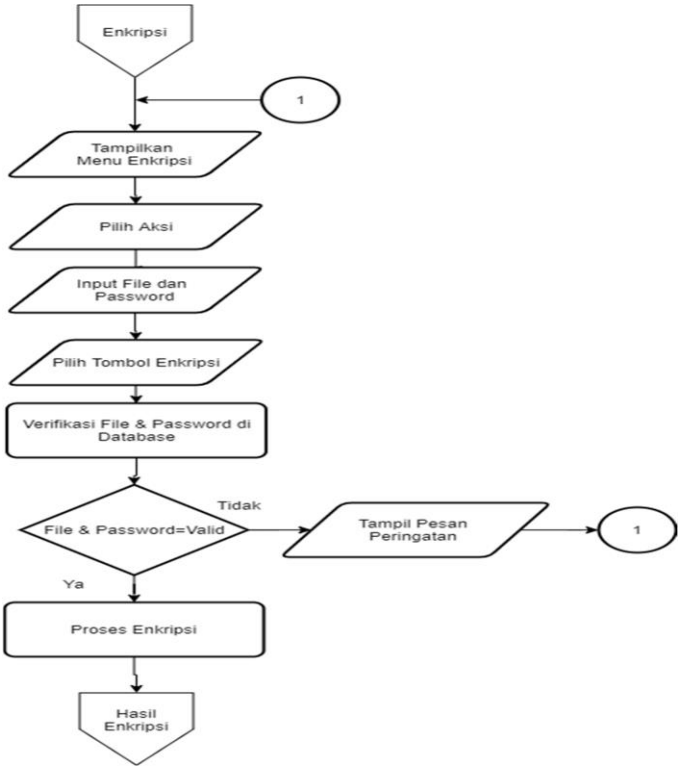
No	Plainteks	Key / Kunci	Chiperteks RC4
1	Enkripsi	12345678	þyy!œFÙ¶
2	Budiluhur	Budiluhur	Ç„o‰N¥˜±
3	nim1811501608	12345678	Õ~ :pÝ …¦¨¯©¡

Tabel 2 Hasil Uji Coba Dekripsi

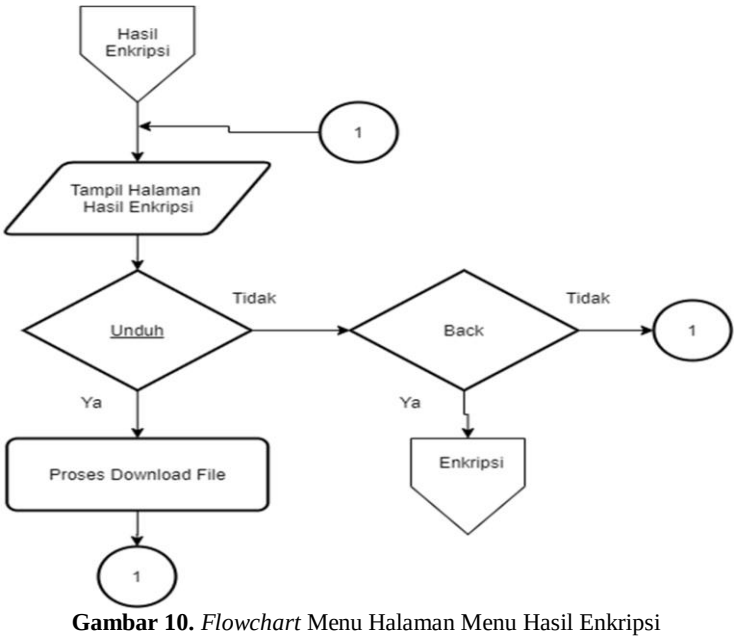
No	Chiperteks RC4	Key / Kunci	Plainteks
1	þyy!œFÙ¶	12345678	Enkripsi
2	Ç„o‰N¥˜±	Budiluhur	Budiluhur
3	Õ~ :pÝ …¦¨¯©¡	12345678	nim1811501608

3.4 *Flowchart*

Flowchart digunakan untuk menggambarkan alur dari sebuah program yang dibuat. Setiap alur tersebut dijelaskan kedalam model diagram yang dihubungkan dengan menggunakan garis. *Flowchart* Halaman Menu Enkripsi bisa dilihat pada Gambar 7 dan *flowchart* Halaman Menu Hasil Enkripsi dapat dilihat pada Gambar 8.



Gambar 9. *Flowchart* Halaman Menu Enkripsi



Gambar 10. *Flowchart* Menu Halaman Menu Hasil Enkripsi

Dalam *flowchart* menggambarkan jalannya proses dari halaman enkripsi dan halaman hasil enkripsi mulai dari menambahkan dokumen, kemudian dilakukan proses enkripsi dengan metode RC4 (*Rivest Code 4*) sehingga dokumen yang telah dienkripsi dapat diunduh oleh pengguna.

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. Apdillah and H. Swanda, “Penerapan Kriptografi RSA Dalam Mengamankan File Berbasis Teks PHP,” *Jurnal Teknologi Informasi*, vol. 2, no. 1, pp. 45-52, 2018.

[2] Munir, Kriptografi, Bandung: Penerbit Informatika Bandung, 2019.

[3] 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.

[4] D. Irwansyah, “Pengamanan Data Teks Dengan Algoritme Modifikasi RC4,” *Jurnal Pelita Informatika*, vol. 6, nol. 3, pp.309-312, 2018.

[5] H. Kusniyati, S. Diansyah and R. Yusuf, “Penerapan Algoritme *Rivest Code* 4 (RC4) Pada Aplikasi Kriptografi Dokumen,” *PETIR*, vol. 11, no. 1, pp. 38-47, 2018.

[6] K. A Seputra and G. A, J, Saskara, "Kriptografi Simetris RC4 Pada Transaksi *Online Booking Engine System*," *Jurnal Pendidikan Teknologi dan Kejuruan*, vol. 17, no. 2, pp. 286-295, 2020.

[7] S. Amin and K. Siahaan, “Analisis Dan Perancangan Sistem Informasi Manajemen Arsip Berbasis Web Pada Sekolah Tinggi Ilmu Tarbiyah (STIT) Kabupaten Tebo,” vol. 1, no. 1, pp. 1-10, 2016.

[8] D. Nurani, “Perancangan Aplikasi Email Menggunakan Algoritme *Caesar Cipher* dan *Base*64,” *JISKa(Jurnal Informatika Sunan Kalijaga)*, vol. 2, no. 3, pp. 175-180, 2018.

[9] N. E. Saragih, “Implementasi Algoritme *One Time Pad* Pada Pesan,” *Jurnal Ilmiah MATRIK* , vol. 20, no. 1, pp. 31-20, 2020.

[10] A. Setiawan and T. Fatimah, “Implementasi Algoritme Kriptografi RC4 Untuk Keamanan *Database* Aplikasi Penggajian Karyawan Berbasis Web Pada PT. Trans Intra Asia,” *SKANIKA*, vol. 4, no. 1, pp. 66-71, 2020.