Jurnal Pendidikan Sains dan Komputer

Jurnal Pendidikan Sains and Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1381

Implementasi Mode Operasi Kombinasi Cipher Block Chaining dan Metode LSB-1 Pada Pengamanan Data text

Melani Afsari[1)], Dadang Iskandar Mulyana[2)], Alfiani Damaiyanti[3)], Naini Sa'adah[4)]
[1] Fisikom, Sistem Informasi, Stikom CKI, Jakarta, Indonesia
[1]melaniafsari012@gmail.com, [2]mahvin2012@gmail.com, [3]alfianidmynt17@gmail.com,
[4]nainisaadah09@gmail.com

***Penulis Korespondensi**

Histori Artikel:
Submit: 2022-02-16
Diterima: 2022-02-17
Dipublikasikan: 2022-02-17

Kata Kunci:
Cipher Block Chaining, Least Significant Bit, Internet, Keamanan, Informasi.

ABSTRAK

Pengamanan data text diperlukan untuk menjaga informasi yang dirahasiakan agar tidak diketahui oleh orang lain kecuali orang yang diberihak untuk itu. Salah satu cara untuk mengamankan data tersebut yaitu dengan mengkombinasikan Cipher Block Chaning (CBC) dan Metode Least Significant Bit (LSB-1) pada pengamanan data text. Cipher Block Chaning memiliki kecepatan dan efisiensi lebih tinggi dan dinilai lebih mudah diimplementasikan. Sedangkan metode Steganografi Least Significant Bit mampu bekerja secara sederhana namun sangat efektif dalam menyisipkan pesan tersembunyi. Namun, beberapa peneliti dapat menemukan kekurangan pada metode LSB. Oleh karna itu LSB harus dikembangkan lagi. Melalui kombinasi Cipher Block Chaning dan Least Significant Bit-Sobel telah terbukti serta berhasil merahasiakan pesan dengan baik dan menghasilkan steganografi yang berkualitas tinggi setelah dilakukan pengujian Peak Signal-to-Noise Ratio (PSNR) dan Mean Square Error (MSE). Proses hasil dari uji coba yang kami lakukan adalah Tahapan penelitian, Diagram Proses Kombinasi CBC dengan LSB-1, ubah karakter huruf menjadi biner, ubah angka menjadi biner, Proses Penukaran Bit Ke-7 (LSB-1) Citra Cover, biner hasil penggabungan antara Blok I Dan Blok II diubah menjadi sebuah kata, mengubah biner menjadi desimal, mengubah desimal menjadi huruf. Selain itu kami juga mebuat program sederhana yang dapat digunakan untuk melakukan proses enkripsi secara otomatis.

LATAR BELAKANG

Seiring berkembangnya teknologi, manusia dapat berkomunikasi lewat berbagai media digital. Kerahasiaan data untuk mengirim informasi menjadi hal yang penting karna menyangkut privasi individu. Para pengguna media digital ingin datanya dilindungi dari orang orang yang tidak berkepentingan. Sehingga keamanan suatu data perlu ditingkatkan, salah satu caranya adalah enkripsi data.

Salah satu metode kriptografi moderen yang memiliki kemampuan cukup handal adalah Cipher Block Chaining (CBC). Proses enkripsi dan dekripsi Cipher Block Chaining memerlukan waktu yang singkat karna metode Cipher Block Chaining (CBC) memiliki kecepatan dan efisiensi yang lebih tinggi dan dinilai lebih mudah di implementasikan. Operasi Cipher Block Chaining (CBC) merupakan algoritma moderen yang beroperasi pada level bit (0 atau 1) maupun sekelompok atau blok bit dan bukan karakter. Penggunaan mode Cipher Block Chaining (CBC) menghasilkan ciphertext yang rumit karena pada tiap blokknya saling bergantung sehingga sebuah kesalahan dalam satu blok akan mempengaruhi blok-blok berikutnya selama proses dekripsi data. Mekanisme mode Cipher Block Chaining (CBC) bekerja efektif untuk meningkatkan keamanan dalam menyediakan kerahasiaan data yang tinggi dan otentikasi. Untuk operasi Cipher Block Chaining (CBC) menerapkan cara kerja umpan balik pada sebuah blok bit dimana hasil dari proses enkripsi blok pertama digunakan untuk initialization vector pada blok berikutnya dan

Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1381

dilakukan secara berulang sampai blok bit terakhir. Hal ini menyebabkan blok pada hasil enkripsi akan saling bergantung.

Teknik kriptografi digunakan untuk melakukan penyandian pesan rahasia berdasarkan mode operasi cipher block chaining dan teknik steganografi digunakan untuk menyembunyikan pesan terenkripsi ke dalam sebuah citra digital berdasarkan algoritma least significant bit-1. Agar proses yang dilakukan lebih mudah, maka dibangun sebuah aplikasi pengamanan pesan rahasia menggunakan bahasa pemrograman visual basic 2008(Ismadiah, Syahrizal, & Ramadhani, 2020).

Teknik steganografi ialah teknik lain yang dipakai untuk menyembunyikan pesan rahasia pada objek lain misalnya citra digital, audio dan video. Metode steganografi digunakan dengan cara menukarkan bit tertentu dari citra digital penampung pesan dengan bit pesan rahasia yang akan disembunyikan. Langkah penukaran bit citra digital penampung dengan bit-bit pesan rahasia dapat dilakukan dengan melakukan modifikasi metode Least Significant Bit (LSB). Metode ini disebut dengan metode Least Significant Bit-1 (LSB-1) yang memiliki cara yang sama dengan menyembunyikan data teks tersandi tersebut ke dalam citra cover berdasarkan metode. (Login Website et al., 2018)

Setiap algoritma memiliki tingkat keamanan yang berbeda-beda, begitu juga dengan tingkat komplektifitas yang berbedabeda pula. Algoritma dengan tingkat keamanan yang tinggi dan dengan komplektifitas yang rendah akan sangat baik untuk diterapkan, hal ini dikarenakan proses enkripsi dan deskripsi menjadi jauh lebih cepat dan hanya memakan sumber daya komputer yang rendah. CBC (Cipher Blok Chaining) ialah salah satu mode operasi blok cipher, dimana hasil enkripsi dari blok pesan sebelumnya akan digunakan sebagai initial vektor untuk mengacak blok pesan selanjutnya sebelum dienkripsi dengan kunci yang digunakan. Sehingga pada mode operasi CBC, plain text akan diproses sebanyak dua kali untuk menjamin tidak adanya pemetaan dari setiap blok cipher text, sehingga jika intruder memiliki potongan dari plain text, namun hal tersebut tidak akan banyak membantu.(Sinta Peringkat, Dirjen Penguatan RisBang Kemenristekdikti, Wati, Sa, & Ariyus, n.d.).

Kelemahan pada metode LSB ini dapat dikurangi dengan menerapkan sebuah metode tambahan yaitu metode pendeteksian tepi. Teknik yang paling umum dipakai untuk mendeteksi tepi pada greylevel yaitu metode pendeteksian tepi. Mendeteksi keypoint penyisipan pesan sehingga LSB tidak lagi bekerja secara standar yaitu menggunakan metode deteksi tepi. Deteksi tepi digunakan untuk menyebarkan lokasi keypoint penyisipan pesan sehingga akan lebih sulit dideteksi oleh pihak yang tidak berkepentingan. Ada beberapa teknik deteksi tepi, salah satunya ialah deteksi tepi Sobel yang memiliki kemampuan mengurangi tingkat noise sebelum melakukan perhitungan pendeteksian tepi. Dari latar belakang tersebut, peneliti berupaya melakukan modifikasi dengan menggunakan model kombinasi kriptografi dan steganografi untuk dapat meningkatkan pengamanan pesan dan penyembunyian informasi yang mana akan dijelaskan secara detail pada bab selanjutnya.(Mahmud, Mintorini, & Kadiri Kediri Jawa Timur Indonesia, n.d.)

STUDI LITERATUR

Kriptografi

Kriptografi (cryptography) dari asal bahasa yunani, yaitu dari istilah cypto serta graphia yg berarti penulisan misteri. Kriptografi artinya ilmu ataupun seni yang menelaah bagaimana menghasilkan suatu pesan yang dikirim oleh pengirim dapat disampaikan kepada penerima menggunakan safety. Kriptografi juga adalah studi terhadap teknik matematis yang terkait menggunakan aspek keamanan suatu sistem

Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1381

informasi[6] Algoritma kriptografi menjadi sebuah langkah logis dalam penyembunyian pesan dari orang yang tidak memiliki izin untuk melihatnya hal ini dilakukan dengan menggunakan metode enkripsi dan dekripsi.[7]

Ada pun aspek aspek krriptografi sebagai berikut :

1. Authority, mengamankan informasi dari orang orang yang tidak memiliki izin untuk melihatnya.
2. Integrity, informasi yang didapat akan dipastikan tidak berubah.
3. Authentication, proses yang saling berhubungan dengan pengguna serta mengindentifikasi kebenaran data.

Nonrepudation, penerima serta pengirim tidak dapat mengelak atas informasi yang telah mereka kirim. [8]

Steganografi

Metode Steganografi adalah teknik yang digunakan untuk menyumbunyikan data rahasia sehingga tak seorang pun selain penerima dan pengirim yang dapat mengetahui informasi tersebut. Steganografi merupakan 2 suku kata dalam bahasa yunani yakni stegonos yang artinya penyamaran dan graphein yang artinya tulisan. Jadi steganografi dapat diartikan sebagai seni penyembunyian pesan dalam data lain tanpa mengubah isi pesan didalamnya [9]

Metode Cipher Block Chaining (CBC)

prosedur pemecahan Cipher Block Chaining (CBC) artinya penerapan prosedur umpan balik pada blok *bit* dimana hasil enkripsi blok sebelumnya diumpan balikkan kedalam proses enkripsi blok *current.* Caranya, blok plaintext yg current di-XOR-kan terlebih dahulu menggunakan blok ciphertext enkripsi sebelumnya. Kemudian hasil peng-XOR-an ini masuk ke dalam fungsi enkripsi. dengan Cipher Block Chaining, setiap blok ciphertext tidak bergantung pada blok plaintextnya tetapi juga pada seluruh blok plaintext sebelumnya. Dekripsi dilakukan dengan memasukkan blok ciphertext yang current ke fungsi dekripsi, kemudian meng-XOR hasilnya dengan blok ciphertext sebelumnya. Blok ciphertext sebelumnya berfungsi sebagai umpan maju (*feedforward*) pada akhir proses dekripsi[10]

Metode Least Significant Bit (LSB)

Metode LSB merupakan metode steganografi yang paling sederhana serta mudah diimplementasikan. Metode LSB ini menggunakan citra digital sebagai covertext. Pada susunan bit di dalam sebuah byte (1 byte = 8 bit), ada bit yang paling berarti most significant bit atau MSB dan bit yang paling kurang berarti atau least significant bit. Sebagai contoh byte 11010010, angka bit 1 pertama ialah bit MSB, dan angka bit 0 terakhir ialah bit LSB. Bit yang cocok untuk diganti adalah bit LSB, sebab perubahan tersebut hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya.[11]

Kombinasi mode operasi Cipher Block Chaining dan Metode Least Significant Bit

Proses enkripsi dengan mode cipher block chaining:

1. Siapkan teks yang akan digunakan, lalu konversikan data teks menjadi biner
2. Bagikan *plaintext* menjadi blok yang jumlah bit-nya telah ditentukan

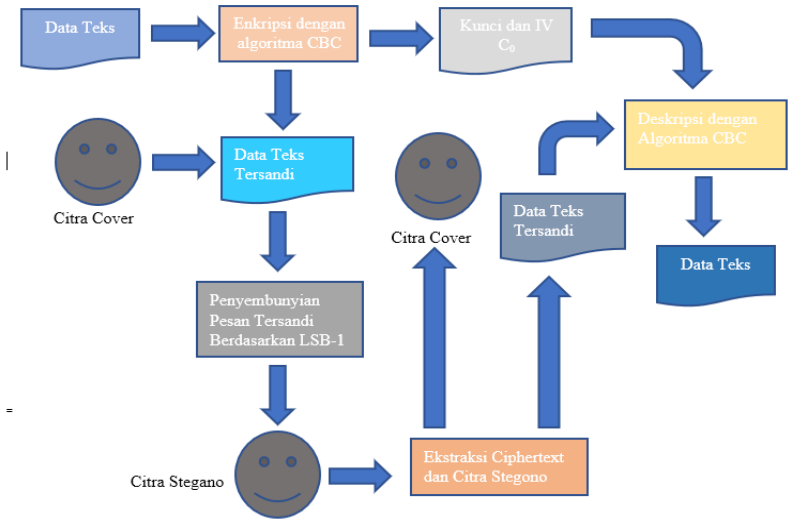
Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1381

3. Masukan nilai biner *initialization* vector/C0
4. Masukan nilai biner kunci
5. Lalu blok *plaintext* yang telah dibagi akan XOR-kan dengan *Initial Vector* (IV/C0) yang telah ditentukan sebelumnya (jika blok awal). Apabila blok *plainteks* yang kedua dan seterusnya, maka nilai IV/C0 yang digunakan adalah nilai cipher block sebelumnya (nilai biner Ci-1).
6. Hasil XOR pada langkah e di XOR kembali dengan kunci yang telah ditentukan sebelumnya
7. Hasil XOR pada langkah f digeser satu bit ke kiri
8. Hasil XOR pada langkah g merupakan cipher block akhir
9. Proses e – g diulang hingga seluruh blok planteks berakhir
10. . Konversikan nilai biner cipher block hasil proses e – g menjadi karakter dan inilah yang menjadi ciphertext akhir.

Adapun proses yang dilakukan untuk meyembunyikan (embeding) informasi pada suatu media berdasarkan metode least significant bit-1 adalah sebagai berikut :

1. Siapkan informasi yang akan disembunyikan misalnya data teks, kemudian konversikan menjadi biner
2. Siapkan kunci proses steganografi (stegano key), kemudian konversikan menjadi biner
3. Siapkan media penyembunyi (cover) misalnya citra digital, kemudian konversikan menjadi biner
4. Lakukan proses pengecekan apakah media penampung informasi mampu menampung sejumlah informasi yang akan disembunyikan atau tidak. Apabila tidak dapat ditampung, maka harus dipilih media penampung yang lebih besar.
5. Lakukan proses penukaran masing-masing bit ke-7 dari bit-bit media cover dengan bit-bit informasi yang akan disembunyikan
6. Simpan hasil steganografi (media stegano) ke dalam media penyimpanan.

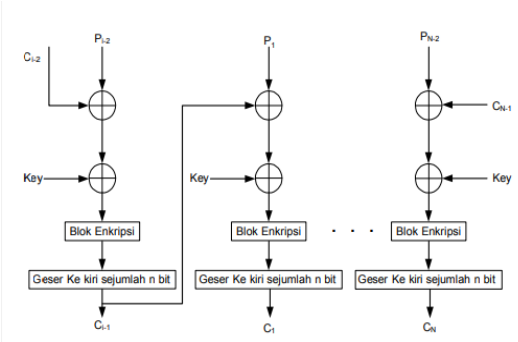
Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1381



Gambar 1.Proses Kombinasi CBC dengan LSB-1

Proses Enkripsi dan Deskripsi pada Kombinasi CBC dengan LSB-1

a. Proses Enkripsi



Gambar 1.Proses Enkripsi

Secara metematis, proses enkripsi dan dekripsi berdasarkan algoritma CBC dapat diformulasikan menjadi : Enkripsi : Ci = Ek (Pi Ci -1) dan Dekripsi = Pi= Dk (Ci – Ci-1)

nilai C0 atau initial vector ditetapkan sendiri oleh pengguna dengan catatan jumlah bitnya harus sama dengan jumlah bit kunci yang digunakan.

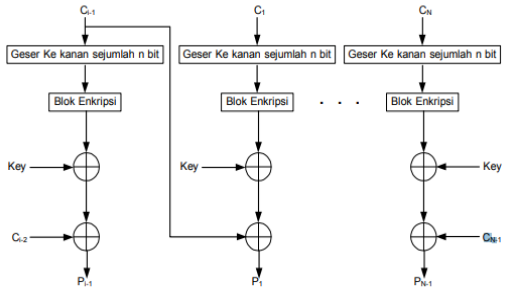
Metode Least Significant Bit (LSB) ialah salah satu metode penyembumyian pesan pada citra yang dipakai pada umumnya serta mudah untuk diimplementasikan, namun metode ini memiliki kerentangan dan kemudahan dalam penghancuran pesan yang telah disembunyikan. Salah satu kelemahan utama dari penerapan metode LSB ini adalah penyusup dapat langsung mengubah bit akhir dari setiap byte pixel medium penampung pesan, dengan cara ini maka pesan yang telah disembunyikan akan mudah diungkap dan dapat mengubah kualitas medium penampung pesan (Joshi, Gagnani, & Pandey, 2013)

Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1381

Kelemahan penerapan metode Least Significant Bit (LSB) di atas, dapat diatasi dengan melakukan pemodifikasian terhadap. Modifikasi LSB dilakukan dengan merubah posisi bit-bit medium pesan yang akan ditukarkan dengan bit pesan yang akan disembunyikan. Beberapa metode hasil modifikasi Least Significant Bit (LSB) meliputi LSB-1, LSB-2, LSB-3.

Least Significant Bit-1 (LSB-1), bekerja dengan teknik menukarkan bit citra penampung dimana posisi bit yang ditukar adalah bit ke 8-1 (bit ke-7). Contoh, asumsikan representasi biner pixel citra sebagai berikut : hasil enkripsi blok sebelumnya diumpanbalikkan ke dalam proses enkripsi blok current. Caranya adalah blok plaintext yang current di- XOR-kan terlebih dahulu dengan blok ciphertext hasil enkripsi sebelumnya, selanjutnya hasil peng-XOR-an ini masuk ke dalam fungsi enkripsi. Dengan algoritma CBC, setiap blok ciphertext tidak hanya bergantung pada blok plaintext-nya tetapi juga pada seluruh blok plaintext sebelumnya. Dekripsi dilakukan dengan memasukkan blok ciphertext yang current ke fungsi dekripsi, kemudian meng-XOR-kan hasilnya dengan blok ciphertext sebelumnya. Dalam hal ini, blok ciphertext sebelumnya berfungsi sebagai umpan maju (feedforward) pada akhir proses dekripsi.

b. Proses Dekripsi



Gambar 2.Proses Dekripsi

11110101 00010110 10101010

11000100 11111001 00000001

00000001 11110001 00011101

karakter T dalam biner = 01010100, maka akan dihasilkan citra hasil dengan urutan bit akhir sebagai berikut :

11110101 00010110 10101000

11000110 11111001 00000001

00000001 11110011 0001110

Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1381

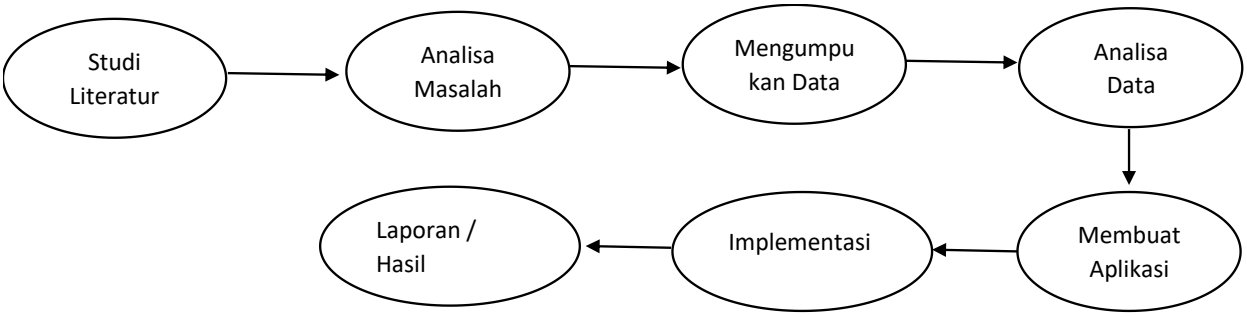
METODE

Metode Pengumpulan Data

Metode penelitian menggunakan studi literatur. Studi literatur merupakan studi yang menggunakan bahan sebagai referensi tertulis untuk mengumpulkan data dengan membaca seperti buku, skripsi, jurnal dan berbagai sumber sumber internet manapun yang berkaitan dengan Algoritma Cipher Bolck Chaining (CBC) dan Least Significant Bit (LSB). Adapun teknik analisa data Miles and Huberman terdapat tahapan-tahapan pengumpulan data,reduksi data,penyajian data dan penarikan kesimpulan atau verifikasi.

Rancangan Penelitian

Dalam penelitian ini penulis menggunakan gambaran berupa diagram dan table. Diagram tersebut menjelaskan bagaimana proses awal untuk log in, mengdeskripsikan dokumen, mengenkripsikan dokumen sampai proses tersebut selesai. Dan untuk tabel menjelaskan bagaimana hasil uji pada aplikasi tersebut.



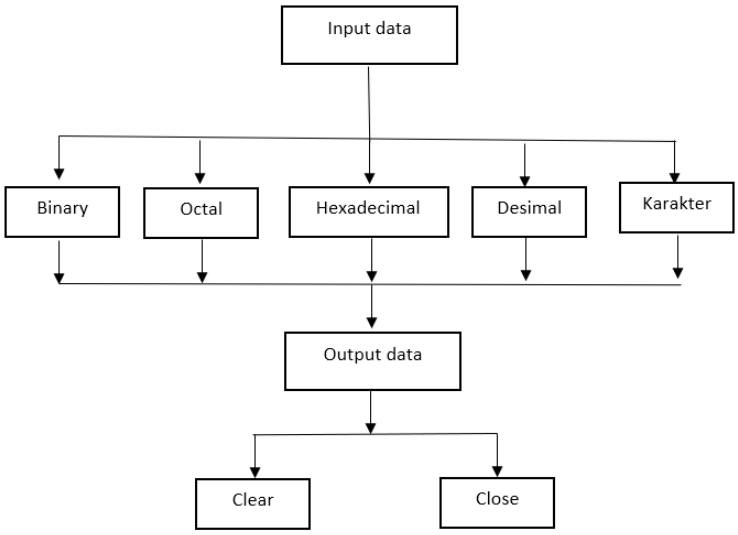
Gambar 1. Tahapan Penelitian

Tahapan penelitian dimulai dari literatur penelitian lalu Analisa masalah serta mengumpulkan data data dan menganalisis data.Selanjutnya membuat membuat aplikasi lalu di implementasikan.Tahapan terakhir yaitu laporan atau hasil..

Rancangan Aplikasi

Penelitian ini penulis merancang sebuah aplikasi proses enkripsi dan deskripsi pada dokumen berbasis web menggunakan Bahasa pemrograman yaitu PHP (Hypertext Preprocessor)

Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1381



Gambar 2. Tampilan rancangan aplikasi

Rancangan aplikasi ini di mulai dari input data yang akan di gunakan . selanjutnya kalian bisa memilih ingin tombol Binary, Octal, Hexadecimal, Desimal, Karakter untuk mengubah data sesuai dengan yang pengguna butuhkan. Selelah mengklik salah satu tombol maka akan keluar hasil nya. Lalu jika pengguna ingin menggunakan kembali aplikasi tersebut dengan biner atau teks yang berbeda mereka cukup mengklik tombol clear untuk menghapus sebelumnya lalu setelah data tersebut hilang anda bisa menggunakan kembali. Selanjutnya jika pengguna sudah tidak memakai aplikasinya maka mereka cukup mengklik tombol close maka otomatis aplikasi akan keluar.

HASIL

Blok I & Blok II	01001101 01000101 01001100 0100001 01001110 01001001					
Pengelompokan	01001101	01000101	01001100	0100001	01001110	01001001
Nilai Desimal	77	69	76	65	78	73
Karakter	M	E	L	A	N	I

Tabel 1.Hasil Uji

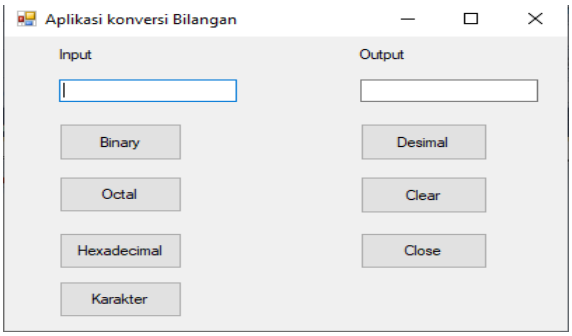
Pada pembahasan ini menghasilkan aplikasi kriptografi berbasis web yang dapat melindungi file dokumen dari pihak orang luar dan ingin mengambil data dokumen tersebut untuk di salah gunakan.

PEMBAHASAN

Rancangan Aplikasi.

a. Tampilan Aplikasi

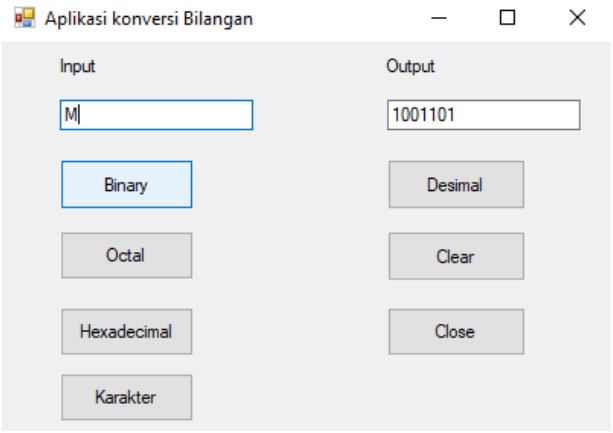
Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1381



Gambar 1.Tampilan Aplikasi

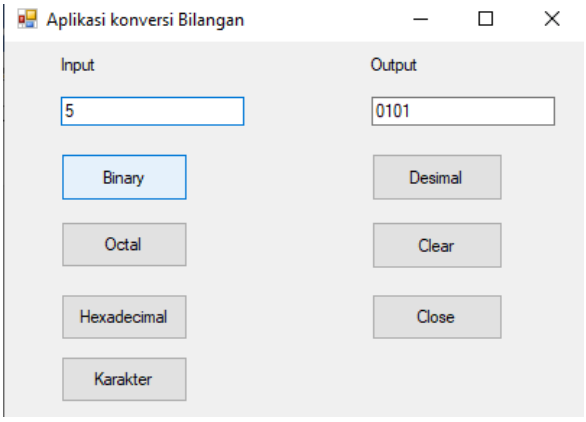
Pada gambar diatas merupakan tampilan dari aplikasi sederhana konversi bilangan

b. Tampilan Biner Pada Aplikasi



Gambar 2. Tampilan ubah karakter huruf menjadi biner

Pada gambar 2 merupakan tampilan saat pengguna menginput data berupa huruf lalu dia mengklik tombol binary maka secara otomatis aplikasi akan mengibah karkter huruf tersebut menjadi bilangan biner

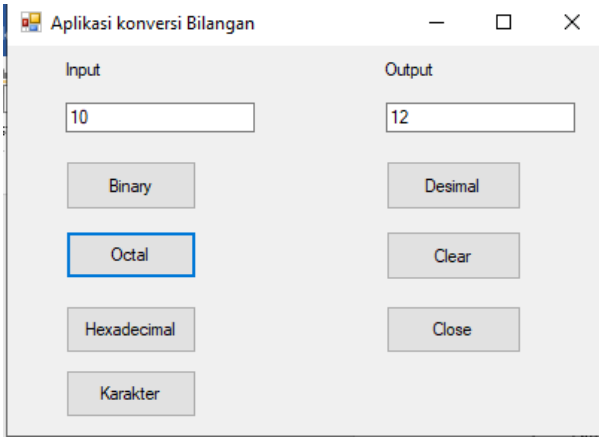


Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1381

Gambar3.Tampilan ubah angka menjadi biner

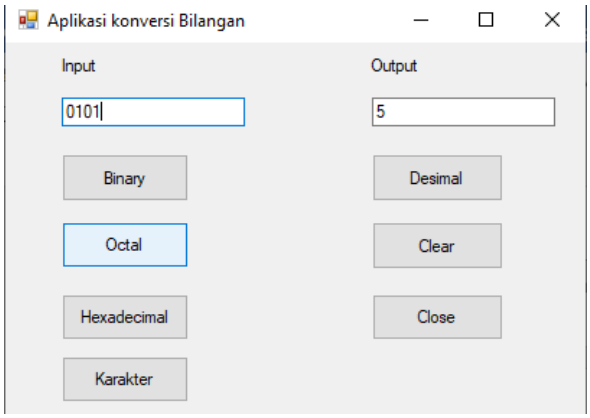
Pada gambar 3 pengguna juga dapat menginput data berupa huruf maka secara otomatis aplikasi akan mengubah data yang anda input menjadi bilangan biner.

c. Tampilan Octal Pada Aplikasi



Gambar 4.Tampilan ubah desimal menjadi Octal

Pada gambar 4 pengguna dapat menginput data berupa bilangan desimal lalu saat pengguna mengklik tombol octal maka secara otomatis aplikasi akan mengubah bilangan desimal ke oktal.

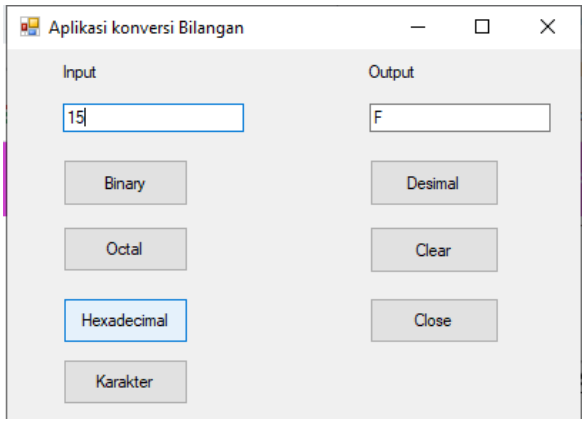


Gambar 5. Tampilan ubah biner menjadi octal

Pada gambar 5. Saat pengguna menginput data berupa bilangan biner lalu mengklik tombol Octal maka secara otomatis aplikasi akan mengubahnya.

d. Tampilan Hexadecimal Pada Aplikasi

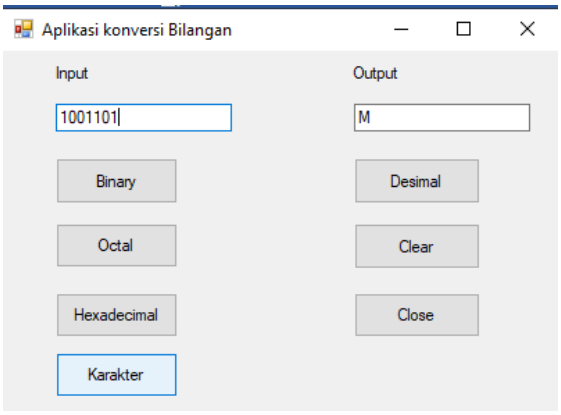
Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1381



Gambar 6. Tampilan mengubah desimal menjadi Hexadecimal

Pada gambar 6. Pengguna dapat menginput data berupa bilangan desimal lalu saat mengklik tombok hexadecimal makan secara otomatis aplikasi akan mengubah nilai desimal tersebut menjadi hexadecimal. Selain nilai desimal kalian juga bisa menginput data berupa nilai biner dan oktal lalu mengklik tombol hexadecimal.

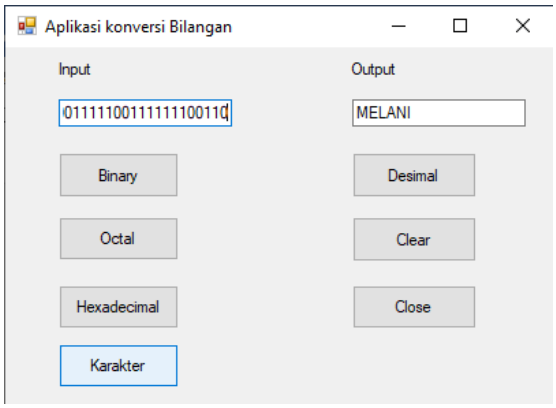
e. Tampilan Karakter Pada Aplikasi



Gambar 7 Tampilan mengubah bilangan biner menjadi huruf

Pada gambar 7 pengguna dapat menginput data berupa bilangan binerlalu saat mengklik tombol karakter maka secara otomatis aplikasi akan mengubah bilangan biner tersebut menjadi huruf

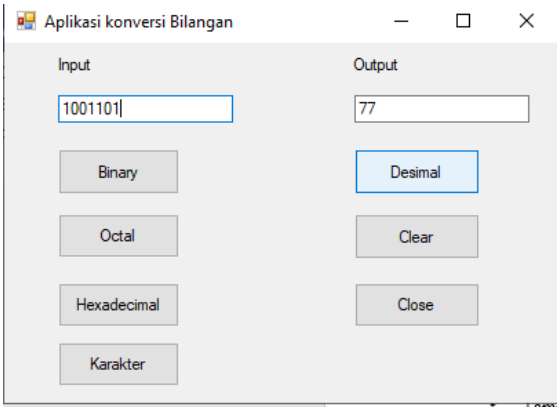
Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1381



Gambar 8 tampilan mengubah kumpulan bilangan biner menjadi sebuah kata

Pada gambar 8 saat pengguna menginput data yang sudah disandikan menjadi bilangan biner maka ketika pengguna mengklik tombol karakter secara otomatis data yang tidak dapat dibaca tersebuat akan berubah menjadi sebuah kata yang berarti.

f. Tampilan Desimal Pada Aplikasi



Gambar 9 tampilan mengubah bilangan biner menjadi desimal

Pada gambar 9 saat pengguna menginput data berupa bilangan biner lalu mengklik tombol desimal maka secara otomatis bilangan biner tersebut akan berubah menjadi bilangan desimal

KESIMPULAN

Pada kesimpulan mengenai penulisan yang berjudul "**Implementasi Mode Operasi Kombinasi Cipher Block Chaining dan Metode LSB-1 Pada Pengamanan Data text**" bertujuan untuk merancang aplikasi kriptografi pada dokumen. Dengan adanya aplikasi sederhana yang kami rancang dapat membantu para pengguna untuk bisa melakukan proses penyandian data secara cepat dan tepat. Aplikasi ini juga menjadi solusi untuk keamanan data text karna sudah menggunakan salah satu algoritma kriptografi.

Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1381

UCAPAN TERIMAKASIH

Terima kasih disampaikan kepada pihak-pihak yang telah mendukung jurnal ini. seperti teman teman yang sudah membantu dan para penulis lain nya.

REFERENSI

Andriani, D. (2017). *Perancangan Aplikasi Penyandian Teks Dengan Menggunakan Algoritma Chiper Block Chaining*.

Diana, M. (2020). *Implementasi Metode GOST(Government Standard) dan LSB-1(Least Significant Bit) Untuk Mengamankan Teks*. *Terapan Informatika Nusantara* (Vol. 1).

Ismadiah, R., Syahrizal, M., & Ramadhani, P. (2020). Kombinasi Algoritma Cipher Block Chaining (CBC) dan Mars Pada Penyandian File PDF. *Journal of Computer System and Informatics (JoSYC)*, *1*(4), 337–345.

Joshi, R., Gagnani, L., & Pandey, S. (2013). *Image Steganography With LSB*. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)* (Vol. 2).

Login Website, P., Lombu, D., Dame Tarihoran, S., Gulo, I., Prorgram Studi Teknik Informatika STMIK Budidarma Medan, M., Sisingamangaraja No, J., & Limun Medan, S. (2018). *Kombinasi Mode Cipher Block Chaining Dengan Algoritma Triangle Chain Cipher Pada Penyandian Login Website*. *Jurnal Sains Komputer & Informatika (J-SAKTI*. Retrieved from http://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Mahmud, W., Mintorini, E., & Kadiri Kediri Jawa Timur Indonesia, S. (n.d.). *Pengamanan Data Kombinasi Metode Cipher Block Chaining dan Modifikasi LSB Data Security Combination of Cipher Block Chaining Method and LSB Modification*. *Februari* (Vol. 19).

Mulyana, D. I., Tinggi, S., Komputer, I., & Karya Informatika, C. (2016). KAJIAN PENERAPAN ENCODE DATA DENGAN BASE64 PADA PEMROGRAMAN PHP. *Jurnal CKI On SPOT*, *9*(1).

Rosmala, D., & Aprian, R. (2012). *IMPLEMENTASI MODE OPERASI CIPHER BLOCK CHAINING (CBC) PADA PENGAMANAN DATA* (Vol. 3).

Sinta Peringkat, T., Dirjen Penguatan RisBang Kemenristekdikti, berdasarkan S., Wati, V., Sa, H., & Ariyus, D. (n.d.). PENDEKATAN STEGO-KRIPTO MODE CIPHER BLOCK CHAINING UNTUK PENGAMANAN INFORMASI PADA CITRA DIGITAL. Retrieved from www.mti.amikom.ac.id

Sukoco, S. H., Sitanggang, I. S., & Sukoco, H. (2018). ANALISIS KINERJA PEGAWAI PUSBINDIKLAT PENELITI LIPI BERDASARKAN POLA PEMANFAATAN INTERNET MELALUI PENDEKATAN WEB USAGE MINING. *Jurnal Penelitian Pos Dan Informatika*, *8*(2), 141. doi:10.17933/jppi.2018.080204

Zainuddin, M. A. (2016). PENERAPAN ALGORITMA RSA UNTUK KEAMANAN PESAN INSTAN PADA PERANGKAT ANDROID. *Jurnal CKI On SPOT*, *9*(2).