PROTEKSI EMAIL ENKRIPSI BASIS ANROID DENGAN MENGGUNAKAN METODE ALGORITMA RIVEST CODE 6 DAN BLOWFISH

Isfan Fajar Satria[1)], Rizky Tahara Shita[2)]
[1]*Teknologi Informasi, Fakultas Teknologi Informasi, Universitas Budi Luhur*
[1,2]*Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260*
E-mail : isfanfajarsatria21@gmail.com[1)], rixky.tahara@gmail.com[2)]

ABSTRAK

Pesatnya perkembangan di dunia teknologi terutama pada bidang informasi sangatlah memungkinkan terjadinya pencurian data yang bersifat rahasia. Terutama bagi perusahan besar yang sering melakukan pengiriman data pesan, file dengan email dan menggunakan perangkat mobile android. Perlu adanya sebuah keamanan informasi yang aman. Dimana pertumbuhan jaman semakin pesat dengan pengaruh perkembangan mobile yang sangat mudah dalam memberikan informasi. Dengan adanya keamanan email maka file attachment digunakan algoritma kriptografi Rivest Code 6 (RC6) dan Blowfish. metode algoritma Rivest Code 6 (RC6) dirancang untuk sistem keamanan mutakhir adalah mampu beroperasi pada blok 128 bit. RC6 menggunakan 4 register 32 bit maka akan terdapat 2 operasi rotasi pada setiap half-round, dengan terdapatnya rotasi mengakibatkan RC6 lebih aman, ditambah dengan satu metode Blowfish yang Sangat cepat dalam proses enkrip dan dekrip, mempunyai kemanan yang bervariasi,tergantung panjang kunci yang akan dipergunakan oleh Blowfish sangat bervariasi dan minimal 32-bit dan maksimal panjang 448 -bit. maka pengamanan pesan dan file yang dikirim ataupun diterima melalui email jadi lebih aman dan cepat. oleh sebab itu pengamanan berdasarkan kriptografi dilakukan berawal dari teks asli yang di istilahkan dengan sebutan plaintext dimana artinya teks asli yang belum di enkripsi, setelah proses enkripsi terjadi, terdapat hasil enkripsi yg disebut dengan chipertext, karena dari itu aplikasi keaman email menggunakan metode kriptografi adalah konsep efektif bagi sistem keamanan email.

Kata Kunci : Keamanan Email, Blowfish, Rivest Code 6, Kriptografi

1. PENDAHULUAN

Dengan pesatnya perkembangan dunia informatika, karena itulah pertumbuhan dunia semakin pesat dimana semua penunjangan kehidupan manusia perlu adanya kemajuan teknologi yang bersifat informasi-informasi penting yang harus terjaga oleh suatu sistem keamanan yang dimana mempengaruhin kebutuhan global.

Jaringan internet pada saat ini menjadi sumber informasi. Berdasarkan kenyataan di atas, perlu ada suatu sistem pengamanan informasi baik saat pengiriman maupun penerimaan email. Untuk melakukan hal ini maka harus adanya penyandian informasi berupa suatu simbol-simbol terenkripsi yang dimana penyandian sangat sulit untuk dipecahkan. Dengan ilmu matematika kriptografi, data dapat diubah menjadi penyandian yang sulit di mengerti oleh sembarang orang dan mengembalikannya ke bentuk semula, proses ini disebut Enkripsi dan Dekripsi. Algoritma enkripsi ternyata sudah cukup banyak dan bermacam-macam. Dalam laporan ini, akan menggunakan metode enkripsi dan dekripsi Rivest Code 6 (RC6) dan Blowfish.

2. LANDASAN TEORI

2.1. Email

Elektronic mail (surat elektronik, e-mail) sebuah metode menggubah, menerima, mengirim, dan menyimpan pesan maupun attachment file melewati jalur komunikasi elektronik. Istilah email Pesan yang diterima berupa teks acak, terkadang mengandung tanda pengenal di bagian awal maupun akhir. Pada mulanya didesain menggunakan 7-bit ASCII, namun sekarang sebagian besar menggunakan 8-bit, namum belum bersifat keseluruhan.

2.2. Kriptografi

Kriptografi merupakan teknik merandomkan suatu data spesifik menggunakan kunci enkripsi penyandian yang sulit dibaca bagi seseorang yang tidak memiliki kunci dekripsi. Sedangkan dekripsi merupakan teknik mendapatkan data asli menggunakan kunci dekripsi. Proses enkripsi menggunakan suatu algoritma dengan parameter.. Kerahasiaan terletak pada parameter yang digunakan.ada dua algoritma yaitu simetris dan asimetris.

.

1) Plaintext

Plaintext adalah pesan asli yang belum diacak menggunakan proses enkripsi.

2) Ciphertext

Chiphertext adalah pesan yang sudang dienkripsi atau dengan kata lain sudah menjadi random teks

3) Cipher

Cipher adalah algoritma matematis yang digunakan untuk proses penyandian plaintext menjadi ciphertext, begitupun sebaliknya.

4) Kunci

Kunci adalah angka yang dirahasiakan, digunakan untuk proses Enkripsi dan Dekripsi.

5) Enkripsi

Enkripsi adalah proses pengubahan plaintext menjadi chipertext.

6) Dekripsi

Dekripsi adalah proses pengubahan chipertext menjadi plaintext.

2.3. ALGORITMA RIVEST CODE (RC6)

RC6 merupakan salah satu dari algoritma simetri kriptografi yaitu algoritma yang menggunakan satu kunci untuk enkripsi dari deskripsinya. RC6 adalah algoritma blok kode yang sangat aman, padat, sederhana dan menawarkan perfomansi yang sangat bagus dan fleksibel, dari algoritma RC5.

a.) Proses Enkripsi

Algoritma RC6 dengan beberapa parameter rumus, dituliskan sebagai RC6-w-r/b, r = 20, w = 32 dan b bertingkat variasi antara 16 , 24, dan 32 byte. Karena RC6 memecah atau memisah blok 128 bit menjadi 4 buah blok 32 bit, maka algoritma ini bekerja dengan 4(empat) buah register 32-bit A, B, C, D. Byte pertama dari plaintext atau chipertext ditempatkan pada byte A, sedangkan byte yang terakhirnya ditempatkan pada byte D. akan terdapat rumus a, b, c, d = b, c, d, a nilai yang terletak pada bagian sisi kanan berasal dari register bagian sisi kiri. diagram blok

a.) Proses Dekripsi

Proses dekripsi chipertext pada algoritma RC6 merupakan kebalikan dari proses enkripsi. Pada proses whitening, bila diproses menjadi pengurangan yang dilakukan dalam proses dekripsi, dimana proses dekripsi sama persis dengan proses enkripsi, hanya saja proses kebalikan dari proses enkripsi

2.4. ALGORITMA BLOWFISH

Blowfish atau yang biasa disebut dengan “OpenPGP.Cipher.4” merupakan algoritma kunci simetrik cipher blok yang dirancang pada tuhan 1993 oleh Bruce Schneier untuk menggantikannya algoritma DES(Data Encryption Standard).

hak paten atau kerahasiaan pemerintah Amerika Serikat. dirangcang dan diharapkan mempunyai kriteria perancangan

2) Enkripsi Data

Terdiri dari iterasi fungsi sederhana (Feistel Network) sebanyak 16 kali putaran (iterasi), masukannya adalah 64 bit elemen data x. Setiap putaran terdiri dari permitaso kunci dependent dan substitusi kunci dan data dependent. Semua operasi adalah penambahan (addition) dan XOR pada variabel 32-bit. Operasi tambahan lainnya hanyalah empat penelusuran tabel array berindeks untuk setiap putaran,

Langkahnya adalah seperti berikut :

a) Bagi x menjadi dua bagian yang masing-masing terdiri dari 32-bit: XL,XR

b) Lakukan langkah berikut

For i = to 16;
XL = XL $\oplus$ Pi
XR = F(XL) $\oplus$ XR
Tukar XL dan XR

c) Setelah iterasi ke-16, tukar XL dan XR lagi untuk melakukan membatalkan pertukaran terakhir.

d) Lalu lakukan XR = XR $\oplus$ P17 XL = XL $\oplus$ P18

e) Terakhir, gabungkan kembali XL dan XR untuk mendapatkan cipherteks.

3) Dekripsi Data

Dekripsi sama persis dengan enkripsi, kecuali bahwa P1, P2, ..., P18 digunakan pada urutan yang berbalik (reverse). Algoritmanya dapat dinyatakan sebagai berikut :

For i = 1 to 16 do
Xri = Xli-1 $\oplus$ P19-i;
XLi = F[Xri] $\oplus$ XRi-1;
XL17 = XR16 $\oplus$ P1;
XR17 = XL16 $\oplus$ P2;

3. Hasil Dan Pembahasan

Pada aplikasi ini menggunakan teknik kriptografi RC6 (Rivest Code 6) dan kriptografi Blowfish. Proses keseluruhan aplikasi ini dapat diuraikan sebagai berikut:

a. Langkah awal untuk menggunakan aplikasi ini adalah user pengirim terlebih dahulu login dengan menggunakan email

sendiri terlebih dahulu dan harus terkoneksi dengan internet.

b. Setelah login berhasil dan masuk ke dalam menu utama aplikasi, user pengirim dapat memilih menu tulis pesan untuk mengirim pesan.

c. Lalu user pengirim memasukkan email penerima dan subjek email

d. Setelah itu memilih jenis file yang ingin dilampirkan dan memasukan kunci pengamanan kemudian kirim kepada user penerima.

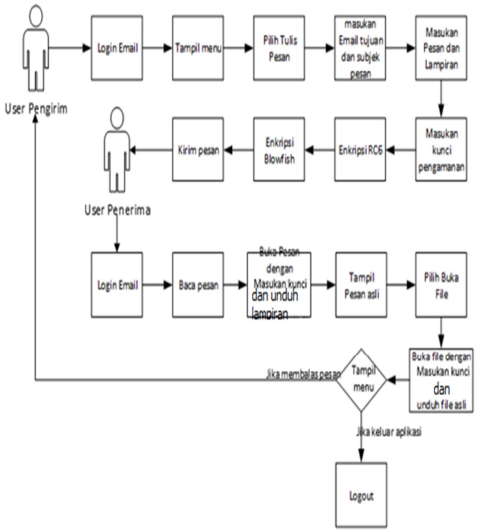
e. User penerima akan menerima pesan serta file yang sudah terenkripsi dan apabila penerima ingin membuka pesan yang telah diterima, maka user penerima terlebih dahulu login dengan menggunakan email sendiri harus terkoneksi dengan internet.

f. User Penerima dapat memilih menu inbox untuk membuka pesan email yang terdapat file atau konten pesan yang telah dienkripsi dan memasukan kunci untuk dapat mengenkrip pesan. Setelah melakukan verifikasi penerima dapat langsung mendekrip pesan dan melihat pesan asli

g. Lalu user penerima memilih menu dekrip file untuk mendekrip file yang sudah diunduh tadi, penerima memasukan kunci sebelum mendekrip file, setelah berhasil penerima dapat langsung mendekrip file dan mengunduh file yang sudah didekrip

h. Jika user penerima ingin keluar bisa pilih menu logout atau jika user penerima ingin membalas pesan tersebut dapat mengulangi ke langkah A.

Untuk dapat memahami konsep aplikasi yang akan dibangun dapat melihat skema proses keseluruhan aplikasi dapat dilihat pada gambar berikut:



Gambar 1 Arsitektur Sistem

Berikut ini akan dipaparkan hasil dari pembuatan aplikasi beserta proses enkrip dan dekrip yang terdapat pada aplikasi yang dibuat. Dimana aplikasi ini menyediakan beberapa menu dan fungsi yang saling terkait satu sama lain. Pada saat program pertama dijalankan maka akan muncul menu *login* seperti pada gambar 2 ini:

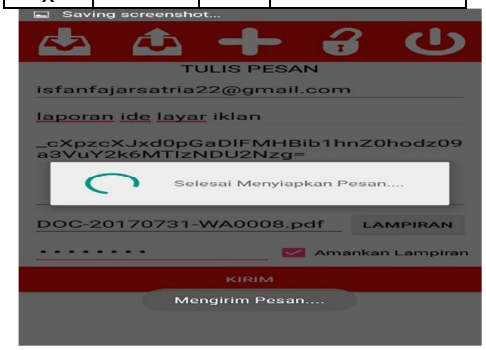
Gambar 2 Tampilan Awal Aplikasi

Setelah login masuk menggunakan email dan password dalam menu login maka akan muncul tampilan menu yang berisi menu tampilan dengan icon-icon pesan masuk, pesan terkirim, tulis pesan, buka file dan log out.

Gambar 3 Menu tampilan awal pesan masuk

Didalam proses ini pengamanan email yang berisi teks pesan email dan attachment file atau lampiran, yang dimana terjadi proses enkripsi.

Input File	Passw ord	size File	Ukuran hasil dekripsi
pend apata n.doc x	11111 11	60 KB	40 KB
koca k.xls x	11111 11	70K B	50 KB



Gambar 4 Proses menu tulis pesan pengamanan email

Didalam Proses ini penerima dapat membuka pesan email yg sudah di enkrip untuk melihat menggunakan kunci agar terdekrip.

Gambar 5 Pesan dan File yang Telah Terdekrip

Dibawah ini merupakan table hasil pengujian yang telah dilakukan dalam file yang sudah di enkripsi dan dekripsi.

File	Pass word	size File	Ukuran Hasil Enkripsi
pend apata n.doc x	1111 111	40 KB	60 KB
koca k.xls	1111 111	50 KB	70 KB
x			

Table 1 Hasil Pengujian file enkrip

Table 2 Hasil Pengujian file dekrip

4. KESIMPULAN

Berdasarkan pembahasan dari aplikasi ini maka dapat diambil kesimpulannya sebagai berikut:

a. Apikasi dibuat semudah mungkin agar pengguna tidak kebingungan untuk menggunakannya.
b. Dengan dibuatnya aplikasi kriptografi ini maka file yang telah dienkripsi terjaga kerahasiannya dari pihak yang tidak bertanggung jawab
c. Aplikasi kriptografi ini menggunakan algoritma RC6 dan Blowfish. dibangun agar dapat mengamankan jenis file .doc, .docx, .pdf, .xls, .xlsx dan isi pesan email.
d. Algoritma Rivest Code (RC6) enkripsi, dekripsi untuk pesan email dan Algoritma Blowfish enkripsi, dekripsi untuk file data lampiran (attachment file)
e. Kecepatan pengiriman file tergantung sambungan internet
f. Dengan adanya aplikasi pengamanan email ini maka setiap proses pengirimian email menjadi lebih aman dari pihak yang tidak diharuskan mengetahui email tersebut.
g. Proses dekripsi tetap berjalan meskipun password yang dimasukan tidak sesuai, namun email dan file yang terdekripsi tidak bias dibaca dan file tidak bisa dibuka.
h. Proses dekripsi dengan password yang benar akan mengembalikan email dan file menjadi email dan file semula tanpa mengalami perubahan.

Setelah menarik kesimpulan, dapat diajukan saran yang mungkin bisa dijadikan rujukan dalam pengembangan aplikasi antara lain:

a. Pada aplikasi ini dapat dikembangan dengan cara menambahkan jenis file yang dapat di enkripsi maupun dekripsi seperti MP3,MP4,dan lainnya.
b. Interface sangat sederhana,diharapkan bisa ditambah beberapa fitur seperti chats,drafts.
c. Aplikasi ini dapat dikembangkan,jika saat pengguna tidak mengingat key yang dapat di input saat enkripsi data. Maka dapat disediakan tools untuk pengguna yang bertujuan untuk memberitahukan key pada saat dekripsi data melalui e-mail.

5. DAFTAR PUSTAKA

[1] F. N. Pabokory, I. F. Astuti, dan A. H. Kridalaksana, "Implementasi Kriptografi

Pengamanan Data pada android sistem memakai rc6" *J. Inform. Mulawarman*, vol. 10, no. 1, hal. 20–31, 2015

[2] Hamid, "Uji Keamanan Aplikasi Email Bawaan Android Pada Jaringan Nirkabel," *J. Cybermatika*, vol. 2, no. 1, hal. 13–19, 2014.

[3] A. Rohmanu, "Implementasi Kriptografi dan Steganografi Dengan Metode Algoritma rc6," vol. 1, no. 2, hal. 1–11, 2017.

[4] M. Zulham, H. Kurniawan, dan I. F. Rahmad, "Perancangan Aplikasi Keamanan Data Email Menggunakan Algoritma Enkripsi Rivest code 6," *Semin. Nas. Inform.*, hal. 96–101, 2014.

[5] R. Primartha, J. T. Informatika, F. I. Komputer, dan U. Sriwijaya, "Penerapan Enkripsi Dan Dekripsi File Menggunakan Algoritma Blowfish," *Enkrip dan Dekrip dengan Blowfish*, vol. 3, no. 2, hal. 371–387, 2013.

[6] P. H. Arjana, T. P. Rahayu, Yakub, dan Hariyanto, "Implementasi Enkripsi Data Dengan Algoritma RC6," *Sentika*, vol. 2013, no. Sentika, hal. 164–169, 2013.