PERANCANGAN MODIFIKASI KRIPTOGRAFI MODERN CBC UNTUK PENGAMANAN DATA/FILE TEXT

Nur Rochmah Dyah P.A
Teknik Informatika Universitas Ahmad Dahlan Yogyakarta
Jl. Prof. Soepomo, Janturan, Yogyakakarta
Email : rochmahdyah@tif.uad.ac.id, rochmahdyah@yahoo.com

ABSTRAK

CBC (Cipher Block Chaining) sebagai salah satu metode dasar kriptografi modern yang bekerja dalam block telah banyak dikaji untuk meningkatkan kemanan data. Penggunaan kunci dalam metode ini terjadi secara berulang dan sama dalam setiap block. Hal ini memungkinkan terjadinya hasil ciphertext yang berulang pada plaintext yang sama. Penelitian ini bertujuan untuk mengembangkan metode cryptography CBC dengan memodifikasi algoritma tersebut. Modifikasi dilakukan dengan menggabungkan atau menerapkan metode Vigenere Cipher dan metode Block Transposition pada proses teknis CBC guna meningkatkan keamanan.

Penelitian ini menghasilkan rancangan proses enkripsi dan dekripsi CBC termodifikasi dengan menggabungkan metode Vigenere cipher dan Block Transposition. Uji validitas pada metode CBC termodifikasi tersebut dilakukan dengan manual proses baik untuk enkripsi maupun dekripsi. Dengan modifikasi pada teknis CBC akan meningkatkan keamanan informasi yang terkirim.

Kata kunci : Kriptografi, Algoritma CBC, Block Transpotition, Vigenere Cipher.

1. PENDAHULUAN

Cryptography merupakan seni dan ilmu yang digunakan untuk menjaga atau mengamankan data/pesan. Suatu *crypto*sistem yang baik tidak bergantung pada kerahasiaan dari algoritma yang digunakan Schneier [1996). Dalam mempelajari *Cryptography*, kreatifitas dalam memodifikasi dan mengimplementasikan sangat penting, karena pemanfaatan dan implementasi di lapangan akan sangat bergantung pada pemahaman tersebut. Menurut Sastry [2010] dalam *cryptanalysis*, modifikasi akan dapat meningkatkan satu kekuatan dari metode tersebut.

Menurut Menezes, dkk [1997, h.242] Algoritma *Cipher Block Chaining* (CBC) merupakan salah satu metode *cryptography* yang berbasis pada *block*, pada metode ini mempunyai kelebihan setiap *block ciphertext* bergantung tidak hanya pada *block plaintext*nya tetapi juga pada seluruh *block plaintext* sebelumnya. Sehingga kesalahan satu bit pada sebuah *block plaintext* akan merambat pada *block ciphertext* yang berkoresponden dan semua *block ciphertext* berikutnya, semua dikarenakan *block ciphertext* yang dihasilkan selama proses enkripsi tergantung pada *block-block ciphertext* sebelumnya.

Untuk meningkatkan tingkat kompleksitas, pengembangan dapat dilakukan dengan improvisasi terhadap teknik-teknik tersebut.

Pada penelitian ini algortima CBC akan dimodifikasi dengan algoritma *Vigenere* dan blok transposition yang hasil dari penelitian dapat meningkatkan keamanan data terkirim,

dapat digunakan sebagai acuan telaah atas pengembangan metode *cryptography*, selain itu juga memberikan pengayaan referensi materi bagi mahasiswa dan peneliti lain untuk konsep atau teknik pengembangan metode *cryptography*.

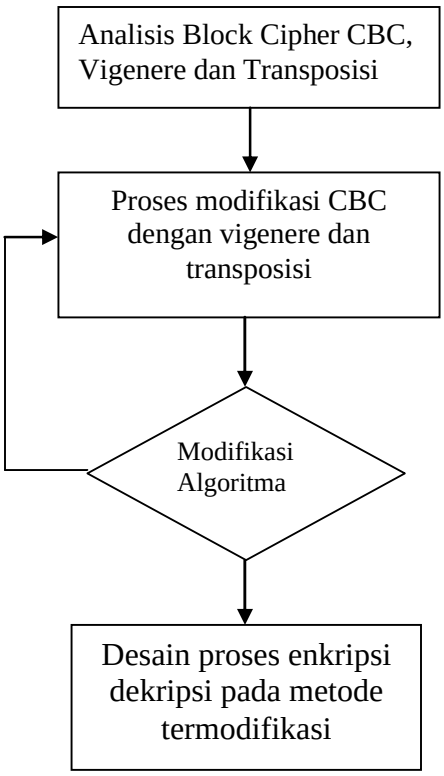
Beberapa permasalahan yang akan diselesaikan dalam penelitian ini antara lain :

a. Bagaimana menentukan teknik memodifikasi metode *cryptography modern Block cipher* CBC baik untuk proses enkripsi maupun dekripsi. Untuk menyelesaikan permasalahan ini akan dilakukan analisis atas algoritma CBC, algoritma *vigenere* dan blok transposition dengan aktivitas yang dilakukan antara lain diskusi dengan ahli dan studi literatur guna menemukan teknik yang dapat digunakan untuk menerapkan proses modifikasi.
b. Bagaimanan merancang modifikasi metode *cryptography modern Block cipher* (CBC) baik untuk proses enkripsi maupun dekripsi hasil dari permasalahan sebelumnya. Perancangan dilakukan dengan mendesain proses teknik modifikasi pada ketiga algortima.
c. Jika permasalahan tersebut terselesaikan, dilanjutkan dengan bagaimana melakukan pengujian atas hasil tersebut baik untuk proses enkripsi maupun dekripsi?
d. Bagaimana menuangkan hasil proses tersebut dalam suatu laporan yang mudah dimengerti oleh peneliti lain. Penyelesaian permasalahan tersebut diharapkan akan memacu peneliti lain untuk melakukan pemanfaatan Kriptografi secara lebih optimal.

2. METODE PENELITIAN

Pada penelitian ini akan dibahas tentang memodifikasi *cryptography modern Cipher Block Chaining (CBC)* dengan menggabungkan metode *Vigenere cipher* dan metode *Block Transposition* guna meningkatkan improvisasi pada teknik yang ada pada metode tersebut. Proses modifikasi akan digunakan untuk karakter-karakter yang dapat dienkripsi dan dekripsi adalah karakter-karakter yang berbentuk teks murni atau *file* teks.

Metode yang digunakan pada proses modifikasi yaitu *Cipher Block Chaining (CBC)*, metode *Vigenere cipher* dan metode *Block Transposition*. Penelitian diawali dengan tahap penganalisaan metode *Cipher Block Chaining (CBC), Vigenere cipher, Block Transposition* yang digunakan untuk mengetahui kelebihan dan kekurangan dari metode algoritma tersebut, analisis dilakukan dengan studi literature, diskusi dengan pakar, maupun studi pustaka. Hasil dari analisis digunakan sebagai dasar proses improvisasi pada teknik yang ada pada ketiga metode untuk dilakukan moodifikasi penggabungan.



Gambar 1. Alur modifikasi algoritma CBC

Proses modifikasi dimulai dari analisis metode *CBC*, *Vigenere* cipher, dan *Block transposition* dengan tujuan menemukan kemungkinan teknik untuk proses dilakukannya modifikasi pada ketiga metode. Setelah ditemukan teknik untuk modifikasi maka dilakukan proses pengembangan dengan memodifikasi proses enkripsi dan dekripsi ketiga metode. Pada proses pengembangan ini apabila tidak berhasil maka akan dilakukan analisis kemungkinan untuk modifikasi kembali.

Secara garis besar proses utama yang terjadi dalam sistem yang akan dibangun pada metode *cryptography* ada dua yaitu enkripsi dan dekripsi.

a. Proses **Enkripsi,** merupakan proses mengamankan suatu data/informasi awal yang disebut plainteks yang akan dikirimkan dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Pada proses pertama ini alur program yang akan dibangun membutuhkan input berbentuk data / informasi berupa teks atau file teks dan *private-key* yang berfungsi sebagai validasi, sedangkan output berupa cipherteks.
b. Proses **Dekripsi,** merupakan proses kebalikan dari proses enkripsi, merubah cipherteks kembali ke dalam bentuk plainteks. Pada proses kedua ini input berupa cipherteks yang akan dirubah menjadi data/informasi yang bisa dibaca dengan memberikan *private-key* untuk mendekripsi pesan.

Terdapat dua buah entitas yaitu pengirim yang akan memberikan masukan ke sistem yang berupa karakter teks yang terdiri dari 81 karakter yaitu huruf besar, huruf kecil, angka, dan simbol-simbol dalam bentuk plainteks ataupun cipherteks Dari hasil masukan yang

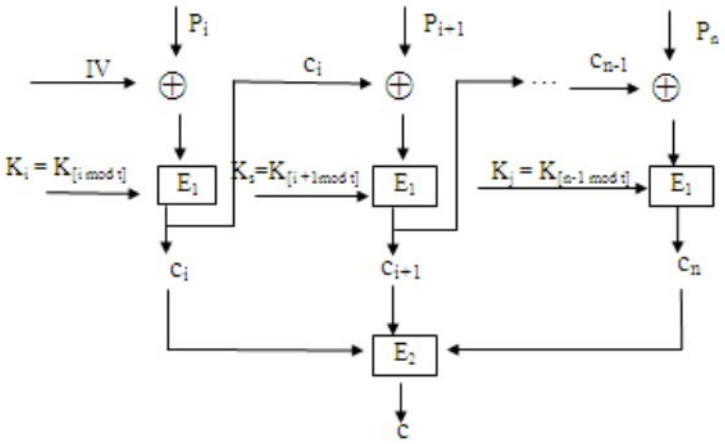
diberikan oleh pengirim, sistem akan memberikan *output* berupa karakter teks dari hasil enkripsi (cipherteks) atau dekripsi (plainteks) kepada penerima.

3. HASIL DAN PEMBAHASAN

3.1 Proses Enkripsi Modifikasi

Dari penelitian ini, dapat dihasilkan metode *CBC* termodifikasi dengan meningkatkan improvisasi pada teknik yang ada dengan menerapkan keunggulan metode *Vigenere cipher* dan metode *Block Transposition*. Hasil improvisasi yang ada pada metode CBC modifikasi adalah terdapat dua proses enkripsi pada teknik CBC modifikasi. Enkripsi modifikasi pertama (*E1*) ada pada proses penempatan kunci. Kunci pada metode *CBC* yang awalnya bernilai tetap untuk setiap *block*, dengan menggabungkan metode *Vigenere cipher* maka kunci akan selalu berubah mengikuti panjang kunci pada setiap block. Proses diawali dengan input-bit plainteks, kunci dan initialisasi vektor ditentukan sebagai C_0 dalam format teks murni, semua input dikonversi dalam bilangan biner. Plainteks ke-1 akan di-XOR-kan dengan *Initialization Vektor (IV)*, lalu di-XOR-kan dengan kunci (K_i), K_i adalah kunci pada indek ke i dengan nilai 31-35i = 1..n yang dimodulus dengan t dimana t < n, hasil dari enkripsi ini adalah cipherteks (C_i). Jika hasil $K_i = 0$ maka i diubah menjadi nilai t. C_i akan digunakan untuk peng-XOR-an P_{i+1} yang hasilnya akan di-XOR-kan dengan kunci (K_s). Untuk plainteks ke n maka bloks plainteks akan di-XOR-kan dengan C_{n-1} yang hasilnya akan di-XOR-kan dengan kunci (K_j), dimana $j=i \ mod \ t$ dengan j=1..t, yang akan menghasilkan cipherteks ke n (C_n).

Enkripsi modifikasi kedua (*E2*) merupakan kelanjutan dari proses pertama, terdapat pada system pembacaan cipherteks hasil enkripsi pertama (*E1*) dilakukan dengan metode *block transposition*, modifikasi ini dimaksudkan untuk mengurangi kelemahan pada *CBC* yaitu pembacaan cipherteks menggunakan konsep blok yang monoton sehingga dengan mudah kripanalis untuk mengetahui pesan yang terkirim, dengan merubah posisi pembacaan hasil enkripsi dengan menggunakan *block.* Pembacaan cipherteks akan berurutan menurut kolom. Cipherteks yang awalnya terbagi dalam 3 block dengan 8 bit tiap blocknya akan menjadi 8 kolom dengan 3 bit setiap kolomnya, sehingga pembacaan akan urut dari kolom pertama sampai kolom ke-8 atau ke-n.Skema metode CBC termodifikasi dapat dilihat pada Gambar 2



Gambar 2. Skema proses enkripsi algoritma *CBC* termodifikasi

Dimana :

t : merupakan panjang kunci
n : merupakan panjang plainteks
i, s : merupakan indek plainteks dengan nilai dari 1 sampai n
j : merupakan indek kunci dengan nilai dari 1 sampai t yang didapat dari nilai (i mod t), nilai j akan menjadi t jika hasil modulus = 0
IV : merupakan *initial vector* yang dapat bernilai random, namun dalam contoh pembahasan diberikan nilai 00000000
Pi : plainteks pada indek ke i
Ci : cipher teks pada indek ke i
C : hasil cipher teks akhir

Deskripsi skema CBC modifikasi sebagai berikut, enkripsi 1 *(E1)* yaitu penempatan kunci yang digunakan *Vigenere cipher* akan diterapkan pada teknik CBC modifikasi. Bloks plainteks yang *current* di-XOR-kan dengan bloks cipherteks hasil enkripsi sebelumnya, yang selanjutnya hasil akan di-XOR-kan dengan kunci.

Pada teknik CBC modifikasi penentuan indeks kunci *K* dinyatakan berturut-turut dengan persamaan :

$$K_i = K_{[\ i \bmod t\ ]} \quad (12)$$

kunci ke-*i* didapat dari nilai i dimodulus dengan *t*, dimana *t* merupakan panjang kunci dan *i* merupakan indek plainteks dengan nilai dari 1 sampai *n*. Untuk plainteks ke-2 dan seterusnya maka indek kunci menjadi K_s dimana s merupakan indek plainteks dengan nilai 1 sampai n, persamaan K_s menjadi

$$K_s = K_{[i+1 \bmod t]} \quad (13)$$

sedangkan untuk plainteks ke-*n*, penentuan kunci K_j menggunakan persamaan

$$K_j = K_{[n-1 \bmod t]} \quad (14)$$

j merupakan indek kunci dengan nilai dari 1 sampai t, indeks kunci akan menjadi *t* jika hasil modulus adalah 0.

Sehingga persamaan enkripsi maupun dekripsi dari CBC modifikasi berturut-turut adalah

$$C_i = E_{Ki}(P_i \oplus C_{i-1}) \quad (15)$$

$$C_{i+1} = E_{Ks}(P_{i+1} \oplus C_{i-1}) \quad (15)$$

.
.
.

$$C_n = E_{Kj}(P_n \oplus C_{i-1}) \quad (16)$$

dan dekripsi adalah

$$P_i = D_{Ki}(C_i \oplus C_{i-1}) \quad (17)$$

$$P_{i+1} = D_{Ks}(C_{i+1} \oplus C_{i-1}) \quad (18)$$

.
.

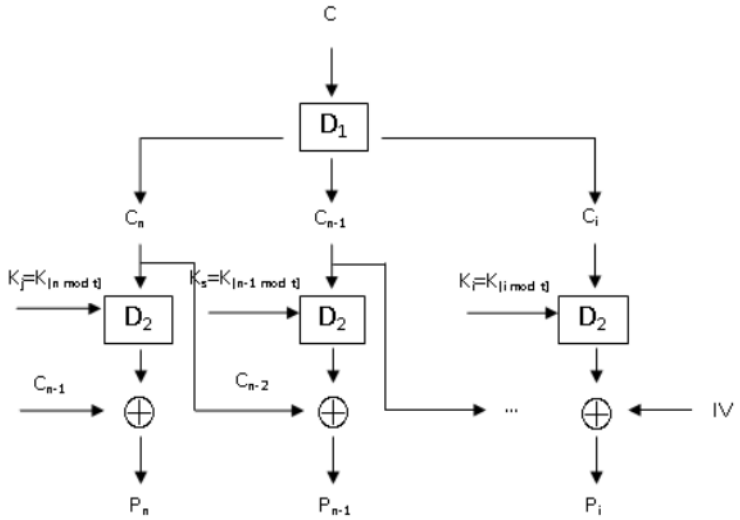
$$P_n = D_{Kj}(Cn \oplus C_{i-1}) \quad (19)$$

Hasil enkripsi 1 disebut dengan output intermediate atau output antara yang akan diproses kembali dengan enkripsi 2 (E2).

Proses enkripsi 2 *(E_2)*, pembacaan cipherteks akhir dilakukan secara *Block Transpotition*. Output intermediate dari C_i sampai C_n akan dibaca secara *Block Transpotition* atau transposisi kolom, output dari proses adalah Ciperteks akhir (C) yang akan diubah ke dalam hexadecimal.

3.2 Proses Dekripsi Modifikasi

Terdapat dua proses dekripsi yaitu D_1 merupakan dekrip dengan *block transpotition* dan D2 merupakan dekrip dengan kunci metode *Vigenere cipher*. Pendekripsian Cipherteks dengan metode *block transposition*, diawali dengan mengkonversi cipherteks hexa ke biner. untuk menetukan jumlah kolom maka jumlah biner cipherteks di DIV 8, hasil persamaan ini adalah jumlah kolom, yang selanjutnya akan didekrip dengan CBC modifikasi *Vigenere cipher*. Dekripsi dimulai dari cipherteks paling akhir (C_n) di-XOR-kan dengan kunci ke-*i* sampai ke-*n*, hasil akan di-XOR-kan kembali dengan cipherteks sebelumnya (C_{n-1}). Pembacaan hasil dekripsi dimulai dari urutan plainteks awal (P_1). Skema proses dekripsi modifikasi CBC dapat dilihat pada Gambar 3



Gambar 3. Skema proses dekripsi algoritma *CBC* termodifikasi

3.3 Pseudocode Algortima CBC Termodifikasi

Pseudocode proses enkripsi pada modifikasi dapat dilihat dalam Gambar 4.2 :

```
ENKRIPSI (input plaintext PT,kunci K tipe char) tipe Char
{
    Deklarasikan variable pjT,pjK, i,j → integer
    Tamp, binPT,binK,C,C2,Output → char
    Tetapkan IV←'00000000'
    pjT ← panjang (PT),  pjK ← panjang (K)
    binPT ← ubahbiner(  PT[1])
    Tamp  ←  binPT[1] XOR IV
    binK ← ubahbiner (K[1])
    Tamp ← Tamp XOR binK
    C[1]← wrapkiri1[tamp]
    C ← C[1]
    // proses enkripsi CBC dengan penggabungan Vigenere
    For  (i=2 ; i<= pjT ; i++ )
    {
        binPT ← ubahbiner(  PT[i])
        Tamp ← binPT[i] XOR C[1]
        j ← i MOD pjK
        If j = 0 then j = pjK
        binK ← ubahbiner (K[j])
        Tamp ← wrapkiri1 (Tamp)
        C[i] ← Tamp XOR binK
        C ← C + C[i]; }
    // proses enkripsi tranposisi block/kolom
    For (j=1 ; j<=8 ; j++ )
    {
        For (i=1 ; i<=panjang(C) MOD 8 ; i++ )
            {C2[j] ←C2 +  C2[i] }
        C2= C2 + C[j] }
    UbahHexa (C2);
    Output = C2
}
```

Gambar 4.2 *Pseudocode* Enkripsi CBC modifikasi.

4. KESIMPULAN

Setelah dilakukan langkah-langkah modifikasi terhadap metode CBC dengan menggabungkan metode *Vigenere* dan *Block* Transposisi kedalamnya maka dapat ditarik beberapa kesimpulan

a. Keunggulan penggunaan kunci majemuk secara berulang dalam metode *Vigenere Cipher* dapat digunakan dalam proses enkripsi maupun dekripsi dalam metode CBC.
b. Metode *block transposition* dapat digunakan untuk menambah proses enkripsi maupun dekripsi pada metode CBC yang dimaksudkan untuk menghindari pembacaan dengan konsep blok yang monoton pada pleinteks dan cipherteks.
c. Proses enkripsi dan dekripsi pada metode CBC modifikasi dengan menggunakan metode *Vigenere Cipher* untuk penempatan kunci dan *Block Transpotition* untuk pembacaan hasil telah memenuhi kaidah yang ada dalam metode Kriptografi.

5. DAFTAR PUSTAKA

Hashem,S.H., AL-Hamami,M.A. dan AL-Hamami,A.H., 2011. *Developing a Block-Cipher-Key Generator Using Philosophy of Data Fusion Technique*, Journal of Emerging Trends in Computing and Information Sciences. Volume 2 No.5.

Husni dan Haret,F., 2006. Tutorial Kriptografi Klasik dan penerapan dalam VB. Kuliah Umum Ilmukomputer.Com.

Khar,S., 2012. *Implementation Of Enhanced Modifies Hill Cipher P-Box and M-Box Technique*, International Journal of Information Technology and Knowledge Management, Januari-Juni 2012, Volume 5, No.1, 53-58.

Kumar,U.S., Sastry,V.U.K. dan Babu,A.V., 2006. *A Large Block cipher using an Iterative Method and the Modular Arithmetic Inverse of a key Matrix*, IAENG International Journal of Computer Science, 32:4, IJCS_32_4_ 2.

Mahdi,G.S., 2010. A *Modification of TEA Block Cipher Algorithm for Data Security (MTEA).* Eng.& Tech. Journal ,Vol.29, No.5, 2011.

Menezes,A.J., 1996. Pengantar Ilmu Kriptografi teori analisis, http://id.shvoong.com/internet-and-technologies/websites/2294629-pengantar-ilmu-kriptografi-teori-analisis/#ixzz20GRIylGd, (01 juni 2012).

Menezes,A.J. dan Oorschot,P.C., 1997. *Handbook of Applied Cryptography*. CRC Press.

Munir,R., 2010. Materi kuliah *Cryptography*. http://www.informatika.org/~rinaldi /Cryptography/2010-2011/baru.ppt.

Sastry,V.U., Shankar,N.R. dan Bhavani, S.D., 2010. *A Modified Hill Cipher Involving Interweaving and iteration*, International Journal of Network Security Vol.11, 11-16.

Wicaksono,K.N., 2009. Modifikasi *Vigenere Cipher* dengan Menggunakan Teknik Substitusi Berulang Pada Kuncinya . http://www.informatika.org/~rinaldi/Cryptography/2008-2009/Makalah1-2009.html., (2 des 2010).

Willam,S., 2003. *Cryptography and Network Security*, Principles and Practices. Pearson Prentice Hall, hal.37.