Journal Global Tecnology Computer
Vol 2, No. 1, Desember, 2022, Hal 8 - 15
ISSN: **2809-6118** (Online - Elektronik)
Website https://ejurnal.seminar-id.com/index.php/jogtc

Analisis Dan Implementasi Algoritma Clefia 128 Untuk Meningkatkan Confusion Record Data Login User

Helpy Eka Putra Gea

Program Studi Teknik Informatika, Fakultas Ilmu Komputer & Teknologi Informasi, Universitas Budi Darma, Medan, Indonesia
Jl. Sisingamangaraja No.338, Siti Rejo I, Kec. Medan Kota, Kota Medan, Sumatera Utara, Indonesia
Email: helpygea88@gmail.com

Abstrak-Analisis dan Implementasi Algoritma CLEFIA 128 Untuk Meningkatkan Confusion Record Data Login User Masalah keamanan adalah salah satu aspek yang sangat penting pada sebuah sistem informasi. Masalah keamanan sering kali kurang diperhatikan para perancang dan pengelolah sistem informasi, bahkan hal keamanan ini di anggap hal yang terakhir diperhatikan setelah tampilan sistem informasi. Sehingga sering terjadi tindakan kejahatan seperti penyadapan terhadap data dan mudahnya dipahami informasi yang terkandung didalamnya. Record data login merupakan. salah satu tabel database pada aplikasi sistem informasi berbasis web yang keberadaan data dan informasi nya wajib diamankan, karena berkaitan dengan password dan id pengguna. Salah satu teknik keamanan data yang dapat digunakan adalah teknik kriptografi. Kriptografi adalah displin ilmu yang mempelajari mengenai cara menggubah bentuk data awal kebentuk data yang lain sehingga informasi yang terkandung dalam data tersebut tidak dapat dipahami oleh orang lain. Algoritma kriptografi yang dapat digunakan adalah Algoritma CLEFIA 128. Algoritma CLEFIA 128 adalah jenis algoritma kriptografi Stream yang dimana sandi yang digunakan pengguna dalam hal ini pengenkrip dan pengdekrip menggunakan kunci yang sama. Hasil yang akan dicapai dalam penelitian ini adalah dapat diterapkannya algoritma CLEFIA 128 untuk memberikan nilai counfusion terhadap baris data login user pada database, yang kemudian menghasilkan sebuah kesimpulan analisis terkait dengan kekuatan algoritma CLEFIA 128 dalam mengamankan record data login user pada aplikasi web**.**

Kata Kunci: Analisis, Algoritma, Kriptografi, Clefia 128.

Abstract-Analysis and Implementation of CLEFIA 128 Algorithm To Improve User Login Data Confusion Record Security issues are one of the most important aspects of an information system. Security issues are often not paid attention to by designers and managers of information systems, even this security issue is considered the last thing to be considered after the appearance of the information system. So that crimes often occur such as wiretapping of data and easy understanding of the information contained therein. The login data record is. one of the database tables in a web-based information system application where the existence of data and information must be secured, because it is related to the password and user id. One of the data security techniques that can be used is cryptography. Cryptography is a discipline that studies how to change the initial data form into other forms of data so that the information contained in the data cannot be understood by others. The cryptographic algorithm that can be used is the CLEFIA 128 Algorithm. The CLEFIA 128 algorithm is a type of Stream cryptographic algorithm where the password used by the user in this case the encrypter and decryptor uses the same key. The result to be achieved in this study is that the CLEFIA 128 algorithm can be applied to provide a confusion value to the user login data line in the database, which then produces an analytical conclusion related to the strength of the CLEFIA 128 algorithm in securing user login data records in web applications.

Keywords: Analysis, Algorithm, Cryptography, Clefia 128.

1. PENDAHULUAN

Penggunaan komputer saat ini telah menjadi suatu kebutuhan yang sangat penting bagi kemajuan teknologi informasi, dimana dengan adanya pengembangan teknologi informasi dapat memberikan kemudahan, tepat guna, akurat dan lebih efisien dalam penerapannya.Penggunaan teknologi informasi meliputi berbagai bidang, diantaranya seperti bidang ekonomi, politik, pendidikan, dan bidang lainnya. Berbagai instansi, perusahaan ataupun lembaga pendidikan telah merata di berbagai tingkat disiplin kerja dalam hal penggunaan sistem komputer. Pada saat sekarang ini, teknologi berkembang dengan pesatnya. Kebutuhan akan peralatan yang dapat mendukungnya juga semakin meningkat [1].

Salah satu teknik teknik pengamanan yang dapat di terapkan adalah teknik kriptografi.Kriptografi adalah ilmu dan seni yang mempelajari tentang bagaimana mengamankan pesan atau data agar tidak dapat diketahui informasinya oleh orang yang tidak berkempentingan. Mendukung kinerja penerapan kriptografi di butuhkan algoritma enkripsi dan dekripsi yang dapat memberikan nilai kebinguan (confusion) terhadap pesan atau data yang dirahasiakan.

Penelitian ini dilakukan untuk menghasilkan analisis terkait dengan penerapan dan performansi algoritma Clefia 128 bit untuk pengamanan jenis data teks, dengan tujuan untuk memberikan alternatif serta solusi kepada pengiat dan pengguna dalam hal penggunaan algoritma teknik kriptografi untuk pengamanan data.Dalam logika, analisis atau pembagian berarti pemecahbelahan atau penguraian secara jelas berbeda ke bagian-bagian dari suatu keseluruhan. Untuk lebih seksama dapat juga mengadakan subbagian, yakni menguraikan atau memecah belah dari suatu bagian sampai ke unsur dasarnya.Menurut KBBI (Kamus Besar Bahasa Indonesia) Implementasi yaitu pelaksanaan/ penerapan. Sedangkan pengertian umum adalah suatu tindakan atau pelaksana rencana yang telah disusun secara cermat dan rinci (matang).

Implementasi adalah suatu tindakan atau pelaksanaan rencana yang telah disusun dengan cermat dan rinci. Implementasi ini biasanya selesai setelah dianggap. Algoritma Clefia 128 bit merupakan algoritma yang didesain atas dasar efisiensi namun tetap memperhatikankeamanan oleh Sony Corporation pada tahun 2007.Algoritma ini berbasis block cipher dengan ukuran 128 bit blok dengan variasi kunci 128, 192 dan 256 bit.CLEFIA menggunakan struktur Feistel yang membagi blokmenjadi 4 jalur masing-masing berukuran 32 bit.Jumlah round pada CLEFIA bervariasi

Journal Global Tecnology Computer
Vol 2, No. 1, Desember, 2022, Hal 8 - 15
ISSN: **2809-6118** (Online - Elektronik)
Website https://ejurnal.seminar-id.com/index.php/jogtc

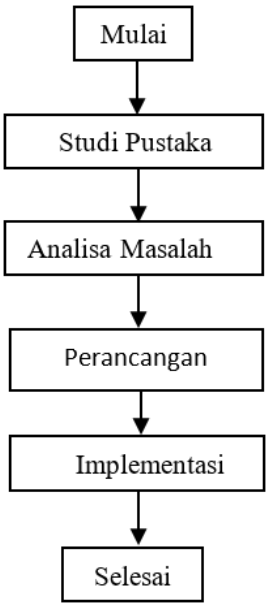
tergantung panjang kuncinya, untuk kunci 128 bit memiliki jumlah round 18, kunci 192 bit memiliki jumlah round 22 dan kunci 256 bit memiliki jumlah round 26 [2].

Berdasarkan uraian di atas, maka penulis tertarik mengangkat topik skripsi yang berjudul "Analisis dan Implementasi Algoritma CLEFIA 128 Untuk Meningkatkan Confusion Record Data Login User".

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Adapun tahapan-tahapan yang dilakukan pada penelitian ini dapat dijelaskan seperti gambar di bawah ini:



Gambar 1. Tahapan Penelitian

Berdasarkan gambar 1 diatas dapat dijelaskan tahapan-tahapan yang dilakukan pada penelitian ini sebagai berikut:

1. Studi Pustaka
   Penelitian yang dilakukan berdasarkan data yang diperoleh dari teori buku - buku penunjang yang berhubungan dengan permasalahan sistem yang akan dikembangkan. Serta mengunjungi situs–situs online penyedia jurnal baik dalambahasa indonesia maupun bahasa inggris untuk dijadikan referensi penelitian yang sedang penulis kerjakan.
2. Analisa Masalah
   Pada tahap ini dilakukan analisis terhadap rumusan masalah dan batasan yang ada dalam skripsi ini. Analisis ini juga dilakukan untuk melakukan analisis spesifikasi sistem yang akan dibuat sesuai dengan batasan yang ada dalam hal ini adalah melakukan penggunaan algoritma Clefia 128.
3. Perancangan
   Pada tahap ini dilakukan analisis desain dan perancangan sistem yang akan dilakukan Pemodelan dan perancangan system.
4. Implementasi
   Pada tahap terakhir ini aplikasi yang sudah dirancangan akan digunakan langsung untuk membuktikan hasil pembuatan program.

2.2 Analisis

Menurut Kamus Besar Bahasa Indonesia (KBBI), pengertian analisis adalah penyelidikan terhadap suatu peristiwa (karangan, perbuatan, dsb) untuk mengetahui keadaan yang sebenarnya (sebab-musabab, duduk perkaranya dsb) (KBBI, 2008: 58).Analisa berasal dari kata Yunani Kuno "analusis" yang berarti melepaskan. Analusis terbentuk dari dua suku kata yaitu "ana" yang berarti kembali dan "luein" yang berarti melepas. Sehingga pengertian analisa yaitu suatu usaha dalam mengamati secara detail pada suatu hal atau benda dengan cara menguraikan komponen-komponen pembentuknya atau menyusun komponen tersebut untuk dikaji lebih lanjut.

2.3 Implementasi

Implementasi merupakan suatu proses yang dinamis, dimana pelaksana kebijakan melakukan suatu aktifitas atau kegiatan, sehingga pada akhirnya akan mendapatkan suatu hasil yang sesuai dengan tujuan atau sasaran kebijakan itu sendiri [3].

Journal Global Tecnology Computer
Vol 2, No. 1, Desember, 2022, Hal 8 - 15
ISSN: **2809-6118** (Online - Elektronik)
Website https://ejurnal.seminar-id.com/index.php/jogtc

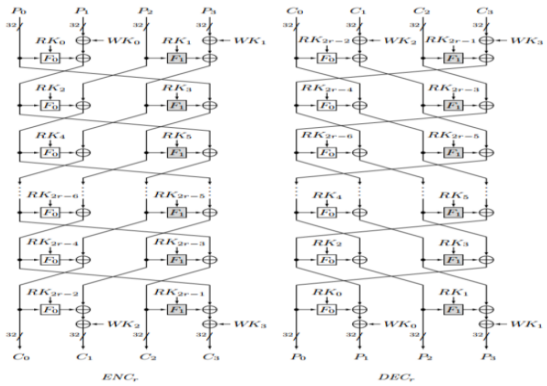
2.4 Kriptografi

Kriptografi (Cryptography) berasal dari bahasa Yunani yaitu “Cryptos” artinya “secret”(rahasia) dan “graphein” artinya “writing”(tulisan). Jadi, kriptografi berarti “secret writing”(tulisan rahasia). Kriptografi adalah ilmu dan seniuntuk menjaga keamanan pesan [4]. (Cryptography isthe art and sience of keeping message secure). Menurut Rinaldi Munir (2006) dalam bukunya menjelaskan data atau informasi yang dapat dibaca dan dimengerti maknanya disebut plaintext. Plaintext yang tersandi disebut ciphertext. Ciphertext harus dapat ditransformasikan kembali menjadi plaintextsemula agar pesan yang diterima bisa dibaca (Muhhamad Zulham, 2016).

Algoritma Clefia 128 bit merupakan algoritma yang didesain atas dasar efisiensi namun tetap memperhatikan keamanan oleh Sony Corporation pada tahun 2007. Algoritma ini berbasis block cipher dengan ukuran 128 bit blok dengan variasi kunci 128, 192 dan 256 bit. CLEFIA menggunakan struktur Feistel yang membagi blok menjadi 4 jalur masing-masing berukuran 32 bit [5]. Jumlah round pada CLEFIA bervariasi tergantung panjang kuncinya, untuk kunci 128 bit memiliki jumlah round 18, kunci 192 bit memiliki jumlah round 22 dan kunci 256 bit memiliki jumlah round 26. Penelitian ini dilakukan untuk menghasilkan analisis terkait dengan penerapan dan performansi algoritma Clefia 128 bit untuk pengamanan jenis data teks, dengan tujuan untuk memberikan alternatif serta solusi kepada pengiat dan pengguna dalam hal penggunaan algoritma teknik kriptografi untuk pengamanan data [3], .

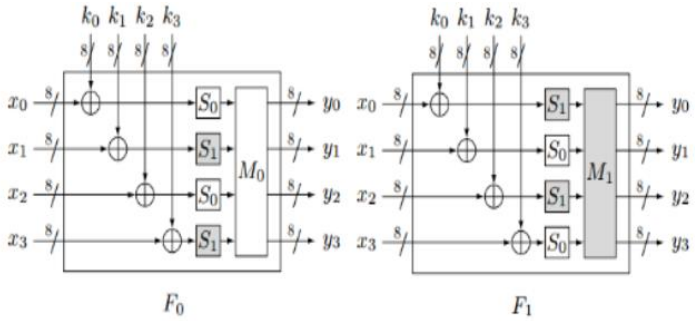
2.5 Algoritma Clefia 128

CLEFIA merupakan algoritma yang didesain atas dasar efisiensi namun tetap memperhatikan keamanan. Algoritma ini telah ditetapkan sebagai algoritma standar untuk pervasive computing yang memiliki kriteria untuk penerapan pada device yang memiliki sumberdaya terbatas melalui ISO/IEC 29192-2 [6]. Algoritma ini berbasis block cipher dengan ukuran 128 bit blok dengan variasi kunci 128, 192 dan 256 bit. CLEFIA menggunakan struktur Feistel yang membagi blok menjadi 4 jalur masing-masing berukuran 32 bit. Jumlah round pada CLEFIA bervariasi tergantung panjang kuncinya, untuk kunci 128 bit memiliki jumlah round 18, kunci 192 bit memiliki jumlah round 22 dan kunci 256 bit memiliki jumlah round 26. Diagram algoritma CLEFIA dapat dilihat pada gambar 1.



Gambar 2. Diagram Algoritma Clefia

Fungsi F merupakan komponen utama dalam struktur algoritma CLEFIA yang berbasis Feistel. Didalamnya harus melibatkan operasi atau fungsi nonlinear dan memiliki sifat difusi yang maksimal. Fungsi F pada CLEFIA terdiri dari 3 komponen operasi yaitu operasi XOR dengan kunci, fungsi nonlinear S-box 8x8 dan fungsi linear mixing. Fungsi F pada CLEFIA dapat dilihat pada Gambar 2**.**



Gambar 3. Fungsi F pada Algoritma Clefia

S0 dan S1 merupakan fungsi nonlinear S-box 8x8, sedangkan M0 dan M1 merupakan fungsi perkalian dengan matriks M0 dan M1 untuk proses linear mixing. Perkalian matriks M0 dan M1 ini didefinisikan berdasarkan pada polinomial primitive z 8 + z 4 + z 3 + z + 1 dengan menggunakan matriks M0 dan M1 berukuran 4 x 4 berikut:

Journal Global Tecnology Computer
Vol 2, No. 1, Desember, 2022, Hal 8 - 15
ISSN: **2809-6118** (Online - Elektronik)
Website https://ejurnal.seminar-id.com/index.php/jogtc

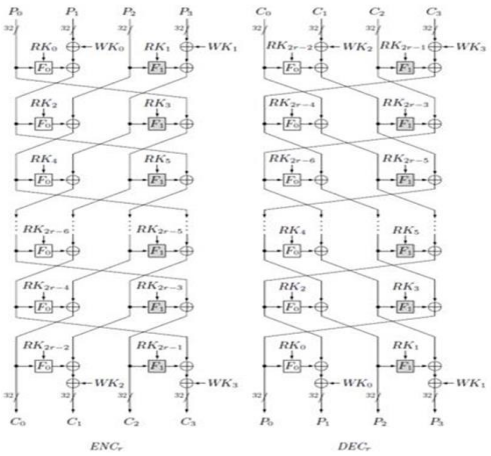
$$M_0 = \begin{pmatrix} 0x01 & 0x02 & 0x04 & 0x06 \\ 0x02 & 0x01 & 0x06 & 0x04 \\ 0x04 & 0x06 & 0x01 & 0x02 \\ 0x06 & 0x04 & 0x02 & 0x01 \end{pmatrix}, \quad M_1 = \begin{pmatrix} 0x01 & 0x08 & 0x02 & 0x0a \\ 0x08 & 0x01 & 0x0a & 0x02 \\ 0x02 & 0x0a & 0x01 & 0x08 \\ 0x0a & 0x02 & 0x08 & 0x01 \end{pmatrix}$$

3. HASIL DAN PEMBAHASAN

3.1 Analisa

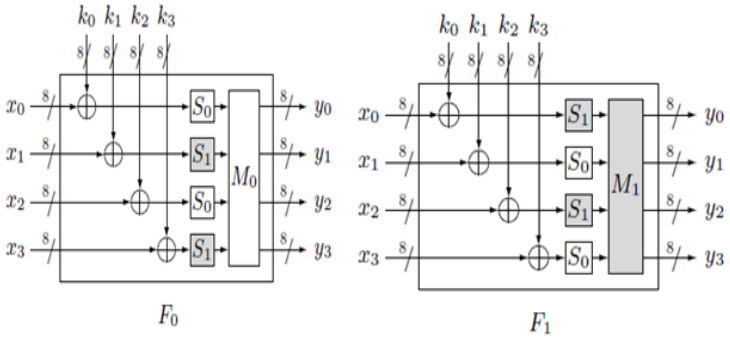
Algoritma Clefia 128 bit merupakan algoritma yang didesain atas dasar efisiensi namun tetap memperhatikan keamanan oleh Sony Corporation pada tahun 2007. Algoritma ini berbasis block cipher dengan ukuran 128 bit blok dengan variasi kunci 128, 192 dan 256 bit. CLEFIA menggunakan struktur Feistel yang membagi blok menjadi 4 jalur masing-masing berukuran 32 bit [3]. Jumlah round pada CLEFIA bervariasi tergantung panjang kuncinya, untuk kunci 128 bit memiliki jumlah round 18, kunci 192 bit memiliki jumlah round 22 dan kunci 256 bit memiliki jumlah round 26. CLEFIA merupakan algoritma yang didesain atas dasar efisiensi namun tetap memperhatikan keamanan [7].

Algoritma ini telah ditetapkan sebagai algoritma standar untuk pervasive computing yang memiliki kriteria untuk penerapan pada device yang memiliki sumberdaya terbatas melalui ISO/IEC 29192-2. Algoritma ini berbasis block cipher dengan ukuran 128 bit blok dengan variasi kunci 128, 192 dan 256 bit. CLEFIA menggunakan struktur Feistel yang membagi blok menjadi 4 jalur masing-masing berukuran 32 bit. Jumlah round pada CLEFIA bervariasi tergantung panjang kuncinya, untuk kunci 128 bit memiliki jumlah round 18, kunci 192 bit memiliki jumlah round 22 dan kunci 256 bit memiliki jumlah round 26 [8]. Diagram algoritma CLEFIA dapat dilihat pada Gambar 3.



Gambar 4. Diagram Algoritma CLEFIA

Fungsi F merupakan komponen utama dalam struktur algoritma CLEFIA yang berbasis Feistel. Didalamnya harus melibatkan operasi atau fungsi nonlinear dan memiliki sifat difusi yang maksimal. Fungsi F pada CLEFIA terdiri dari 3 komponen operasi yaitu operasi XOR dengan kunci, fungsi nonlinear S -box 8x8 dan fungsi linear mixing. Fungsi F pada CLEFIA dapat dilihat pada Gambar 4.



Gambar 5. Fungsi F0 dan F1 CLEFIA

S0 dan S1 merupakan fungsi nonlinear S-box 8x8, sedangkan M0 dan M1 merupakan fungsi perkalian dengan matriks M0 dan M1 untuk proses linear mixing. Perkalian matriks M0 dan M1 ini didefinisikan berdasarkan pada polinomial primitive z8+ z4 + z3+ z2+ 1dengan menggunakan matriks M0 dan M1 berukuran 4 x 4 berikut :

Journal Global Tecnology Computer
Vol 2, No. 1, Desember, 2022, Hal 8 - 15
ISSN: **2809-6118** (Online - Elektronik)
Website https://ejurnal.seminar-id.com/index.php/jogtc

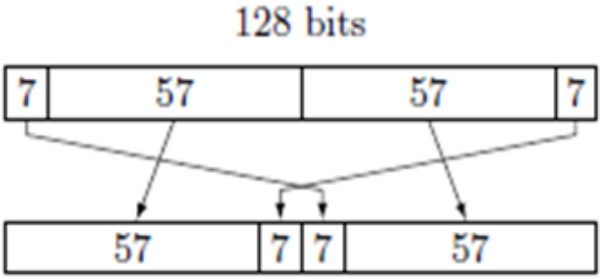
$$M_0\begin{pmatrix} 0x01 & 0x02 & 0x04 & 0x06 \\ 0x02 & 0x01 & 0x06 & 0x04 \\ 0x04 & 0x06 & 0x01 & 0x02 \\ 0x06 & 0x04 & 0x02 & 0x01 \end{pmatrix}, \quad M_1\begin{pmatrix} 0x01 & 0x08 & 0x02 & 0x0a \\ 0x08 & 0x01 & 0x0a & 0x02 \\ 0x02 & 0x0a & 0x01 & 0x08 \\ 0x0a & 0x02 & 0x08 & 0x01 \end{pmatrix}$$

Penjadwalan kunci pada CLEFIA-128, digunakan untuk menyediakan kunci pada proses whitening dan kunci round untuk proses tiap round. Fungsi DoubleSwap yang digunakan pada proses penjadwalan kunci didefinisikan sebagai berikut.

$X_{(128)} \rightarrow Y_{(128)}$

$\mathrm{Y} = \mathrm{X}[7-63] \mid \mathrm{X}[121-127] \mid \mathrm{X}[0-6] \mid \mathrm{X}[64-120] \mid$

$X[a-b]$ menotasikanstring sepanjang a bit dipotong dari bit ke-a sampai bit ke-b pada X. Bit ke-0 adalah Most Significant Bit (MSB). Fungsi dapat digambarkan sebagai berikut



Gambar 6. Fungsi DoubleSwap

Misal K adalah kunci dan L adalah kunci intermediate dan penjadwalan kunci terdiri dari 2 (dua) langkah:

1. Membangkitkan L dari K
2. Perluasan (ekspansi) K dan L (pembangkitan dan).

Untuk membangkitkan L dari K, pada 128 bit kunci menggunakan 128 bit permutasi, sedangkan struktur sama seperti diagram algoritma CLEFIA (Gambar 1) dengan jumlah iterasi (round) sebanyak 12.

step 1. $L \leftarrow GFN_{4,12}(CON_{23}^{(128)}, K_0, \dots, K_3$
(Expanding K and L)

step 2. $WK_0 \mid WK_1 \mid WK_2 \mid WK_3 \leftarrow K \mid$

step 3. $For\ i = 0\ to\ 8\ do\ the\ following$:

$T \leftarrow L \oplus \left(CON_{24+4i}^{(128)} \mid CON_{24+4i+1}^{(128)} \mid CON_{24+4i+2}^{(128)} \mid CON_{24+4i+3}^{(128)}\right)$

$L \leftarrow \sum(L)$

$if\ i\ is\ odd : T \leftarrow T \oplus K$

$RK_{4i} \mid RK_{4i+1} \mid RK_{4i+2} \mid RK_{4i+3} \leftarrow T \mid$

CON merupakan konstanta berukuran 32 bit yang digunakan dalam algoritma penjadwalan kunci. CLEFIA-128 membutuhkan 60 nilai konstan. Pseudocode untuk membangkitkan nilai adalah sebagai berikut :

step 1. $T_0 \leftarrow IV^{(k)}$
$Step\ 2.\ For\ i = 0\ to\ l^{(k)} - 1\ do\ the\ following$:
$Step\ 2.1\ CON_{2i}^{(k)} \leftarrow (T_i \oplus P) \mid \overline{T_i} <<< 1)$
$Step\ 2.2\ CON_{2i+1}^{(k)} \leftarrow (T_i \oplus Q) \mid \overline{T_i} <<< 8)$
$Step\ 2.3\ T_{i+1} \leftarrow T_i . 0x0002^{-1}$
Parameter dalam pembangkitan nilai ($CON^{(k)}$)
P(16) = 0xb7e1 (= (e - 2) . 216)

Q(16) = 0x243f (= (- 3) . 216)

e = basis dari logaritma natural (2,71828...)

= 3,14159

= 3,14159

Journal Global Tecnology Computer
Vol 2, No. 1, Desember, 2022, Hal 8 - 15
ISSN: **2809-6118** (Online - Elektronik)
Website https://ejurnal.seminar-id.com/index.php/jogtc

Tabel 1. Nilai$^{(k)}$ dan IV $^{(k)}$

k	# of # $of\ CON_i^{(k)}$	$l^{(k)}$	$IV^{(k)}$	
128	60	30	0x428a	$(=(\sqrt[3]{2}-1).2^{16})$
192	84	42	0x7137	$(=(\sqrt[3]{3}-1).2^{16})$
258	92	46	0xb5c0	$(=(\sqrt[3]{5}-1).2^{16})$

3.1.1 Penerapan Algoritma Clefia 128

Algoritma CLEFIA sebagai standar algoritma lighweight block cipher harus dibuktikan memenuhi kriteria kekuatan kriptografis yang memadai. Pada penelitian sebelumnya penulis telah melakukan analisis terhadap salah satu komponen utama dalam algoritma CLEFIA, yaitu -box. S- box S0 dan S1 berukuran 8x8 pada CLEFIA memiliki ketahanan terhadap serangan linear dan differential cryptanalysis yang memadai berdasarkan penghitungan LAT , XOR Table dan nilai nonlinearity (A'mas, 2015).

Selain ketahanan terhadap serangan linear dan differentialcryptanalysis, algoritma ini perlu pembuktian apakah layak saat digunakan dalam mode operasi tertentu seperti mode Counter [9]. Mode Counter merupakan salah satu mode operasi yang direkomendasikan sesuai NIST SP 800 - 38 A, dalam mengimplementasikan suatu algoritma block cipher Apakah algoritma CLEFIA dengan mode operasi Counter menghasilkan barisan acak sehingga sulit untuk dianalisis dengan metode statistik. Berdasarkan hal tersebut penulis melakukan pengujian keacakkan sesuai standar NIST SP 800 - 22 terhadap output yang dihasilkan. Algoritma yang diuji dalam paper ini yaitu CLEFIA - 128, yaitu dengan ukuran blok dan kunci sebesar 128 bit. dengan penelitian ini kita dapat menyimpulkan apakah algoritma ini layak digunakan dalam aplikasi kriptografi jika diimplementasikan mode operasi Counter.

3.2 Implementasi

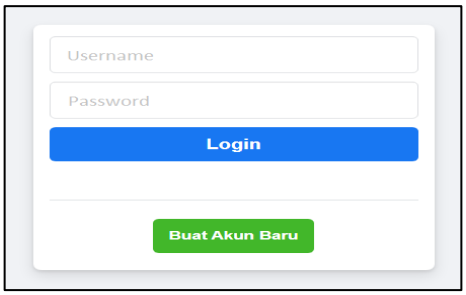
Pada sub bab penelitian yang berhubungan dengan tampilan program penulisan menjelaskan tentang penggunaan input dan output program atau aplikasi yang digunakan untuk mengujipenerapan Clefia 128. Adapun objek yang digunakan untuk di enkripsi dengan Clefia 128 yaitu menggunakan data yang ada pada suatu record table login pada suatu database. Untuk implementasi penulis membangun 3 form website untuk melakukan pengujian terdahap algoritma Clefia 128 yang dimana pembangkitan di enkripsi secara blok, dengan tujuan dapat menghasilakn karakter terenkripsi yang dapat memberikan nilai confolusion terhadap record data.

Berikut tampilan tiga form yang dibangun penulis untuk menguji algoritma Clefia 128 yang telah di modifikasi untuk meningkatkan nilai confusion terhadap record data login pada database.

3.2.1 Tampilan Input

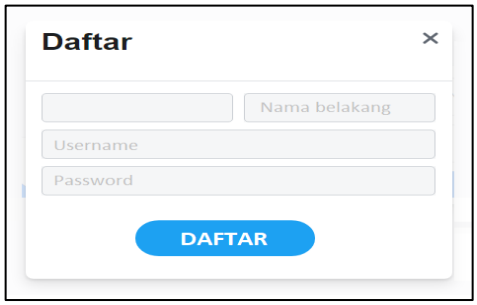
Berikut tampilan tiga form yang dibangun penulis untuk menguji algoritma Clefia 128 yang telah di modifikasi untuk meningkatkan nilai confusion terhadap record data login pada database.

1. Bentuk Tampilan *Form Login*



Gambar 7. Tampilan Form Login

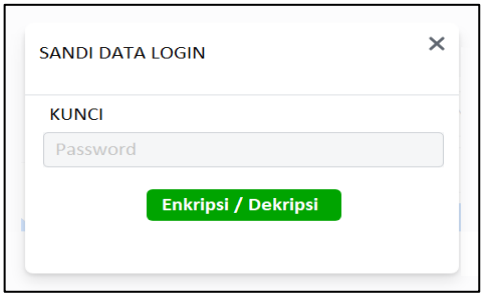
2. Bentuk Tampilan Form *Create New Account*



Gambar 8. Tampilan *Form Create Account Login*

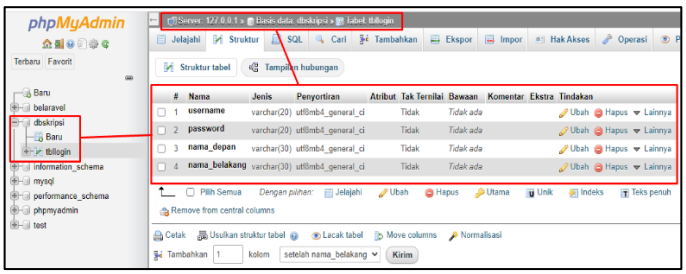
Journal Global Tecnology Computer
Vol 2, No. 1, Desember, 2022, Hal 8 - 15
ISSN: **2809-6118** (Online - Elektronik)
Website https://ejurnal.seminar-id.com/index.php/jogtc

3. Tampilan Form untuk Memasukan Kata Kunci Enkripsi/Dekripsi



Gambar 9. Form Input Key Enkripsi/Dekripsi

4. Tampilan Table Login Pada Phpmyadmin database

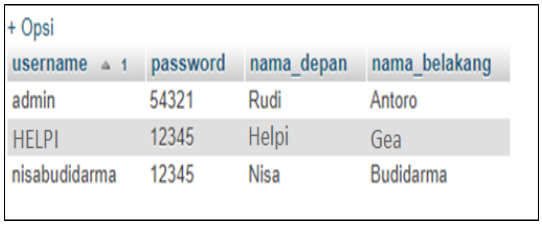


Gambar 10. Tampilan table login dalam database

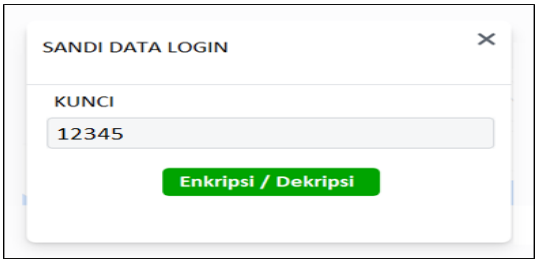
3.2.2 Tampilan Output

Pada sub bab berikut ini penulis menjelaskan bentuk tampilan luaran pada saat melakukan pengujian terhadap penerapan algoritma RC2 yang pembangkitan kunci nya telah di modifikasi dengan menggunakan michali blum generator.

Gambar 11. Form Input Data User Baru

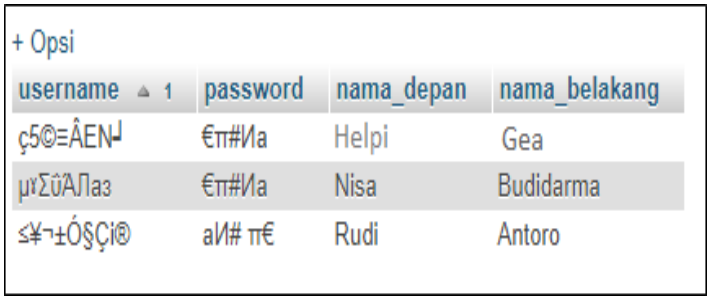


Gambar 12. Bentuk data pada tabel sebelum di enkripsi



Gambar 13. Form Input Data Kunci Proses Enkripsi

Journal Global Tecnology Computer
Vol 2, No. 1, Desember, 2022, Hal 8 - 15
ISSN: **2809-6118** (Online - Elektronik)
Website https://ejurnal.seminar-id.com/index.php/jogtc



+ Opsi

username	password	nama_depan	nama_belakang
ç5©≡ÂEN┘	€π#Иa	Helpi	Gea
µ¥ΣΰÄЛаз	€π#Иa	Nisa	Budidarma
≤¥¬±Ó§Çi®	aИ# π€	Rudi	Antoro

Gambar 14. Bentuk Tampilan Karakter Setelah Proses Enkripsi

3.2.3 Hasil Pengujian Program

Dari beberapa karakter username dan password yang dimasukan dalam form daftar new account login, berikut bentuk karakter yang di hasilkan.

Tabel 2. Hasil Pengujian

Uji	Field	Plaintext	Ciphertext	Keterangan Enkripsi dan Dekripsi
1	Username	HELPI	ç5©≡ÂEN┘	Sukses
	Password	12345	€π#Иa	
2.	Username	admin	µ¥ΣΰÄЛаз	Sukses
	Password	54321	€π#Иa	
3	Username	nisabudidarma	≤¥¬±Ó§Çi®	Sukses
	Password	12345	€π#Иa	

4. KESIMPULAN

Setelah penelitian dilakukan dan hasil pengujian diperoleh, maka penulis dapat menyimpulkan garis besar dari keseluruhan rangkuman skripsi ini ialah Algoritma Clefia 128 dapat diterapkan pada proses pengamanan record login yang menghasilkan bentuk karakter terenkripsi yang sulit untuk dipahami, Algotima Clefia 128 dapat digunakan untuk pengamanan data yang berbasis bit 128dan proses yang sangat cepat karena menggunakan perhitungan yang sederhana. Dan berdasarkan pengujian yang dilakukan terhadap agoritma Clefia 128 dalam mengamankan data yang ada pada record tabel login, Algoritma Clefia 128 mampu memberikan nilai confusion yang cukup baik.

REFERENCES

[1] W. Dewobroto, "Aplikasi Rekayasa Konstruksi dengan Visual Basic 6.0," *Jakarta PT Elex Media Komputindo*, 2005.
[2] S. Mulyani, *Analisis dan Perancangan Sistem Informasi Manajemen Keuangan Daerah: Notasi Pemodelan Unified Modeling Language (UML)*. Abdi Sistematika, 2017.
[3] S. Sumandri, "Studi Model Algoritma Kriptografi Klasik dan Modern," *Semin. Mat. dan Pendidik. Mat. UNY*, pp. 265–272, 2017.
[4] H. Mukhtar, *Kriptografi Untuk Keamanan Data*. Deepublish, 2018.
[5] R. Sadikin, "Kriptografi untuk keamanan jaringan," 2020.
[6] P. D. F. Adobe, "101-quick overview of PDF file format," *Adobe Syst. [cit. 2.5. 2013] Dostupné z http//partners. adobe. com/public/developer/tips/topic tip31. html Lit. Lit.*, 2010.
[7] T. S. Waruwu and K. Telaumbanua, "Kombinasi Algoritma OTP Cipher dan Algoritma BBS dalam Pengamanan File," *J. SIFO Mikroskil*, vol. 17, no. 1, pp. 119–126, 2016.
[8] DjonIrwanto, "No Title," *Peranc. Object Oriented Softw. dengan UML*, 2007.
[9] O. Setiawan, R. Fiati, and T. Listyorini, "Algoritma Enkripsi Rc4 Sebagai Metode Obfuscation Source Code Php," *Pros. SNATIF*, pp. 113–120, 2014.