Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 3 Nomor 2 September 2019, pp. 393-400
ISSN:2548-9771/EISSN:2549-7200
http://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Teknik Keamanan Data Menggunakan *Vigenere Cipher* Dan *Electronic Code Book* (ECB)

Adi Widarma[1], Helmi Fauzi Siregar[3], M.Dedi Irawan[3]
[1,2]Program Studi Teknik Informatika, Universitas Asahan
[3]Program Studi Sistem Informasi, Universitas Islam Negeri Sumatera Utara
adiwidarma10@gmail.com, fauzi.helmi.hf@gmail.com, temanseja2ti.dedi@gmail.com

Abstract

Data is important information both personal, group and company. Because of the importance of the data, many parties have kept the data very confidential so that it is not publicly recognized. But it cannot be denied that data can be stolen by unauthorized people. Request the data to be unsafe. A technique is needed to move data, namely by using cryptography. One of the existing cryptography techniques is classical cryptography such as vigenere cipher. However, this classic has a low level of security so it needs to be upgraded again. Then a combination of cryptography algorithms using modern cryptography, Electronic Code Book (ECB) is carried out. Using a combination of these two algorithms will improve data security.

Keywords*: cryptography, vigenere cipher, ECB, data security.*

Abstrak

Data merupakan informasi yang penting baik pribadi, kelompok maupun perusahaan. Karena pentingnya data banyak pihak yang sangat merahasiakan data tersebut agar tidak diketahui oleh umum. Tapi tidak bisa dipungkiri juga bahwasanya data bisa dicuri oleh orang yang tidak berhak. Akibatnya data tersebut menjadi tidak aman. Sehingga butuh teknik untuk mengamankan data yaitu dengan menggunakan kriptografi. Salah satu teknik kriptografi yang ada yaitu kriptografi klasik seperti vigenere cipher. Tetapi algoritma klasik ini memiliki tingkat kemanan yang rendah sehingga perlu ditingkatkan lagi keamanannya. Maka dilakukan kombinasi algoritma kriptografi dengan menggunakan kriptografi modern yaitu Electronic Code Book (ECB). Dengan menggunakan kombinasi dua algoritma tersebut akan meningkatkan keamanan data.

Kata kunci*: kriptografi, vigenere cipher, ECB, keamanan data.*

1. PENDAHULUAN

Pada era sekarang ini pengiriman dan pertukaran data secara digital tidak bisa dipungkiri sudah terjadi dan proses pengiriman data dilakukan dengan sangat cepat. Data yang dikirim kadang sering berisi data informasi yang penting bahkan sangat rahasia dan harus dijaga keamanannya [1].

Adanya pengiriman data tersebut terjadinya pertukaran data dimana didalam proses pertukaran data harus bisa dijamin data tersebut tidak diketahui oleh orang yang tidak berhak. Pengiriman pesan atau data digital perlu dirahasiakan untuk menjamin kemanan dan keutuhan data sehingga setiap orang yang memiliki data secara pribadi dan rahasia akan melakukan segala cara untuk menyimpan data tersebut agar tidak diketahui orang lain [2]. Masalah keamanan data merupakan salah satu aspek penting dari sebuah sistem informasi, sehingga masalah keamanan ini harus dijadikan perhatian khusus untuk menjamin data sebagai sistem informasi tetap aman [3][4].

Untuk mengamankan data digunakan teknik kriptografi. Kriptografi merupakan ilmu yang mempelajari bagaimana data atau pesan agar tetap rahasia. Untuk memenuhi aspek keamanan informasi salah satu tujuan kriptografi yaitu kerahasiaan data (*confidentiality*) dimana menjaga data agar tetap rahasia dari pihak-pihak yang tidak berwenang yang munkin membaca data tersebut [5]. Kerahasiaan data menggunakan teknik kriptografi adalah dengan mengenkripsi data atau pesan tersebut sehingga tidak mudah untuk diketahui isinya oleh pihak yang tidak berwenang. Pengamanan data ini menggunakan kombinasi algoritma kriptografi yaitu algoritma klasik *vigenere cipher* dan algoritma *Electronic Code Book* (ECB). *Vigenere cipher* adalah salah satu kriptografi algoritma standar, algoritma ini sangat sederhana dengan menggunakan substitusi untuk menyandikan teks pesan [6]. Sehingga dilakukan peningkatan keamanan dengan mengkombinasikan algoritma modern *Electronic Code Book* (ECB). Sehingga dengan menggunakan kombinasi kedua algoritma tersebut akan dapat meningkatkan keamanan dan kerahasiaan data tetap terjaga.

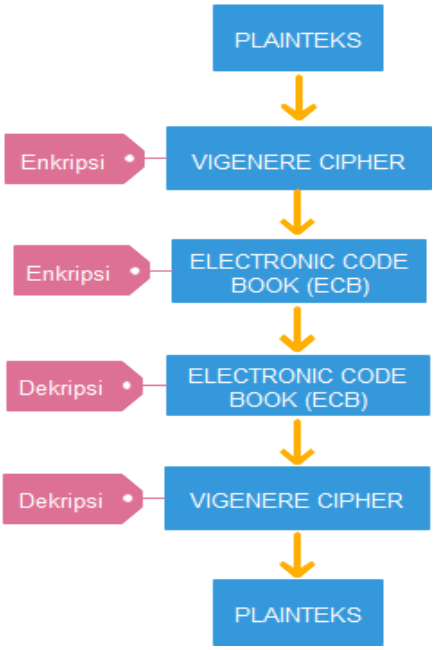
2. METODOLOGI PENELITIAN

2.1. Model Pengembangan

Metode pengembangan pada penelitian ini adalah kombinasi 2 algoritma kriptografi yaitu algoritma klasik menggunakan *vigenere cipher* dan algoritma modern menggunakan *Electronic Code Book* (ECB). Dari kombinasi dua algoritma tersebut proses enkripsi dan dekripsi dilakukan seperti tahapan berikut ini:

a. Pesan asli/plainteks akan dienkripsi dengan menggunakan *Vigenere Cipher*.
b. Hasil dari enkripsi *Vigenere Cipher* (cipherteks nya) dienkripsi kembali menggunakan *Electronic Code Book* (ECB).
c. Untuk mengembalikan pesan asli/plainteksnya, hasil enkripsi ECB akan didekripsi menggunakan algoritma ECB.
d. Hasil dari dekripsi ECB akan didekripsi kembali menggunakan algoritma *Vigenere Cipher*. Sehingga akan didapat pesan seperti semula.

Untuk lebih jelasnya, lihat gambar 3 model perancangan kombinasi algoritma vigenere cipher dengan *Electronic Code Book* (ECB).

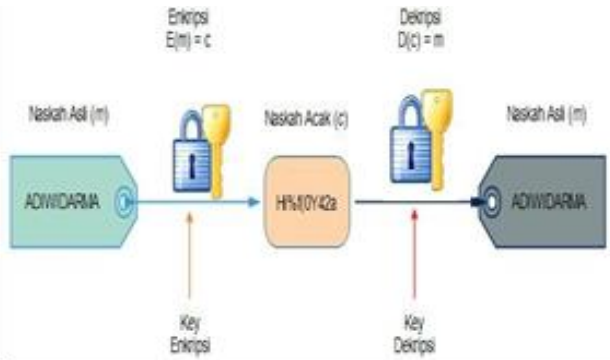


Gambar 1. Alur proses model pengembangan

2.2. Landasan Teori

1. Kriptografi

Kriptografi menurut Munir mengartikan Kriptografi (cryptography) berasal dari Bahasa Yunani kuno: "cryptós" yakni "secret" (rahasia), sedangkan "gráphein" yakni "writing" (tulisan). Jadi, kriptografi adalah "secretwriting" (tulisan rahasia). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain [7]. Secara umum, proses enkripsi dan dekripsi dapat dilihat seperti pada gambar dibawah ini.



Gambar 2. Proses Enkripsi dan Dekripsi [1]

2. Algoritma *Vigenere Cipher*

Vigenere Cipher ini adalah suatu metode yang dirancang untuk memperbaiki kelemahan dari algoritma subtitusi tunggal. *Vigenere cipher*

merupakan teknik kriptografi sederhana yang lebih aman. Dikembangkan dari metode *caesar cipher*, metode ini menggunakan karakter huruf sebagai kunci enkripsi [8].

Pada setiap baris di dalam bujursangkar Vigènere menyatakan huruf-huruf cipherteks yang diperoleh dengan *Caesar cipher*, dimana jumlah pergeseran huruf plainteks ditentukan nilai numeric huruf kunci tersebut (yaitu, a=0, b=1, c=2, d=3, e=5…, z=25).

Model matematis algoritma *vigenere cipher* dapat dihitung dengan menggunakan persamaan (1) dan (2):

Enkripsi : Ci = Pi + ki mod 26 (1)
Dekripsi : Pi = Ci - ki mod 26 (2)

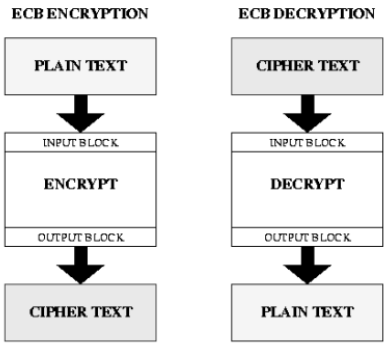
Kunci pada Vigenere Cipher dipakai berulang kali sebanyak pesan yang akan dienkripsi. Semakin beragam huruf alfabetik yang dipakai sebagai kunci, maka semakin kuat juga keamanan algoritma *Vigenere Cipher* ini [7].

3. *Electronic Code Book* (ECB)

Pada mode operasi ECB sebuah blok input plaintext dipetakan secara statis ke sebuah blok output ciphertext. Sehingga tiap plaintext yang sama akan menghasilkan ciphertext yang selalu sama pula. Sifat- sifat dari mode operasi ECB [4]:

a) Sederhana dan efisien
b) Memungkinkan implementasi parallel
c) Tidak menyembunyikan pola Plaintext

Adapun skema dari system kriptografi *Electronic Code Book* (ECB) adalah sebagai berikut :



Gambar 3. Mode Operasi ECB

3. HASIL DAN PEMBAHASAN

Diberikan contoh kasus kombinasi algoritma klasik dan modern yaitu *vigenere cipher* dan *Electronic Code Book* (ECB) dengan plainteks "KEAMANAN" sedangkan kuncinya "CIPHER". Proses pertama sekali yaitu mengenkripsi plainteks menggunakan *vigenere cipher*.

3.1. Proses Enkripsi tahap pertama menggunakan Vigenere Cipher

Dalam contoh ini panjang kunci lebih pendek daripada panjang plainteks maka kunci diulang secara periodik sampai panjang kunci sama dengan panjang plainteks. Setelah dilakukan pengulangan maka kunci menjadi:

Plainteks : KEAMANAN
Kunci : CIPHERCI

Dengan menggunakan rumus secara matematis : Ci = (Pi + Ki) mod 26 maka didapat hasil perhitungan seperti tabel 1.

Tabel 1. Enkripsi menggunakan *Vigenere Cipher*

Plainteks (P)	K	E	A	M	A	N	A	N
Indeks	10	4	0	12	0	13	0	13
Kunci (K)	C	I	P	H	E	R	C	I
Indeks	2	8	15	7	4	17	2	8
(P+K) mod 26	12	12	15	19	4	4	2	21
Cipherteks	M	M	P	T	E	E	C	V

Dari tabel 1 didapat hasil cipherteksnya adalah "MMPTEECV". Hasil cipherteks tersebut kemudian dienkripsi kembali menggunakan ECB.

3.2. Proses Enkripsi tahap kedua menggunakan Electronic Code Book (ECB)

Plainteksnya adalah cipherteks hasil enkripsi Vigenere Cipher.

Plainteks : MMPTEECV
Kunci : ADI

Untuk mengenkripsi menggunakan ECB melalui tahapan berikut:

1. Konversi plainteks ke dalam bentuk decimal setelah itu konversi ke biner.

Tabel 2. Konversi Plainteks ke Biner

Plainteks (P)	ASCII	Biner
M	77	01001101
M	77	01001101
P	80	01010000
T	84	01010100
E	69	01000101
E	69	01000101
C	67	01000011
V	86	01010110

2. Konversi kunci ke dalam bentuk decimal setelah itu konversi ke biner.

Tabel 3. Konversi Kunci ke Biner

Kunci (K)	ASCII	Biner
A	65	01000001
D	68	01000100
I	73	01001001

3. Lakukan operasi XOR plainteks dengan kunci

Tabel 4. Operasi XOR plainteks dengan kunci

Plainteks (P)	Kunci (K)	P XOR K
01001101	01000001	00001100
01001101	01000100	00001001
01010000	01001001	00011001
01010100	01000001	00010101
01000101	01000100	00000001
01000101	01001001	00001100
01000011	01000001	00000010
01010110	01000100	00010010

4. Lakukan penggeseran tiap block satu bit ke kanan dari hasi operasi XOR dan hasil dari pergeseran konversi ke hexadecimal.

Tabel 5. Pergeseran 1 bit ke kanan dan hasil konversi ke hexadesimal

P XOR K	Geser 1 bit ke kanan	Konversi ke Hexadesimal
00001100	00011000	18
00001001	00010010	12
00011001	00110010	32
00010101	00101010	2A
00000001	00000010	2
00001100	00011000	18
00000010	00000100	4
00010010	00100100	24

Maka didapat hasil cipherteksnya dalam hex adalah 18 12 32 2A 2 18 4 24. Hasil dari cipherteks tahap ke dua ini kemudian didekripsi menggunakan ECB.

3.3. Proses Dekripsi tahap pertama menggunakan ECB

Dari hasil enkripsi tahap kedua didapat cipherteks “18 12 32 2A 2 18 4 24”, kemudian dekripsikan dengan menggunakan kunci “ADI”. Untuk melakukan proses dekripsi tahapannya dapat dilihat pada tabel 6.

Tabel 6. Tahapan proses dekripsi menggunakan ECB

Cipherteks (C)	Konversi ke Biner	Geser 1 bit ke kiri	Kunci (K)	Hasil geser XOR Kunci	Konversi ke Hexasimal
18	00011000	00001100	01000001	01001101	77
12	00010010	00001001	01000100	01001101	77
32	00110010	00011001	01001001	01010000	80
2A	00101010	00010101	01000001	01010100	84
2	00000010	00000001	01000100	01000101	69
18	00011000	00001100	01001001	01000101	69
4	00000100	00000010	01000001	01000011	67
24	00100100	00010010	01000100	01010110	86

Dari tabel 6 hasil dari konversi ke decimal kemudian kita konversi ke bentuk Character menjadi “MMPTEECV”

3.4. Proses Dekripsi tahap kedua menggunakan Vigenere Cipher.

Dari hasil dekripsi tahap pertama didapat cipherteks “MMPTEECV” kemudian lakukan proses dekripsi tahap kedua dengan menggunakan kunci “CIPHERCI”. Dengan menggunakan rumus secara matematis : Pi = (Ci - Ki) mod 26 maka didapat hasil perhitungan seperti tabel 7.

Tabel 7. Dekripsi menggunakan *Vigenere Cipher*

Ciphertkes (C)	M	M	P	T	E	E	C	V
Indeks	12	12	15	19	4	4	2	21
Kunci (K)	C	I	P	H	E	R	C	I
Indeks	2	8	15	7	4	17	2	8
(C+K) mod 26	10	4	0	12	0	13	0	13
Plainteks	K	E	A	M	A	N	A	N

Dari tabel 7 didapat hasil plainteks adalah “KEAMANAN”. Sama dengan plainteks awalnya.

4. SIMPULAN

Dari hasil penelitian diatas dapat disimpulkan bahwa:

a) Teknik Keamanan data dengan mengkombinasikan Electronic Code Book (ECB) dan Vigenere Cipher dapat dilakukan serta dapat meningkatkan keamanan, karena kompleksitas dua algoritma hasil ciphertext juga jauh lebih rumit daripada menggunakan satu algoritma.
b) Kerugiannya ada pada enkripsi dan dekripsi proses karena melibatkan dua algoritma yang berbeda membutuhkan waktu tambahan untuk diproses.

DAFTAR PUSTAKA

[1] A. Widarma, "Kombinasi Algoritma AES, RC4 dan Elgamal Dalam Skema Hybrid Untuk Keamanan Data," *J. Comput. Eng. Syst. Sci.*, vol. 1, no. 1, pp. 1–8, 2016.

[2] F. Anita, "Implementasi Algoritma Modular Multiplication Based Block Cipher Dalam Mengamankan Data Teks," *MEANS (Media Inf. Anal. dan Sist.*, vol. 3, no. 2, pp. 121–125, 2018.

[3] E. Gunadhi and A. Sudrajat, "Pengamanan Data Rekam Medis Pasien Menggunakan Kriptografi Vigenere Cipher," *J. Algoritm.*, vol. 13, no. 1, pp. 1–7, 2016.

[4] A. Mufid, "Teknik Enkripsi Dan Deskripsi Menggunakan Algorithma Electronic Code Book (ECB)," *J. Tek. Unisfat*, vol. 6, no. 1, pp. 21–25, 2010.

[5] H. Mukhtar, *Kriptografi Untuk Keamanan Data*. Yogyakarta: Deepublish, 2018.

[6] S. D. Nasution, G. L. Ginting, M. Syahrizal, and R. Rahim, "Data Security Using Vigenere Cipher and Goldbach Codes Algorithm," *Int. J. Eng. Res. Technol.*, vol. 6, no. 1, pp. 360–363, 2017.

[7] R. Munir, *Kriptografi*. Bandung: Informatika, 2006.

[8] B. Ariska, Suroso, and J. Endri, "Rancangan Kriptografi Hybrid Kombinasi Metode Vigenere Cipher Dan Elgamal Pada Pengamanan Pesan," in *Seminar Nasional Inovasi dan Aplikasi Teknologi di Industri*, 2018, pp. 328–336.