Jurnal Ilmu Komputer, Teknologi Dan Informasi
Vol 2, No. 1, Januari 2024, Hal 32 – 38
ISSN: **2963-0169** (Online - Elektronik)
https://journal.grahamitra.id/index.php/jurikti

Modifikasi Metode Cipher Block Chaining (CBC) Dengan Pembangkit Kunci Mid Square

Annisa Fitria Lubis

Program Studi Teknik Informatika, Fakultas Ilmu Komputer Dan Teknologi Informasi, Universitas Budi Darma, Medan, Indonesia
Jl. Sisingamangaraja No. 338, Medan, Sumatera Utara, Indonesia
Email: annisafitrialubis26@gmail.com

Abstrak− *Cipher block chaining* (CBC) merupakan salah satu mode operasi *block cipher* yang menggunakan vektor inisialisasi (*initialitation vector*/IV) dengan ukuran tertentu (ukurannya sama dengan satu blok *plaintext*). Seiring dengan perkembangan ilmu pengetahuan manusia, kelemahan dari *cipher block chaining* berhasil ditemukan. Salah satu cara yang dapat dilakukan untuk mengatasi kelemahan *Cipher Block Chaining* adalah dengan melakukan pembangkitan kunci yang lebih acak. Penelitian ini menguraikan bagaimana prosedur yang dilakukan untuk memodifikasi pembangkitan kunci yang digunakan pada algoritma *cipher block chaining*. Proses pembangkitan kunci dilakukan berdasarkan pembangkit kunci *midsquare*, artinya kunci yang digunakan pada proses enkripsi dan dekripsi adalah kunci yang dibangkitkan berdasarkan pembangkit kunci *midsquare*, sehingga proses modifikasi yang dilakukan dalam pembangkitan kunci tersebut dapat meminimalkan tindakan pemecahan kunci yang dilakukan pihak lain serta algoritma ini dapat lebih optimal dalam mengamankan data. Hasil dari penelitian ini adalah merancang sebuah aplikasi pengaman data berbasis *android* dengan menggunakan metode *cipher block chaining* yang telah dimodifikasi menggunakan pembangkit kunci *MidSquare*. Aplikasi ini dapat digunakan untuk mengmankan data berupa teks, sehingga tidak dapat diambil oleh orang lain. Selain itu, aplikasi yang akan dirancang ini lebih mudah untuk digunakan dalam pengamanan data.

Kata Kunci: *Keamanan, Kunci, Algoritma, Kriptografi, Cipher Block Chaining, MidSquare*

Abstract−Cipher block chaining (CBC) is a block cipher operating mode that uses an initialization vector (IV) of a certain size (the same size as one block of plaintext). Along with the development of human science, weaknesses in cipher block chaining were discovered. One way that can be done to overcome the weaknesses of Cipher Block Chaining is to generate more random keys. This research describes the procedures used to modify the key generation used in the cipher block chaining algorithm. The key generation process is carried out based on a midsquare key generator, meaning that the key used in the encryption and decryption process is a key generated based on a midsquare key generator, so that the modification process carried out in generating the key can minimize key breaking actions carried out by other parties and this algorithm can be more efficient. optimal in securing data. The result of this research is to design an Android-based data security application using the cipher block chaining method which has been modified using the MidSquare key generator. This application can be used to secure data in the form of text, so that it cannot be taken by other people. Apart from that, the application that will be designed is easier to use for data security.

Keywords: Security, Keys, Algorithms, Cryptography, Cipher Block Chaining, MidSquare

1. PENDAHULUAN

Kriptografi merupakan suatu teknik pengamanan data yang dapat digunakan untuk menjamin kerahasiaan data. Pada kriptografi menggunakan tekni matematis sehingga data yang ada di dalamnya dapat terjaga dan aman dari pihak yang hendak mengambil data tersebut [1]. Kriptografi bertujuan untuk mengamankan data mulai dari keaslian data, integritas data dan lain sebagainya yang berhubungan dengan data agar tidak disalah gunakan oleh pihak yang tidak brtanggung jawab dengan tujuan merusak nama baik seseorang atau perusahaan dan berbagai macam tujuan lainnya. Kriptografi memiliki beberapa algoritma yang dikhususkan untuk mengamankan data yang salah satunya adalah *Cipher Block Chaining* (CBC) [1].

Operasi *Cipher Block Chaining* (CBC) merupakan salah satu mode operasi *block cipher* yang cara kerjanya menggunakan vektor inisialisasi (*initialitation vector*/IV) dengan ukuran tertentu (ukurannya sama dengan satu blok *plaintext)*. Cera kerja dari metode ini adalah *plaintext* dibagi menjadi beberapa blok, kemudian masing-masing blok dienkripsi dengan ketentuan blok *plaintext* pertama dienkripsi lebih dahulu. Sebelum dienkripsi, *plaintext* di-XOR dengan IV. Lalu, hasil XOR tersebut dienkripsi hingga menghasilkan *ciphertext*. Selanjutnya, *ciphertext* tersebut digunakan sebagai IV untuk proses penyandian blok *plaintext* selanjutnya. Namun, seiring berkembangnya teknologi, kelemahan dari CBC berhasil ditemukan.

Kelemahan CBC ini terletak pada kunci yang terdiri dari satu blok yang selanjutnya blok tersebut akan disandikan ke *plaintext* selanjutnya hingga terpenuhi. Sebab, kunci yang dimiliki oleh CBC panjang tidak sama dengan panjang *plaintext*.[4] Kelemahan lainnya adalah untuk mendekripsi *ciphertext*, dipengaruhi oleh *ciphertext* sebelumnya, artinya jika *ciphertext* awal berbeda dengan *ciphertext* yang di dapat, maka menghasilkan *plaintext* yang berbeda. Untuk mengatasi masalah tersebut, maka perlu dilakukan pembangkitan kunci untuk meningkatkan ketahanan dari algortima CBC. Salah satu metode pembangkit kunci yang dapat digunakan adalah pembangkit kunci *mid square*. Cara kerja dari *mid square* adalah mengambil nilai kuadrat tengah dari bilangan inisial/awal [4].

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Metodologi Penelitian adalah ilmu yang menjelaskan tentang bagaimana sebuah penelitian itu dilakukan, langkah-langkah yang testruktur dilakukan oleh peneliti untuk menemukan penyelesaian terhadap objek yang ditelitinya. Adapun langkah-langkah tersebut:

a. Studi pustaka
   Dilakukan dengan membaca literatur yang berkaitan dengan pembahasan dan tema yang dibuat. Cara yang dilakukan antara lain dengan membaca buku kriptografi, buku-buku pendukung lain yang membahas tentang kriptografi dan penerapan berbagai metode yang ada di dalamnya, dan juga dari situs-situs hasil *browsing* di *internet*.
b. Tahapan analisa dan perancangan
   Melakukan analisa terhadap kekurangan algoritma CBC khususnya dalam proses pembangkitan kunci, kemudian menganalisa proses penerapan solusi yang dapat menyelesaikan kekurangan algoritma CBC dengan mengkombinasikan dengan pembangkit kunci *mid square*. Tahap ini juga menguraikan proses perancangan aplikasi pengamanan data yang digunakan untuk membuktikan dan mengimplementasikan solusi yang diberikan.
c. Tahapan pengujian dan implementasi
   Tahap ini merupakan tahap pengujian terhadap hasil modifikasi CBC dengan pembangkit kunci *mid square*, apakah setelah dimodifikasi kunci tersebut kuat dan tidak mudah untuk dipecahkan atau sebaliknya. Setelah memastikan bahwa kunci tersebut kuat, maka dilakukan tahapan implementasi terhadap algoritma CBC yang telah dimodifikasi dengan pembangkit kunci *mid square* tersebut.

2.2 Kriptografi

Kriptografi berasal dari bahasa Yunani dengan memadukan kata dari bahasa Yunani, yaitu *kryptos* dan *graphein*. *Kryptos* berarti tersembunyi atau rahasia, sedangkan *graphein* memiliki arti menulis. Makna dari kriptografi secara harfiah ialah menulis secara tersembunyi untuk menyampaikan pesan-pesan yang dirasa perlu dijaga kerahasiaannya. Kriptografi adalah suatu ilmu tentang teknik enkripsi naskah asli (plaintext) yang diacak memanfaatkan sebuah kunci enkripsi sehingga naskah asli berubah menjadi naskah yang sulit dibaca (ciphertext) oleh pihak yang tidak memiliki kunci dekripsi. Ada tiga fungsi dasar di dalam algoritma kriptografi, antara lain; enkripsi, dekripsi, dan kunci. Enkripsi berarti proses penyembunyian data pesan, mengubah *plaintext* menjadi *ciphertext*. Sedangkan dekripsi merupakan kebalikan dari enkripsi, bertujuan untuk memahami pesan yang ada, dan kunci adalah teknik yang digunakan untuk enkripsi maupun dekripsi. Ilmu kriptografi berkembang selaras dengan kemajuan teknologi. Menurut kronologi waktunya ilmu kriptografi dapat dibedakan menjadi dua pemahaman, yakni kriptografi klasik dan kriptografi *modern*. Kedua pemahaman tersebut bergantung pada penggunaan perangkat analasis dan pembuat pesan yang bersifat kriptologis. Semua algoritma kriptografi dari kriptografi klasik termasuk dalam sistem kriptografi yang bersistem simetris. Teknik enkripsi pada kriptografi klasik semuanya sama seperti kunci enkripsi. Artinya untuk memahami sebuah teks tersembunyi dapat dilakukan secara serupa seperti saat pembuatannya [1].

Aplikasi yang dibuat untuk kriptografi berarti sebuah program yang memungkinkan untuk dilakukannya enkripsi dan dekripsi pada saat melakukan proses pengamanan sebuah pesan didalam data *desktop* maupun *handphone*. Aplikasi ini biasanya digunakan untuk mengamankan perangkat maupun isi di dalam perangkat itu sendiri dengan melakukan penguncian yang menggunakan metode algoritma kriptografi [2].

2.3 Metode *Cipher Block Chaining* (CBC)

Ada dua ide utama di balik *Cipher Blok Chaining* (CBC). Pertama, enkripsi semua blok adalah "dirantai bersama-sama". Kedua, enkripsi secara acak dengan menggunakan inisialisasi vektor. Mode ini menerapkan umpan-balik (feedback) pada sebuah blok, dalam hal ini hasil enkripsi blok sebelumnya di umpan balikan ke dalam enkripsi blok yang *current*. Blok *plaintext* yang *current* di-XOR-kan terlebih dahulu dengan blok *ciphertext* hasil enkripsi sebelumnya, selanjutnya hasil peng-XOR- an masuk ke dalam fungsi enkripsi. Pada mode CBC, setiap blok *ciphertext* tidak hanya tergantung pada blok *plaintext* tetapi juga pada seluruh blok *plaintext* sebelumnya [3]. Persiapan dan langkah-langkah proses enkripsi perancangan kriptografi dijelaskan sebagai berikut:

a. Menyiapkan *plainteks* yang akan dienkripsi.
b. Menyiapkan *key* untuk digunakan dalam proses enkripsi.
c. Melakukan proses *generate key*.
d. Melakukan pergeseran pada *state plainteks* sesuai pola yang ditentukan.
e. Menentukan IV (initialization vector).
f. Melakukan *Exlusive OR* terhadap hasil proses *plainteks* dengan IV dan hasil proses *key* dan menghasilkan *cipherteks* [4].

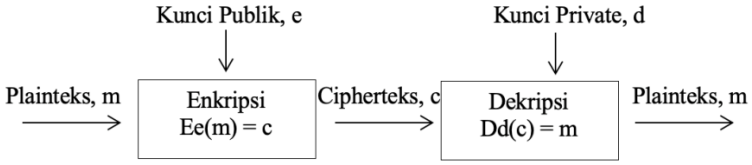
Proses dekripsi merupakan proses yang dilakukan terbalik dengan proses enkripsi. Hanya saja yang menjadi inputan bukan *plainteks* tetapi *cipherteks*. Selain itu juga, kunci yang dimasukkan diregenerasi secara terbalik untuk mengambalikan *cipherteks* menjadi *plainteks*. [4]

2.4 Modifikasi

Pengertian Modifikasi secara umum adalah mengubah atau menyesuaikan. Mengenai pengertian modifikasi, Bahagia (2010), mengemukakan bahwa: Modifikasi dapat diartikan sebagai upaya melakukan perubahan dengan penyesuaian-penyesuaian baik dalam segi fisik material (fasilitas dan perlengkapan) maupun dalam tujuan dan cara (metoda, gaya, pendekatan, aturan serta penilaian). Sehingga, modifikasi merupakan suatu usaha perubahan yang dilakukan berupa penyesuaian- penyesuaian baik dalam bentuk fasilitas dan perlengkapan atau dalam metoda, gaya, pendekatan, aturan serta penilaian [5].

2.5 Pembangkit Kunci

Sampai akhir tahun 1970, hanya ada sistem kriptografi kunci-simetri. Mengirim kunci rahasia pada saluran publik (telepon, internet, pos) sangat tidak aman. Oleh karena itu, kunci harus dikirim melalui saluran kedua yang benar-benar aman. Saluran kedua tersebut umumnya lambat dan mahal. *Whitfield Diffie* dan *Martin Hellman*, penemu kriptografi kunci-publik [6]. Kriptografi kunci-nirsimetri disebut juga kriptografi kunci publik jika kunci untuk enkripsi dibuat publik. Pada kriptografi kunci-publik, masing-masing pengirim dan penerima mempunyai sepasang kunci kunci publik: untuk mengenkripsi pesan kunci privat: untuk mendekripsi pesan. $E_e(m) = c$ dan $D_d(c) = m$.



Gambar 1. Proses Metode *Mid Square*

Proses pembangkitan kunci adalah merupakan proses yang dilakukan untuk memperoleh kunci publik yang akan digunakan pada proses enkripsi, hal ini tidak berlaku pada proses dekripsi yang mana dapat dilakukan tanpa proses pembangkitan kunci. Pembentukan kunci terdiri atas pembentukan kunci publik dan kunci rahasia. Pada proses ini dibutuhkan sebuah bilangan prima p yang digunakan untuk membentuk grupZp*, elemen primitif α dan sembarang a∈{0,1,..., p − 2}. Kunci publik algoritma *ElGamal* terdiri atas pasangan 3 bilangan (p, α, β). Ketiga bilangan tersebut memenuhi persamaan β = α a mod p (3) yang digunakan sebagai kunci rahasia adalah bilangan a.

Proses enkripsi menggunakan kunci public (p, α ,β) dan sebuah bilangan integer acak k ∈({0,1,..., p − 1}) yang dijaga kerahasiaannya oleh penerima yang mengenkripsi pesan. Untuk setiap karakter dalam pesan dienkripsi dengan menggunakan bilangan k yang berbeda-beda. Satu karakter yang direpresentasikan dengan menggunakan bilangan bulat ASCII akan menghasilkan kode dalam bentuk blok yang terdiri atas dua nilai (r, t). Proses dekripsi dari *ciphertext* ke *plaintext* menggunakan kunci rahasia a yang disimpan kerahasiaanya oleh penerima pesan. Teorema yang digunakan adalah diberikan (p, α, β)sebagai kunci publik dan a sebagai kunci rahasia pada algoritma *ElGamal*. Jika diberikan *ciphertext* (r, t), maka M = t (ra) -1 mod p (a) (4) dengan M adalah *plaintext* [7].

2.6 Mid Square

Metode *Mid Square* (MiddleSquare) dalam pembangkitan bilangan acak. Metode ini ditemukan oleh *Johnvon Neumann* dan *Metropolis* (1940). Metode ini sangat sederhana, algoritmanya adalah pilih bilangan sembarang kuadratkan bilangan tersebut ambil beberapa *digit* ditengah dari hasil kuadrat tersebut. Bilangan yang diambil merupakan bilangan acak yang dihasilkan dari metode ini, bilangan tersebut juga merupakan umpan untuk iterasi menghasilkan bilangan acak selanjutnya. Sebagai contohnya dipilih bilangan 1234 kemudian dikuadratkan menjadi 1522756 atau dapat ditulis 01522756 dalam format 8 *digit* karena bilangan yang dipilih pertama adalah 4 *digit*. 5227 merupakan bilangan yang dihasilkan pada iterasi pertama sebagai bilangan acak. Iterasi selanjutnya menghasilkan 3215 [7].

3. HASIL DAN PEMBAHASAN

Pengamanan data yang dirancang dan dibangun adalah aplikasi pengamanan data berbasis *mobile* dengan sistem operasi *android*. Perancangan akan dilakukan dengan menggunakan *software* IDE *eclipse* sebagai editor kode program dan SDK (*software development kit*) yang diperlukan untuk mulai mengembangkan aplikasi pada *platform android* menggunakan bahasa pemrograman *java* serta *android development tools* (ADT) sebagai *plugin* yang didesain untuk IDE *eclipse* yang memberikan kemudahan dalam mengembangkan aplikasi *android*. Setelah dibuat *source code* pada *eclipse galileo* dan aplikasi dapat dijalankan pada emulator di laptop, maka untuk menjadikannya suatu aplikasi yang dapat dijalankan pada *android* apk yang ada pada tempat tempat aplikasi yang diinstal pada *mobile android*. Aplikasi pengamanan data ini dapat dijalankan pada *smartphone* dengan sistem operasi *android*.

Perancangan aplikasi pengamanan data menggunakan metode *cipher block chaining*. Metode ini memiliki kelemahan yang sering dimanfaakan oleh pihak pencuri data atau *hacker* yaitu dalam mendeskripsikan *ciphertext*, dipengaruhi oleh *ciphertext* sebelumnya. Sehingga dengan mudah *ciphertext* ditebak. Jika hal ini terus dibiarkan, maka untuk mengamankan data menggunakan metode ini sangat tidak efesien. untuk itu perlu adanya peningkatan atau

modifikasi terhadap metode ini. Permasalahan di atas dapat diselesaikan dengan melakukan modifikasi terhadapa algoritma tersebut. modifikasi yang dilakukan adalah dengan melakukan pembangkitan kunci. Proses pembangkitan kunci sangat cocok untuk meningkatkan kualitas pengamanan data menggunakan algoritma *cipher block chaining*. Sebab jantung dari keamanan informasi adalah terletak pada kunci yang digunakan.

3.1 *Algoritma* Cipher Block Chaining

Cipher block chaining menggunakan subtitusi majemuk yang artinya mengekripsi setiap setiap huruf yang ada dengan menggunakan kunci yang berbeda. Proses dekripsi juga sama dengan proses enkripsi. Kunci yang digunakan adalah kunci sama yang digunakan pada proses enkripsi.

Plaintext: RAHASIA KEHIDUPAN
Kuncinya: MAHASISWA

Proses enkripsi yang terjadi adalah sebagai berikut:

Misalkan A = 0, B= 1, C = 2,…,…,Z = 25

Tahap enkripsi *cipher block chaining*:

Pi =	R	A	H	A	S	I	A	K	E	H	I	D	U	P	A	N
Ki	M	A	H	A	S	I	S	W	A	M	A	H	A	S	I	S
=																

Maka proses pencarian *ciphertext* adalah:

Ci = (Pi + Ki) mod 26
C1 = (17 + 12) mod 26 = 3 = D
C2 = (0 + 0) mod 26 = 0 = A
C3 = (7 + 7) mod 26 = 14 = O
C4 = (0 + 0) mod 26 = 0 = A
C5 = (18 + 18) mod 26 = 10 = K
C6 = (8 + 8) mod 26 = 16 = Q
C7 = (0 + 18) mod 26 = 18 = S
C8 = (10 + 22) mod 26 = 4 = G
C9 = (4 + 0) mod 26 = 4 = E
C10 = (7 + 12) mod 26 = 19 = T
C11 =(8 + 0) mod 26 = 8 = I
C12 = (3 + 7) mod 26 = 10 = K
C13 = (20 + 0) mod 26 = 20 = U
C14 = (15+ 18) mod 26 = 7 = H
C15 = (0 + 8) mod 26 = 8 = I
C16 = (13 + 18) mod 26 = 5 = F

Pi =	R	A	H	A	S	I	A	K	E	H	I	D	U	P	A	N
Ki =	M	A	H	A	S	I	S	W	A	M	A	H	A	S	I	S
Ci =	D	A	O	A	K	Q	S	G	E	T	I	K	U	H	I	F

Tahap dekripsi *cipher block chaining*

Ci =	D	A	O	A	K	Q	S	G	E	T	I	K	U	H	I	F
Ki =	M	A	H	A	S	I	S	W	A	M	A	H	A	S	I	S

Maka proses pencarian *plaintext* sebagai berikut:

Pi = (Ci - Ki) mod 26
P1 = (3 - 12) mod 26 = 17 = R
P2 = (0 - 0) mod 26 = 0 = A
P3 = (14 - 7) mod 26 = 7 = H
P4 = (0 - 0) mod 26 = 0 = A
P5 = (10 - 18) mod 26 = 18 = S
P6 = (5 - 8) mod 26 = 13 = N
P7 = (16 - 18) mod 26 = 8 = I
P8 = (18 - 22) mod 26 = 0 = A
P9 = (6 - 0) mod 26 = 10 = K
P10 = (4 - 12) mod 26 = 4 = E
P11 =(19 - 0) mod 26 = 7 = H
P12 = (8 - 8) mod 26 = 8 = I
P13 = (10 - 0) mod 26 = 3 = D
P14 = (20 - 18) mod 26 = 20 = U
P15 = (7 - 8) mod 26 = 15 = P
P16 = (8 - 18) mod 26 = 0 = A

Ci =	D	A	O	A	K	Q	S	G	E	T	I	K	U	H	I	F
Ki =	M	A	H	A	S	I	S	W	A	M	A	H	A	S	I	S
Pi =	R	A	H	A	S	I	A	K	E	H	I	D	U	P	A	N

Jurnal Ilmu Komputer, Teknologi Dan Informasi
Vol 2, No. 1, Januari 2024, Hal 32 – 38
ISSN: **2963-0169** (Online - Elektronik)
https://journal.grahamitra.id/index.php/jurikti

3.1.1 Pembangkit

Berikut adalah langkah-langkah dalam membangkitkan bilangan acak menggunakan pembangkit kunci *Mid Square*:

a. Pilih bilangan bulat positif sembarang yang terdiri dari 2 digit angka atau lebih yang dilambangkan dengan x0.
b. Kuadratkan bilangan tersebut sehingga membentuk digit sejumlah dua kali dari nilai sebelumnya yang dilambangkan x1, jika tidak berjumah 2 kali dari nilai sebelumnya, maka tambahkan dengan angka 0 .
c. Kemudian ambil jumlah digit tengah sesuai jumlah digit sebelumnya.
d. Lakukan sampai langkah ke n.

Sebagai contoh pembangkit kunci dijelaskan sebagai berikut:

a. Pilih bilangan bulat positif sembarang.
   Bilangan bulat positif yang digunakan adalah:
   X0 = 76.
b. Kemudian kuadratkan x0.
   $X0^2 = 76^2 = 5776$.
c. Lalu ambil nilai tengah dari hasil kuadrat X0 sebanyak 2 digit yang merupakan nilai x selanjutnya.
   X1 = 77.

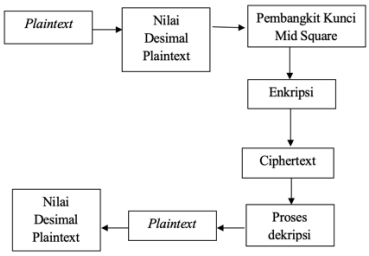
Lakukan langkah di atas lakukan sebanyak yang dibutuhkan.

3.1.2 Modifikasi *Cipher Block Chaining* dengan Pembangkit Kunci

Tahapan pertama yang dilakukan dalam proses modifikasi *cipher block chaining*, yaitu menginputkan teks yang akan diamankan, kemudian dilakukan proses pembangkitan kunci berdasarkan. Hasil dari pembangkitan kunci inilah yang akan dijadikan kunci. Berikut adalah prosedur yang dilakukan dalam mengamankan data berdasarkan algortma *cipher block chaining* yang dimodifikasi:

a. Proses enkripsi.
b. Bangkitkan kunci berdasarkan pembangkit kunci.
c. Lakukan proses enkripsi berdasarkan algoritma *cipher block chaining* dengan menggunakan kunci hasil proses pembangkitan kunci menggunakan pembangkit kunci.

Proses dari modifikasi algoritma *cipher block chaining* dengan pembangkit kunci , dapat dilihat pada gambar di bawah ini:



Gambar 2. Diagram Proses Modifikasi *Cipher Block Chaining*

Adapun contoh modifikasi *cipher block chaining* menggunakan pembangkit kunci seperti di bawah ini. Dimisalkan *plaintext* yang digunakan adalah **RAHASIA KEHIDUPAN**

a. Proses pembangkitan kunci berdasakan algoritma *cipher block chaining* bahwa jumlah kunci yang digunakan pada proses enkripsi dan dekripsi harus sama dengan jumlah karakter *plaintext*. Jumlah *plaintext* pada contoh di atas adalah 16 karakter, oleh karena itu akan dibangkitkan 16 karakter kunci berdasarkan pembangkit kunci. Langkah-langkah yang dilakukan adalah:
   1. Pilihlah bilangan bulat positif yang berjumlah 2 digit
      $x_0 = 89$
   2. Kemudian kuadratkan x_0
   3. $x_1 = (x_0)^2 = 89^2 = 7921$ kemudian ambil 2 digit nilai tengah dari hasil kuadrat x_0
   4. Maka $x_1 = 92$
   5. Untuk mendapatkan x_{17} lakukan langkah proses untuk menghasilkan x_1
      $x_2 = (x_1)^2 = 92^2 = 8464 = 46$
      $x_3 = (x_2)^2 = 46^2 = 2116 = 11$
      $x_4 = (x_4)^2 = 11^2 = 121$ = karena tidak mencapai 2 kali lipat jumlah digit sebelumnya, maka tambahkan angka 0 dibagian kiri bilangan maka nilainya adalah 0121 dan $x_4 = 12$
      $x_5 = (x_4)^2 = 21^2 = 144$menjadi 0144 = 44
      $x_6 = (x_5)^2 = 44^2 = 1936 = 93$
      $x_7 = (x_6)^2 = 93^2 = 8649 = 49$
      $x_8 = (x_7)^2 = 49^2 = 2401 = 40$
      $x_9 = (x_8)^2 = 40^2 = 1600 = 60$

$x_{10} = (x_9)^2 = 60^2 = 3600 = 60$
$x_{11} = (x_{10})^2 = 60^2 = 3600 = 60$
$x_{12} = (x_{11})^2 = 60^2 = 3600 = 60$
$x_{13} = (x_{12})^2 = 60^2 = 3600 = 60$
$x_{14} = (x_{13})^2 = 60^2 = 3600 = 60$
$x_{15} = (x_{14})^2 = 60^2 = 3600 = 60$
$x_{16} = (x_{15})^2 = 60^2 = 3600 = 60$

Jadi kunci yang dihasilkan adalah 92 46 11 12 44 93 49 40 60 60 60 60 60 60 60 60 Proses Enkripsi

b. Proses enkripsi yang dilakukan berdasarkan modifikasi *cipher block chinning* yang menggunakan pembangkit kunci. Berikut adalah proses modifikasinya:

$C_1 = (R + x_1) \bmod 26 = (17 + 92) \bmod 26 = 109 \bmod 26 = 5 = F$
$C_2 = (A + x_2) \bmod 26 = (0+46) \bmod 26 = 20 \bmod 26 = 20 = U$
$C_3 = (H + x_3) \bmod 26 = (7 + 11) \bmod 26 = 18 \bmod 26 = 18 = S$
$C_4 = (A + x_4) \bmod 26 = (0 + 12) \bmod 26 = 12 \bmod 26 = 12 = M$
$C_5 = (S + x_5) \bmod 26 = (18 + 44) \bmod 26 = 62 \bmod 26 = 10 = K$
$C_6 = (I + x_6) \bmod 26 = (8 + 93) \bmod 26 = 101 \bmod 26 = 23 = X$
$C_7 = (A + x_7) \bmod 26 = (0 + 49) \bmod 26 = 49 \bmod 26 = 23 = X$
$C_8 = (K + x_8) \bmod 26 = (10 + 40) \bmod 26 = 50 \bmod 26 = 24 = Y$
$C_9 = (E + x_9) \bmod 26 = (4 + 60) \bmod 26 = 64 \bmod 26 = 12 = M$
$C_{10} = (H + x_{10}) \bmod 26 = (7 + 60) \bmod 26 = 67 \bmod 26 = 15 = P$
$C_{11} = (I + x_{11}) \bmod 26 = (8 + 60) \bmod 26 = 68 \bmod 26 = 16 = Q$
$C_{12} = (D + x_{12}) \bmod 26 = (3 + 60) \bmod 26 = 63 \bmod 26 = 11 = L$
$C_{13} = (U + x_{13}) \bmod 26 = (20 + 60) \bmod 26 = 80 \bmod 26 = 2 = C$
$C_{14} = (P + x_{14}) \bmod 26 = (15 + 60) \bmod 26 = 75 \bmod 26 = 23 = X$
$C_{15} = (A + x_{15}) \bmod 26 = (0 + 60) \bmod 26 = 60 \bmod 26 = 8 = I$
$C_{16} = (N + x_{16}) \bmod 26 = (13 + 60) \bmod 26 = 73 \bmod 26 = 21 = V$

Hasil enkripsi di atas akan menjadi *ciphertext*. *Ciphertext* yang didapat dari hasil perhitungan di atas adalah **FUSMKXXYMPQLCXIV**

c. Proses Dekripsi

Setelah *ciphertext* didapat dari proses enkripsi, maka proses dekripsi untuk mendapatkan *plaintext* hampir sama dengan proses enkrispsi. Kunci yang digunakan sama dengan kunci yang dihasilkan dari proses pembangkit kunci yang digunakan pada proses enkripsi. Adapun proses dekripsi modifikasi *cipher block chaining* dengan pembangkit kunci yang menggunakan persamaan bab sebelumnya, yaitu:

$P_1 = (F - x_1) \bmod 26 = (5 - 92) \bmod 26 = -87 \bmod 26 = 0 = R$
$P_2 = (U - x_2) \bmod 26 = (20-46) \bmod 26 = -26 \bmod 26 = 0 = A$
$P_3 = (S - x_3) \bmod 26 = (18 - 11) \bmod 26 = 7 \bmod 26 = 7 = H$
$P_4 = (M - x_4) \bmod 26 = (12 - 12) \bmod 26 = 0 \bmod 26 = 0 = A$
$P_5 = (K - x_5) \bmod 26 = (10 - 44) \bmod 26 = -34 \bmod 26 = 18 = S$
$P_6 = (X - x_6) \bmod 26 = (23 - 93) \bmod 26 = -70 \bmod 25 = 8 = I$
$P_7 = (X - x_7) \bmod 26 = (23 - 49) \bmod 26 = -26 \bmod 26 = 0 = A$
$P_8 = (Y - x_8) \bmod 26 = (24 - 40) \bmod 26 = -16 \bmod 26 = 10 = K$
$P_9 = (M - x_9) \bmod 26 = (12 - 60) \bmod 26 = -48 \bmod 26 = 4 = E$
$P_{10} = (P - x_{10}) \bmod 26 = (15 - 60) \bmod 26 = -45 \bmod 26 = 7 = H$
$P_{11} = (Q - x_{11}) \bmod 26 = (16 - 60) \bmod 26 = -44 \bmod 26 = 8 = I$
$P_{12} = (L - x_{12}) \bmod 26 = (11 - 60) \bmod 26 = -49 \bmod 26 = 3 = D$
$P_{13} = (C - x_{13}) \bmod 26 = (2 - 60) \bmod 26 = -58 \bmod 26 = 20 = U$
$P_{14} = (X - x_{14}) \bmod 26 = (23 - 60) \bmod 26 = -37 \bmod 26 = 15 = P$
$P_{15} = (I - x_{15}) \bmod 26 = (8 - 60) \bmod 26 = -52 \bmod 26 = 0 = A$
$P_{16} = (V - x_{16}) \bmod 26 = (21 - 60) \bmod 26 = -39 \bmod 26 = 13 = N$

Maka *plaintext* dari proses dekripsi di atas adalah **RAHASIA KEHIDUPAN**.

Berdasarkan contoh kasus di atas dapat diketahui bahwa hasil modifikasi *cipher block chaining* dengan pembangkit kunci lebih efektif dan sulit untuk dipecahkan. Kunci yang dihasilkan dari proses pembangkitan kunci lebih sederhana dan tidak terdapat perulangan karakter kunci sehingga kunci yang digunakan hanya dipakai satu kali.

4. KESIMPULAN

Kesimpulan yang dapat diambil dari hasil penelitian modifikasi *cipher block chaining* dengan pembangkit kunci *mid square*, yaitu Prosedur pengamanan data berdasarkan algoritma *cipher block chaining* memiliki kelemahan yaitu kuncinya yang berulang sehingga dapat ditebak dengan tepat. Oleh sebab itu algoritma *cipher block chaining* kurang efektif dalam mengamankan data. Hasil dari modifikasi *cipher block chaining* dengan pembangkit kunci *mid square* menghasilkan kunci yang lebih sulit dipecahkan dibandingkan dengan kunci pada *cipher block chaining* yang belum

dimodifikasi. Aplikasi pengamanan data menggunakan modifikasi *cipher block chaining* dengan pembangkit kunci *mid square* dapat membantu untuk mempermudah pengguna dalam mengamankan data penting atau data yang bersifat rahasia

REFERENCES

[1] R. Munir, "Pengantar Kriptografi," *Dep. Tek. Inform. Inst. Teknol. Bandung*, no. Buku, p. 12, 2016.
[2] R. Lingkup, K. Untuk, and M. Data, "Ruang Lingkup Kriptografi," vol. IX, no. 2, 2004.
[3] Yusharmen *et al.*, "Digital Digital Repository Repository Universitas Universitas Jember Jember Digital Digital Repository Repository Universitas Universitas Jember diakses tahun 2018," *Karya Tulis Ilmiah. Progr. Stud. DIII Keperawatan. Fak. Keperawatan. Univ. Sumatera Utara. Medan*, pp. 9–35, 2017, [Online]. Available: http://repository.unimus.ac.id/411/.
[4] A. Muzakir, "Prototype Model Keamanan Data Menggunakan Kriptografi Data Encryption Standar (Des) Dengan Mode Operasi Chiper Block Chaining (Cbc)," *Semin. Nas. Inov. dan Tren 2014*, vol. 20, pp. 1–4, 2014.
[5] M. W. A. Bangun, "Pemanfaatan Hasil Modifikasi Pembelajaran Pendidikan Jasmani Di Slb-Ypac Cabang Medan," *J. Phys. Educ. Heal. Recreat.*, vol. 2, no. 2, p. 97, 2018, doi: 10.24114/pjkr.v2i2.9553.
[6] A. Susanto, "Penerapan Teori Chaos di dalam Kriptografi," no. 13506087, 2008.
[7] A. Ramadhan, "Perbandingan Algoritma Linear Congruential Generators , BlumBlumShub , dan MersenneTwister untuk Membangkitkan Bilangan Acak Semu," pp. 36–38, 2010.
[8] S. Dharwiyanti and R. S. Wahono, "Pengantar Unified Modeling LAnguage (UML)," *IlmuKomputer.com*, pp. 1–13, 2003, [Online]. Available: http://www.unej.ac.id/pdf/yanti-uml.pdf.
[9] N. Oktaviani and S. Sauda, "Pemodelan dan Implementasi Aplikasi Mobile Umrah Guide Menggunakan Unified Modeling Language," *J. Sains dan Inform.*, vol. 5, no. 2, p. 177, 2019, doi: 10.34128/jsi.v5i2.184.
[10] K. Kawano, Y. Umemura, and Y. Kano, " Field Assessment and Inheritance of Cassava Resistance to Superelongation Disease 1 ," *Crop Sci.*, vol. 23, no. 2, pp. 201–205, 1983, doi: 10.2135/cropsci1983.0011183x002300020002x.
[11] G. Urva, H. F. Siregar, J. Prof, M. Y. Kisaran, and S. Utara, "Pemodelan UML E- Marketing Minyak Goreng," no. 9, pp. 92–101, 2015.
[12] G. Karyono and N. Hermanto, "Rancang Bangun Sistem Tracer Study Online pada STMIK AMIKOM PURWOKERTO," *Semantik*, vol. 3, no. 1, pp. 126–133, 2013, [Online]. Available: http://publikasi.dinus.ac.id/index.php/semantik/article/view/730.
[13] gunadharma, "Definisi dan Simbol Flowchart," *Defin. Dan Simbol Flowchart*, pp. 1–9, 2016.
[14] F. R. Ariyan, R. I. Rokhmawati, and K. C. Brata, "Pengembangan Antarmuka Website E-Learning untuk Meningkatkan Minat Belajar Pemrograman Dasar Dalam Bahasa Pemrograman Java bagi Mahasiswa Fakultas Ilmu Komputer Universitas Brawijaya," vol. 3, no. 10, pp. 9920–9928, 2019.
[15] N. A. Pratama and C. Hermawan, "Aplikasi Pembelajaran Tes Potensi Akademik Berbasis Android," *J. Penelit. Dosen FIKOM*, vol. 6, no. 1, pp. 1–6, 2016.
[16] I. Ripai, "Rancang Bangun Aplikasi Android Kitab Bulughul Maram Menggunakan Eclipse," *J. ICT Learn.*, vol. 2, no. 2, pp. 19–24, 2016.