ALGORITMA: Jurnal Ilmu Komputer dan Informatika
Volume: 07, Number: 01, April 2023 ISSN 2598-6341 (online)

Implementasi Liniear Congruential Generator Pada Pembangkitan Inizialization Vector Pada Kriptografi CBC Sederhana

Sari Kurnia Riski[1], Tommy[2], Arief Budiman[3]

[1,2,3]Program Studi Teknik Informatika Fakultas Teknik dan Komputer
Universitas Harapan Medan
Jl. H.M. Jhoni No 70 Medan, Indonesia
Email: sarikurnia310599@gmail.com

Abstract

In this era of increasingly advanced technology, data security is very important in maintaining the confidentiality of information, especially those containing sensitive information whose contents should only be known by the entitled party, especially if the delivery is made through a public network, if the data is not secured first. , will be very easy to be tapped and the contents of the information known by parties who do not have the authority. One way that is used for data security is to use a cryptographic system, namely by encoding or keying the information content using a data locking algorithm method. Here this author will discuss aboutgenerating IV using the LCG algorithm are combined by XORing everyption method in simpleCBC cryptography where these two algorithm are combined by XORing every bit that exists with the key or block provided. Aims to produce plaintext that has been convertd into ciphertext or secret data.

Keywords : data security, cryptographic algorithm lcg, xor cipher, simple cbc method.

Abstrak

Di era teknologi yang semakin maju ini keamanan data merupakan hal yang sangat penting dalam menjaga kerahasian informasi terutama yang berisi informasi sensitif yang hanya boleh di ketahui isinya oleh pihak yang berhak saja, apalagi jika pengiriman dilakukan melalui jaringan publik, apabila data tersebut tidak diamankan terlebih dahulu, akan sangat mudah disadap dan di ketahui isi informasinya oleh pihak-pihak yang tidak memiliki wewenang. Salah satu cara yang digunaakan untuk pengaman data adalah menggunakan sistem kriptografi yaitu dengan menyandikan atau member kunci pada isi informasi menggunakan metode algoritma pengunci data, disini penulis akan membahas tentang membangkitkan IV menggunakan algoritma LGC dalam metode enkripsi dan pendekripsian di kriptografi CBC sederahana dimana dua algoritma ini disatuka dengan cara mengXOR kan tiap tiap bit yang ada dengan kunci atau blok yang disedikan. Bertujuan untuk menghasilkan palinteks yang sudah di ubah menjadi cipherteks atau data rahasia.

Kata kunci : keamanan data, kriptografi, algoritma lcg, xor cipher,r metode cbc sederhana

1. PENDAHULUAN

Keamanan data merupakan hal yang sangat penting dalam menjaga kerahasian informasi terutama yang berisi informasi sensitif yang hanya boleh di ketahui isinya oleh pihak yang berhak saja, apalagi jika pengiriman dilakukan melalui jaringan publik, apabila data tersebut tidak diamankan terlebih dahulu, akan sangat mudah disadap dan di ketahui isi informasinya oleh pihak-pihak yang tidak memiliki wewenang. Salah satu cara yang digunaakan untuk pengaman data adalah menggunakan sistem kriptografi yaitu dengan menyediakan isi informasi (*plaintext*) tersebut menjadi isi yang tidak dipahami melalui proses enkripsi (*encipher*), dan untuk memproleh kembali informasi yang asli, dilakukan proses (*decipher*), disertai dengan menggunakan kunci yang benar, *cryptografi* merupakan seni dan ilmu yang menyembunyikan informasi dari penerima yang tidak

berhak. Namun pada pengertian modern kriptografi adalah ilmu yang berdasarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasian, keutuhan data dan otentikasi entitas [1]. Pada penelitian (Deny Nugroho Triwibowo, Universitas Harapan Bangsa 2021) yyang berjudul Enkripsi Pesan Menggunakan Algoritma Linier *Congruential Generator* (LCG) dan Konversi Kode *Morse* menyatakan bahwa, hasil yang didapatkan dari modifikasi algoritma LCG dan konversi kode *morse* dapat membantu untuk proses kriptogarfi yang membuat hasil enkripsi pesan cukup susah untuk dibaca karena dalam proses enkripsi pesan tiap-tiap karakter *plaintext* akan dikonversikan dengan tanda titik (.) dan tanda kurang (-) pada cipherteksnya. pada penelitian terdahulu LCG masih digunakan sebagai kunci acak pada pesan. *Cipher Block Chaining* adalah salah satu pengembangan dari algoritma *Block Cipher*, algoritma ini akan membagi-bagi teks terang yang akan dikirimkan dengan ukuran tertentu (disebut blok) dengan panjang bit tiap blok sesuai dengan panjang bit pada kunci, dan setiap blok dienkripsikan dengan menggunakan kunci yang sama, tahapan proses enkripsi algoritma (CBC) adalah dengan carameng-XOR kan blok plainteks dengan *inizialization vector* (IV). Hasil XOR yang didapat diawal kemudian akan dilakukan XOR kembali dengan menggunakan kunci sehingga menghasilkan cipherteks untuk blok pertama.cipherteks di blok pertama selanjutnya digunakan sebagai (IV) untuk enkripsi pada blok selanjutnya [2].

2. METODOLOGI PENELITIAN

Adapun metodologi yang digunakan dalam penelitian ini adalah :

a) Studi Literatur

Studi Literatur merupakan proses pengumpulan sumber dengan mengumpulkan artikel dan jurnal yang berhubungan dengan penelitian.

b) Analisis Data

Anlisis data diperlukan untuk menentukan kebutuhan data.

c) Perancangan

Perancangan yaitu proses dalam merancang program yang akan di jalankan dalam penelitiaan ini.

3. HASIL DAN PEMBAHASAN

a) Kriptografi

merupakan seni dan ilmu menyembunyikan informasi dari penerima yang tidak berhak. Kata *Cryptography* berasal dari kata Yunani *kripto*s (tersembunyi) dan *Graphein*. Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian modern kriptografi adalah ilmu yang berdasarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasian, keutuhan data dan otentikasientitas [3].

b) Cipher Block Chaining

Cipher Block Chaining adalah salah satu pengembangan dari algoritma *Block Cipher*, algoritma ini akan membagi-bagi teks terang yang akan dikirimkan dengan ukuran tertentu disebut *block* dengan panjang bit tiap *block* sesuai dengan panjang bit pada kunci, dan setiap block dienkripsikan dengan menggunakan kunci yang sama, tahapan proses enkripsi algoritma (CBC) adalah dengan carameng-XOR kan blok plainteks dengan *inizialization vector* (IV). Hasil XOR yang didapat diawal kemudian akan dilakukan XOR kembali dengan menggunakan kunci sehingga menghasilkan cipherteks untuk blok pertama.cipherteks di blok pertama selanjutnya digunakan sebagai (IV) untuk enkripsi

pada blok selanjutnya.
Metode CBC ini menutupi kelemahan dari mode operasi ECB karena pada CBC dapat menyembunyikan pola dari plainteks , mengapa demikian? Karena sebelum dienkripsikan, plainteks di xor kan dengan IV atau cipherteks sebelumnya, sehingga plainteks yang sama belum tentu menghasilkan cipherteks yang sama, kecuali jika memiliki IV/ Cipherteks sebelumnya yang sama. Kelemahan dari CBC adalah untuk mendekripsikan cipherteks,

c) Xor Cipher

XOR merupakan salah satu operaor yang amat terkenal selain AND dan OR. Saya mengenal operator XOR ketika praktik rangkaian digital untuk membuat simulasi lampu LED. Lebih detail, saya menerapkan XOR untuk pemodelan proses bisnis, dimana arus proses dalam model harus memilih salah satu cabang jika ditemukan percabangan XOR. Bahkan kali ini, XOR dapat kita jadikan sebagai algoritma untuk kriptografi. Populer dengan sebutan XOR *Chiper*. Meskipun simpel, tapi amat mumpuni.
Secara umum, nilai *true* dan *false* pada operator XOR saya rangkum sebagai berikut:
Jika 0 XOR 0 maka 0 (*false*)
Jika 1 XOR 0 maka 1 (*true*)
Jika 0 XOR 1 maka 1 (*true*)
Jika 1 XOR 1 maka 0 (*false*)
Tujuan untuk memahami cara menghitung XOR *chiper* secara manual beserta peneraannya dalam program.XOR *chiper* meliputi perhitungan untuk melakukan enkripsi dan deskripsi. Enkripsi yaitu proses untuk membentuk *chipertext*, atau teks yang telah terenkripsi. Teks enkripsi bisa dikembalikan ke asalnya jika sudah di deskripsi. Syaratnya, proses enkripsi dan deskripsi harus menggunakan kunci yang sama.

d) ASCII

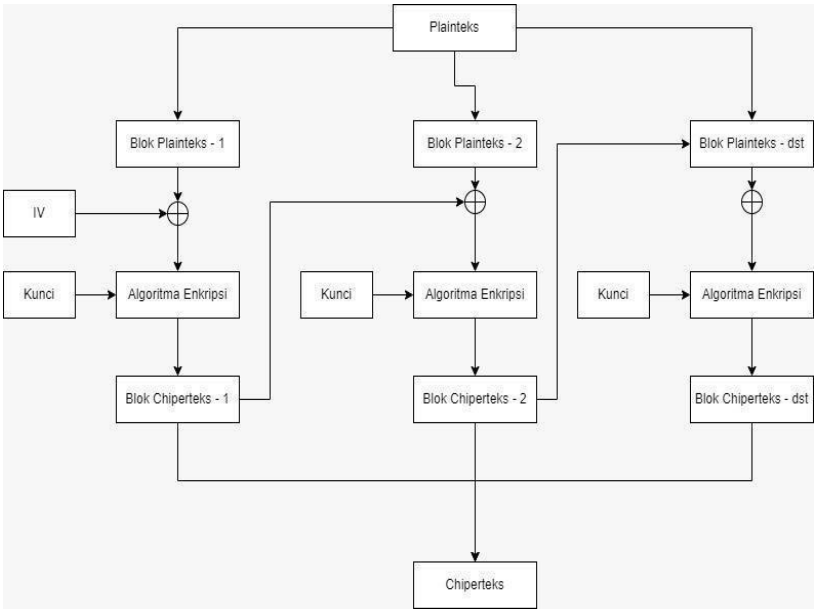
Komputer merupakan salah satu penemuan terbesar dalam peradapan manusia. Dengan adanyakomputer berbagai aspek kegiatan bisa dilakukan dengan mudah. Tidak hanya itu, komputer juga bisa melakukan hal-hal yang sulit dikerjakan bagi manusia. Komputer bekerja dengan bahasa pemrograman yang rumit dan kompleks. Komputer sebenarnya memiliki bahasa tersendiri yang berbeda dengan manusia. Akan tetapi sebenarnya bahasa komputer hanya terdiri dari angka 0 dan 1.
Kode ASCCI mempresentasikan kode – kode untuk :
1. Angka (0, 1,2,3,4,5,6,7,8,9)
2. Huruf (a-z, A-Z)
3. Simbol (&, ^, %, $, @,.)
4. Tombol (Enter, Esc, Backspace, Space, Tab, Shift, Ctrl)
5. Karakter Grafis (Kode ASCCI Standar nomor 128 s/d 255)
6. Kode Komunikasi (ETX, STX,ENQ,ACK)

e) Visual Basic 2010

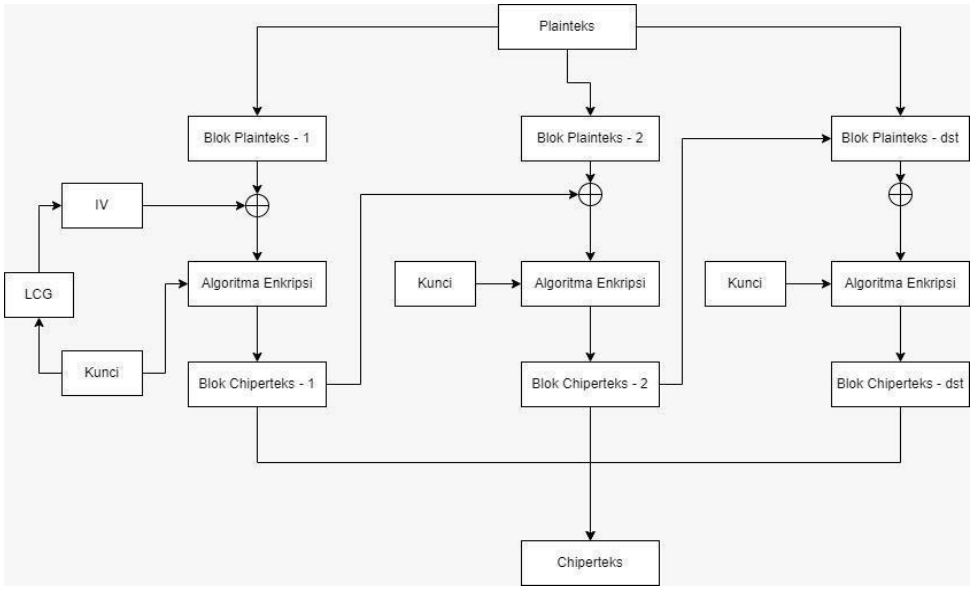
Microsoft Visual Studio 2010 atau biasa disebut VB .Net 2010 merupakan salah satu aplikasi yang sering digunakan oleh para *programer* yang sifatnya berbasis *Windows*, maka dari itu alangkah baiknya sebelum belajar lebih jauh mengenai VB .Net 2010 anda mengetahui dulu pengertian, keistimewaan dan juga sejarah dari *Microsoft Visual Studio* 2010. Pengertian *Microsoft Visual Studio* 2010, pada dasarnya adalah sebuah bahasa pemrograman komputer. Dimana pengertian dari bahasa pemrograman itu adalah perintah-perintah atau instruksi yang 32 dimengerti oleh komputer untuk melakukan tugas-tugas tertentu. Visual Studio 2010 yang sering juga disebut dengan VB .Net 2010 selain disebut

dengan bahasa pemrograman, juga sering disebut sebagai sarana *tool* untuk menghasilkan program-program aplikasi berbasiskan *Windows.* Beberapa kemampuan atau manfaat dari Visual Studio 2010 diantaranya seperti : 1 Untuk membuat program aplikasi berbasiskan *Windows.*

Berikut ini adalah gambar diagram alur proses dari yang sederhana sampai proses yang diinginkan :



Gambar 1. Diagram Alur Proses Sederhana

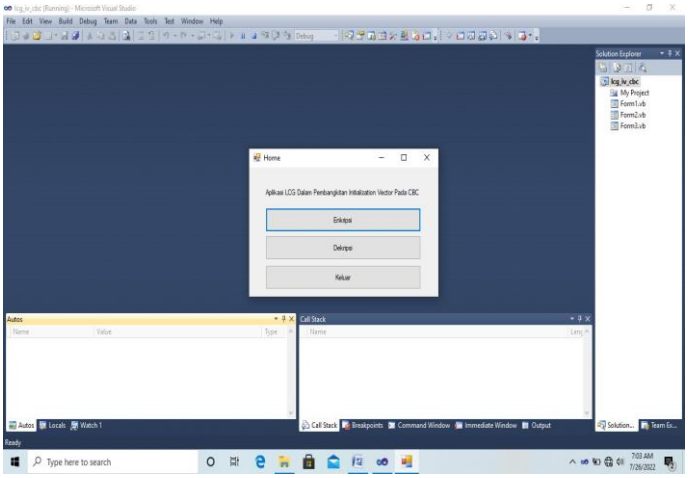


Gambar 2. Diagram Alur Proses yang Diinginkan

f) Implementasi Sistem

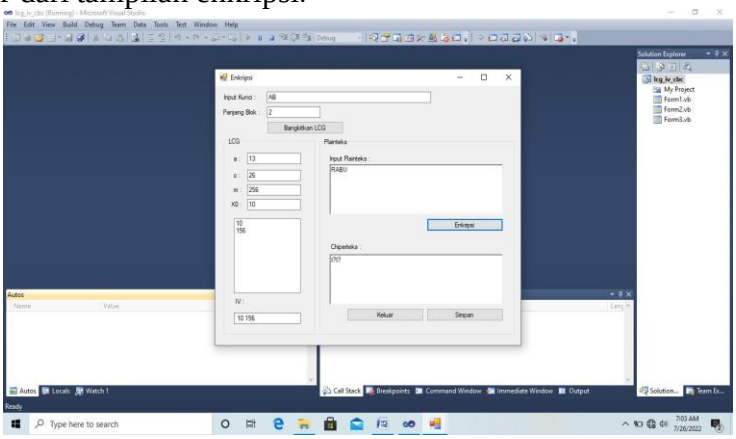
Berikut adalah tampilan dari Liniear Congruential Generator Pada pembangkitan Inizialization Vector pada kriptografi CBC :

Tampilam *Home* adalah tampilan awal dalam melakukan tahapan – tahapan pengujian. Berikut ini adalah gambar dari tampilan *Home*



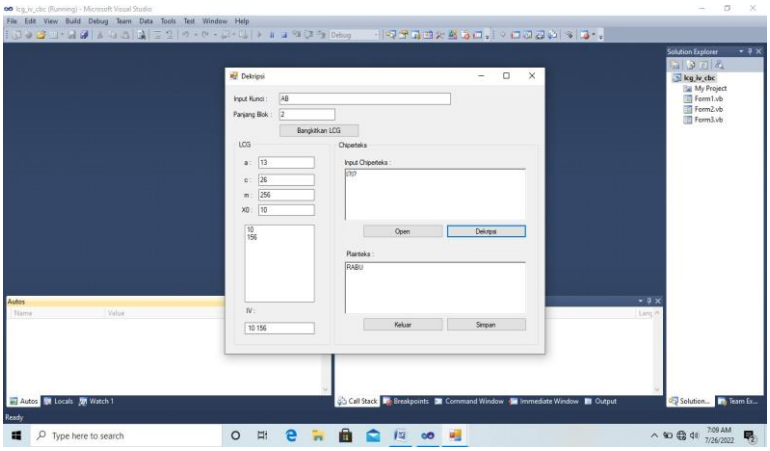
Gambar 3. Tampilan Home

Tampilan Enkripsi adalah tampilan dalam melakukan proses pengenkripsian teks.Berikut ini adalah gambar dari tampilan enkripsi.



Gambar 4. Tampilan Enskripsi

Tampilan Dekripsi adalah tampilan dalam melakukan proses pendekripsian teks.Berikut ini adalah gambar dari tampilan dekripsi



Gambar 5. Tampilan Deskripsi

Dan yang terakhir adalah Pengujian Teks dan Kunci

Plainteks	Kunci	LCG	IV	Cipherteks	Dekripsi balik	Status
JIKA BENAR	GHIJ	a : 40 c : 30 x0: 100	100 190 206 78	I??El?? Ny??$	JIKA BENAR	Berhasil
YUDA	SA	a : 12 c : 54 x0: 21	21 50	&‖&	YUDA	Berhasil
SARI	AB	a : 13 c : 26 x0: 156	156 6	?‖?‖	SARI	Berhasil
SEMANGAT	MNOP	a : 25 c : 35 x0: 50	50 5 160 195	.‖??/‖??	SEMANGAT	Berhasil
SUDAHISAJA	SDHSS	a : 10 c : 5 x0 : 15	15 155 19 195 163	‖? ??‖?‖??	SUDAHISAJA	Berhasil

4. KESIMPULAN

Berdasarkan hasil dari pengujian yang telah dilakukan, pada Implementasi LCG pembangkit IV dengan kriptografi CBC sederhana, dapat ditarik kesimpulan seperti berikut:

- Pemanfaatan pengujian pada implementasi ini sangat bermanfaat untuk masyarakat atau perusahaan yang bekerja dalam bidang transmisi data.
- Dengan memanfaatkan teknologi informasi kususnya kriptografi, sangat membantu untuk mengamankan sebuah data atau informasi yang bersifat kusus atau privasi.
- Pada pengujian ini kita tahu bahwa data yang menggunakan dua algoritma dari LCG dan CBC ini tidak mudah untuk dibaca atau dimengerti oleh orang yang tidak bersangkutan dan menambah kekuatan dalam melindungi kerahasian pesan.

Hal yang diutamakan dalam pembuatan program yang di uji ini adalah bagaimana caranya agar data atau pesan tetap aman dari si pengirim pesan dan sampai ke penerimapesan tanpa ada yang mengetahui apa isi dari data atau pesan tersebut.

DAFTAR PUSTAKA

Abood, O. G., & Guirguis, S. K. (2018). A Survey on Cryptography Algorithms.International Journal of Scientific and Research Publications (IJSRP), 8(7). https://doi.org/10.29322/ijsrp.8.7.2018.p7978

Agustina Felisia. (2020) https://caraharian.com/kode-ascii-adalah.html#

Deny Nugroho Triwibowo. (2021) Enkripsi Pesan Menggunakan Algoritma LiniearVol.3.No.3. http://doi.org/10./2928/biste.v313.5546

Devi Andriani (2017) Perancangan Aplikasi Penyandian Teks Dengan Menggunakan Algoritma Chiper Block Chaining. *Jurnal Teknik Informatika Unika St. Thomas*

(JTIUST), Volume 02 Nomor 02, Desember 2017, ISSN : 2548-1916

Dropbox.(2021) https://experience.dropbox.com/id-id/resources/flowcharts

Dwi Latifatul Fajri (2022). https://katadata.co.id/agung/digital/62a8742d8c024/flowchart-adalah-bagan-alir-berikut-pengertian-dan-jenisnya

Hak Cipta © 2022 KK. https://www-crypto--it-net.translate.goog/eng/theory/pseudorandom-generator.html?_x_tr_sch=http&_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=sc

Helmi Sahara.(2018) Implementasi Pengamanan Pesan Chatting Menggunakan Metode Vigenere Cipher dan Cipher Block Chaining. *Jurnal Means.* Vol 3. No.2, http://ejournal.ust.ac.id/indexphp/jurnal_Means

Kita Informatika (2018). http://www.kitainformatika.com/2018/07/algoritma-xor-chiper- untuk-mengatasi.html

Kurniawan (2017) Apa yang dimaksud dengan Inizialization Vector. https://www.dellenpedia.com/2017/07/apa-yang-dimaksud-dengan-initialization.html?m=1

Maya utami dewi,M.Kom (2021) Universitas Stekom. http://sistem-informasi-s1.stekom.ac.id/informasi/baca/JENIS-JENIS-KEAMANAN-DATA/15d1ee116284b85e5de3e00564518367fe994de7

Muhammad Robith Adani (2021) blog programming. https://www.sekawanmedia.co.id/blog/pengertian-kriptografi/

OMG. (2017) Pengertian Use Case Diagram. *Unified Modeling Language*

Rachmat Aulia, dkk.(2019) Penerapan Algoritma One Time Pad dan Liniear Congruential Generator Untuk Keamanan Pesan Teks. *Jurnal Nasional Informatika dan Teknologi Jaringan.*Vol.4 No.1. Avalible Online at : http://bit.ly/InfoTekjar

Sebastian Suhandinata, dkk. (2019) Analisa Performa Kriptografi Hybrid Algoritma Blowfish dan Algoritma RSA. *Jurnal Teknologi Informasi*, VI(01):1-10. Doi: http://doi.10.33330/jurteksi.v6i1.395

Waruwu, T.S.,dan Nasution,S. (2018) Pengembangan Keamanan Web Login Portal DosenMenggunakan UML. *Jurnal Mahajana Informasi*, 3(1) 34-40.

Wikipedia.(2022) https://en-m-wikipediaorg.translate.goog/wiki/Linear_congruential_generator?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=tc,sc

123dok.com.https://text-id.123dok.com/document/ozll1rooz-pengertian-microsoft-visual-studio-2010-sejarah-singkat-microsoft-visual-studio-2010.html