APLIKASI ENKRIPSI DAN KOMPRESI FILE PADA BLACKBERRY DENGAN MENGGUNAKAN MODE CFB 8-BIT DAN 3DES

Denny Dwi Mavianto[1], Arif Fadillah[2]

[1, 2)]Program Studi Sistem Informasi, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Pesanggrahan, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5853752
[1]snorzo@gmail.com, [2]arif_fadillah_home@yahoo.co.id

ABSTRAK

BlackBerry bukan sekedar smartphone biasa yang lengkap fitur multimedianya, BlackBerry juga memiliki layanan internet yang sangat baik. Namun layanan yang melalui BlackBerry Internet Service (BIS) ini belum tentu aman, karena dari sekian banyak pesan dan file yang terkirim melalui media BIS harus melalui server yang terletak di server BIS. Oleh karena itu dibutuhkan sebuah perangkat lunak yang dapat melakukan enkripsi dan dekripsi terhadap pesan maupun file, baik yang akan dikirim melalui media internet BlackBerry atau yang hanya disimpan pada perangkat BlackBerry tersebut. Pada penulisan ini digunakan algoritma enkripsi cipher block dengan mode Cipher Feedback (CFB) 8-bit dan Triple Data Standard Encryption (3DES).Mode ini dipilih karena cocok untuk melakukan enkripsi terhadap data pada perangkat BlackBerry, karena mode enkripsinya yang umum dan memerlukan penggunaan memory yang sedikit sehingga cocok digunakan pada smartphone ini. Pada algoritma enkripsinya, digunakan algoritma cipher block dengan ukuran blok sebesar 64 bit. Algoritma ini menggunakan basis jaringan Feistel serta beberapa algoritma enkripsi dekripsi lainnya. Kemudian, algoritma enkripsi CFB dan 3DES ini diimplementasikan kesebuah perangkat lunak berbasis Java untuk BlackBerry. Dalam pembangunan perangkat lunak ini, digunakan bantuan IDE Eclipse Ganymede serta beberapa plugins lainnya yang akan dijelaskan secara detail pada penulisan ini.Selain enkripsi dan deskripsi pada penulisan ini juga terdapat kompresi terhadap file pada blackberry. Fungsi dari fitur ini adalah untuk mengompres ukuran file tersebut menjadi lebih kecil sehingga tercapainya efisiensi data storage yang ada pada Blackberry tersebut. Algoritma yang digunakan pada metode kompresi ini adalah Algoritma Huffman Tree. Algoritma ini dipilih karena sifatnya yang umum dan mampu mengkompres ukuran file dan pesan hingga 20 – 80% lebih kecil dari ukuran aslinya. Sehingga algoritma Huffman Tree ini juga cocok digunakan dalam metode kompresi pada Blackberry

Kata Kunci : BlackBerry, Enkripsi dan Kompresi, CFB, 3DES, Deflate

I. PENDAHULUAN

1.1 Latar Belakang

Seperti yang diketahui, sebagian besar pengguna Blackberry memilih Blackberry karena *fitur Instant Messaging* dan *e-mail* yang sangat baik, yang hingga saat ini belum dimiliki *vendor-vendor smartphone* lainnya. Blackberry memiliki fitur Instant Messaging yang eksklusif, yaitu BBM (*Blackberry Messenger*). Fasilitas aplikasi BBM ini hanya dapat digunakan antar sesama pengguna Blackberry saja, karena aplikasi ini menggunakan nomor pin unik yang terintegrasi pada setiap perangkat Blackberry dan tidak dapat dimiliki perangkat smartphone lainnya. Berdasarkan jumlah pengguna Blackberry saat ini, dapat dibayangkan seberapa banyaknya pesan teks, gambar, video, dan file dokumen yang dikirim melalui BBM ini. Hal inilah yang menjadi perhatian beberapa negara dan juga pemerintah Indonesia, yaitu sangat banyak data masyarakat negaranya, baik pesan teks, gambar, video, dan file dokumen yang tersimpan di server Kanada ketika melakukan pengiriman melalui media BBM. Kemudian yang terpenting apakah data tersebut benar-benar dijaga privasinya oleh pihak RIM, atau disalahgunakan oleh beberapa pihak tertentu, semuanya itu tidak dapat diketahui oleh pihak negara pengguna yang jelas tidak memiliki akses langsung ke server RIM yang berada di Kanada. Oleh karena itu dibuatlah aplikasi enkripsi dan kompresi file atau data pada Blackberry.

1.2 Masalah

Sampai saat ini proses pengiriman file atau pesan yang dilakukan lewat media Blackberry ini masih belum disertai adanya enkripsi, sedangkan server media ini tidak berada di Negara kita sendiri sehingga keamanan dari file atau pesan yang kita kirim tidak bisa kita jamin.

1.3 Tujuan dan Manfaat

Mencegah terjadinya penyalahgunaan file dan pesan pada media ini sekaligus menjaga privasi suatu file dan pesan dari si pengguna dan memanfaatkan penggunaan storage yang lebih efisien dikarenakan adanya pengompressan file.

1.4 Pembatasan Masalah

Metode yang digunakan pada aplikasi ini adalah dua metode Enkripsi (CFB 8-bit dan 3DES). untuk metode kompresi memanfaatkan algoritma deflate. Aplikasi ini hanya dipergunakan pada semua perangkat Blackberry dengan OS (*Operating Sistem*) yang sudah ditentukan 4.0, 5.0, dan 6.0. dan untuk bahasa pemrograman yang digunakan adalah bahasa pemrogaman java.

II. LANDASAN TEORI

2.1 Teknik Kriptografi

Kriptografi, secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita [1]. Selain pengertian tersebut terdapat pula pengertian ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data [2]. Namun tidak semua aspek keamanan informasi ditangani oleh kriptografi.

2.2 Teknik Enkripsi

Enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus [1]. atau bisa didefinisikan juga Enkripsi, merupakan proses untuk mengubah plainteks menjadi cipherteks. Planteks sendiri adalah data atau pesan asli yang ingin dikirim, sedangkan cipherteks adalah data hasil enkripsi. Definisi lain tentang enkripsi adalah proses mengacak data sehingga tidak dapat dibaca oleh pihak lain.

2.3 Teknik Dekripsi

Dekripsi dalam dunia keamanan komputer merupakan proses untuk mengubah cipherteks menjadi plainteks atau pesan asli jadi Dekripsi merupakan kebalikan dari enkripsi upaya pengolahan data menjadi sesuatu yang dapat diutarakan secara jelas dan tepat dengan tujuan agar dapat dimengerti oleh orang yang tidak langsung mengalaminya sendiri [3].

2.4 Teori *Block Cipher*

Block-cipher adalah skema algoritma sandi yang akan membagi-bagi teks terang yang akan dikirimkan dengan ukuran tertentu (disebut blok) dengan panjang t, dan setiap blok dienkripsi dengan menggunakan kunci yang sama [4]. Pada umumnya, *block-cipher* memproses teks terang dengan blok yang relatif panjang lebih dari 64 bit, untuk mempersulit penggunaan pola-pola serangan yang ada untuk membongkar kunci. Untuk menambah kehandalan model algoritma sandi ini, dikembangkan pula beberapa tipe proses enkripsi, yaitu : ECB, CBC, OFB, CFB.

2.5 Teori *Stream Cipher*

Stream-cipher adalah algoritma sandi yang mengenkripsi data persatuan data, seperti bit, byte, nible atau per lima bit (saat data yang dienkripsi berupa data Boudout) [4]. Setiap mengenkripsi satu satuan data digunakan kunci yang merupakan hasil pembangkitan dari kunci sebelum. Oleh karena itu dikembangkan pula beberapa tipe proses enkripsi, yaitu : DES, Blowfish, Twofish, MARS, IDEA, 3DES, AES.

2.6 Teori Kompresi Data

Kompresi Data adalah salah satu subyek di bidang teknologi informasi yang saat ini telah diterapkan secara luas [5]. Gambar-gambar yang anda dapatkan di berbagai situs internet pada umumnya merupakan hasil kompresi ke dalam format GIF atau JPEG. File video MPEG adalah hasil proses kompresi pula. Penyimpanan data berukuran besar ada server pun sering dilakukan melalui kompresi. Sayangnya tidak banyak mata kuliah yang memberikan perhatian pada subyek ini secara memadai. Tulisan berikut ini akan memperkenalkan tentang dasar-dasar Kompresi Data kepada anda.

2.7 Java Programming

Java diciptakan oleh suatu tim yang dipimpin James Gsoling dalam suatu proyek dari Sun Microsystem pada tahun 1991 untuk menghadapi suatu dampak besar dari adanya penggunaan peralatan canggih. Proyek ini dinamakan kode "green" dengan tujuan untuk menghasilkan bahasa komputer sederhana yang dapat dijalankan di peralatan sederhana dengan tidak terikat pada arsitektur tertentu. Mulanya hasil penelitian ini disebut OAK, akan tetapi nama OAK sudah digunakan sebagai nama dari bahasa pemrograman komputer sebelumnya, maka Sun mengubahnya menjadi Java. Nama Java diambil ketika sebuah group dari orang-orang Sun mengunjungi sebuah coffee Shop [6].

2.8 Aplikasi Pada Blackberry

Perangkat Blackberry pertama, 850, diperkenalkan pada tahun 1999 sebagai pager dua arah di Munich, Jerman. Nama Blackberry ini diciptakan oleh perusahaan pemasaran leksikon Branding. Nama ini dipilih karena kemiripan dari tombol keyboard yang drupelets yang membentuk buah blackberry. Pada tahun 2003, yang lebih sering dikenal smartphone Blackberry dirilis, yang mendukung push email, telepon selular, pesan teks, Fax, Internet Web browsing dan lain layanan nirkabel informasi. Ini adalah contoh perangkat konvergen. Perangkat Blackberry yang asli, RIM 850 dan 857, menggunakan jaringan DataTac.

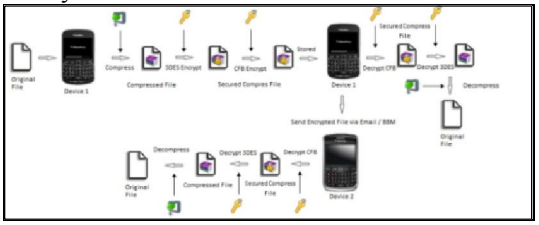
III. ANALISA DAN PERANCANGAN PROGRAM

3.1 Program Aplikasi Usulan

Untuk program aplikasi usulan yang dirancang untuk membuat suatu solusi pemecahan dalam pengamanan data, dalam hal ini enkripsi file dan data pada perangkat Blackberry adalah membuat aplikasi enkripsi dengan metode CFB dan 3DES sehingga membuat keamanan data yang double secure. Serta untuk menjaga kapasitas storage yang efisien maka pada aplikasi ini juga diterapkan teknik kompresi dalam program ini akan menggunakan algoritma deflate, dan untuk bahasa yang digunakan yaitu bahasa pemrograman java dengan editornya IDE Eclipse.

3.2 Struktur Skema Aplikasi Usulan

Dalam aplikasi ini kita memanfaatkan kedua kelas skema kriptografi symmetric-key tersebut yaitu dengan metode *Cipher Feedback 8-bit* (CFB) untuk block-cipher dan Tripple Data Encryption Standard (3DES) untuk stream-cipher, serta teknik kompresi dengan menggunakan algoritma deflate tree, Berikut skema penerapan kinerja aplikasi usulan pada Blackberry :



Gambar 1: Skema Umum Proses Enkripsi, Dekripsi dan Kompresi File.

3.3 Metode Kerja Aplikasi Usulan

3.3.1 Kompresi GZIP File

Pada bahasa pemrograman java untuk aplikasi kompresi pada device mobile memafaatkan gabungan dari algoritma LZ77 dan Huffman yang terkenal dengan teknik kompresi deflate atau LZW [7]. Kerja dari algoritma kompresi deflate atau LZW ini yang menggabungan algoritma LZ77 dan Huffman dapat dilihat dari tahapan tahapan sebagai berikut :

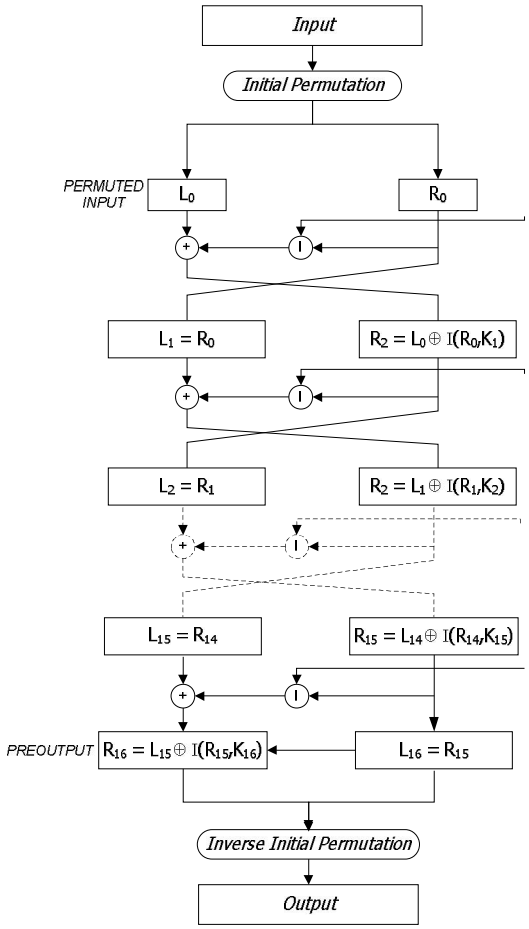
a. Dictionary diinisialisasi dengan semua karakter dasar yang ada : {'A'..'Z','a'..'z','0'..'9'}.
b. P karakter pertama dalam stream karakter.
c. C karakter berikutnya dalam stream karakter.
d. Apakah string (P + C) terdapat dalam dictionary ?
e. Jika ya, maka P =P + C (gabungkan P dan C menjadi string baru).
f. Jika tidak, maka :
   1) Output sebuah kode untuk menggantikan string P.
   2) Tambahkan string (P + C) ke dalam dictionary dan berikan nomor/kode berikutnya yang belum digunakan dalam dictionary untuk string tersebut.
   3) P=C.
g. Apakah masih ada karakter berikutnya dalam stream karakter ?
h. Jika ya, maka kembali ke langkah 2.
i. Jika tidak, maka output kode yang menggantikan string P, lalu terminasi proses (stop).

Tabel 1: Tahapan proses kompresi LZW

Langkah	Posisi	Karakter	*Dictionary*	*Output*
1.	1	A	[4] A B	[1]
2.	2	B	[5] B B	[2]
3.	3	B	[6] B A	[2]
4.	4	A	[7] A B A	[4]
5.	6	A	[8] A B A	[7]
6.	9	C	- - -	[3]

3.3.2 *Tripple Data Encryption Standard* (3DES)

3DES (*Triple Data Encryption Standard*) merupakan suatu algoritma pengembangan dari algoritma DES (*Data Encryption Standard*). Pada dasarnya algoritma yang digunakan sama, hanya pada 3DES dikembangkan dengan melakukan enkripsi dengan implementasi algoritma DES sebanyak tiga kali. DES beroperasi pada ukuran blok 64-bit. DES mengenkripsikan 64-bit plainteks menjadi 64-bit cipherteks dengan menggunakan 56-bit kunci internal yang dibangkitkan dari kunci eksternal yang panjangnya 64-bit [4]. Berikut proses kunci yang dilakukan pada DES, kunci eksternal yang diinputkan akan diproses untuk mendapatkan 16 kunci internal. Pertama, Kunci eksternal yang panjangnya 64-bit disubstitusikan pada matriks permutasi kompresi PC-1. Dalam permutasi ini, setiap bit kedelapan (*parity bit*) dari delapan byte diabaikan. Hasil permutasi panjangnya menjadi 56-bit, yang kemudian dibagi menjadi dua bagian, yaitu kiri (C0) dan kanan (D0) masing-masing panjangnya 28-bit. Kemudian, bagian kiri dan kanan melakukan pergeseran bit pada setiap putaran sebanyak satu atau dua bit tergantung pada tiap putaran. Pada proses enkripsi, bit bergeser kesebelah kiri (left shift). Sedangkan untuk proses dekripsi, bit bergeser kesebelah kanan (right shift). Setelah mengalami pegeseran bit, 58id an Di digabungkan dan disubstitusikan pada matriks permutasi kompresi dengan menggunakan matriks PC-2, sehingga panjangnya menjadi 48-bit. Proses tersebut dilakukan sebanyak 16 kali secara berulang-ulang. Berikut gambar detail proses 3DES :

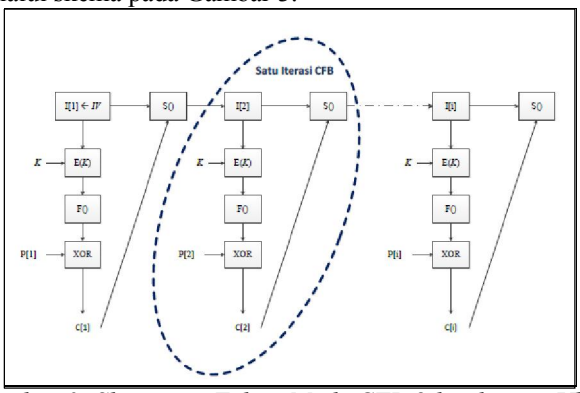


Gambar 2: Proses Enkripsi 3DES

3.3.3 Cipher Feedback 8-bit (CFB 8-bit)

Pada mode Cipher Feedback, data dienkripsi ke dalam unit yang lebih kecil dari ukuran blok data stream. Dengan mode ini dapat digunakan untuk mengenkripsi sejumlah bit tertentu, contoh sebuah bit atau sebuah karakter (byte) [4]. Pada awalnya shift register diinisialisasi dengan initialization vector (IV) kemudian algoritma enkripsi dilakukan untuk menghasilkan output 64 bit. IV sendiri merupakan sebuah vektor binari yang digunakan untuk meninisialisasikan blok input pada mode CFB dan OFB sebagai blok yang nilainya acak. Setelah itu, 8 bit terkiri (left-most) dari output diambil untuk di-XOR kan dengan stream data plainteks. Hasil XOR ini yang akan disimpan untuk menjadi cipherteks, kemudian 8 bit hasil XOR ini juga dimasukkan ke belakang input blok yang baru untuk, sementara 8 bit terkirinya akan dibuang. Kemudian, algoritma enkripsi ini dilakukan lagi dengan cara yang sama hingga semua data selesai dienkripsi. Initialization vector yang digunakan pada mode CFB memiliki sifat yang sama dengan

initialization vector yang digunakan pada CFB. Yaitu IV tidak harus bersifat rahasia, namun sebaiknya berbeda untuk setiap pesan yang dienkripsi dengan kunci yang sama. Kesalahan bit (bit errors) pada cipher block akan menyebabkan kesalahan bit pada posisi yang sama pada blok plainteks yang didekripsi. Karena itu jika saat menggunakan mode CFB 8-bit terdapat kesalahan pada beberapa bit di blok cipherteks, maka blok plainteks sebesar 64 bit yang berkorespondensi dengan blok cipherteks akan rusak informasinya, sementara blok lainnya tetap akan dapat didekripsi dengan benar. Untuk memperjelas cara kerja CFB 8-bit dengan ukuran blok 64 bit, akan dijelaskan melalui skema pada Gambar 3.



Gambar 3: Skema per Tahap Mode CFB 8-bit dengan Ukuran Blok 64-bit

Berikut adalah keterangan notasi yang digunakan:

IV : Initialization Vector, bersifat acak dan berbeda untuk setiap pesan yang dienkripsi. Panjang IV yang digunakan adalah 64 bit.

I[i] : Input block, digunakan sebagai blok input yang akan dienkripsi kemudiannya. Panjang I[i] adalah 64 bit. Khusus untuk blok input pertama (I[1]), nilainya adalah IV, sedangkan untuk I[2] dan selanjutnya diperoleh dari fungsi S().

E(K) : Fungsi enkripsi, yaitu fungsi yang mengenkripsi blok 64 bit dengan menggunakan kunci K yang dimasukkan pengguna.

F() : Fungsi filter, yaitu sebuah fungsi untuk mengambil left-most 8 bit dari blok hasil enkripsi yang berukuran 64 bit, yang kemudian akan dilakukan XOR dengan blok plainteks.

P[i] : Blok plainteks yang akan dilakukan operasi XOR dengan hasil fungsi filter, berukuran 8 bit setiap bloknya.

C[i] : Blok cipherteks, yang akan disimpan kemudian digabungkan dengan blok cipherteks lainnya hingga menjadi data cipherteks yang utuh. Setiap bloknya berukuran 8 bit data.

S() : Fungsi shifting, yaitu fungsi geser dengan membuang 8 bit terawal blok input, kemudian memasukan blok cipher 8 bit pada bagian akhirnya. Hasil fungsi shifting ini kemudian dijadikan blok input untuk iterasi selanjutnya.

I : Iterasi pada mode CFB. Jumlah iterasi yang dilakukan pada mode CFB 8 bit adalah sebesar (ukuran data dalam bits / 8 bit).

IV. IMPLEMENTASI DAN ANALISA PROGRAM

4.1 Tujuan Implementasi Program

Dibuatnya sebuah aplikasi kriptografi, diharapkan ketika pertukaran informasi dan data melalui Blackberry akan menjadi lebih aman, sehingga perusahaan tidak lagi mengirimkan data lewat jasa kurir yang dapat memakan waktu sangat lama. Sehingga dengan dibuatkannya aplikasi kriptografi ini dapat menjadi solusi untuk mengatasi kendala yang ada.

4.2 Spesifikasi Hardware dan Software

4.2.1 Hardware

Di bawah ini merupakan spesifikasi hardware (perangkat keras) yang mendukung dalam pengoperasian aplikasi kriptografi,

a. Notebook dengan spesifikasi sebagai berikut :
   1) Core i5 (2.40 GHz)
   2) RAM / Memory 4 GB
   3) Harddisk 160GB

b. Handphone Blackberry dengan spesifikasi sebagai berikut :
   1) Tipe Bold 9790
   2) Storage memory 2G

4.2.2 Software

Di bawah ini merupakan spesifikasi software (perangkat lunak) yang dibutuhkan dalam aplikasi kriptografi dan harus dipenuhi agar aplikasi dapat berjalan dengan baik.

a. Sistem operasi Microsoft Windows 7 Ultimate
b. Eclipse Java EE IDE, Version Juno Service Release 2
c. Blackberry java plug-in (Core)
d. Blackberry java SDK

4.3 Implementasi program

Implementasi program berguna untuk mengetahui apakah program yang telah dibuat dapat berjalan secara maksimal atau bahkan terjadi kesalahan-kesalahan yang tidak diinginkan, maka dari itu program tersebut harus diuji terlebih dahulu agar dapat berjalan sesuai dengan yang diharapkan pada saat implementasi nantinya. Tahap pengujian ini, user/pengguna yang akan langsung mencoba, karena dari seorang user/pengguna tersebut akan mendapatkan masukan-masukan yang diharapkan dapat menjadi acuan.

4.3.1 Tampilan Layar Menu Utama

Pada aplikasi ini ketika kita jalankan program maka akan langsung menuju halaman menu utama dimana hanya ada 4 menu yang dapat digunakan/enable yaitu Menu Encrypt, Decrypt, About, dan Exit.

Gambar 4: Tampilan Layar Menu Utama

4.3.2 Tampilan Layar Aplikasi Encrypt

Encrypt pada menu utama. Pada layar ini terdapat beberapa komponen-komponen yaitu 3 text box dan 2 button, Berikut tampilan layarnya :

Gambar 5: Tampilan Layar Aplikasi Encrypt

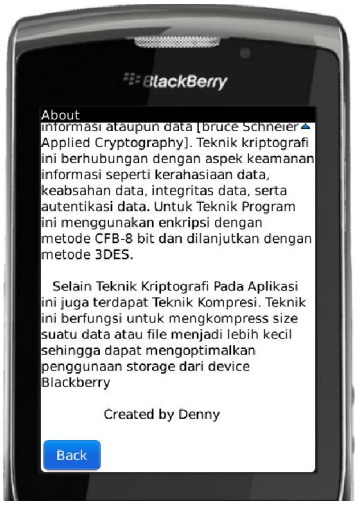
4.3.3 Tampilan Layar Aplikasi Decrypt

Pada aplikasi decrypt ini akan tampil ketika user/pengguna menekan tombol decrypt pada menu utama. Pada layar ini terdapat beberapa komponen-komponen yaitu 3 text box dan 2 button, Berikut tampilan layarnya :

Gambar 6: Tampilan Layar Aplikasi Decrypt

4.3.4 Tampilan Layar Menu About

Pada Menu ini berisi tentang penjelasan secara garis besar proses dari aplikasi kriptografi ini, dan menjelaskan bagaimana aplikasi enkripsi, kompresi dan dekripsi tersebut berjalan. Dalam tampilan layar ini terdapat 1 text box dan 1 button. Text box berfungsi untuk menampilkan text about, dan back button berfungsi untuk kembali ke menu utama.



Gambar 7: Gambar Menu About

4.4 Kekurangan dan Kelebihan Program

4.4.1 Kekurangan Program

a. Aplikasi ini belum terintegrasi dengan aplikasi lain yang ada pada Blackberry tersebut.
b. Aplikasi kompresi belum bisa bekerja secara optimal pada file yang berbentuk gambar, audio, dan video.
c. Dengan spesifikasi Blackberry standard yang digunakan pada saat ini, aplikasi ini hanya bisa memproses file dan data kurang dari 5MB.
d. Aplikasi ini hanya bisa di gunakan pada perangkat mobile Blackberry, belum dikembangkan untuk perangkat mobile yang lainya.

4.4.2 Kelebihan Program

a. Aplikasi ini membuat data atau file menjadi sangat secure, dikarenakan menggunakan 2 metode enkripsi yang digabung.
b. Selain secure aplikasi ini menggunakan teknik kompresi yang mampu mengkompres file hingga 90%.
c. File yang sudah di encrypt tidak akan pernah bisa dibaca tanpa di decrypt dari aplikasi ini dan dilanjutkan juga dengan key yang sama.
d. Ukuran aplikasi yang kecil dan mudah di install, sehingga sedikit membutuhkan resource dari storage Blackberry.

V. PENUTUP

5.1 Kesimpulan

a. Dengan adanya program aplikasi ini membuat pengiriman file atau document yang dikirimkan menjadi lebih aman dikarenakan pada aplikasi ini menggunakan dua metode enkripsi yaitu CFB 8-bit dan 3DES.
b. Secara umum, algoritma block-cipher pada mode CFB 8-bit dan stream-cipher pada mode 3DES dapat diimplementasikan dan berhasil berjalan dengan baik pada perangkat Blackberry. Melalui pengujian ditunjukkan bahwa aplikasi dapat berjalan dengan baik pada berbagai jenis perangkat Blackberry.
c. File yang mampu dijalankan oleh program aplikasi ini secara optimal enkripsi maupun kompresinya file tersebut harus bertipe Text ataupun data, dikarenakan teknik

kompresi pada aplikasi ini kurang begitu optimal untuk file bertipe gambar, audio maupun video.

5.2 Saran

a. Memperbaiki design algoritma enkripsi agar program aplikasi menjadi lebih baik, lebih efisien, dan proses enkripsi file lebih cepat dan akurat.
b. Semakin kecil kapasitas size dari sebuah file maka semakin cepat proses encrypt-nya, begitu juga dengan proses decrypt-nya.
c. Menambahkan fitur penintegrasian aplikasi ke sistem operasi Blackberry, sehingga fitur enkripsi terhadap pesan mudah diakses, baik melalui media SMS, IM, maupun BBM.

DAFTAR PUSTAKA

[1] Schneier, Bruce 1996, *Applied Cryptography*, Canada, John Wiley and Sons

[2] Alfred J. Menzes, Paul C. van Orschot, Scott A. Vanstone, 1997, *Handbook of Applied Cryptography*, CRC Press, United States.

[3] Kurniawan, Yusuf 2004, *Keamanan Internet dan Jaringan Komunikasi,* Kriptografi, Informatika, Bandung.

[4] Stinson, Doug, 2002, *Cryptography Theory and Pratice,* CRC Press, United States.

[5] Torer, J.A., Rockville, MD Witten, Ian H., Neal, Radford M 1988, *Data Compression*, *Computer Science Press.*

[6] Nugroho, Adi 2008, *Pemrograman Java Menggunakan IDE ECLIPSE Aplikasi Mandiri (STAND-ALONE),* Andi Publisher.

[7] Nelson, Mark, 1987, *LZW Data Compression,* Doctor Dobb's Journal, October