Jurnal Teknik Informatika Vol. 15 No. 1, April 2022
ISSN: p-ISSN 1979-9160 (Print)| e-ISSN 2549-7901 (Online)
DOI: http://dx.doi.org/10.15408/jti.v10i2.(id article)

JURNAL TEKNIK INFORMATIKA
Jurnal Teknik Informatika Homepage : http://journal.uinjkt.ac.id/index.php/ti

HYBRID CRYPTOGRAPHIC CIPHERS BLOCK CHAINING AND ELGAMAL FOR TEXT DATA SECURITY

Rinday Zildjiai Salji[1], Nur Rochmah Dyah Puji Astuti [2]

[1,2]Informatika,Fakultas Teknologi Industri
[1.2]Tamanan, Kec. Banguntapan, Kabupaten Bantul, Daerah Istimewa Yogyakarta 55191
E-mail: [1]rinday2000018135@webmail.uad.ac.id, [2]rochmahdyah@tif.uad.ac.id

Article:
Accepted: xxx xx, 20xx
Revised: xxx xx, 20xx
Issued: xxx xx, 20xx

***Correspondence Address:**
rochmahdyah@tif.uad.ac.id

ABSTRACT

Dalam pertukaran pesan, menjaga kerahasiaan informasi penting untuk mencegah pihak yang tidak berwenang memahaminya.Keamanan data digunakan agar data yang kita miliki terlindungi dan terjamin, terdapat tiga perspektif pada keamanan data yaitu kerahasian data, keutuhan data, dan ketersediaan data. Kebocoran data dapat terjadi karena kurangnya pengamanan pada sistem informasi, kriptografi merupakan upaya untuk melakukan keamanan data text.Algoritma kriptografi yang digunakan dalam penelitian adalah algoritma cipher block chaining yang merupakan kriptografi simetris dan algoritma elgamal yang merupakan kriptografi asimetri. Metode yang akan dilakukan adalah hybrid pada kedua algoritma pada pengamanan data text.Pengujian terhadap hybrid kriptografi menggunakan metode white box dengan hasil proses hybrid berjalan sesuai dengan alur, Dari hasil perhitungan black box terbukti bahwa pengujian black box terhadap fungsi aplikasi Hybrid Kriptografi Cipher Block Chaining dan Elgamal mendapatkan persentase penerimaan sebesar 100%, pengujian kecepatan yang sudah diterapkan menggunakan 5 data dengan panjang plaintext yang berbeda proses enkripsi membutuhkan waktu yang lebih lama dibandingkan dengan proses dekripsi.

Keywords: *Kriptografi, Algoritma Hybrid, Elgamal, Cipher Block Chaining, Data text.*

1 INTRODUCTION

Keamanan data digunakan agar data yang kita miliki terlindungi dan terjamin, terdapat tiga perspektif pada keamanan data yaitu kerahasian data,keutuhan data, dan ketersediaan data [1]. Kerahasian data pada era teknologi informasi saat ini perlu diimplementasikan, karena terdapat data-data rahasia yang tidak semua orang boleh mengetahuinya seperti email dan password[2]. kerahasiaan informasi penting untuk mencegah pihak yang tidak berwenang dapat memahaminya . [3]. Kebocoran data dapat terjadi karena kurangnya pengamanan pada sistem informasi terutama pada data berupa text, seperti nama, email, password dan username. Data yang telah bocor jika jatuh pada orang yang salah beresiko identitas dan keamanan terancam, kerugian finansial dan kerusakan reputasi. Metode yang biasa digunakan untuk mengamankan data adalah kriptografi.

ISSN: p-ISSN 1979-9160 (Print)| e-ISSN 2549-7901 (Online)
DOI: http://dx.doi.org/10.15408/jti.v10I2.(id article)

Ilmu kriptografi berisi tentang menjaga keamanan data informasi menggunakan teknik matematika untuk pesan rahasia yang hanya dipahami oleh pemilik dan penerima pesan [4]. Kriptografi bertujuan agar pesan rahasia dapat terjaga privasi, keaslian dan keutuhan dari pesan tersebut [5]. Kriptografi berdasarkan kunci terdapat dua yaitu kunci simetri dan kunci asimetri. Kriptografi dengan kunci simetri salah satu nya adalah kriptografi Cipher Block Chaining (CBC) . Kriptografi CBC menggunakan blok bit, pada proses enkripsi dan dekripsi. Proses enkripsi menggunakan blok bit yang digunakan pada proses pengamanan data text akan membagi data menjadi ukuran yang sama dengan blok-blok biner yang telah ditentukan, lalu dengan menggunakan XOR untuk nilai blok dan nilai blok sebelumnya [6]. Untuk proses dekripsi, menggunakan chipertext yang telah ada kemudian di XOR dan akan menghasilkan plaintext. Kelebihan dari algoritma Cipher Block Chaining dapat menyembunyikan pola dari plaintext, mampu mencegah serangan brute-force dan linear cryptanalysis karena Cipher Block Chaining mempunyai sifat non linear yang membuatnya sulit untuk di serangan. Cipher Block Chaining memiliki kelemahan pada proses dekripsi ciphertext sebelumnya akan berakibat pada deskripsi selanjutnya, jika terjadi kesalahan maka chipertext setelahnya akan mengalami kesalahan juga [7].

Kriptografi elgamal merupakan kriptografi asimetri, karena pada kriptografi ini terdapat dua kunci yang akan digunakan. Kunci public yang berisi tiga bilangan dan kunci privat yang berisi dua bilangan [8]. Algoritma kriptografi ElGamal, yang menggunakan kunci publik, bekerja seperti mesin sandi untuk melindungi pesan. Ia mengubah setiap blok teks biasa menjadi blok teks teracak, yang kemudian dapat dikembalikan menjadi teks biasa. Keamanan algoritma ini berasal dari kesulitan menghitung logaritma pada bilangan prima besar, membuatnya sulit untuk disusupi. Keunggulan ElGamal termasuk dalam cara dia membuat kunci serta proses enkripsi dan dekripsinya yang melibatkan komputasi besar, menghasilkan pesan terenkripsi dengan ukuran dua kali lipat dari pesan aslinya[9].

Untuk meningkatkan kekuatan algoritma maka pada penelitian ini akan dilakukan proses hybrid dua algoritma yaitu CBC dan elgamal. CBC digunakan karena mempunyai kelebihan proses block yang saling berkaitan antara satu block dengan lainnya, elgamal digunakan untuk meningkatkan kekuatan kunci pada CBC. Dengan demikian, data text dapat dijaga kerahasiaannya dan integrasinya terjaga secara baik.

2 PREVIOUS RESEARCH

Dalam tinjauan pustaka ini, peneliti akan mengkaji beberapa penelitian yang telah dilakukan sebelumnya untuk mendapatkan pemahaman yang lebih komprehensif tentang topik ini. Tinjauan pustaka ini akan mencakup analisis kekurangan dan kelebihan penelitian sebelumnya serta informasi teoritis. Dengan demikian, tinjauan pustaka ini bertujuan untuk menyusun landasan teoritis yang kuat dan menyajikan gambaran yang jelas mengenai topik yang akan diteliti dalam skripsi ini.

Fahri Husain , melakukan penelitian yang membahas tentang enkripsi menggunakan metode elgamal untuk meningkatkan keamanan data text dan gambar. Kelebihan dari penelitian ini adalah perhitungan dimulai dengan alur yang benar yaitu menentukan plaintext, bilangan acak prima, bilangan acak, kunci private, kunci public dan bilangan acak pengirim. Melakukan perhitungan secara manual dan dicek melalui sistem yang telah dibuat. Kekurangan dari penelitian ini adalah tidak terdapat proses dekripsi pada file text dan dekripsi pada file doc[9].

Melani Afsari , pada penelitian ini membahas tentang mengamankan data text dengan tujuan agar tidak mudah diketahui oleh orang lain menggunakan kombinasi kriptografi Cipher Block Chaining dan Steganografi metode Least Significant Bit. Kelebihan dari penelitian ini, proses pengamanan data text dilakukan dengan kombinasi tidak hanya berupa kriptografi saja namun dengan menggunakan teknik steganografi LSB-1 (penyisipan gambar) sehingga menghasilkan program sederhana yang dapat membantu mengamankan data text. Kekurangan pada penelitian ini,menurut penulis proses untuk melakukan pengamanan data text dengan

kombinasi Cipher Block Chaining dan Least Significant Bit-1 membutuhkan waktu yang lama serta ketelitian karena kombinasi kriptografi yang dilakukan sangat bergantung pada proses enkripsi sebelum nya[10]

Sartana Sinurat , penelitian ini membahas tentang mengamankan data text dengan tujuan perlindungan pada data yang kita miliki kerahasiaannya semakin meningkat menggunakan ilmu kriptografi Cipher Block Chaining (CBC). Kelebihan dari penelitian ini menggunakan algoritma kriptografi Cipher Block Chaining (CBC) yang proses perhitungan nya menggunakan sistem matematika termasuk fungsi permutasi dan fungsi substitusi, blok enkripsi pada penelitian ini memenuhi istilah confucius dan diffusion karena dapat mencegah kriptanalis. Kelemahan dari penelitian ini perlunya pengembangan pada proses enkripsi kriptografi Cipher Block Chaining agar data yang diamankan dapat lebih terjaga kerahasiaannya dari serangan kriptanalis [11].

Irwansyah Putra Sinaga menerapkan keamanan gambar berbasis desktop melalui implementasi Kriptografi Hybrid dengan menggunakan algoritma ElGamal dan Double Playfair Cipher. Keunggulan dari penelitian ini terletak pada pendekatan manual yang digunakan untuk memahami proses hybrid secara menyeluruh sebelum implementasi. Namun, ada beberapa kekurangan yang perlu diperhatikan, yaitu seharusnya proses hybrid dimulai dengan kriptografi simetri terlebih dahulu, baru kemudian kunci yang digunakan di enkripsi dengan kriptografi asimetri. Di dalam penelitian ini, proses tersebut tidak dijalankan sesuai dengan urutan yang diinginkan. Hal ini perlu diperbaiki agar implementasi Kriptografi Hybrid dapat lebih optimal dan sesuai dengan prinsip dasar keamanan informasi[8].

Abdul Halim , Penelitian ini menunjukkan kelebihan dalam menerapkan metode keamanan file teks menggunakan algoritma ElGamal pada dokumen Microsoft Word. Keamanan yang tinggi terbukti melindungi informasi sensitif dari akses yang tidak sah, dan aplikasi ini membuktikan kebermanfaatannya dalam mengamankan berbagai jenis file teks. Penggunaan pemrograman Visual Basic 2012 mempermudah pengembangan aplikasi, memungkinkan penerapan algoritma ElGamal dan proses keamanan file dengan efisiensi yang baik. Meskipun demikian, kekurangan terdapat pada ketidakjelasan pengantar masalah yang dapat memberikan konteks lebih jelas, kurangnya penjelasan tentang proses hybrid atau penggabungan dengan metode lain yang disebutkan, dan absennya diskusi mengenai keterbatasan atau kelemahan yang mungkin dimiliki oleh metode ElGamal yang diimplementasikan. Dengan memperbaiki aspek-aspek ini, penelitian ini dapat menjadi lebih komprehensif dan memberikan kontribusi yang lebih substansial terhadap pengembangan keamanan file teks[12].

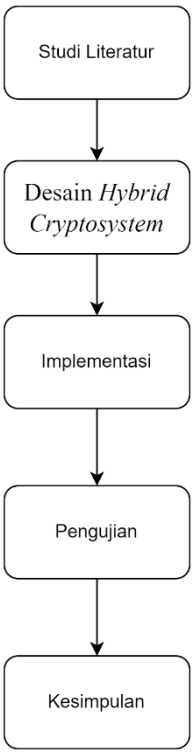
khairani khairani , hasil dari penelitian ini adalah penerapan algoritma ElGamal dan XOR untuk meningkatkan keamanan data pada teks. Algoritma XOR digunakan karena sederhana namun efektif dalam memberikan keamanan data berdasarkan prinsip logika. Sementara itu, Algoritma ElGamal dipilih karena kekuatan kuncinya terletak pada kesulitan pemecahan masalah logaritma diskrit, yang menggunakan bilangan prima besar.

Dengan menggabungkan kedua algoritma ini, pesan teks menjadi lebih aman karena memiliki banyak lapisan keamanan yang dihasilkan dari gabungan kunci dari algoritma ElGamal dan operasi XOR. Oleh karena itu, penelitian ini bertujuan untuk memberikan metode yang lebih andal dalam melindungi kerahasiaan informasi, terutama saat pengiriman data melalui jaringan publik, di mana risiko penyadapan sangat tinggi.

3 METHODOLOGY

Jurnal Teknik Informatika Vol. 15 No. 1, April 2022
ISSN: p-ISSN 1979-9160 (Print)| e-ISSN 2549-7901 (Online)
DOI: http://dx.doi.org/10.15408/jti.v10I2.(id article)

Tahapan penelitian merupakan suatu langkah-langkah yang diterapkan secara berurut dan terstruktur dalam rangka mengimplementasikan penelitian yang telah direncanakan. Proses penelitian ini mempunyai peranan penting dalam memudahkan peneliti dalam mengembangkan sistem yang efektif dan efisien



Studi literatur merupakan proses pencarian ,pengumpulan dan analisis literatur yang relevan yang berkaitan dengan metode penelitian. Pada proses nya melibatkan identifikasi , membaca, dan memahami. Tujuan pada studi literatur adalah memperoleh pemahaman yang mendalam tentang topik penelitian hybrid kriptografi pada Cipher Block Chaining dan elgamal.

Pada tahap ini merupakan membuat desain untuk hybrid cryptosystem yang menggabungkan kriptografi cipher block chaining dan elgamal. Menentukan bagaimana elgamal yang akan digunakan untuk mengenkripsi kemudian kunci yang digunakan pada elgamal akan di enkripsi menggunakan algoritma cipher block channing yang akan meningkatkan keamanan data text tersebut.

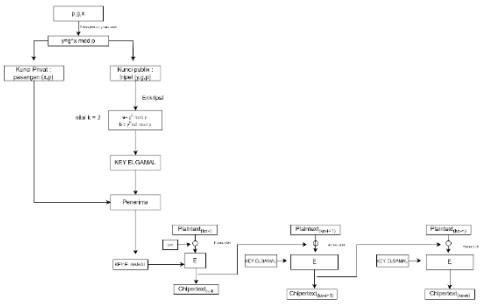
deskripsi dari software dan hardware yang digunakan dalam penelitian khususnya pada tahap eksperimen atau pengembangan perangkat lunak. Jabarkan mulai dari spesifikasi beserta penggunaannya.

kegiatan analisis yang dilakukan terkait analisis data, proses bisnis, kebutuhan sistem dan kebutuhan pengguna, dan analisis lainnya yang mendukung penelitian. tahapan perancangan sistem/metode/model atau skenario yang disesuaikan dengan topik penelitian yang disertai dengan diagram alir. Implementasi menjelaskan hasil perwujudan perancangan sistem/metode/model atau skenario dengan menggunakan Bahasa pemrograman/tools tertentu. metode pengujian yang digunakan untuk pembuktian/validasi dari hasil implementasi yang telah diwujudkan

4 RESULTS AND DISCUSSION

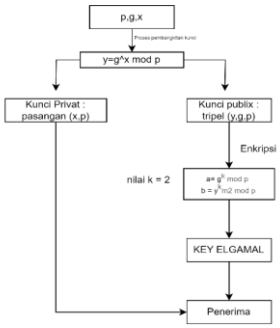
4.1 Perancangan Proses Hybrid Cryptosystem

Tahapan algoritma Cipher Block Chaining (CBC) membagi pesan menjadi blok-blok data, lau setiap blok akan di enkripsi secara terpisah dengan operasi XOR bersama dengan blok sebelumnya atau IV. Proses CBC memerlukan kunci yang sama untuk setiap blok dan menghasilkan ciphertext yang dapat di dekripsi Kembali dengan kunci yang sesuai. Hybrid yang dilakukan pada algoritma CBC adalah pada kunci, kunci akan di enkripsi dengan algoritma elgamal sehingga akan menghasilkan nilai a,b yang disebut dengan kunci elgamal. Sehingga proses enkripsi dan dekripsi pada CBC tidak lagi menggunakan kunci biasa tetapi kunci elgamal yang telah dihitung. Alur dari proses hybrid dapat di lihat pada gambar di bawah:



Untuk melakukan pembentukan kunci di perlukan beberapa bilangan yaitu nilai p yang merupakan bilangan prima, nilai g yang kurang dari p dan nilai x yang x < p . berikut alur untuk mendapatkan nilai a,b :

ISSN: p-ISSN 1979-9160 (Print)| e-ISSN 2549-7901 (Online)
DOI: http://dx.doi.org/10.15408/jti.v10i2.(id article)



Pada Gambar merupakan proses enkripsi yang dimulai dengan pembangkitan kunci menggunakan algoritma ElGamal. Setelah itu, akan diperoleh nilai a dan b. Karena nilai k pada proses ini sudah digunakan, maka nilai a akan mendapatkan hasil yang sama, sementara nilai b akan menghasilkan nilai yang berbeda tergantung pada nilai m. Kunci ElGamal yang dihasilkan akan digunakan pada proses enkripsi dari algoritma *Cipher Block Chaining* (CBC). Contoh Pembagkitan kunci elgamal.

p = 19
g = 2
x = 2
k = 2
kunci = TIF

pembangkitan kunci elgamal

y = $g^x \ mod \ p = 2^2 \ mod \ 19 = 4$
Kunci Publik = (pgp,y) = (19,2,4)
Kunci Privat = (p,x) = (19,2)

T	I	F
84	73	70

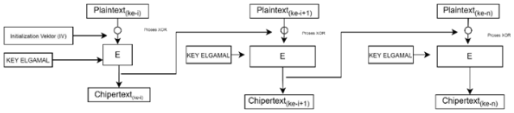
Enkripsi Pesan (dilakukan setiap blok)

	ASCII	K(acak)	a= $2^k \ mod \ 19$	B = $4^k . m \ mod \ 19$	*Ciphertext*
T	84	2	4	14	4,14
I	73	2	4	9	4,9
F	70	2	4	18	4,18

Nilai (a,b) untuk karakter T = (4,14) , I = (4,9), dan F = (4,18) sehingga karena nilai a = 4 dan b = 14,9,18 yang akan menjadi nilai kunci elgamal pada proses enkripsi dan dekripsi pada CBC.

Plaintext	*Karakter*	Desimal	Biner
P_1	RIND	82,73,78,68	01010010010010010100111001000100
P_2	AY	65,89	01000001010110010000000000000000

Proses enkripsi CBC akan membagi plaintext yang dikirimkan menjadi blok-blok sesuai dengan panjang kunci Elgamal. Setelah itu, mengubah blok plaintext dan kunci yang telah dibagi menjadi bilangan biner sesuai dengan tabel ASCII. Blok bilangan biner akan di-XOR dengan IV (Initialization Vector) pada blok pertama. IV yang digunakan dalam proses ini telah ditentukan, yaitu nilai 0 sebanyak panjang kunci. Hasil dari XOR pertama akan di-XOR kembali dengan kunci. Langkah terakhir adalah melakukan operasi XOR sebanyak 4 bit. Blok kedua akan di-XOR dengan hasil operasi XOR blok pertama, dilanjutkan dengan operasi XOR menggunakan kunci ElGamal, proses ini berlanjut hingga blok terakhir plaintext.



Contoh enkripsi menggunakan *hybrid* CBC, dengan menggunakan *plaintext* RINDAY kunci yang berasal dari perhitungan elgamal yaitu 4,14,9 dan 18. Berikut proses perhitungan enkripsi *hybrid* CBC

a. Pembangkitan kunci elgamal

1) Proses pembangkitan kunci dengan menentukan nilai p, g,x ,k dan karakter kunci. Akan menghasilkan nilai a,b sebagai nilai kunci elgamal.
2) Konversi nilai kunci elgamal kedalam bentuk biner berdasarkan tabel ASCII

Key Elgamal (a,b)	***Biner***
4,14,9,18	00000100000011100000100100010010

b. Proses perhitungan CBC
   1) Membagi *plaintext* sesuai dengan blok kunci elgamal.
   2) Mengubah block *plaintext* ke dalam bentuk biner dengan ukuran 8 bit

      Contoh *plaintext* yang digunakan yaitu "RINDAY" dibagi menjadi beberapa blok menjadi dua sesuai dengan panjang biner kunci elgamal masing-masing memiliki 4 karakter berupa biner berjumlah tiga puluh dua bit.

c. IV(*initial Vektor*) yang digunakan adalah nilai 0 dengan banyaknya akan mengikuti dari bit kunci elgamal.

Jurnal Teknik Informatika Vol. 15 No. 1, April 2022
ISSN: p-ISSN 1979-9160 (Print)| e-ISSN 2549-7901 (Online)
DOI: http://dx.doi.org/10.15408/jti.v10I2.(id article)

Tabel 4. 1 Initia vektor

Jenis	Biner
Initial Vector (C_0)	00000000000000000000000000000000

d. Menerapkan metode enkripsi algoritma CBC pada teks asli dengan menggunakan kunci elgamal dan Vektor Awal (Co) untuk menghasilkan teks terenkripsi yang nantinya akan diterima oleh penerima pesan. Langkah-langkah enkripsinya adalah sebagai berikut:

$C_1 = Blok\ (P_1) \oplus C_0$	=01010010010010010100111001000100 ⊕ 00000000000000000000000000000000
	=01010010010010010100111001000100
$Blok\ (P_1) \oplus K$	=01010010010010010100111001000100 ⊕ 00000100000011100000100100010010
	= 01010110010001110100011101010110
Wrapping 4 bit ke kiri	=01100100011101000111010101100101
Hexa	=100,116,117,101
Ciphertext	=dtue
$C_2 = Blok\ (P_2) \oplus C_1$	=01000001010110010000000000000000 ⊕ 01100100011101000111010101100101
	=00100101001011010111010101100101
$Blok\ (P_2) \oplus K$	=00100101001011010111010101100101 ⊕ 00000100000011100000100100010010
	=00100001001000110111110001110111
Wrapping 4 bit ke kiri	=00010010001101111100011101110010
Hexa	=18,55,142,114
Ciphertext	= DC27Ãr

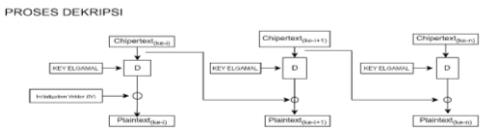
e. Hasil dari perhitungan enkripsi hybrid CBC adalah dengan menggunakan *plaintext* dan kunci elgamal seperti yang ada pada table di bawah :

Plaintext	RINDAY
Kunci elgamal	4,14,9,18

Menghasilkan *ciphertext* seperti yang terdapat pada tabel di bawah

Ciphertext	01100100011101000111010101100101000100011011111000111011100 10
Hexa	100,116,117,101,18,55,142,114
karakter	dtue DC27Ãr

untuk proses dekripsi CBC, Kunci elgamal akan digunakan pada proses dekripsi. Mulai dari membagi karakter *ciphertext* menjadi blok sesuai dengan panjang kunci kemudian setiap blok dan kunci elgamal akan di ubah ke bilangan biner. Setelah semua dirubah maka tahap selanjutnya adalah warping 4 bit terlebih dahulu lalu menentukan berapa panjang nilai IV (Initialization Vector) sepanjang kunci , Proses dekripsi pertama akan di xor dengan kunci elgamal kemudian xor blok pertama dengan IV. Pada blok berikut nya tidak lagi menggunakan IV tetapi blok biner *ciphertext* yang belum dilakukan warping. Berikut merupakan gambar dari proses dekripsi :



a. Wrapping *Ciphertext* ke arah kanan sebanyak 4 bit

C_1 = 01100100011101000111010101100101 → C_1' = 01010110010001110100011101010110
C_2= 00010010001101111000111011100 10→ C_2' =00100001001000110111110001110111

b. Menjalankan langkah-langkah dekripsi sebagai berikut

$P_1 = Blok\ (C'_{1i}) \oplus K$	=01010110010001110100011101010110 ⊕ 00000100000011100000100100010010 =01010010010010010100111001000100
$= Blok\ (C'_{1i}) \oplus C_0$	=01010010010010010100111001000100 ⊕ 00000000000000000000000000000000 = 01010010010010010100111001000100
Plaintext	= RIND
$P_2 = Blok\ (C'_2) \oplus K$	=00100001001000110111110001110111 ⊕ 00000100000011100000100100010010 =00100101001011010111010101100101
$= Blok\ (C'_{1i}) \oplus C_1$	=00100101001011010111010101100101 ⊕ 01100100011101000111010101100101 =01000001010110010000000000000000
Plaintext	=AY

c. Hasil Akhir dari dekripsi hybrid CBC

Ciphertext	01100100011101000111010101100101000100011011111000111011100 10
Hexa	100,116,117,101,18,55,142,114
karakter	dtue DC27Ãr

Menghasilkan *plaintext* sesuai dengan hasil enkripsi

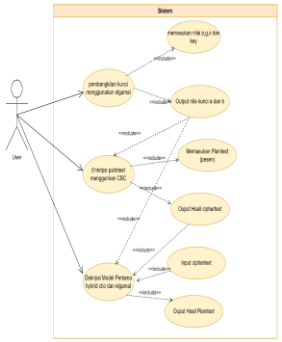
Plaintext	01010010010010010100111001000100010000010101100100000000 00000000
karakter	RINDAY

4.2 Implementasi *Hybrid Cryptosystem*

Penerapan algoritma CBC (Cipher Block Chaining) dan algoritma elgamal dalam aplikasi menggunakan bahasa pemrograman PHP, javascript dan HTML untuk melakukan proses enkripsi dan dekripsi pesan. Dalam aplikasi ini, pesan yang dijalani prosesnya merupakan teks, dan melalui proses tersebut, dilakukan enkripsi dan dekripsi.

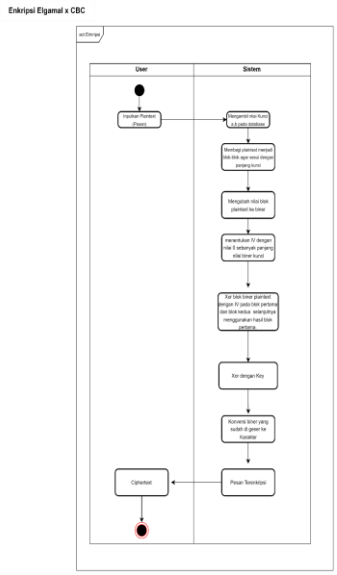
Use Case Diagram merupakan salah satu jenis dari diagram Unified Modeling Language

(UML) yang bergunakan untuk menjelaskan interaksi antara sistem dan aktor-aktor yang berinteraksi dengannya. Berikut adalah gambar dari use case sistem hybrid kriptografi.

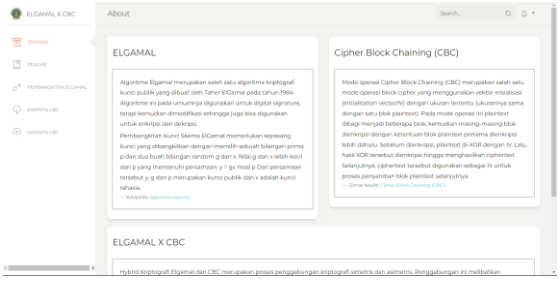


Use Case Diagram Hybrid Cryptosystem, pengguna dapat mengakses halaman pembangkit elgamal, enkripsi CBC, dan dekripsi CBC. Setiap halaman pada sistem ini saling berhubungan, dimana pengguna dapat memulai dari halaman pembangkitan elgama. Kemudian, dari halaman ini akan terdapat tombol untuk membawa nilai yang telah dihitung. Dengan membawa nilai tersebut, pengguna hanya akan menginputkan pesan yang akan dienkripsi. Hasil enkripsi tersebut dapat dibawa ke halaman dekripsi atau pengguna dapat menginputkan ciphertext lainnya.

Activity diagram merupakan komponen dari Unified Modeling Language (UML) yang digunakan untuk menggambarkan alur kerja atau proses bisnis dalam sebuah sistem. Tujuan utama dari activity diagram adalah untuk mengilustrasikan urutan langkah-langkah atau aktivitas-aktivitas yang terjadi dalam proses tersebut.

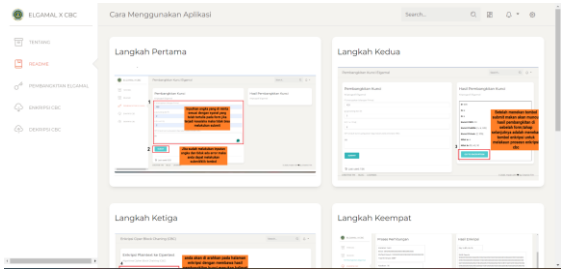


proses Enkripsi Elgamal dengan mode CBC, pengguna diberikan kesempatan untuk memasukkan pesan yang ingin dienkripsi melalui formulir yang disediakan. Setelah melakukan input, pengguna dapat memilih untuk mengenkripsi pesan tersebut dengan menekan tombol "enkripsi". Tindakan ini akan memicu sistem untuk memulai proses enkripsi menggunakan algoritma Elgamal dengan mode Cipher Block Chaining (CBC). Selain menampilkan ciphertext yang dihasilkan dari pesan yang dienkripsi, sistem juga akan menampilkan langkah-langkah atau proses yang dilakukan selama pengerjaan enkripsi, sehingga memberikan pengguna pemahaman yang lebih baik tentang bagaimana proses tersebut berlangsung.

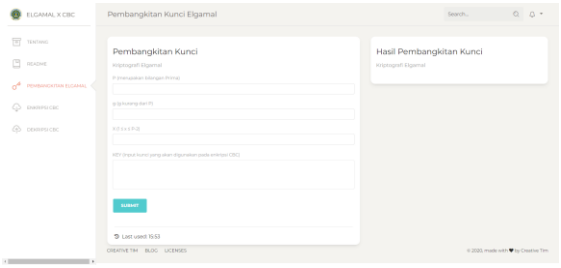


menampilkan halaman "About" dalam sistem kriptografi hybrid yang menggabungkan teknik kriptografi Elgamal dan Cipher Block Chaining (CBC). Pada halaman ini, terdapat teori tentang Elgamal dan CBC, serta penjelasan mengenai proses hybrid yang dilakukan.

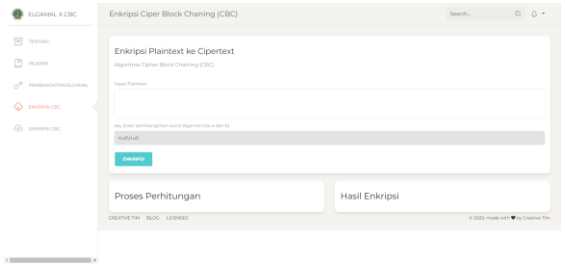
Jurnal Teknik Informatika Vol. 15 No. 1, April 2022
ISSN: p-ISSN 1979-9160 (Print)| e-ISSN 2549-7901 (Online)
DOI: http://dx.doi.org/10.15408/jti.v10i2.(id article)



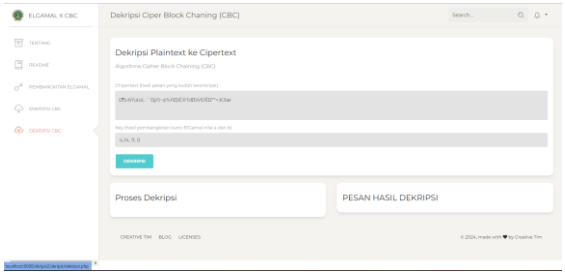
halaman tutorial yang dirancang untuk memperlihatkan pengguna cara-cara menggunakan sistem hybrid dengan detail. Di sini, pengguna dapat melihat langkah-langkah yang harus dilakukan untuk menggunakan sistem secara efektif.



menampilkan halaman pembangkitan unci yang bertujuan untuk menghasilkan nilai a dan b sebagai hasil dari proses yang dilakukan. Di sini, pengguna diminta untuk memasukkan nilai-nilai seperti p, g, x, dan kunci Elgamal yang akan digunakan dalam proses enkripsi CBC. Melalui formulir input ini, sistem dapat menghitung nilai a dan b yang akan digunakan dalam proses enkripsi, memastikan bahwa kunci yang dihasilkan sesuai dengan kebutuhan dan spesifikasi yang telah ditentukan sebelumnya. Dengan menggunakan halaman ini, pengguna dapat mempersiapkan kunci yang diperlukan dengan akurat sebelum melanjutkan ke langkah-langkah selanjutnya dalam proses kriptografi.



halaman enkripsi di mana pengguna diminta untuk mengisi teks biasa atau pesan yang akan disampaikan. Hal ini memungkinkan proses enkripsi dilakukan untuk memastikan keamanan informasi yang dikirim, dengan mengubah teks asli menjadi bentuk terenkripsi sebelum dikirimkan ke penerima.



halaman dekripsi di mana pengguna diminta untuk memasukkan ciphertext atau pesan terenkripsi yang kemudian akan dikembalikan ke bentuk pesan asli. Hal ini memungkinkan proses dekripsi dilakukan untuk mengembalikan kalimat asli dari teks terenkripsi tersebut.

4.3 Pengujian *Hybrid Cryptosystem*

Pengujian white box merupakan pengujian yang dilakukan untuk perangkat dilakukan pada struktur internal pada sistem dan kode sumber yang diuji. Pengujian ini berhubungan dengan pemahaman dan pemeriksaan langsung pada logika algoritma elgamal dan CBC yang digunakan. Tujuan utama untuk memastikan bahwa kode algoritma yang digunakan berfungsi dengan benar dan efisien, serta untuk memperbaiki kelemahan dalam algoritma implementasi kode. Pengujian ini dilakukan oleh dosen informatika yaitu bapak Guntur Maulana Zamroni, B.Sc., M.Kom., berikut hasil pengujian yang dilakukan :

No Path	Node (n)	Hasil yang diterapkan	Hasil Sesuai Uji Kasus	Keterangan
1	1-3-4-5-6-7-8	Menghasilkan nilai a,b	sesuai	[✓] Alur Terlewati [] Alur tidak terlewati
2	1-2	Tidak dapat menghitung nilai a,b karena inputan tidak valid	sesuai	[✓] Alur Terlewati [] Alur tidak terlewati

Metode Pengujian black box merupakan pengujian yang memiliki tujuan untuk memastikan apakah sistem yang berjalan menghasilkan output yang diharapkan atau tidak. Tampilan sistem merupakan salah satu titik interaksi, karena langsung berinteraksi dengan pengguna sehingga perlu dilakukan pengujian agar mendapatkan kesesuaian.

Pengujian ini dilakukan oleh 10 orang mahasiswa teknik informatika, berikut data para penguji. Hasil dari skenario yang dibuat dalam pengujian black box dari hybrid kriptografi Cipher Block Chaining dan Elgamal.

No	Output yang Diharapkan	Validasi	
		Ya	Tidak
1.	Mampu melakukan input nilai p	10	
2.	Mampu melakukan input nilai g	10	
3.	Mampu melakukan input nilai x	10	
4.	Mampu melakukan input kunci	10	
5.	Mampu melakukan perhitungan Pembangkit kunci	10	
6.	Mampu mengalihkan ke halaman enkripsi	10	
7.	Mampu melakukan input *plaintext*	10	
8.	Mampu memproses hasil enkripsi	10	
9.	Mampu mengalihkan ke halam dekripsi	10	
10.	Mampu melakukan inputan *ciphertext*	10	
11.	Mampu memproses hasil dekripsi	10	

Pengujian Black Box dapat memperoleh persentase kelayakan dengan menggunakan rumus berikut:

Presentasi Kelayakan (%) = Nilai Hasil Pengujian/Nilai Maksimal x 1

= 11/11 x 100%

=100%

Dari hasil perhitungan di atas, terbukti bahwa pengujian black box terhadap fungsi aplikasi Hybrid Kriptografi Cipher Block Chaining dan Elgamal mendapatkan persentase penerimaan sebesar 100%, menandakan bahwa aplikasi beroperasi sesuai dengan yang diharapkan

Kecepatan proses hybrid dicoba dengan lima data menggunakan kunci yang sama tetapi panjang plaintext yang berbeda.

Kunci	*Plaintext*	Waktu Enkripsi (detik)	Waktu Dekripsi (detik)	Panjang plaintext (bit)	
				Sebelum	Sesudah
uad	informatika	0.001	0.00060000000238418579	88	98
uad	Fakultas teknologi industri	0.001	0.0007999999523162842	216	224
uad	tifuad	0.001	0.0007000000476837158	48	64
uad	FTI	0.002	0.0005	24	32
uad	Universitas Ahmad Dahlan	0.002	0.0008999999761581421	192	192

Berdasarkan dari pengujian yang sudah diterapkan menggunakan 5 data dengan panjang plaintext yang berbeda proses enkripsi membutuhkan waktu yang lebih lama dibandingkan dengan proses dekripsi.

5 CONCLUSION

Dari hasil penelitian yang telah dilakukan kesimpulan yang dapat diambil dari keamanan data text menggunakan hybrid algoritma Cipher Block Chaining dan elgamal adalah:

1 Proses penentuan kunci algoritma Cipher Block Chaining menggunakan algoritma elgamal sebagai hasil hybrid algoritma.
2 Hybrid algoritma mampu untuk proses enkripsi dan dekripsi.
3 Dari hasil pengujian white box semua alur berjalan sesuai skenario, black box mencapai kelayakan pada fungsionalitas sistem, kecepatan proses enkripsi dan dekripsi yang telah dilakukan menghasilkan kesimpulan proses enkripsi lebih lama dibandingkan dengan dekripsi jika berdasarkan panjang plaintext.

BIBLIOGRAPHY

[1] A. G. Gani, “Pengamanan Komputer Menggunakan Kriptografi CIPHER BLOCK CHAINING (CBC),” J. Sist. Inf. Univ. Suryadarma, vol. 3, no. 2, pp. 79–100, 2014, doi: 10.35968/jsi.v3i2.65.

[2] I. Gunawan, “Keamanan Data: Teori dan Implementasi,” p. 141, 2021.

[3] Makhomah, R., Santoso, K. A., & Kamsyakawuni, A. (2021). Pengkodean Teks Menggunakan Kombinasi HillCipher dan Operasi XOR. PRISMA, Prosiding Seminar Nasional Matematika, 4, 548–552.

[4] R. Munir, “KRIPTOGRAFI Kuliah Pengantar”.

[5] A. P. N. Nurdin, “Analisa Dan Implementasi Kriptografi Pada Pesan Rahasia,” Jesik, vol. 3, no. 1, pp. 1–11, 2017, [Online]. Available: nnurdin69@gmail.com

[6] Devi Andriani, “View of Perancangan Aplikasi Penyandian Teks Dengan Menggunakan Algoritma Chiper Block Chaining.” http://www.ejournal.ust.ac.id/index.php/JTIUST/article/view/186/189 (accessed Jun. 23, 2023).

[7] I. Gunawan, “Modifikasi Keamanan File dengan Algoritma Hill Cipher Untuk Mengantisipasi Dari Serangan Brute Force,” TECHSI - J. Tek. Inform., vol. 11, no. 2, pp. 237–246, Jul. 2019, doi: 10.29103/TECHSI.V11I2.1272.

[8] I. Putra Sinaga, "Implementasi Kriptografi Hybrid Algoritma Elgamal Dan Double Playfair Cipher Dalam Pengamanan File Jpeg Berbasis Desktop," J. Informatics, Electr. Electron. Eng., vol. 1, no. 2, pp. 67–74, 2021, [Online]. Available: https://djournals.com/jieeeJIEEE,

[9] A. Y. N. Harahap, H. Gunawan, A. B. Nst, and R. E. Sari, "Penerapan Elgamal Guna Meningkatkan Keamanan Data Text Dan Docx," It (Informatic Tech. J., vol. 10, no. 1, p. 76, 2022, doi: 10.22303/it.10.1.2022.76-86.

[10] M. Afsari, A. Damaiyanti, and N. Sa'adah, "Implementasi Mode Operasi Kombinasi Cipher Block Chaining dan Metode LSB-1 Pada Pengamanan Data text," J. Pendidik. Sains dan Komput., vol. 2, no. 1, pp. 2809–476, 2022, doi: 10.47709/jpsk.v2i1.1381.-to-scrape-news-articles-with-python/ (accessed May 21, 2021)

Jurnal Teknik Informatika Vol. 15 No. 1, April 2022
ISSN: p-ISSN 1979-9160 (Print)| e-ISSN 2549-7901 (Online)
DOI: http://dx.doi.org/10.15408/jti.v10I2.(id article)