Jurnal Ilmu Komputer Indonesia (JIKI) Vol : 5, No. 1, Februari 2020
ISSN (Print) : 2615-2703 , ISSN (Online): 2615-2711

PERBANDINGAN WAKTU ENKRIPSI ANTARA METODE ELECTRONIC CODEBOOK (ECB) DAN CHIPHER BLOCK CHAINING (CBC) DALAM ALGORITMA BLOWFISH

[1]Ida Ayu Widyantari Arnawa, [2]Putu Eka Widastra Hary C., [3]A. A. Gede Bimantara Putra
[1,2,3]Program Pasca Sarjana Ilmu Komputer, Universitas Ganesha
Email: [1]dayu.infor@gmail.com, [2]arycandana@gmail.com, [3]gungdebima08@gmail.com

ABSTRAK

Seiring dengan perkembangan dunia teknologi dan informasi, kriptografi menjadi hal yang amat penting karena kriptografi banyak digunakan untuk menjaga kerahasiaan dan keamanan informasi. Pengoptimalan kerja dari kriptografi ini, perlu ditunjang oleh algoritma – algoritma pendukung. Perkembangan algoritma – algoritma pendukung untuk ilmu kriptografi sudah sangat banyak dikembangkan dan diimplementasikan. Algoritma chipper blok banyak dikembangkan seiring dengan perkembangan era teknologi. Penemuan algoritma Blowfish ini mulai banyak dianalisis kembali sehingga semakin lama algoritma ini mulai dapat diterima sebagai sebuah algoritma enkripsi yang memiliki keamanan level tinggi. Dalam pengimplementasian algoritma blowfish memerlukan adanya suatu memori yang besar sehingga dengan pemanfaatan memori yang besar ini akan berdampak terhadap waktu eksekusi dari algoritma. Berdasarkan hasil pengimplementasian dan pengujian terhadap metode algoritma blowfish, metode ECB memerlukan waktu yang lebih cepat dalam melakukan enkripsi teks jika dibandingkan dengan menggunakan metode CBC. Sehingga ini dapat dijadikan suatu pertimbangan dalam pemilihan metode yang tepat dalam pemanfaatan algoritma blowfish.

Kata Kunci: Kiptografi, Algoritma Blowfish, Metode ECB, Metode CBC

ABSTRACT

Along with the development of the world of technology and information, cryptography becomes very important because cryptography is widely used to maintain the confidentiality and security of information. Optimization of the work of cryptography, needs to be supported by supporting algorithms. The development of supporting algorithms for cryptography has been very much developed and implemented. The block chipper algorithm was developed in line with developments in the technological era. The discovery of the Blowfish algorithm began to be analyzed again so that the longer the algorithm began to be accepted as an encryption algorithm that has a high level of security. In implementing the blowfish algorithm requires a large memory so that the utilization of large memory will have an impact on the execution time of the algorithm. Based on the results of the implementation and testing of the blowfish algorithm method, the ECB method requires a faster time to do text encryption when compared to using the CBC method. So that this can be taken into consideration in the selection of the right method for using the blowfish algorithm.

***Keywords** : Ciptography, Blowfish Algorithm, ECB Method, CBC Method*

I. PENDAHULUAN

Dalam perkembangan dunia teknologi dan informasi, kriptografi meenjadi hal yang sangat penting dan wajib karena kriptografi banyak digunakan untuk menjaga kerahasiaan dan keamanan informasi. Pengoptimalan kerja dari kriptografi ini, perlu ditunjang oleh algoritma – algoritma pendukung. Perkembangan algoritma – algoritma pendukung untuk ilmu kriptografi sudah sangat banyak dikembangkan dan diimplementasikan. Beberapa algoritma yang banyak dimanfaatkan dalam kriptografi misalnya seperti algoritma blok, yang dimana algoritma ini akan beroperasi setiap saat dengan ukuran 64 bit. Selain itu juga algoritma aliran juga banyak dimanfaatkan dalam kriptografi, dimana algoritma ini bekerja dengan membuat suatu potongan data dengan ukuran potongan yang lebih bervariasi. Dilihat dari sisi desain dan pengimplementasiannya dalam kriptografi algoritma chiper blok lebih lebih sulit dan rumit daripada algoritma chiper aliran.

Algoritma chipper blok banyak dikembangkan seiring dengan perkembangan era teknologi, salah satunya adalah metode Blowfish yang ditemukan oleh Bruce Schneier tahun 1993. Penemuan algoritma Blowfish ini mulai banyak dianalisis kembali sehingga semakin lama algoritma ini mulai dapat diterima sebagai sebuah algoritma enkripsi yang memiliki keamanan level tinggi. Algoritma blowfish sendiri adalah algoritma yang tidak mempunyai hak paten dan juga algoritma ini memiliki free lisensi. Walaupun perkembangan teknologi informasi sangat tinggi namun sampai sekarang belum dapat ditemukan suatu *attack* yang dapat memecahkan kode enkripsi dari algoritma blowfish ini.

Dalam pengimplementasian algoritma blowfish memerlukan adanya suatu memori yang besar sehingga dengan pemanfaatan memori yang besar ini akan berdampak terhadap waktu eksekusi dari algoritma. Kesalahan dalam penyusunan strategi implementasi akan berpengaruh terhadap tidak optimalnya kerja algoritma blowfish. Terkait permasalahan ini maka penulis membuat suatu implementasi terkait pengujian waktu eksekusi algoritma dalam melakukan enkripsi teks dengan metode Electronic Codebook (ECB) dan Chipher Block Chaining (CBC) sehingga algoritma blowfish akan dapat bekerja lebih optimal.

II. LANDASAN TEORI

A. Kriptografi

Ilmu Kriptografi berkaitan dengan teknik penjagaan keamanan dari suatu data atau pesan, sehingga data yang dikirim dapat sampai kepada si penerima dengan aman dan tanpa ada gangguan dari pihak manapun. Di dalam buku "Applied Cryptography" yang di tulis Bruce Scheiner, kriptografi merupakan ilmu pengetahuan dan seni menjaga keamanan message-message(pesan). Ilmu kriptografi ini mempunyai dua konsep dasar yaitu enkripsi dan deskripsi. Enkripsi merupakan suatu proses yang dimana data maupun informasi yang dikirim oleh pengirim diubah menjadi suatu data maupun informasi yang tidak dapat dikenali dan sangan berbeda dengan data aslinya. Sedangkan deskripsi adalah mengubah data yang telah dienkripsi menjadi sesuai dengan data awal yang sudah dikirimkan. Berdasarkan jenis kuncinya algoritma kriptografi dikategorikan menjadi dua jenis yaitu sebagai berikut.

a. Algoritma Simetris
   Pada algoritma ini memiliki jenis kunci yang sama dalam proses enkripsi dan deskripsinya.
b. Algoritma asimetris
   Pada algoritma ini memiliki jenis kunci yang berbeda dalam proses enkripsi dan deskripsi.

Di dalam satu kali proses terhadap besar data yang diolah Kriptografi memiliki dua jenis algoritma yaitu sebagai berikut.

a. Algoritma block cipher
   Pada algoritma ini data maupun informasi yang dikirim akan berbentuk suatu blok –

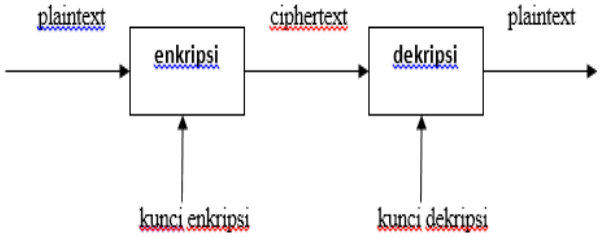
blok besar. Blok – blok yang telah terbentuk akan dioperasikan dengan menggunakan fungsi enkripsi yang sama sehingga terbentuk suatu informasi yang rahasia dan memiliki ukuran blok yang sama

b. Algoritma stream cipher
Pada algoritma ini data maupun informasi yang dikirim akan memiliki ukuran blok lebih kecil jika dibandingkan dengan algoritma block chipper. Data maupun informasi yang diproses menggunakan algoritma ini akan mengalami perubahan setiap waktunya dalam melakukan tahapan enkripsi.

Antara kriptografi modern dan kriptografi klasik memilki beberapa perbedaan yaitu pada kriptografi klasik lebih menekankan pada kerahasian dari algoritma yang digunakan sedangkan pada kriptografi modern lebih menekankan pada kerahasiaan dari kunci yang digunakan dalam algoritma tersebut. Beberapa istilah – istilah yang banyak digunakan dalam ilmu kriptografi adalah sebagai berikut.

a. Plaintext (M) merupakan pesan yang akan dikirim dan merupakan data asli
b. Ciphertext (C) merupakan hasil enkripsi yang berbentuk pesan ter-enkrip (tersandi)
c. Enkripsi (fungsi E) adalah proses perubahan dari plaintext menjadi ciphertext.
d. Dekripsi (fungsi D) merupakan lawan dari enkripsi dengan melakukan perubahan dari ciphertext menjadi plaintext dan merupakan data asli
e. Kunci merupakan bilangan rahasia yang dimanfaatkan dalam melakukan proses enkripsi dan dekripsi

Berdasarkan pemaparan diatas, gambar 1 menggambarkan mengenai gambaran umum dari proses terjadinya enkripsi dan deskripsi.



Gambar 1. Diagram proses enkripsi dan dekripsi

Dalam melakukan proses enkripsi dan deskripsi, *kunci* memilki peranan sangat penting selain peran dari algoritma itu sendiri. Berdasarkan hal ini maka dapat ditarik tiga persamaan dengan variabel – variabel sebagai berikut.

E = Enkripsi
e = kunci enkripsi
M = plaintext
C = ciphertext
D = deskripsi

Ee(M) – C (1)

Pada proses deskripsi adalah mengoperasikan fungsi D (deskripsi) dan menggunakan d (kunci dekripsi) pada C (ciphertext) agar dihasilkan M (plaintext), notasinya :

Dd(C) = M (2)

Berdasarkan dua persamaan diatas muncul persamaan ke-3 yaitu sebagai berikut.

Dd(Ee(M)) = M (3)

B. Algoritma Blowfish

Pada mode operasi ECB akan dilakukan pemetaan secara statis dari blok input plaintest ke blok output chipertext. Cihpertext yang selalu sama akan dihasilkan pada proses ini.

A. Cipher Block Chaining

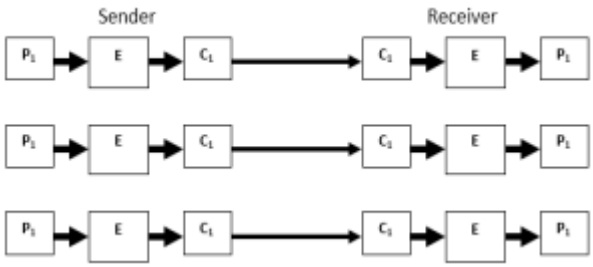
Cipher block chaining memiliki hasil enkripsi yang berkaitan dengan hasil enkripsi dari block sebelumnya. Sehingga pada proses ini setiap block chipertext tidak hanya ditentukan

dari block tersebut tapi ditentukan juga dari block plaintext sebelumnya dan walupun plaintexnya sama hasilnya bisa saja berbeda.

B. Electronic Codebook (ECB)

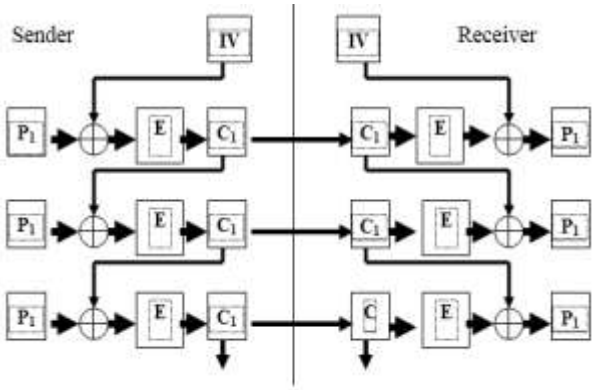
Electronic Code Book (ECB) adalah mode operasi untuk cipher blok, dimana karakteristiknya setiap blok plaintext yang mungkin mempunyai nilai ciphertext yang ditentukan dan sebaliknya. Atau lebih tepatnya, nilai plaintext yang sama akan selalu menghasilkan nilai ciphertext yang sama.

III. METODOLOGI



Gambar 2. Skema Mode Operasi ECB

Gambar 2 merupakan mode operasi dari ECB. Pada mode operasi ECB sebuah blok input plaintext akan dipetakan secara statis dalam sebuah blok output ciphertext, sehingga berdasarkan hal tersebut maka akan menghasilkan suatu ciphertext yang selalu sama.



Gambar 3. Skema Mode Operasi CBC

Gambar 3 merupakan skerma dari mode operasi CBC. Pada mode ini pengiriman data dimulai dengan meng-XOR suatu plaintext dengan IV (initialization vector) dan setelah itu barulah dilakukan enkripsi yang dimana setelah enkripsi dilakukan maka chipertext pertama akan dikirim kepada sipenerima. Plaintext ke-2 pun demikian, harus di-XOR terlebih dahulu dengan ciphertext sebelumnya, sebelum mengalami proses enkripsi dan setelah proses ini selesai barulah penerima akan mendapatkan chipertext kedua dan proses ini dilakukan secara berulang.

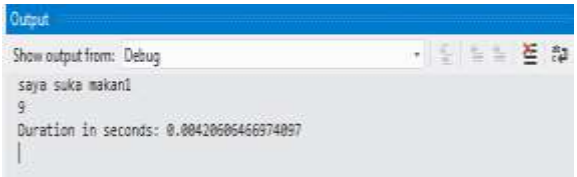
IV. IMPLEMENTASI

A. Implementasi Sistem

Untuk tahap implementasi, dibuat dua buah program, dimana masing-masing program mewakili algoritma blowfish mode ECB dan program yang lainya menggunakan algoritma twofish.

Gambar 1 Tampilan Awal Sistem Blowfish

Pada gambar 5 merupakan hasil dari waktu eksekusi dalam proses enkripsi teks dengan algoritma blowfish



Gambar 5. *Output* sistem

B. Hasil Pengujian

Berdasarkan hasil pengimplementasian dari pemanfaatan ekripsi dengan menggunakan metode ECB dan CBC, maka hasil pengujian dapat dilihat pada tabel 1. Tahap pengujian ini dilaksanakan dengan melakukan enkripsi terhdap file yang memiliki ukuran yang berbeda, yang dimana ukuran filenya terus ditingkatkan pada setiap pengujian, sehingga semakin bertambahnya ukuran file maka waktu yang dbutuhkan juga semakin banyak, selain itu juga metode ECB membutuhkan durasi waktu yang lebih sedikit jika dibandingkan dengan durasi metode CBC.

Tabel 1. Hasil Pengujian Perbandingan Metode ECB dan CBC

NO	PENGUJIAN KE-	UKURAN FILE	DURASI ECB	DURASI CBC
1	1	1 Kb	0.0014	0.0015
2	2	10 Kb	1.7232	1.86
3	3	50 Kb	10.5915	10.6089
4	4	100 Kb	22.8865	23.0848
5	5	307 Kb	94.1629	95.3569
6	6	645 Kb	281.9444	291.6284
7	7	860 Kb	437.1055	438.3978
8	8	1,04 Mb	640.4346	667.0611
9	9	1,48 Mb	1155.3553	1278.2239
10	10	2,08 Mb	2144.073	2229.6943

V. SIMPULAN

Berdasarkan hasil pembahasan diatas maka dapat ditarik suatu kesimpulan bahwa waktu yang yang dibutuhkan dalam proses enkripsi teks akan berbanding lurus dengan ukuran teks yang akan dienkripsi. Selain itu juga metode ECB membutuhkan waktu yang lebih cepat dalam melakukan enkripsi teks jika dibandingkan dengan menggunakan metode CBC. Sehingga ini dapat dijadikan suatu pertimbangan dalam pemilihan metode yang tepat dalam pemanfaatan algoritma blowfish.

REFERENSI

[1] Adhitya Randy. **Studi dan Perbandingan Algoritma Blowfish dan Twofish.Laboratorium** Ilmu dan Rekayasa Komputasi Progam Studi Teknik Informatika, Institut Teknologi Bandung 2010.

[2] Jawahar Thakur, Nagesh Kumar. 2011. **DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis. International Journal of Emerging Technology and Advanced Engineering**. ISSN 2250-2459, Volume 1, Issue 2, December 2011

[3] Mollin, R. A. 2007. **An Introduction to Cryptography. 2nd ed.** Florida: Chapman & Hall/CRC.

[4] Dimas,Herlina.2015 **Analisis Perbandingan Kinerja Algoritma Blowfish dan Algoritma Twofish Dalam Peoses Enkripsi dan Deskripsi.** Fakultas Ilmu Komputer Universi tas Dehasen Bengkulu.2015

[5] Jawahar Thakur, Nagesh Kumar. 2011. **DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis. International Journal of Emerging Technology and Advanced Engineering**. ISSN 2250-2459, Volume 1, Issue 2, December 2011

[6] Candra Alim Sutanto. 2009**Penggunaan Algoritma Blowfish Dalam Kriptografi**. Jurnal Teknologi Informasi. Jakarta : Teknik Informatika ITB.

[7] Munir, Rinaldi (2004). **Bahan Kuliah IF5054 Kriptografi**.Departemen Teknik Informatika, Institut Teknologi Bandung.