DESAIN KRIPTOGRAFI CBC MODIFIKASI PADA PROSES PENGAMANAN PESAN MELALUI EMAIL

Nur Rochmah D.P.A, ST, M.Kom [1], Ardiansyah ST., M.Cs [2]

(1) Fakultas Teknik Indutri,Pgoram Studi Teknik Informatika, Universitas Ahmad Dahlan Yogyakarta, Email rochmahdyah@tif.uad.ac.id
(2) Fakultas Teknik Indutri,Pgoram Studi Teknik Informatika, Universitas Ahmad Dahlan Yogyakarta, Email ardiansyah@tif.uad.ac.id

Abstrak

Keamanan data untuk pertukaran data berbasis internet menjadi suatu keharusan karena jaringan internet yang bersifat publik dan global pada dasarnya kurang aman. Begitu juga untuk E-dokumen yang menggunakan media internet dalam pertukaran datanya. E-document dapat berupa e-mail atau dokumen dalam pesan e-mail. Metode yang banyak digunakan salah satunya dengan teknik penyandian atau kriptografi. Dengan memodifikasi Algortima kriptografi maka tingkat kekuatan dari penyadap *(attacker)* algoritma dapat ditingkatkan. Modifikasi CBC dengan menggabungkan metode vigenere dan transposisi telah terbukti dapat digunakan pada data/file berbentuk teks. Untuk lebih membuktikan keberhasilan CBC modifikasi maka akan dibuat aplikasi pengamanan e-document menggunakan konsep kriptografi CBC modifikasi tersebut. Metode yang digunakan dalam penelitian ini dengan tahapan perancangan system dengan menggunakan *use case diagram,* activity diagram dan sequence diagram. Dan mengimplementasikannya dalam bahasa pemrograman. Testing dilakukan untuk membuktikan bahwa pada proses enkripsi, plainteks dapat dirubah dalam bentuk cipherteks. Dalam bentuk cipherteks inilah maka document akan terkirimkan lewat email. Setelah terkirim maka akan dibuktikan bahwa cipherteks dapat dikembalikan kedalam bentuk plainteks (pesan asli) dengan proses dekripsi.

Key Word : Kriptografi, CBC modifikasi, E-Document

1. Pendahuluan

E-dokumen merupakan pertukaran data yang berbasis komputer dengan menggunakan media internet, dapat berupa e-mail atau dokumen dalam pesan e-mail. Keamanan data berbasis internet menjadi suatu keharusan karena jaringan internet yang bersifat publik dan global pada dasarnya kurang aman. Untuk menjaga kerahasiaan suatu pesan maupun data dari pihak yang tidak berhak atau penyadap *(attacker)* salah satu proses yang sudah banyak digunakan adalah dengan kriptografi. Kriptografi adalah bidang ilmu dan seni yang bertujuan menjaga kerahasiaan suatu pesan yang berupa data-data dari pihak lain. Banyak algortima yang bisa digunakan dalam kriptografi, yang masing-masing algoritma mempunyai karakter dan spesifikasi yang berbeda-beda. Kekuatan suatu kriptografi tergantung pada bagaimana memodifikasi metode atau algortima yang ada. Modifikasi biasanya dilakukan dengan tujuan meningkatkan keamanan terhadap data.

Dari penelitian terdahulu yang dilakukan oleh Nur Rochmah dengan judul "Perancangan Modifikasi Kriptografi Modern CBC Untuk Pengamanan Data/File Text", telah dihasilkan modifikasi algortima CBC dengan menggabungkan algoritma Vigenere cipher dan transposisi. Pembuktian modifikasi masih dilakukan menggunakan data atau file berbentuk text (.doc / .docs).

Algortima CBC modifikasi akan diterapkan dalam proses pengamanan data yang akan dikirim melalui email. Untuk menerapkannya maka akan dibangun aplikasi berupa sistem pengiriman email dengan proses enkripsi dan dekripsi dengan menggunakan algortima CBC termodifikasi dengan Vigenere dan Transposisi dengan bentuk data teks yang dapat meningkatkan keamanan data terkirim.

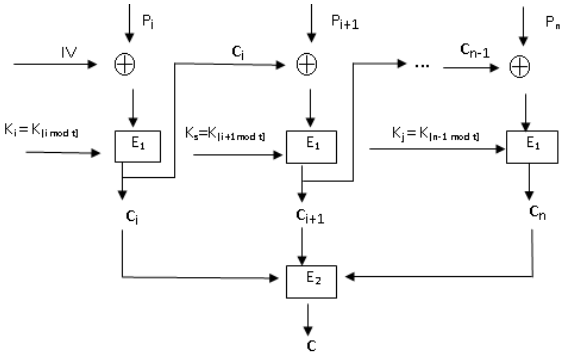
2. Kajian Teori

Penelitian Rano Alyas : 2014, dihasilkan aplikasi *hybrid cryptosystem* untuk pengamanan e-dokumen menggunkana algoritma RC4, RSA dan MD5. Aplikasi ini mampu meningkatkan keamanan dalam mengirim dokumen rahasia dengan cara enkripsi dan dekripsi karena RC4 digunakan sebagai pengamanan data, RSA sebagai pengamanan kunci dan MD5 sebagai integritas data.

Cipher Block Chaining (CBC) Termodifikasi

Metode CBC modifikasi adalah hasil modifikasi algortima CBC dengan vigenere ipher dan transposisi. Terdapat dua proses enkripsi dan dua proses dekripsi. 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. Perubahan setiap kunci pada setiap blok akan mempersulit kripanalis dalam memperkirakan keterhubungan setiap blok plainteks yang akhirnya untuk keseluruhan pesan.

Enkripsi modifikasi kedua (*E2*) merupakan pembacaan cipherteks hasil enkripsi pertama (*E1*) dilakukan dengan metode *block transposition*, pembacaan cipherteks menggunakan konsep *block tansposition*.



Gambar 1. *Skema algortima CBC termodifikasi (Astuti: 2012)*

penentuan indeks kunci *K* dinyatakan berturut-turut dengan persamaan :

$$K_i = K_{[\,i \bmod t\,]} \quad \text{.....(1)}$$

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

$$K_s = K_{[i+1 \bmod t]} \quad \text{.....(2)}$$

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

$$K_j = K_{[n-1 \bmod t]} \quad \text{.....(3)}$$

Sehingga persamaan enkripsi CBC modifikasi adalah

$$C_i = E_{Ki}\,(P_i \oplus C_{i-1})$$
$$C_{i+1} = E_{Ks}\,(P_{i+1} \oplus C_{i-1})$$
.
.
.
$$C_n = E_{Kj}\,(P_n \oplus C_{i-1}) \quad \text{.....(4)}$$

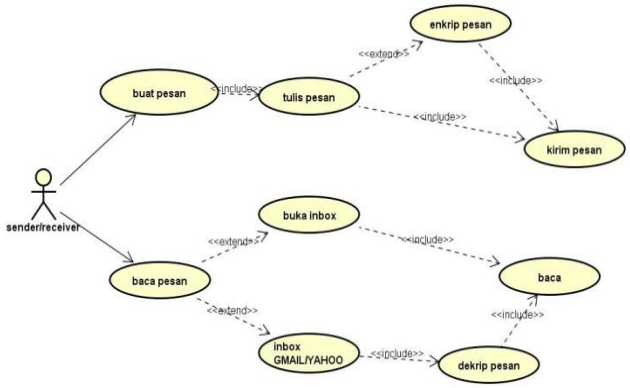
Sedangkan untuk persamaan dekripsi CBC modifikasi adalah

$$P_i = D_{Ki}(C_i \oplus C_{i-1})$$
$$P_{i+1} = D_{Ks}\,(C_{i+1} \oplus C_{i-1}) \quad .$$
.
.
$$P_n = D_{Kj}\,(Cn \oplus C_{i-1}) \quad \text{.....(5)}$$

3. Pembahasan

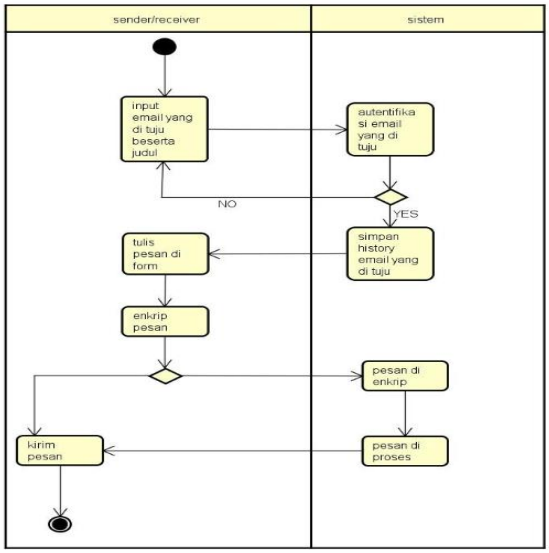
Proses analisis sistem menggunakna metode terstruktur (*structures approach*). Target dan kebutuhan sistem akan digambarkan secara terstruktur dengan use case. Aplikasi K-Email menggunakan input teks berbentuk data/teks maupun file, dalam proses enkripsi maupun dekripsi menggunakan algoritma CBC modifikasi.

Use case diargam pada gambar 2 menggambarkan proses pengiriman email yang terdapat dua pilihan proses, pesan yang akan diemail berupa teks asli dan pesan yang terenkripsi yang bertujuan agar isi email tidak dapat terbaca oleh user yang bukan tujuan pengiriman.



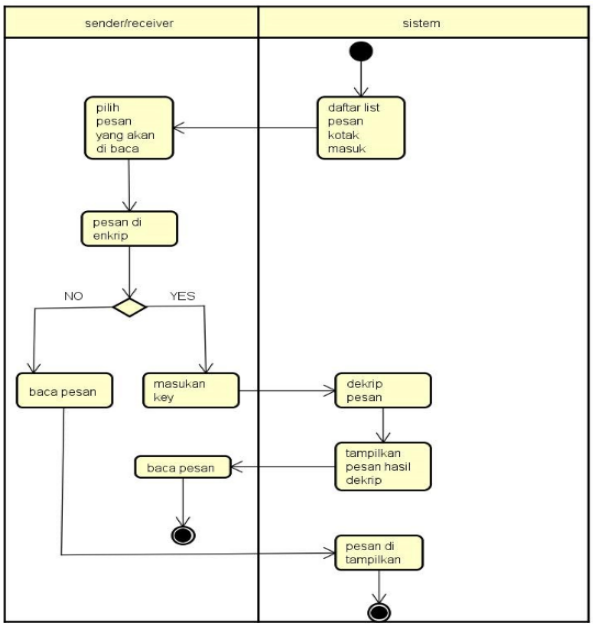
Gambar 2. *Use Case diagram K-Email*

Activity diagram menggambarkan proses pengiriman dengan baik menggunakan proses enkripsi pesan terlebih dahulu maupun pesan asli, untuk pengiriman pesan dalam bentuk cipherteks sistem akan meminta key untuk proses enkripsinya sebelum mengirimkan email. Apabila pengiriman. Jika pengiriman email tanpa proses enkripsi maka sistem akan langsung memproses kirim.



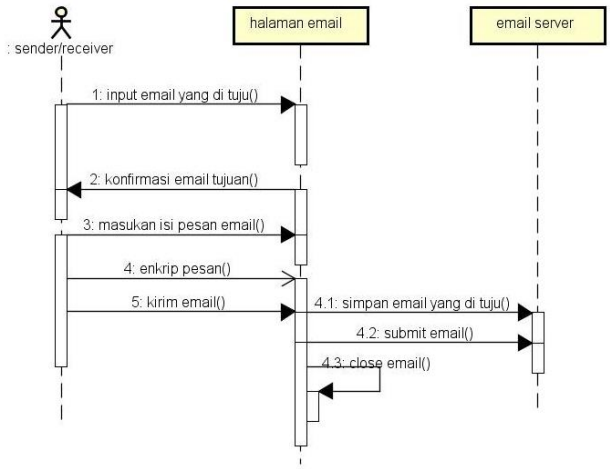
Gambar 3*. Activity diagram menulis pesan*

Proses pembacaan pesan terkirim jika pesan biasa maka sistem akan langsung membuka pesan yang ada pada inbox. Jika pesan yang akan dibaca merupakan pesan berbentuk cipherteks maka akan melalui proses dekripsi dengan memasukkan key dan sistem akan memproses dekripsi pesan dan menampilkan pesan bentuk plainteks atau asli.



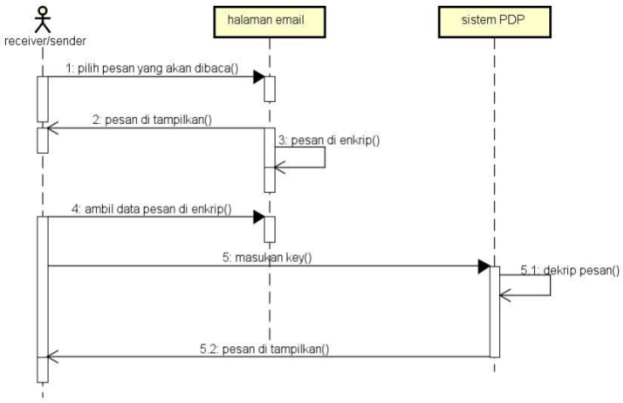
Gambar 4. *Activity diagram proses baca email*

Pengiriman email dengan pesan berbentuk cipherteks diawali dengan memasukkan pesan yang akan dikirim dihalaman email yang sudah disediakan, proses kirim pesan dengan memasukkan key sebagai kunci untuk proses enkripsi data/pesan. Hasil dari proses enkripsi pesan berbentuk cipherteks yang tidak dapat dibaca maknanya dilanjutkan proses kirim.



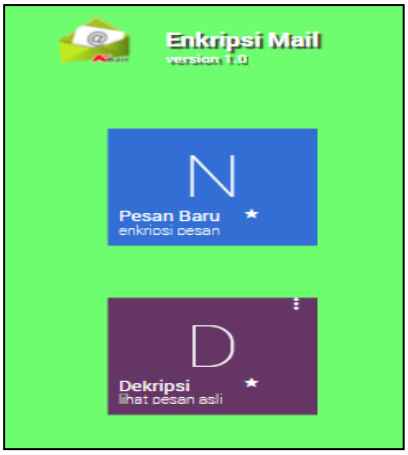
Gambar 5. *Sequence diagram kirim email dengan proses enkripsi.*

Untuk membaca email masuk pesan berbentuk plainteks atau pesan asli maka tidak perlu ada proses dekripsi, jika pesan masuk berupa cipherteks maka pesan dibuka untuk proses dekripsi pesan. Proses dekripsi diawali dengan memasukkan key untuk membuka kunci pesan, jika berhasil maka sistem akan menampilkan pesan asli yang terkirimkan ke pada penerima.



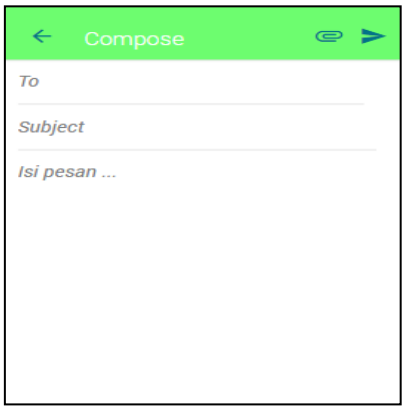
Gambar 6. *Sequence diagram baca email dengan proses dekripsi*

Pada menu utama terdapat dua proses yaitu proses enkripsi pesan dan proses dekripsi. Proses enkripsi digunakan untuk pesan yang akan dikirim dalam bentuk cipherteks. Menu dekripsi digunakan untuk mengembalikan pesan bentuk cipherteks ke bentuk plainteks sehingga penerima dapat membaca isi pesan.



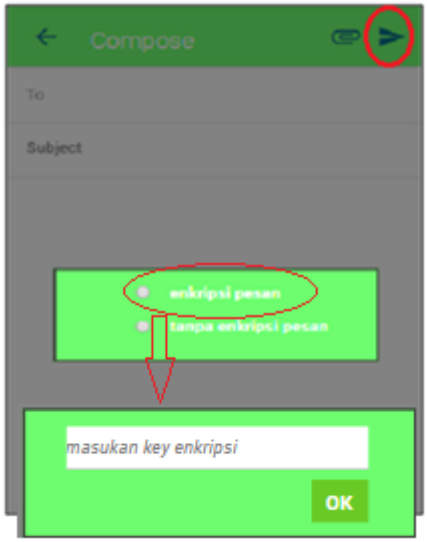
Gambar 7. *Tampilan Menu Utama*

Form tulis pesan berfungsi untuk proses penulisan pesan yang akan dikirim. Terdapat tiga masukan yaitu *to* untuk memasukkan alamat email yang akan dituju, *subject* merupakan judul dari isi pesan, dan *isi pesan* untuk menulis atau membuat pesan yang akan dikirm.



Gambar 8. *Form Tulis Pesan*

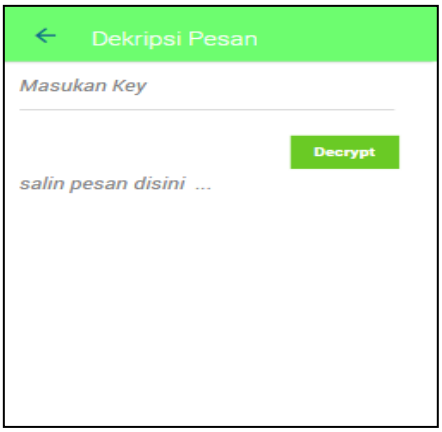
Icon kirim akan memunculkan dialog pemilihan bentuk pesan yang akan terkirim. Terdapat dua pilihan yaitu pesan dengan proses enkripsi dan pesan tidak dengan proses enkripsi. Pada proses enkripsi pesan yang akan dikirim sistem akan meminta masukkan key.



Gambar 9. *Dialog Memasukkan Key*

Setelah memasukkan key maka sistem akan memproses enkripsi pesan dan mengirimkan pesan yang berbentuk cipherteks ke alamat email yang telah ditentukan.

Pada interface membaca pesan berbentuk ciphertek maka sistem akan melalui proses dekripsi pesan dengan memasukkan key yang sudah ditentukan dan menyalin pesan berbenttuk cipherteks ke form salin pesan, setelah itu proses dekripsi bisa diproes setelah buttom decrypt dipilih.



Gambar 10. *Form proses dekripsi pesan.*

PRoses pengujian sistem dapat Dilakukan untuk proses pengiriman pesan email berbentuk cipherteks dengan proses enkripsi dan mengembalikan pesan bentuk cipherteks ke bentuk asli yang dapat dibaca oleh penerima dengan memasukkan key.

4. Kesimpulan

Sistem K-Email dengan menggunakan algortima CBC modifikasi pada proses enkripsi dan dekripsi pesan yang terkirim dapat meningkatkan keamanan pada proses email, sistem mempunyai layanan inbox untuk membaca email baik yang pesan bentuk cipherteks maupun pesan asli dan kirim email baik dengan proses enkripsi maupun email biasa tanpa proses enkripsi.

Daftar Pustaka

[1] Alfred J. Menezes,Paul C. van Oorschot , "Handbook of Applied *Kriptografi* , CRC Press, 1997

[2] Alyas Rano, "*Hybrid Cryptosystem* Untuk Pengamanan E-Dokumen Menggunakan Algoritma Rc4, Rsa Dan Md5", naskah publikasi, amikom Yogyakarta, 2014

[3] Amorita Kurnia Dewi, Nia Kaniawati, dan Rizki Hustiniasari; 2010; *Keamanan Blok Cipher dengan Algoritma COBRA-F64;* http://www.informatika.org/~rinaldi/Kriptografi/Makalah/Keamanan Blok Cipher dengan Algoritma COBRA-F64.pdf ; diakses 04 Sept 2010.

[4] Hadi Ahmaddul, *"Rancang bangun sistem pengamanan dokumen pada sistem informasi akademik dengan menggunakan digital signature",* jurnal teknologi informasi dan pendidikan vol.6 no.2 september 2013.

[5] Menezes Alfred J., Oorschot Paul C. van . 1997. *Handbook of Applied Cryptography*. CRC Press.

[6] Munir, Renaldi. 2010. *Materi kuliah Cryptography*. http://www.informatika.org/~rinaldi/*Cryptography*/2010-2011/Algoritma%20*Cryptography*%20Modern_bag2%20(baru).ppt

[7] Willam Stallings, *Cryptography and Network Security*, Principles and Practices. Pearson Prentice Hall, 2003

[8] umi fatimah, 2014:3, *Use Case diagram*; fatimahumi.blogspot.co.id/2014/03/**uml-usecase-diagram**.html; diakses 07 agustus 2016.

[9] nn, 2013, *activity diagram*; http://informatika.web.id/activity-diagram-2.htm, Posted on **January 25, 2013**