Penerapan Algoritma Affine Cipher dan Algoritma Electronic Code Book (ECB) dalam Pengamanan Pesan Teks

Ema Satriana Br Karo
STMIK Budidarma Medan, Jl. Sisingamangaraja No.338 Simpang Limun Medan
Email : ema.karo2@gmail.com

Abstrak

Keamanan sangat penting dalam segala aspek untuk melindung data. Pesan teks pada alat komputer atau laptop yaitu pesan teks yang merupakan salah satu data penting yang perlu dalam sistem keamanan data. Keamanan data digunakan untuk menjaga kerahasiaan data penting pada perangkat komputer ataupun laptop. Proses enkripsi digunakan agar pesan tidak dapat dibaca oleh pihak lain yang tidak di inginkan. Sedangkan proses dekripsi digunakan agar pesan dapat dibaca kembali oleh pihak yang dituju. Dengan melakukan enkripsi terhadap pesan teks maka tingkat keamanan informasi dari pesan tersebut dapat ditingkatkan. Enkripsi menggunakan algoritma affine cipher dan algoritma electronic code book (ecb). Algoritma affine cipher dan algoritma electronic code book (ecb) diimplementasikan dengan software Visual Basic 2008. Hasil penelitian ini adalah melindungi pesan dengan mengubah pesan asli menjadi sebuah rahasia yang dilakukan dengan pergeseran kunci.

Kata Kunci : Affine cipher, Electronic code book, Kriptografi, Pesan, Teks, Data

Abstract

Security is very important in all aspects to protect data. Text messages on a computer or laptop are text messages which are one of the important data needed in a data security system. Data security is used to maintain the confidentiality of important data on a computer or laptop device. The encryption process is used so that messages cannot be read by unwanted parties. Meanwhile, the decryption process is used so that the message can be read back by the intended party. By encrypting text messages, the information security level of these messages can be increased. Encryption uses an affine cipher algorithm and an electronic code book (ecb) algorithm. The affine cipher algorithm and electronic code book (ecb) algorithm are implemented with Visual Basic 2008 software. The results of this study are to protect messages by converting the original message into a secret which is done by shifting the key.

Keywords: Affine cipher, Electronic code book, Cryptography, Message, Text, Data

1. PENDAHULUAN

Pertukaran data maupun pesan dapat dilakukan dengan mudah dan banyak yang tersedia media untuk melakukan pertukaran data maupun pesan tersebut antara lain melalui media *internet* seperti fasilitas *e-mail*, melalui transfer data antar perangkat *mobile* (*handphone* dan *flashdisk*) maupun dengan teknologi radio *frequency* (*bluetooth, GPRS*). Seiring dengan berkembangnya teknologi informasi dan komunikasi muncul sebuah kehawatiran bagi *user* tentang keamanan data maupun pesan yang mereka kirimkan, apakah terjadi penyadapan saat proses pengiriman[1], [2]. Dengan itu dibutuhkan suatu teknik untuk pengamanan data maupun pesan guna menghindari penyadapan saat proses pengiriman berlangsung.

Keamanan dan kerahasiaan merupakan aspek penting yang dibutuhkan dalam proses pertukaran pesan atau informasi. Tanpa adanya jaminan keamanan, orang lain dapat dengan mudah mendapatkan pesan atau informasi yang dikirimkan melalui jaringan atau *internet*. Berbagai macam teknik keamanan yang telah dikembangkan untuk melindungi dan menjaga kerahasiaan pesan agar terhindar dari orang yang tidak berhak, salah satunya yaitu teknik Kriptografi[3].

Affine cipher merupakan perluasan dari *Caesar cipher*, yang mengalikan plainteks dengan sebuah nilai dan menambahkannya dengan sebuah pergeseran. *Affine cipher* bukanlah *cipher* yang aman sebab kuncinya (m dab b) dapat ditemukan dengan *exhaustive key search. Electronic Code Book* merupakan enkripsi dan dekripsi yang sifatnya acak yang cocok untuk mengenkripsi *file* yang diakses

secara acak karena tiap blok plainteks dienkripsi secara independen. Bahkan jika *ECB* dikerjakan dengan prosesor paralel, maka dekripsi blok plainteks yang berbeda-beda[4], [5].

2. LANDASAN TEORI

2.1. Kriptografi

Kriptografi berasal dari bahasa Yunani, menurut bahasa dibagi menjadi dua *kripto* dan *graphia*, kripto berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan). Menurut temologinya kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ketempat lain. Kriptografi sudah digunakan 400 tahun yang lalu yang diperkenalkan oleh orang-orang Mesir untuk mengirim pesan kepasukan militer yang berada di lapangan dan supaya pesan tersebut tidak terbaca oleh musuh walaupun kurir yang membawa pesan tersebut tertangkap oleh musuh[6]. Secara historis ada empat kelompok orang yang berkontribusi terhadap perkembangan kriptografi, dimana mereka menggunakan kriptografi untuk menjaga kerahasiaan dalam komunikasi pesan penting, yaitu kalangan militer (termasuk intelijen atau mata-mata), kalangan diplomatik, penulis buku harian,dan pencinta (*lovers*). Diantara keempat kelompok ini, kalangan militer yang memberikan kontribusi paling penting karena pengiriman pesan di dalam suasana perang membutuhkan teknik enkripsi dan dekripsi yang rumit[7].

2.2. Affine Cipher

Affine cipher adalah perluasan dari *Caesar cipher*, yang mengalikan plainteks dengan sebuah nilai dan menambahkannya dengan sebuah pergeseran. Secara matematis enkripsi plainteks *P* menghasilkan cipherteks *C* dinyatakan dengan fungsi kongruen:

$C=mP+b(\mathrm{mod}\ n)$

Yang didalam hal ini *n* adalah ukuran alfabet, *m* adalah bilangan bulat yang harus ralatif prima dengan *n* (Jika tidak relative prima, maka dekpripsi tidak bisa dilakukan) dan b adalah jumlah pergeseran (*Caesar chipper* adalah khusus dari *affine cipher* dengan dengan faktor pengali satu sehingga menghasilkan cipherteks yang hanya berupa penggeseran[1].

Enkripsi: $C=mP+b(\mathrm{mod}\ n)$

Dekripsi: $P=m^{-1}(C-b)(\mathrm{mod}\ n)$ (1)

Pada mode ini, setiap blok plainteks P_i dienkripsi secara individual dan independen menjadi blok cipherteks C_i. Secara matematis, enkripsi dengan metode ECB dinyatakan sebagai

$C_i = E_k (P_i)$

Dan Dekripsi sebagai

$P_i = D_k (C_i)$

Yang dalam hal ini K adalah kunci dan P_i dan C_i masing-masing blok plainteks dan cipherteks ke-i.

Ada kemungkinan panjang plainteks tidak habis dibagi dengan panjang kurang blok yang ditetapkan (misalnya 64 Bit atau lainnya). Hal ini mengakibatkan blok terakhir berukuran lebih pendek daripada blok-blok lainnya. Satu cara untuk mengatasi hal ini adalah *padding*, yaitu menambahkan blok terakhir dengan pola bit yang teratur agar panjangnya sama dengan ukuran blok yang ditetapkan, Misalnya ditambahkan bit 0 semua, atau bit 1 semua, atau bit 0 dan bit 1 berselang seling. Misalkan ukuran blok adalah 64 bit (8 byte)dan blok terakhir terdiri dari 24 bit(3 byte). Tambahkan blok terakhir dengan 40 bit (5 byte) agar menjadi 64 bit, misalnya dengan menambahkan 4 buah byte 0 dan satu buah byte angka 5. Setelah dekripsi, hapus 5 byte terakhir dari blok dekripsi tetakhir.

Contoh:

Misalkan plainteks (dalam biner) adalah

10100010001110101001

Bagi plainteks menjadi blok berukuran 4 bit

1010 0010 0011 1010 1001

Kunci=1010

Misalkan fungsi enkripsi E yang sederhana adalah XOR antara P_i dengan K kemudian geser secara *wrapping* bit-bit dari $P_i \oplus$ K satu posisi ke kiri.

P_i1010 0010 0011 1010 1001

1010 1010 1010 1010 1010 $\oplus$

Hasil 0000 1000 1001 0000 0011

Geser 1 bit ke kiri: 00000001 0011 0000 0110

Dalam notasi HEX: 0 1 3 0 6
Jadi, hasil enkripsi plainteks
10100010001110101001
Adalah : 000010001001000000011.

3. PEMBAHASAN

3.1. Analisa Masalah

Masalah adalah tahap untuk menentukan masalah apa yang harus diselesaikan dengan menggunakan aplikasi yang akan akan dibuat. Tahap analisa nya yaitu:

1. Pesan teks akan dienkripsi dengan *affine cipher*
2. Pesan teks dienkripsi kembali dengan *electronic code book* (ecb).
3. Hasil dari enkripsi *electronic code book* (ecb) didekripsi dengan *electronic code book* (ecb) untuk mengembalikan pesan teks yang di enkripsi dengan *electronic code book* (ecb).
4. Hasil dari dekripsi *electronic code book* (ecb) didekripsi lagi dengan *affine cipher* agar pesan teks kembali ke semula atau kembali ke pesan asli.

3.2 Enkripsi Affine Cipher

Proses enkripsi terlebih dahulu dilakukan dengan algoritma *affine cipher* dan hasil dari enkripsi tersebut di enkripsi kembali dengan algoritma *electronic code book* (ECB). Misalkan P_i "EMASATRIANABRKAR"
di enkripsi dengan algoritma *affine cipher* dengan persamaan sebagai berikut :

C =mP +b (mod n)

Dengan:
m = bilangan bulat yang harus relatif prima dengan n
n =ukuran alfabet
b = jumlah pergeseran
Plainteks : EMASATRIANABRKAR
Perhitungannya adalah sebagai berikut:

$P_1 = 4$
$C = mP + b \pmod{26}$
$C_1 = 7.4 + 4 \pmod{26}$
$= 32 \bmod 26$
= 6 dengan huruf G
$P_2 = 12$
$C_2 = 7 . 12 + 4 \pmod{26}$
$= 84 \bmod 26$
= 10 dengan huruf K

$P_7 = 17$
$C_7 = 7 . 17 + 4 \pmod{26}$
$= 119 + 4 \bmod 26$
$= 123 \bmod 26$
= 19 dengan huruf T
$P_{16} = 17$
$C_{16} = 7 . 17 + 4 \pmod{26}$
$= 119 + 4 \bmod 26$
$= 123 \bmod 26$
= 19 dengan huruf T

Jadi hasil enkripsi dari :
EMASATRIANABRKAR
Adalah :
GKEAEHTIERELTWET

3.3 Enkripsi Dengan Electronic Code Book

Hasil dari enkripsi algoritma *affine cipher* dienkripsi kembali ke algoritma *electronic code book*(ecb).
Cipherteks = GKEAEHTIERELTWET
Ubah ke biner
01000111010010110100010101000001 01000101 01001000 01010100 01001001
01000101010100100100010101001100010101000101011101000101010100
Plainteksnya :
01000111010010110100010101000001 01000101 01001000 01010100 01001001
01000101010100100100010101001100010101000101011101000101010100
Kunci: 01000111
bagi plainteks menjadi blok-blok yang berukuran 8 bit
01000111 01001011 01000101 01000001 01000101 01001000 01010100 01001001 01000101
01010010 01000101 01001100 01010100 01010111 01000101 01010100
misalkan kunci (k) yang digunakan adalah

01000111 (G dalam bilangan ASCII)

Misalkan fungsi enkripsi E yang sederhana adalah XOR, P_i dengan K geser dengan *wrapping* bit-bit dari P ⊕ K satu posisi ke kiri.

Proses enkripsi untuk setiap blok sebagai berikut:

01000111 01001011 01000101 01000001
01000111 01000111 01000111 01000111⊕
XOR: 00000000 00001100 00000010 00000110
Geser: 00000000 00011000 00000100 00001100

Dalam bilangan ASCI : NUL CAN EOT FF

Jadi, hasil enkripsi plainteks
01000111 01001011 01000101 01000001
(GKEA dalam bilangan ASCII)
Adalah
00000000 00011000 00000100 00001100
(NUL CAN EOT FF dalam bilangan ASCII)

01000101 01001000 01010100 01001001
01000111 01000111 01000111 01000111⊕
XOR: 00000010 00001111 00010011 00001110
Geser: 00000100 00011110 00100110 00011100

Jadi enkripsi dari plainteks
01000111 01001011 01000101 01000001
01000101 01001000 01010100 01001001
01000101 01010010 01000101 01001100
01010100 01010111 01000101 01010100
(GKEAEHTIERELTWETY dalam bilangan ASCII)
Adalah
00000000 00011000 00000100 00001100 00000100 00011110 00100110 00011100 00000100 00101010 00000100 00010110 00100110 00100000 00000100 00100110
(NUL CAN EOT FF EOT RS & FS EOT + EOT SYN & SP EOT & dalam bilangan ASCII)

3.4 Proses Dekripsi ECB

Kebalikan dari proses enkripsi yaitu untuk mengubah kode dari yang tidak dapat dimengerti (cipherteks) menjadi sebuah kode yang dapat dimengerti (plainteks).

Dekripsi ECB
Cipherteks NUL CAN EOT FF EOT RS & FS EOT + EOT SYN & SP EOT &
Ubah ke biner
00000000 00011000 00000100 00001100 00000100 00011110 00100110 00011100 00000100 00101010 00000100 00010110 00100110 00100000 00000100 00100110
Geser Cipherteks 1 bit ke kanan
00000000 00001100 00000010 00000110 00000010 00001111 00010011 00001110 00000010 00010101 00000010 00001011 00010011 00010000 00000010 00010011
Kunci: 01000111 (G dalam bilangan ASCII)
Proses Dekripsi untuk setiap blok yaitu:

00000000 00001100 00000010 00000110
01000111 01000111 01000111 01000111 ⊕
XOR: 01000111 01001011 01000101 01000001
Jadi hasil dekripsi :
00000000 00001100 00000010 00000110
Adalah
01000111 01001011 01000101 01000001
(GKEA dalam bilangan ASCII)

00000010 00010101 00000010 00001011
01000111 01000111 01000111 01000111 ⊕
XOR: 01000101 01010010 01000101 01001100
Jadi hasil dekripsi
00000010 00010101 00000010 00001011
Adalah
01000101 01010010 01000101 01001100
(EREL dalam bilangan ASCII)

00000010 00001111 00010011 00001110
01000111 01000111 01000111 01000111 ⊕
XOR: 01000101 01001000 01010100 01001001
Jadi hasil dekripsi
00000010 00001111 00010011 00001110
Adalah
01000101 01001000 01010100 01001001
(EHTI dalam bilangan ASCII)

00010011 00010000 00000010 00010011
01000111 01000111 01000111 01000111 ⊕
XOR: 01010100 01010111 01000101 01010100
Jadi hasil dekripsi
00010011 00010000 00000010 00010011
Adalah
01010100 01010111 01000101 01010100
(TWET dalam bilangan ASCII)

Maka hasil dekripsi
00000000 00001100 00000010 00000110 00000010 00001111 00010011 00001110 00000010 00010101 00000010 00001011 00010011 00010000 00000010 00010011
(NUL CAN EOT FF EOT RS & FS EOT + EOT SYN & SP EOT & dalam bilangan ASCII)

Adalah
01000111 01001011 01000101 01000001 01000101 01001000 01010100 01001001 01000101 01010010 01000101 01001100 01010100 01010111 01000101 01010100
(GKEAEHTIERELTWETY dalam bilangan ASCII)

3.5 Dekripsi Affine Cipher

Cipherteks yang di hasilkan adalah :GKEAEHTIERELTWET
(yang ekivalen dengan 6, 10, 4, 0, 4, 7, 19, 8, 4, 17, 4, 11,19, 22, 4, 19 dengan 'A'=0, 'B'=1,……,'Z'=25)
Rumus
$P = m^{-1}(c-b) \pmod{26}$
X=15 (mod 26) sebab 7 . 15 =105 =1 (mod 26)
P= 15 (c-4) mod 26

C1= 6 → P1 = 15 . (6 - 4) mod 26
= 15 . 2 mod 26
= 30 mod 26
= 4 → E
C2= 10 → P2 = 15 . (10 - 4) mod 26
= 15 . 6 mod 26
= 90 mod 26
=12 → M
=0 → A
C16= 19→P16= 15 . (19 - 4) mod 26
= 15 . 15 mod 26
= 225 mod 26
=17 → R
Jadi dekripsi dari :
GKEAEHTIERELTWET
Adalah :
EMASATRIANABRKAR

5. KESIMPULAN

Adapun kesimpulan yang diperoleh dari penulisan skripsi ini adalah sebagai berikut:

1. Dengan menentukan kunci yang telah ditetapkan lalu diplainteks dan melakukan proses enkripsi sehingga menghasilkan cipherteks.
2. Pengamanan pesan dapat diterapkan dengan enkripsi *affine cipher* dan *electronic code book* (ecb).
3. Merancang aplikasi pengamanan pesan teks dari proses enkripsi dan dekripsi dengan menggunakan *software Visual Basic* 2008.

DAFTAR PUSTAKA

[1] R. Munir, "Algoritma & Pemrograman dalam Bahasa Pascal dan C Edisi Revisi," *Andi Yogyakarta*, 2011. https://openlibrary.telkomuniversity.ac.id/pustaka/21198/algoritma-pemrograman-dalam-bahasa-pascal-dan-c-edisi-revisi.html (accessed Feb. 19, 2020).
[2] D. Ariyus, "Kriptografi keamanan data dan komunikasi," *Yogyakarta Graha Ilmu*, 2006.
[3] T. Arianti and B. Nadeak, "Perancangan Aplikasi Pembelajaran Kriptografi Algoritma GOST dengan Menggunakan Metode Computer Based Instruction," *KAKIFIKOM (Kumpulan Artik. Karya Ilm. Fak. Ilmu Komputer)*, vol. 1, no. 1, pp. 40–46, 2019, [Online]. Available: http://ejurnal.stmik-budidarma.ac.id/index.php/jurikom/article/view/340.
[4] B. Silaban and T. Limbong, "Aplikasi Pembelajaran Pengenalan Kriptografi Algoritma Affine Cipher Dan Vigenere Cipher Menggunakan Metode Computer Assisted Instruction," *Media Inf. Anal. dan Sist.*, vol. 2, no. 2, pp. 14–20, 2017.
[5] H. Widya, "Sistem Pembelajaran dan Pemahaman Algoritma Electronic Code Book (ECB) Menggunakan Metode Computer Assisted Instruction (CAI)," *J. Electr. Technol.*, vol. 3, no. 3, 2018.
[6] R. Munir, "Kriptografi," *Inform. Bandung*, 2006.
[7] T. Limbong, "Pengujian Kriptografi Klasik Caesar Chipper Menggunakan Matlab," *no. Sept.*, vol. 2017, 2015.