KETIK : Jurnal Informatika
ISSN: 3026-183X (Media Online)
Vol. 01, No. 04, Maret 2024 Hal. 1-7
DOI : 10.70404/ketik.v1i04.58
Faatuatua Media Karya
https://jurnal.faatuatua.com/index.php/KETIK

Implementasi Algoritma Kriptografi Simetris Dalam Pengamanan Data Absensi Guru Dan Pegawai Pada Website Sekolah Smk Dharma Caraka Teluk Dalam Menggunakan RC4 Chiper

Sepiyanto Hulu

Universitas Budi Darma, Indonesia, email: sepiyantohulu2024@gmail.com

Info Artikel

Diajukan: 26 Maret 2024
Diterima: 27 Maret 2024
Diterbitkan: 31 Maret 2024

Kata Kunci:
Algoritma kriptografi simetris;
RC4;
Keamanan data;
Absensi;
Website;
SMK Dharma Caraka Teluk Dalam.

Keywords:
Symmetric cryptography algorithm;
RC4;
Data security;
Timesheet;
Website;
SMK Dharma Caraka Teluk Dalam.

Abstrak

Penelitian ini bertujuan untuk mengimplementasikan algoritma kriptografi simetris RC4 untuk mengamankan data absensi guru dan pegawai pada website SMK Dharma Caraka Teluk Dalam. Data absensi merupakan data penting yang perlu dirahasiakan untuk menjaga privasi dan integritas data. Algoritma RC4 dipilih karena memiliki tingkat keamanan yang tinggi dan mudah diimplementasikan. Metode penelitian yang digunakan adalah metode eksperimen dengan menggunakan perangkat lunak XAMPP dan bahasa pemrograman PHP. Data absensi dienkripsi dengan algoritma RC4 sebelum disimpan pada database website. Hasil penelitian menunjukkan bahwa algoritma RC4 dapat digunakan untuk mengamankan data absensi dengan baik. Data absensi yang terenkripsi tidak dapat dibaca oleh orang yang tidak memiliki kunci dekripsi. Implementasi algoritma RC4 pada website SMK Dharma Caraka Teluk Dalam dapat meningkatkan keamanan data absensi guru dan pegawai. Hal ini dapat membantu menjaga privasi dan integritas data absensi, serta mencegah penyalahgunaan data.

Abstract

This research aims to implement the RC4 symmetric cryptography algorithm to secure teacher and employee attendance data on the SMK Dharma Caraka Teluk Dalam website. Attendance data is important data that needs to be kept confidential to maintain data privacy and integrity. The RC4 algorithm was chosen because it has a high level of security and is easy to implement. The research method used is the experimental method using XAMPP software and PHP programming language. Attendance data is encrypted with the RC4 algorithm before being stored in the website database. The results showed that the RC4 algorithm can be used to secure attendance data well. Encrypted attendance data cannot be read by people who do not have the decryption key. The implementation of the RC4 algorithm on the website of SMK Dharma Caraka Teluk Dalam can increase the security of teacher and employee attendance data. This can help maintain the privacy and integrity of attendance data, and prevent data misuse.

1. PENDAHULUAN

Sekolah SMK Dharma Caraka adalah sekolah menengah kejuruan yang terletak di Baloho Indah No.14 Teluk Dalam, Pasar Teluk Dalam, Kec. Teluk Dalam, Kab. Nias Selatan Prov. Sumatera Utara. Sekolah ini didirikan pada tahun 2008 dengan SK Izin Opersional 420/305/K/2008 sesuai paparan kepala sekolah dan data yang tercantum pada situs dapo.kemdikbud.go.id.

Sistem absensi pada sekolah SMK Dharma Caraka merupakan salah satu hal yang sangat penting dilakukan untuk mendata kehadiran guru dan pegawai yang ada pada sekolah. Sistem pengelolaan data absensi dikelola unit tata usaha sekolah atas penugasan yang diberikan oleh kepala sekolah, dimana guru dan pegawai melakukan absensi mulai dari aktifitas masuk hingga selesai jadwal pekerjaan. Data absensi guru dan pegawai merupaka data yang sangat penting bagi kepala sekolah yang mana digunakan sebagai indikator utama dalam memantau kedisplinan dari pada guru dan pegawai, sehingga histori pelaksaan terhadap absensi tersebut harus nyata adanya. Sistem absensi disekolah SMK Dharma Caraka sudah menggunakan sistem yang terhubung dengan perangkat

komputer namun dalam sisi pengamanan data nya masih rentan terhadap proses pemanipulasian data kehadiran yang disebabkan oleh oknum tata usaha, guru dan pegawai. Hal ini terjadi pada masa pelaksanaan kegiatan belajar mengajar masa pandemi covid tahun 2021-2022. Berdasarkan permasalahan tersebut maka diperlukan penerapan teknik pengamanan terhadap dokumen atau record data absensi yang tersimpan dalam database yang tersimpan dalam perangkat komputer.

Berdasarkan penelitian terdahulu terkait dengan pentingnya pengamanan dokumen yang dilakukan Ghanang Ilham Ramadhan, menyatakan bahwa setiap data yang terhubung dalam sistem komputer wajib diterapkan teknik pengamanan dengan tujuan menghindari tindakan-tindakan pemanfaatan data oleh orang yang tidak berkepentingan terhadap informasi yang terkandung dalam data tersebut [1].

Teknik keamanan data ada beberapa macam, diantaranya enkripsi, *firewall, Secure Socket Layer, Cryptography, Pretty Good Privacy*. Kriptografi adalah seni menyandikan data. Menyandikan tidak harus berarti menyembunyikan meskipun kebanyakan algoritma yang dikembangkan di dunia kriptografi berhubungan dengan menyembunyikan data. Salah satu proses yang ada pada kriptografi adalah Enkripsi. Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti (tidak terbaca), sementara proses kebalikannya disebut Dekripsi.

Berdasarkan penelitian terdahulu oleh Esti Rahmati, yang menggunakan kriptografi sebagai teknik pengamanan data dalam artikel penelitiannya menyatakan bahwa kriptografi dapat mewujudkan keamanan informasi yang terkandung dalam sebuah data yang telah di enkripsi. Selain itu juga kriptografi dapat mendukung aspek-aspek keamanan informasi yang meliputi kerahasiaan, integritas data, otentikasi dan nir penyangkalan [2].

Algoritma kriptografi memiliki sejumlah kelemahan diantaranya terletak pada algoritma dan sandi yang digunakan. Berdasarkan penelitian terdahulu Chaerul Umam, menyatakan bahwa Tingkat keamanan dari data sandi terhadap upaya proses dekripsi secara paksa oleh orang yang tidak berhak ditentukan oleh kekuatan algoritma yang digunakan dan kerahasiaan kunci, sehingga pada proses penerapan kriptografi diperlukan teknik-teknik kombinasi algoritma dan teknik pembangkitan kunci yang lebih acak [3].

Algoritma RC4 (Ron's Code / Rivest's Cipher) adalah salah satu algoritma yang dapat digunakan untuk melakukan enkripsi data sehingga data asli hanya dapat dibaca oleh seseorang yang memiliki kunci enkripsi tersebut. Contoh yang dibahas kali ini adalah mengenai enkripsi dan dekripsi dari sebuah kalimat. Algoritma ini merupakan pengembangan dari RC2 dan dikembangkan oleh penemu algoritma tersebut, yaitu Ronald Rivest. Perbedaan dengan algoritma sebelumnya adalah ukuran blok, ukuran key, dan jumlah round yang dilakukan, dengan nilai yang direkomendasikan adalah ukuran blok 64 bit, ukuran key 128 bit, dan jumlah round 12 kali [4].

2. METODE PENELITIAN

2.1 Kerangka Kerja Penelitian

Kerangka kerja penelitian merupakan struktur yang didesain dengan tujuan sebagai landasan dalam melakukan sebuah penelitian. Desain dari kerangka kerja penelitian ini terdiri dari garis-garis besar penelitian mulai dari awal permasalahan yang akan diteliti hingga mendapatkan hasil penelitian.

1. Identifikasi Masalah, Pada tahap ini merupakan tahap yang bertujuan untuk menduga, memperkirakan dan menguraikan apa yang sedang menjadi masalah pada pengolahan data data absensi guru dan pegawai sekolah SMK Dharma Caraka Teluk, sehingga diperlukan teknik pengamanan.
2. Studi Pustaka, Tahapan ini dilakukan untuk menghimpun data-data atau sumber-sumber yang berhubungan dengan penggunaan algoritma kriptografi simetris dalam pengamanan data, yang diperoleh dari berbagai sumber seperti artikel jurnal, buku, dokumentasi, internet dan pustaka lainnya.
3. Analisis Kebutuhan Data, Proses menganalisis kebutuhan data dilakukan untuk memastikan penggunaan objek dan algoritma dalam penelitian sudah sesuai, yang datanya bersumber dari studi referensi yang dilakukan penulis, dan sehingga menemukan sebuah solusi penyelesaian masalah terkait dengan pengamanan data absensi pegawai dan guru di SMK Dharma Caraka Teluk Dalam.
4. Implementasi RC4 Cipher, Tahapan ini penulis melakukan Implementasi algoritma kriptografi, dalam penelitian ini membahas tentang algoritma RC4 Cipher. Tahapan ini lakukan terlebih dahulu sebelum proses implementasi formula algoritma RC4 Cipher. Dimana dilakukan pembangkitan kunci untuk enkripsi dan dekripsi menggunakan cipher RC4
5. Implementasi merupakan tahapan dimana dari sekumpulan data yang di peroleh diimplementasikan melalui perangkat lunak yang dibuat sehingga, perangkat tersebut dapat dipergunakan oleh user semestinya.

6. Pengujian merupakan tahapan dimana dilakukan proses uji coba terhadap penerapan teknik pengamanan data absensi guru dan pegawai SMK Dharma Caraka Teluk Dalam dengan mengkombinasi dua algoritma RC4 Cipher, dengan menggunakan aplikasi yang telah dirancangan dan dibangun serata tahapan ini berguna untuk memastikan aplikasi berjalan sesuai dengan semestinya.
7. Pendokumentasian adalah tahap dimana seseorang memeriksa kemajuan kegiatan penelitian termasuk temuan dan hasil penelitian. Hambatan yang dihadapi dan upaya mengatasinya juga disajikan. Pengalaman dalam menjalankan setiap kegiatan serta pencapaiannya hendaknya dilengkapi dengan analisis yang mendalam.

2.2 Kriptografi

Teknik keamanan data ada beberapa macam, diantaranya Enkripsi, *Firewall*, *Secure Socket Layer*, Kriptografi, *Pretty Good Privacy*. Kriptografi adalah seni menyandikan data. Menyandikan tidak harus berarti menyembunyikan meskipun kebanyakan algoritma yang dikembangkan di dunia kriptografi berhubungan dengan menyembunyikan data. Salah satu proses yang ada pada kriptografi adalah Enkripsi. Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti (tidak terbaca), sementara proses kebalikannya disebut Dekripsi [2].

Pengertian kriptografi secara umum, kriptografi adalah suatu ilmu pengetahuan yang dapat dipelajari pemakaian persamaan matematika dalam melakuka penyandian data. Tujuan kriptografi untuk keamanan isi data dan untuk menjaga informasi dari orang yang tidak diperkenankan untuk mengetahui isi data tersebut. Dengan adanya proses enkripsi *(encrypt)* yang merupakan teknik dari algoritma tertentu, data akan diubah menjadi data yang mempunyai sandi yang berbeda dengan data yang asli. Orang yang mempunyai hak untuk menerima data dapat mengetahui algoritma yang dipakai dan memiliki kunci untuk mengembalikan data yang sudah disandi menjadi data kedalam bentuk aslinya , proses ini disebut dengan dekripsi *(decrypt)*. Bentuk data sandi ini yang akan diperlukan untuk proses penyimpanan atau pengiriman data.

Berikut ini ada beberapa istilah-istilah yang berhubungan erat dengan proses penerapan atau penggunaan kriptografi [2]:

1. *Plaintext*, Pesan yang hendak dikirimkan (berisi data asli).
2. *Ciphertext*, Pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.
3. Enkripsi, Proses pengubahan plaintext menjadi *ciphertext*.
4. Dekripsi, Merupakan kebalikan dari enkripsi yakni mengubah *ciphertext* menjadi *plaintext*, sehingga berupa data awal/asli.
5. Kunci, Suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi.

2.3 Jenis-jenis Kriptografi

Kunci enkripsi dan dekripsi algoritma kriptografi dibagi menjadi 2:

1. Kriptografi Simetris, Konsep dasar kriptografi simetris merupakan kunci enkripsi dan dekripsi yang sama. Nama lain kriptografi ini adalah kriptografi kunci *private*, kriptografi kunci rahasia, atau kriptografi konvensional. Kriptografi ini mengasumsikan penerima dan pengirim pesan telah berbagi kunci tertentu sebelum pesan dikirim sehingga keamanan terletak pada kerahasiaan kunci. Umumnya cipher yang termasuk dalam kriptografi ini beroperasi dalam mode blok, yaitu setiap kali enkripsi atau dekripsi dilakukan pada satu blok data (yang berukuran tertentu), atau beroperasi dalam mode aliran, yaitu setiap kali enkripsi atau dekripsi dilakukan terhadap satu bit atau satu byte data.
2. Kriptografi Asimetris, Berbeda dengan kriptografi kunci simetris, kriptografi kunci publik memiliki dua kunci yang berbeda pada enkripsi dan dekripsi. Nama lain kriptografi ini adalah kriptografi kunci publik. Kunci untuk enkripsi pada kriptografi ini tidak rahasia *(private key)*. Pengirim akan mengenkripsi dengan kunci publik, sedangkan penerima mendekripsikan kunci privat.

2.4 Tujuan Kriptografi

Kriptografi dimaksudkan untuk memberikan layanan keamanan. Yang disebut aspek keamanan:

1. Kerahasiaan *(confidentiality)*, sebuah layanan yang dimaksudkan untuk mencegah pihak yang tidak berkepentingan membaca pesan.
2. Integritas data *(data integrity)*, layanan yang memastikan keaslian pesan atau tidak diubah selama transmisi.
3. Otentikasi *(authentication)*, merupakan layanan yang berkaitan dengan identifikasi, baik penentuan kebenaran pihak yang berkomunikasi (otentikasi pengguna).
4. *Non-repudiation*, sebuah layanan yang dimaksudkan untuk mencegah entitas komunikasi melakukan penolakan.

2.5 RC4 Cipher

Algoritme RC4 (Ron's Code / Rivest's Cipher) adalah salah satu algoritme yang dapat digunakan untuk melakukan enkripsi data sehingga data asli hanya dapat dibaca oleh seseorang yang memiliki kunci enkripsi tersebut. Contoh yang dibahas kali ini adalah mengenai enkripsi dan dekripsi dari sebuah kalimat. Algoritme ini merupakan pengembangan dari RC2 dan dikembangkan oleh penemu algoritme tersebut, yaitu Ronald Rivest. Perbedaan dengan algoritme sebelumnya adalah ukuran blok, ukuran key, dan jumlah round yang dilakukan, dengan nilai yang direkomendasikan adalah ukuran blok 64 bit, ukuran key 128 bit, dan jumlah round 12 kali [6].
Berikut beberapa langkah tahapan penerapan RC4 Cipher[6]:
Langkah 1: Menentukan data kunci dan *plaintext/ciphertext* yang akan di enkripsi atau dekripsi.
Langkah 2: Pembentukan kunci (*Keystream*)

1. *Key Schedulling Algorithm* (KSA)
   Proses KSA merupakan proses pembentukan tabel S-Box (Tabel Array S) dan Kunci (Tabel array [T]) yang di permutasi sebanyak 256 iterasi. Pseudocode untuk proses inisialisasi S-Box dan Array T.

   ```
   for (i = 0 ; i<=255; i++){ S-Box[i] = i
   T[i] = kunci[ i mod panjang_kunci] }
   ```

   Pseudocode untuk permutasi isi array S-Box :

   ```
   j = 0
   for (i = 0 ; i<=255; i++){
   j = (j + S-Box[i] + T[i]) mod 256 Swap( S-Box[i], S[j] )
   j = j
   }
   ```

   setelah dua proses ini dilakukan, maka array S-Box dan array Kunci (T) telah terbentuk.

2. *Pseudo Random Generator Algorithm* (PRGA)
   Tabel array S-Box akan digunakan pada proses ini untuk menghasilkan key stream yang jumlahnya sama dengan jumlah banyaknya karakter *plaintext* kemudian akan di- XOR dengan *plaintext*. Adapun pseudocode proses PRGA ini adalah

   ```
   i = 0; j = i
   for (i = 0 ; i <= jlh_karakter_plaintext; i++){ i = (i + 1) mod 256
   j = (j + S-Box[i]) mod 256 Swap( S-Box[i], S-Box[j] )
   t = (S-Box[i] + S-Box[j]) mod 256 Kunci[i] = S-Box[t]
   }
   ```

Langkah 3: Proses enkripsi atau dekripsi
Proses enkripsi atau dekripsi dengan operasi XOR. Proses enkripsi atau dekripsi di awali dengan merubah setiap nilai plaintext atau ciphertext ke biner. Formula untuk melakukan proses enkripsi dan dekripsi:
Ci = Pi Ki .....(1)
Formula proses dekripsi:
Pi = Ci Ki .....(2)

2.6 Database

Sistem pangkalan data atau basis data *(database)* adalah kumpulan informasi yang disimpan di dalam komputer secara sistematik sehingga dapat diperiksa menggunakan suatu program komputer untuk memperoleh informasi dari basis data tersebut. Perangkat lunak yang digunakan untuk mengelola dan memanggil kueri *(query)* basis data disebut sistem manajemen basis data *Database Management System* (DBMS)

Record data absensi guru dan pegawai sebagai objek utama yang digunakan oleh penulis dalam penelitian ini. *Record* adalah kumpulan elemen-elemen data yang terkait sebuah basis data. *Database* adalah sebuah sistem pemberkasan terpadu yang dirancang untuk dapat meminimalkan pengulangan data [7]. Maka dapat disimpulkan, bahwa *database* atau basis data merupakan suatu kumpulan data yang dapat berupa berbagai macam file yang tersimpan di dalam storage khusus yang digunakan untuk

kepentingan suatu organisasi dan dapat diakses ataupun digunakan oleh siapapun yang berhak dan juga membutuhkannya. Secara ringkas, database dapat dikatakan sebagai sebuah tabel yang memiliki baris *record* dan kolom atau field. *Record* mirip dengan array, yang bisa digunakan untuk membuat sebuah variabel yang berisi berbagai element. Perbedaannya, *record* bisa menampung berbagai jenis tipe data, tidak hanya satu tipe data seperti array [7].

3. HASIL DAN ANALISIS

Implementasi alogarima RC4 dengan mode 4 byte (untuk lebih menyederhanakan dalam perhitungan manual) serta untuk kebutuhan sistem yang sangat terbatas. S-Box dengan panjang 4 byte, dengan S[0]=0,S[1]=1,S[2]=2 dan S[3]=3 sehingga array S menjadi: 0 1 2 3.

Inisialisasi 4 byte kunci array, K. Misalkan kunci ulang kunci sampai memenuhi seluruh adalah 2 5 7 3, sehingga array K berisi 2 5 7 3 dan mencoba untuk mengenkripsikan kata HALO. Inisialisasi i dan j dengan 0 kemudian dilakukan KSA (Key-schedulingalgorithm) agar tercipta state-array yang acak.
Penjelasan interasi lebih lanjut dapat dijelaskan sebgaai berikut:
Iterasi 1
i = 0
j = (0 + S[0] + K [0 mod 4]) mod 4
= (0 + 0 + 2) mod 4 = 2 Swap(S[0], S[2])
Hasil Array S
2 1 0 3

Lakukan proses perhitungan iterasi selanjutnya hingga intersi 4
Iterasi 4
i = 2
j = (3 + S[3] + K [3 mod 4]) mod 4
= (3 + 0 + 3) mod 4 = 2 Swap (S[3],S[2])
Hasil Array S
1 2 0 3

Setelah melakukan KSA, PRGA (pseudo-random generation algoritma) akan dieksekusi. PRGA akan dieksekusi sebanyak 4 kali karena plaintext terenkripsi panjangnya 4 karakter. Hal ini disebabkan oleh teks biasa.
Berikut adalah tahapan penghasilan kunci enkripsi dengan PRGA.
Array S 1 2 0 3
Inisialissai i = 0
j = 0
Iterasi 1
I = (0 + 1) mod = 1
j = (0 + S[1]) mod 4 = (0 + 2) mod 4 = 2
Swap (S[1],S[2]) 1 0 2 3
K1 = S[(S[1]+S[2]) mod 4] = S[2 mod 4] = 2
K1` = 00000010

Lakukan proses perhitungan hingga iterasi ke 4
Iterasi 4
i = (3 + 1) mod 4 = 3
j =(3 + S[0]) mod 4 = (3 + 1) mod 4 = 0
Swap (S[0],S[0]) 1 0 2 3
K4 = S[S[0]+S[0]) mod 4] = S[2 mod 4] = 2
K4 = 00000010
Berikut table hasil

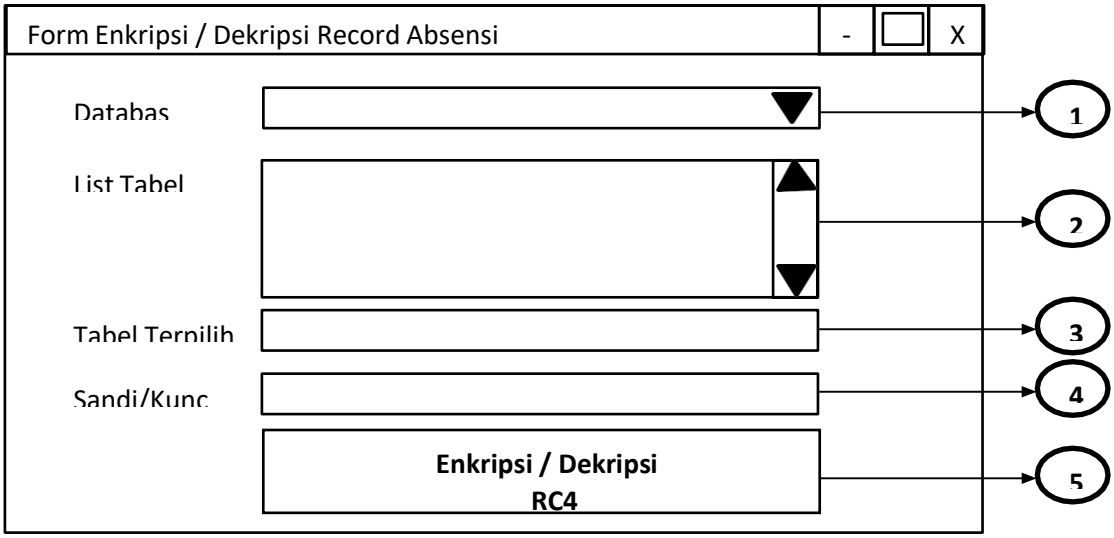
Tabel 1. Hasil PRGA

Huruf Kode ASCII	Binary 8 bit
H	01001000
A	01000001
L	01001100
O	01001111

Setelah kunci untuk setiap karakter ditemukan, dilakukan operasi XOR antar karakter terhadap teks palin berkunci yang dihasilkan. Berikut tabel ASCII untuk setiap karakter plain text yang digunakan Berikut adalah XOR dari *plaintext* dengan kunci yang diperoleh:

H A L O	01001000 01000001 01001100 01001111
Key	00000010 00000011 00000010 00000010
Cipherteks	01001010 01000010 01001110 01001101

Perancangan form untuk pengamanan data absensi guru dan pegawai pada website sekolah SMK Dharma Caraka teluk dalam menggunakan RC4 chiper, sebagai berikut:



Gambar 1. Rancangan Form Enkripsi / Dekripsi Record Absensi

Keterangan gambar:

1. Komponen *combo box* yang berfungsi untuk memilih *database* yang digunakan dalam proses enkripsi atau dekripsi RC4.
2. Komponen *list view* yang berfungsi menampilkan seluruh tabel yang ada pada database yang dipilih.
3. Komponen *text box* berfungsi menampilkan nama tabel yang dipilih berdasarkan *list* tabel.
4. Komponen *text box* berfungsi sebagai tempat data kunci yang digunakan dalam proses enkripsi dan dekripsi RC4.
5. Komponen *button* berfungsi sebagai tombol proses untuk mengeksekusi perintah terkait dengan proses Enkripsi atau Dekripsi RC4 Cipher.

4. KESIMPULAN

Kesimpulan dari penelitian implementasi algoritma kriptogrfi simetris dalam pengamanan data absensi guru dan pegawai pada website sekolah SMK Dharma Caraka teluk dalam menggunakan RC4 chiper, sebagai berikut:

1. Berdasarkan prosedur pengolahan data absensi guru dan pegawai pada Website sekolah SMK Dharma Caraka Teluk Dalam menjadi lebih aman, dan dapat diimplementasi metode pengamanan kriptografi.
2. Pengimplementasikan pengamanan data dengan RC4 Cipher pada aplikasi absensi guru dan pegawai berhasil dilakukan terbukti data absen berubah kedalam bentuk *ciphertext* yang tidak dapat dipahami maknanya.
3. Pengujian algoritma RC4 Chiper dalam pengamanan data absensi guru dan pegawai SMK Dharma Caraka dapat menggunakan aplikasi OCTAV, terbukti tampil *ciphertext* yang memiliki kualitas cipher dan memiliki enkripsi yang baik.

REFERENSI

[1] G. I. Ramadhan and S. Alfarisi, “Penerapan Caesar Cipher Pada Absensi dan Cuti Karyawan PT. Datacomindo Mitrausaha Berbasis Java,” JRKT, vol. 1, no. 04, Dec. 2021. [Available]

[2] W. Setiawan, “Keamanan Data & Informasi.” BKPSDMD, 2022. [Available]

[3] E. R. Agustina and A. Kurniati, “Pemanfaatan Kriptografi Dalam Mewujudkan Keamanan Informasi PADA e-Voting Di Indonesia,” 2009. [Available]
[4] Chaerul Umam, Muslih Muslih, and Daffa Fadillah, “Kombinasi Steganografi LSB dan Kriptografi AES dalam Sekuriti Teks Rahasia Pada Citra Berwarna,” SEMNASTEKMU, vol. 2, no. 1, pp. 109–118, Dec. 2022. [Available]
[5] H. Seo et al., “Compact Implementation of ARIA on 16-Bit MSP430 and 32-Bit ARM Cortex-M3 Microcontrollers,” Electronics, vol. 10, no. 8, p. 908, Apr. 2021, doi: 10.3390/electronics10080908.
[6] G. Paul and S. Maitra, RC4 Stream Cipher and Its Variants. CRC Press, 2011. [Available]
[7] Wandi, Sistem Basis Data. 2021.
[8] R. Maulana, R. M. Simanjorang, and J. I. M. No, “Implementasi Kriptografi Untuk Pengamanan Data Pribadi Siswa SMA Swasta Jaya Krama Beringin Dengan Algoritma RC4,” vol. 4, no. 6, 2021.
[9] D. Kwon et al., “New Block Cipher: ARIA,” in Information Security and Cryptology - ICISC 2003, J.-I. Lim and D.-H. Lee, Eds., in Lecture Notes in Computer Science, vol. 2971. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 432–445. [Available]
[10] S. Waluyo and D. V. Kanahebi, “Sistem Pengamanan File Menggunakan Algoritma RC4 Berbasis Webbase Studi Kasus: PT. Tjipta Jaya Bersama,” 2021.
[11] A. Setiawan and T. Fatimah, “Implementasi Algoritma Kriptografi RC4 untuk Keamanan Database Aplikasi Penggajian Karyawan Berbasis Web Pada PT. Trans Intra Asia,” SKANIKA Budi Luhur, vol. 4, no. 1, pp. 66–71, Jan. 2021. [Available]
[12] N. Ratama and M. Munawaroh, “Implementasi Metode Kriptografi dengan Menggunakan Algoritma RC4 dan Steganografi Least Significant Bit Dalam Mengamankan Data Berbasis Android,” MIB, vol. 6, no. 2, p. 1272, Apr. 2022. [Available]