IMPLEMENTASI ALGORITMA DES BERBASIS BLOWFISH UNTUK ENKRIPSI DAN DEKRIPSI DATA

Hafid Rosianto
Teknik Elektro, Teknik, Universitas Negeri Surabaya
e-mail : hafidrosi@gmail.com

Lilik Anifah
Teknik Elektro, Teknik, Universitas Negeri Surabaya
e-mail : anifahl@yahoo.com

Abstrak

Penelitian ini dilakukan untuk mengimplementasikan gabungan dari dua metode algoritma yang berbeda yaitu DES dan blowfish untuk enkripsi dan dekripsi data. Proses enkripsi bertujuan untuk mengamankan data dengan mengacak bit-bit data tersebut dengan password/*key* masukan. Sedangkan proses dekripsi bertujuan untuk mengembalikan bit-bit acakan dari proses enkripsi dengan kunci sama yang dipakai pada proses enkripsi. Sampel data yang digunakan adalah data berekstensi .txt, .doc, .pdf, .jpeg, .gif, .mp3, .mp4, .avi. Perancangan dan desain program menggunakan *software* visual studio 2012 dengan bahasa pemrograman VB.NET. Proses diawali dengan enkripsi data awal atau *plaintext* menggunakan algoritma blowfish, kemudian *cipherfile* dari enkripsi algoritma blowfish di enkripsi lagi menggunakan algoritma DES. Untuk urutan penggunaan algoritma pada proses dekripsi adalah kebalikan dari proses enkripsi dan menghasilkan *plainfile*/file awal. Hasil pengujian dari kedua proses enkripsi dan dekripsi data dapat digunakan dan berjalan dengan lancar untuk menjaga keaslian data (*authentication*) dan keutuhan data (*data integrity*).
Kata Kunci: keamanan data, kriptografi, algoritma kriptografi, *plaintext*, *ciphertext*, *key*.

Abstract

This research is to implement a combination of the two methods are different algorithms DES and Blowfish for the encryption and decryption of data. The process aims to secure data encryption to scramble the data bits with a password / key input. While the decryption process aimed at restoring wild bits of the encryption process with the same key used in the encryption process. The data's sample used are data extented in .txt, .doc, .pdf, .jpeg, .gif, .mp3, .mp4, .avi. The plan and the design of software programs using Visual Studio 2012 with VB.NET programming language. This process begins with the beginning or the plaintext data encryption using blowfish algorithm, then cipherfile of blowfish encryption algorithm is encrypted again using the DES algorithm. To order the use of algorithms in the decryption process is the reverse of the encryption process and generate plainfile / file early. The test results of both data encryption and decryption processes can be deployed and running smoothly to keep the authenticity of the data (authentication) and the integrity of the data (data integrity).
Keywords: Data security, cryptography, cryptographic algorithms, *plaintext*, *ciphertext*, *key*

PENDAHULUAN

Perkembangan teknologi informasi di era global ini berkembang sangat pesat. Teknologi mampu memudahkan manusia untuk memenuhi kebutuhan sehari-hari mulai dari melakukan komunikasi sederhana sampai bertukar informasi penting. Saling bertukar informasi penting menggunakan teknologi yang berkembang sudah tidak bisa dihindari lagi. Akan tetapi, banyak pihak yang menginginkan agar informasi yang dikirim bisa terjaga kerahasiaannya hingga sampai ditangan penerima informasi.

Keamanan suatu informasi merupakan hal wajib bagi para *komunikator*. Dengan terbentuknya keamanan suatu informasi yang dikirim oleh pengirim membuat pengirim menjadi tidak khawatir lagi akan informasi yang dikirim. Sehingga informasi yang dikirim dapat aman hingga sampai di tangan penerima yang sudah mendapat ijin oleh pihak pengirim informasi.

Salah satu disiplin ilmu yang mempelajari tentang keamanan informasi adalah kriptografi. Sudah banyak algoritma kriptografi yang dikembangkan diantaranya adalah algoritma DES (*Data Encryption Standard*) dan blowfish. Algoritma DES dan blowfish merupakan algoritma kriptografi simetris. Akan tetapi, perbedaan kedua algoritma tersebut berada pada kunci yang digunakan. Dengan menggabungkan dua algoritma menjadi satu enkripsi membuat suatu informasi menjadi lebih aman dan membuat seorang *Cryptanalysis* kesulitan untuk memecahkan dua algoritma enkripsi yang digabungkan.

KAJIAN PUSTAKA

Keamanan dan Kerahasiaan Data

Keamanan dan kerahasiaan data sangat berkaitan dengan betapa pentingnya suatu informasi dapat dikirim dan diterima oleh orang yang berkepentingan. Informasi tidak akan berguna lagi apabila informasi tersebut disadap atau dibajak oleh pihak yang tidak berhak. Hal-hal yang menyangkut keamanan informasi adalah kemanan fisik, keamanan akses, keamanan file dan data, dan keamanan jaringan.

Kriptografi

Kriptografi (*crytography*) merupakan ilmu dan seni untuk menjaga suatu pesan agar aman. Kriptografi berasal dari bahasa yunani yaitu "*crypto*"berarti "*secret*" (rahasia) dan "*graphy*" berarti "*writing*" (tulisan). Para pelaku atau praktisi kriptografi disebut *cryptographers*. Sebuah algoritma kriptografi (*cryptography algoritm*) disebut cipher yang merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi.

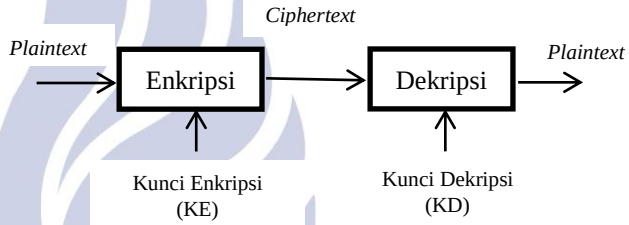
Proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut *plaintext*) menjadi pesan yang tersembunyi (disebut *ciphertext*) adalah enkripsi (*encryption*). Menurut ISO 7498-2, terminologi yang lebih tepat digunakan adalah "*encipher*". Proses sebaliknya, untuk mengubah *ciphertext* menjadi *plaintext*, disebut dekripsi (*decryption*). Menurut ISO 7498-2, terminologi yang lebih tepat untuk proses ini adalah "*decipher*".

Cryptanalysis adalah seni dan ilmu untuk memecahkan *ciphertext* tanpa bantuan kunci. *Cryptanalyst* adalah pelaku atau praktisi yang menjalankan *cryptanalysis. Cryptology* merupakan gabungan dari *cryptography* dan *cryptanalysis.*

Untuk mengenkripsi dan mendekripsi data, kriptografi menggunakan suatu algoritma (*cipher*) dan kunci (*key*).

Algoritma Kriptografi

Algoritma kriptografi telah mengalami perkembangan sehingga hasilnya lebih memuaskan, misalnya pada algoritma Blowfish, RSA, AES, DES dan lainya. Algoritma kriptografi terdiri dari algoritma enkripsi (E) dan algoritma dekripsi (D). Algoritma enkripsi menggunakan kunci enkripsi (KE), sedangkan algoritma dekripsi menggunakan kunci dekripsi (KD). Untuk lebih jelasnya dapat dilihat pada gambar 1 dibawah ini:



Gambar 1. Proses Enkripsi dan Dekripsi Kunci Simetris.

Kunci Simetris

Kunci simetris adalah jenis kunci kriptografi yang paling umum digunakan untuk membuat pesan yang disandikan sama dengan kunci untuk membuka pesan yang disandikan tersebut. Jadi pembuat pesan dan penerimanya harus memiliki kunci yang sama persis.

Dasar Matematis

Dasar matematis yang mendasari proses enkripsi dan dekripsi adalah relasi antara dua himpunan berisi elemen *plaintext*dan himpunan berisi *ciphertext.* Enkripsi dan dekripsi merupakan fungsi transformasi antara dua himpunan tersebut. Bila himpunan *plaintext* dinotasikan dengan P dan himpunan *ciphertext* dinotasikan dengan C, sedangkan fungsi enkripsi dengan E dan fungsi dekripsi dengan D, maka proses enkripsi dan dekripsi dapat dinyatakan dalam notasi matematis dengan :

$$E(P)=C \text{ dan} \quad (1)$$

$$D(C)=P \quad (2)$$

Karena proses enkripsi dan dekripsi bertujuan memperoleh kembali data asal, maka :

D(E)=P (3)

Pada metode kriptografi simetris atau konvensional digunakan satu buah kunci. Bila kunci dinotasikan dengan "K", maka proses enkripsi-dekripsi metode kriptografi simetris dapat dinotasikan dengan:

EK(P)=C (4)

DK(C)=P (5)

Dan keseluruhan sistem dinyatakan sebagai:

DK(EK(P))=P (6)

***Data Encryption Standard* (DES)**

DES (Data Encryption Standard) merupakan nama dari sebuah algoritma untuk mengenkripsi data yang dikeluarkan oleh *Federal Information Processing Standard* (FIPS) 46-1 Amerika Serikat. Algoritma dasarnya dikembangkan oleh IBM, NSA, dan NBS yang berperan penting dalam pengembangan bagian akhir algoritmanya. DEA dan DES telah dipelajari secara ekstensif sejak publikasi pertamanya, dan diketahui sebagai algoritma simetris yang paling baik dan paling banyak digunakan di dunia.

DES memiliki blok kunci 64 bit tetapi yang digunakan dalam proses eksekusi adalah 56 bit. Pada awalnya dirancang untuk implementasi secara hardware. Penggunaan dalam sistem komunikasi mengharuskan pengirim dan penerima memiliki kunci rahasia yang sama, yang dapat digunakan untuk mengenkripsi dan mendeskripsi data yang dikirim atau diterima. DES juga dapat digunakan untuk enkripsi data-data pribadi dalam harddisk.

a. Enkripsi DES

Algoritma DES dirancang untuk menulis dan membaca blok data yang terdiri dari 64 bit dibawah kontrol kunci 64 bit. Sebuah blok ditujukan pada permutasi dengan inisial IP, kemudian melewati perhitungan yang sangat bergantung pada kunci. Pada akhirnya melewati permutasi yang invers dari permutasi dengan inisial P^{-1}. Skema global dari algoritma DES adalah sebagai berikut:

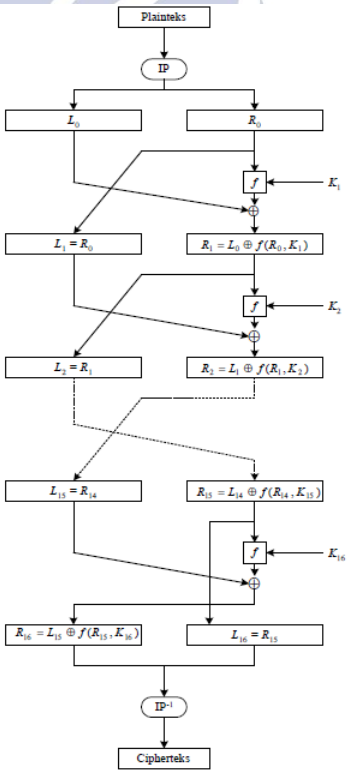
1. Blok plainteks dipermutasi dengan matriks permutasi awal (initial permutation atau IP).
2. Hasil permutasi awal kemudian di-enciphering- sebanyak 16 kali (16 putaran). Setiap putaran menggunakan kunci internal yang berbeda.
3. Hasil enciphering kemudian dipermutasi dengan matriks permutasi balikan (*invers initial permutation* atau IP^{-1}) menjadi blok cipherteks.

Secara matematis, satu putaran DES dinyatakan sebagai:

Li = Ri – 1 (7)

Ri = Li – 1 XOR *f*(Ri – 1, Ki) (8)

Dapat dilihat dari gambar 2 dibawah ini, Jika (L16, R16) merupakan keluaran dari putaran ke-16, maka (R16, L16) merupakan pra-cipherteks (*preciphertext*) dari *enciphering* ini. Cipherteks yang sebenarnya diperoleh dengan melakukan permutasi awal balikan, IP^{-1}, terhadap blok pra-cipherteks.



Gambar 2. Proses Enkripsi Algoritma DES.

b. Dekripsi DES

Proses dekripsi terhadap cipherteks merupakan kebalikan dari proses enkripsi. DES menggunakan algoritma yang sama untuk proses enkripsi dan dekripsi. Jika pada proses enkripsi urutan kunci internal yang digunakan adalah K1, K2, …, K16, maka pada proses

dekripsi urutan kunci yang digunakan adalah K16, K15, …, K1.

Untuk tiap putaran 16, 15, …, 1, keluaran pada setiap putaran *deciphering* adalah:

$$Li = Ri - 1 \quad (9)$$

$$Ri = Li - 1 \text{ XOR } f(Ri - 1, Ki) \quad (10)$$

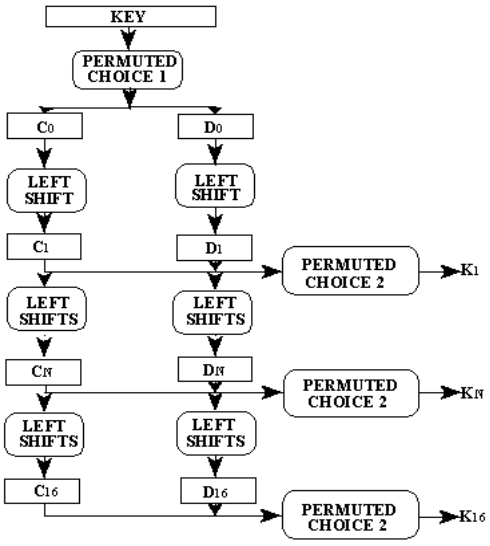
Yang dalam hal ini, (R_{16}, L_{16}) adalah blok masukan awal untuk deciphering. Blok (R_{16}, L_{16}) diperoleh dengan mempermutasikan cipherteks dengan matriks permutasi IP^{-1}. Pra-keluaran dari *deciphering* adalah adalah (L_0, R_0). Dengan permutasi awal IP akan didapatkan kembali blok plainteks semula.

c. Pembentukan Kunci

Karena ada 16 putaran, maka dibutuhkan kunci internal sebanyak 16 buah, yaitu K_1, K_2, …, K_{16}. Kunci-kunci internal ini dapat dibangkitkan sebelum proses enkripsi atau bersamaan dengan proses enkripsi. Kunci internal dibangkitkan dari kunci eksternal yang diberikan oleh pengguna. Kunci eksternal panjangnya 64 bit atau 8 karakter.

Algoritma Key Generator dimulai dari *Permutated Choice* 1. Pada tahapan ini, menggunakan sebuah SBox, 56 bit kunci eksternal dipecah menjadi C_0 dan D_0 (masing-masing 28 bit).

Proses pembentukan kunci dapat dilihat pada gambar 3 berikut:



Gambar 3. Proses pembentukan kunci algoritma DES

Blowfish

Blowfish merupakan sebuah algoritma kunci simetris cipher blok yang dirancang pada tahun 1993 oleh Bruce Schneier. Pada saat itu banyak sekali rancangan yang ditawarkan, tetapi hampir semuanya terhalang oleh paten atau kerahasiaan pemerintah Amerika. Schneier menyatakan bahwa blowfish bebas paten dan akan berada dalam domain publik. Pernyataan Schneier tersebut memberikan tempat bagi blowfish di dunia kriptografi, khususnya dalam masyarakat yang membutuhkan algoritma kriptografi yang cepat, kuat dan tidak terhalang oleh lisensi.

Blowfish adalah algoritma kriptografi kunci simetris cipher blok dengan panjang blok yang tetap, yakni sepanjang 64 bit. Blowfish menerapkan teknik kunci berukuran sembarang. Ukuran kunci yang bisa diterima oleh blowfish adalah antara 32 bit hingga 448 bit, dengan ukuran *default* sebesar 128 bit. Algoritma blowfish memanfaatkan teknik pemanipulasian bit dan teknik pemutaran ulang serta pergiliran kunci yang dilakukan sebanyak 16 kali. Algoritma utama terbagi menjadi dua sub algoritma utama, yaitu bagian ekspansi kunci dan bagian enkripsi-dekripsi data.

Ekspansi kunci dilakukan saat-saat awal dengan masukan sebuah kunci dengan panjang 32 bit hingga 448 bit, dan keluarannya adalah sebuah array subkunci dengan total 4168 *byte.* Bagian enkripsi-dekripsi data algoritma blowfish terjadi dengan memanfaatkan perulangan 16 kali terhadap jaringan feistel. Setiap perulangan terdiri atas permutasi dengan masukan berupa kunci dan substitusi data. Semua operasi dilakukan dengan memanfaatkan operator XOR dan penambahan operator dilakukan empat array *lookup* pada setiap putarannya.

a. Enkripsi Blowfish

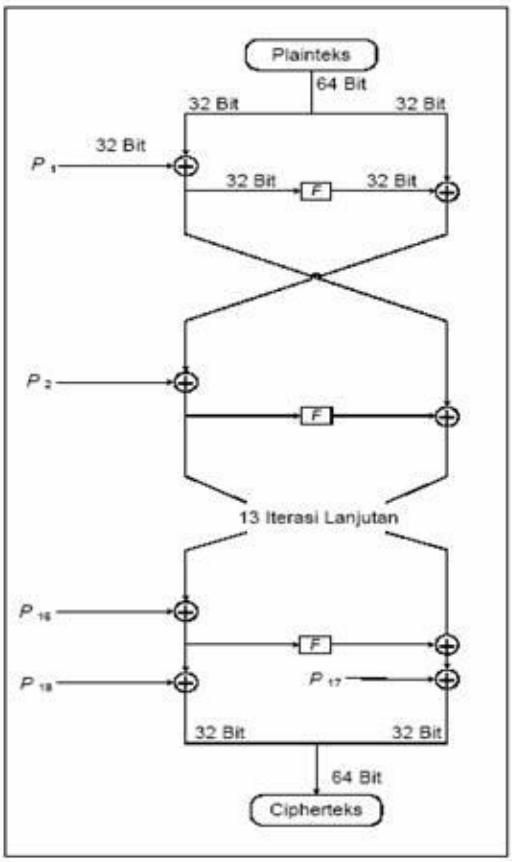
Enkripsi algoritma blowfish Terdiri dari iterasi fungsi sederhana (Feistel Network) sebanyak 16 kali putaran (iterasi), masukannya adalah 64-bit elemen data X. Setiap putaran terdiri dari permutasi kunci-dependent dan substitusi kunci- dan datadependent. Semua operasi adalah penambahan (addition) dan XOR pada variabel 32-bit. Operasi tambahan lainnya hanyalah empat penelusuran tabel array berindeks untuk setiap putaran. Langkahnya adalah seperti berikut :

1. Bagi data X menjadi dua bagian yang masing-masing terdiri dari 32-bit: XL, XR.
2. Lakukan langkah berikut :

For i = 1 to 16:
XL = XL XOR Pi
XR = F(XL) XOR XR
Tukar XL dan XR

3. Setelah iterasi ke-16, tukar XL dan XR lagi untuk melakukan membatalkan pertukaran terakhir.
4. Lalu lakukan :
   XR = XR XOR P17
   XL = XL XOR P18
5. Terakhir, gabungkan kembali XL dan XR untuk mendapatkan cipherteks.

Untuk lebih jelasnya, gambaran tahapan pada proses enkripsi dengan jaringan feistel yang digunakan Blowfish adalah seperti pada Gambar 4 berikut :

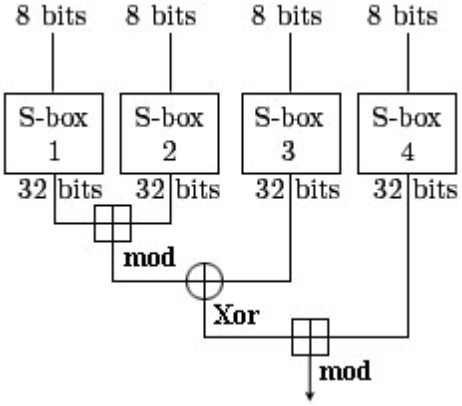


Gambar 4. Proses Enkripsi Algoritma Blowfish.

Pada langkah kedua, telah dituliskan mengenai penggunaan fungsi F. Fungsi F adalah dengan membagi XL menjadi empat bagian 8-bit: a,b,c dan d.

$F(XL) = ((S1,a + S2,b \bmod 2^{32}) \text{ XOR } S3,c) + S4,d \bmod 2^{32}$ (11)

Agar dapat lebih memahami fungsi F, tahapannya dapat dilihat pada Gambar 5 berikut :



Gambar 5. Fungsi F pada Blowfish.

b. Dekripsi Blowfish

Dekripsi sama persis dengan enkripsi, kecuali bahwa P1, P2,…, P18 digunakan pada urutan yang berbalik (reverse). Algoritmanya dapat dinyatakan sebagai berikut (Schneier, 1996):

for i = 1 to 16 do
Xri = Xli-1 XOR P19-i;
Xli = F[Xri] XOR Xri-1;
XL17 = XR16 XOR P1;
XR17 = XL16 XOR P2;

c. Ekspansi Kunci Blowfish

Subkunci dihitung menggunakan algoritma Blowfish, dengan langkah-langkah sebagai berikut :

1. Pertama inisialisasi P-array dan kemudian empat S-box secara berurutan dengan string tetap. String ini terdiri dari digit 125 hexadecimal dari *phi*. Dimana P-array terdiri dari 18 subkunci dengan ukuran 32 bit :
   P1, P2, …, P18 (12)
   P1, P2, …, P18 (13)
2. XOR P1 dengan 32 bit pertama kunci , XOR P2 dengan 32 bit kedua dari kunci dan seterusnya untuk setiap bit dari kunci (sampai P18). Ulangi terhadap bit kunci sampai seluruh P-array di XOR dengan bit kunci.
3. Enkripsikan semua string nol dengan algoritma Blowfish menggunakan subkunci seperti yang dijelaskan pada langkah 1 dan langkah 2.

4. Gantikan P1 dan P2 dengan keluaran dari langkah 3.
5. Enkripsikan keluaran langkah 3 dengan algoritma Blowfish dengan subkunci yang sudah termodifikasi.
6. Gantikan P3 dan P4 dengan keluaran dari langkah 5.
7. Teruskan proses tersebut, gantikan seluruh elemen dari P-array, dan kemudian seluruh keempat S-box berurutan, dengan keluaran yang berubah secara kontinyu dari algoritma Blowfish.

Secara keseluruhan diperlukan 521 iterasi untuk membangkitkan semua subkunci yang dibutuhkan.

METODE

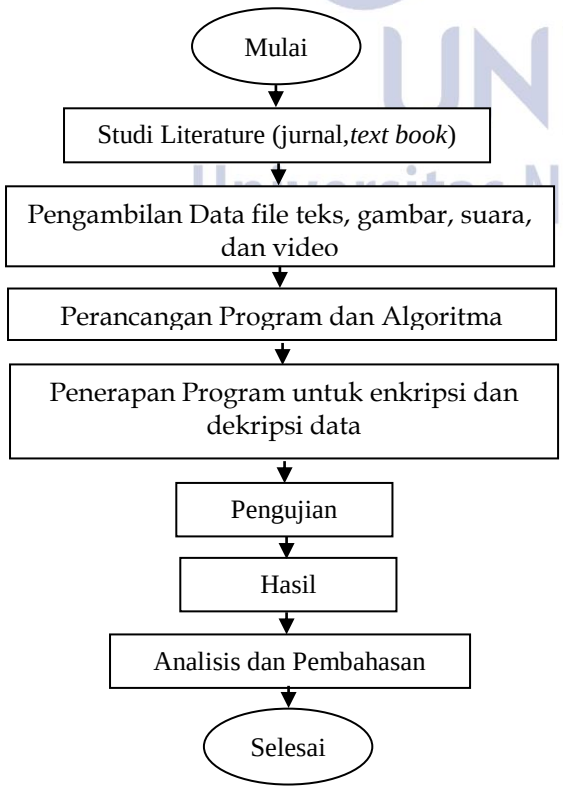
Pendekatan Penelitian

Penelitian tugas akhir ini untuk merancang dan menerapkan implementasi algoritma DES berbasis blowfish untuk enkripsi dan dekripsi data.

Pada penelitian ini, proses perancangan dan penerapan algoritma DES berbasis blowfish menggunakan *software* visual studio 2012 yang menggunakan bahasa pemrograman VB.NET.

Teknik Analisis Data

Analisis data yang diperoleh dalam penelitian ini bertujuan untuk menjawab permasalahan dalam rangka merumuskan kesimpulan, seperti dijelaskan pada gambar 6 berikut**:**



Gambar 6. Diagram alir tahapan penelitian

Tempat dan Waktu Penelitian

Penelitian dilakukan di Lab Komputer, Teknik Elektro, Fakultas Teknik, Universitas Negeri Surabaya. Penelitian berlangsung dalam waktu 7 bulan, dimulai dari bulan September 2016 hingga April 2017.

HASIL DAN PEMBAHASAN

Fase Perancangan

Perancangan implementasi algoritma DES berbasis blowfish terbagi menjadi dua perancangan, yaitu perancangan antarmuka dan perancangan algoritma.

a. Perancangan antarmuka

Perancangan antarmuka yang dibangun pada aplikasi ini terdiri atas beberapa halaman, antara lain:

1. Halaman Utama
2. Halaman Enkripsi
3. Halaman Dekripsi

b. Perancangan Algoritma

Algoritma yang dikembangkan untuk enkripsi dan dekripsi data menggunakan gabungan dari dua metode algoritma kriptografi dalam mengenkrip dan mendekrip file/data. Metode algoritma yang dirancang untuk aplikasi keamanan data ini adalah algoritma DES dan algoritma blowfish.

Dalam merancang gabungan dari dua algoritma yang telah disebutkan, proes enkripsi awal menggunakan algoritma enkripsi blowfish, kemudian hasil *ciphertext* dari enkripsi blowfish dienkripsi lagi menggunakan algoritma enkripsi DES. Untuk proses dekripsi adalah kebalikan dari urutan proses enkripsi.

Fase Penerapan

Untuk penerapan agar aplikasi bisa dijalankan, maka perlu menggabungkan dari perancangan antarmuka dan algoritma dengan bahasa pemrograman yang dipakai yaitu bahasa pemrograman VB.NET. penerapan dilakukan supaya proses enkripsi dan dekripsi dapat dijalankan pada aplikasi. Langkah penerapan dijelaskan sebagai berikut :

a. Proses Enkripsi Blowfish

Pertama yang perlu dilakukan untukproses enkripsi blowfish adalah mengambil *bytes* kunci untuk di ekspansi menggunakan ekspansi kunci algoritma blowfish.

```
BF.Key=System.Text.Encoding.UTF8.GetBytes(pass)
```

Kemudian ambil *bytes* plain file.

```
Dim fBytes As Byte()= File.ReadAllBytes(inputfile)
```

Setelah mendapatkan *bytes* kunci dan plain file, maka langkah selanjutnya adalah proses enkripsi blowfish.

```
Dim eBytes As Byte() = BF.EncodeBytes
(fBytes)
```

b. Proses Enkripsi DES

Ciphertext hasil dari enkripsi blowfish akan dienkripsi menggunakan algoritma enkripsi DES.

Pertama, ambil *bytes* kunci untuk enkripsi algoritmaDES.

```
Dim secret As String = TextBox3.Text
des.Key=ASCIIEncoding.ASCII.GetBytes(sec
ret)
```

Setelah itu ambil *bytes* plain file.

```
Dim fsinput As New FileStream(inputfile,
FileMode.Open, FileAccess.Read)
```

Setelah mendapatkan *bytes* kunci dan plain file, maka langkah selanjutnya adalah proses enkripsi DES.

```
Cs=NewCryptoStream(fsoutput,des.CreateEn
cryptor,CryptoStreamMode.Write)
```

c. Proses Dekripsi DES

Untuk mengembalikan *cipherfile* algoritma DES berbasis blowfish, maka proses dekripsi awal yang dilakukan adalah proses dekripsi algoritma DES.

Pertama, ambil *bytes* kunci untuk dekripsi algoritma DES.

```
Dim secret As String = TextBox1.Text
des.Key=ASCIIEncoding.ASCII.GetBytes(sec
ret)
```

Setelah itu ambil *bytes cipherfile*.

```
Dim fsinput As New FileStream(inputfile,
FileMode.Open, FileAccess.Read)
```

Setelah mendapatkan *bytes* kunci dan plain file, maka langkah selanjutnya adalah proses dekripsi DES.

```
cs=NewCryptoStream(fsoutput,des.CreateDe
cryptor(des.Key,des.IV),CryptoStreamMode
.Write)
```

d. Proses Dekripsi Blowfish

Hasil dari dekripsi DES selanjutnya akan didekripsi lagi menggunakan algoritma dekripsi blowfish. Pertama, ambil *bytes* kunci untuk enkripsi algoritma blowfish.

```
Dim pass As String = TextBox3.Text
BF.Key=System.Text.Encoding.UTF8.GetByte
s(pass)
```

Kemudian ambil *bytes cipherfile*.

```
Dim inputfile As String = TextBox1.Text
Dim fBytes As Byte() = File.ReadAllBytes
(inputfile)
```

Setelah mendapatkan *bytes* kunci dan plain file, maka langkah selanjutnya adalah proses dekripsi blowfish.

```
Dim dBytes As Byte() = BF.DecodeBytes
(fBytes)
```

Pengujian

Pengujian aplikasi dilakukan secara *blackbox* mandiri yaitu pengujian yang dilakukan secara langsung menggunakan PC/laptop. Pengujian proses enkripsi dan dekripsi data sebagai berikut :

Tabel 1. Hasil Pengujian Proses Enkripsi dan Dekripsi

Nama File	Ukuran awal (*byte*)	Ukuran enkripsi blowfish (*byte*)	Ukuran enkripsi DES (*byte*)	Ukuran dekripsi (*byte*)
test	4	16	24	4
Proposal Porjur	258,048	258,064	158,072	258,048
modul lengkap vb	694,116	694,128	694,136	694,116
image1	87,484	87,496	87,504	87,484
gif1	128,062	128,080	128,088	128,062
video1	2,138,308	2,138,320	2,138,328	2,138,308
Musik1	4,254,302	4,254,320	4,254,328	4,254,302
Avi1	1,399,046	1,399,064	1,399,072	1,399,046

Dari tabel diatas dapat dilihat bahwa keakuratan aplikasi dalam pengujian pada data yang telah diperoleh dapat diverifikasi dengan baik.

PENUTUP

Simpulan

Dari hasil penelitian tugas akhir implementasi algoritma DES berbasis blowfish untuk enkripsi dan dekripsi data pada pembahasan diperoleh kesimpulan sebagai berikut :

Pada penelitian ini perancangan program enkripsi dan dekripsi data menggunakan algoritma DES berbasis blowfish dilakukan dengan menggunakan *software* visual studio 2012 dan bahasa pemrograman VB.NET. Perancangan dilakukan dengan memproses bit pada data .txt, .doc, .pdf, .jpeg, .gif, .mp3, .mp4, .avi. Penerapan

aplikasi implementasi algoritma DES berbasis blowfish untuk enkripsi dan dekripsi data .txt, .doc, .pdf, .jpeg, .gif, .mp3, .mp4, .avi memiliki tingkat akurasi 100% dengan menjaga keaslian data (*authentication*) dan keutuhan data (*data integrity*) dibuktikan dengan kualitas data sebelum dan setelah dienkripsi.

Saran

Dari hasil penelitian yang telah dilakukan, berikut beberapa saran untuk penelitian mendatang:

Untuk para peneliti yang ingin pengembangan aplikasi enkripsi dan dekripsi menggunakan dua metode algoritma yang berbeda disarankan untuk menggunakan dua metode algoritma yang lebih modern dan gunakan tipe metode algoritma yang berbeda untuk mengenkripsi dan mendekripsi data. Sebagai contoh penggabungan tipe metode algoritma simetris dan asimetris.

DAFTAR PUSTAKA

Ariyus, Dony (2005). *Computer Security*. Yogyakarta:Andy Offset.

Ariyus, Dony (2006). Kriptografi Keamanan Data dan Komunikasi. Yogyakarta:Graha Ilmu.

Ariyus, Dony (2009). Keamanan Multimedia. Yogyakarta:Andi Offset.

Bofandra (2009). Implementasi Data Encryption Standard Untuk Enkripsi – Dekripsi berkas PDF. Bandung.

Komputer, Wahana (2003). Memahami Model Enkripsi & Security Data. Yogyakarta:Andi Offset.

Munir, Rinaldi (2004). Bahan Kuliah *Data Encryption Standard* (DES). Bandung.

Preissig, Stephen (2000). Data Encryption Standard (DES) Implementation on the TMS320C6000. Texas.

Schneier, Bruce (1996). *Applied Cryptography Second Edition John Wiley & Son*. New York.

Suriski, Sutinjak (2010). Kriptografi file menggunakan algoritma blowfish. Yogyakarta.

Tambunan, Shanty (2010). Algoritma kriptografi blowfish untuk keamanan dokumen pada *Microsoft Office*. Yogyakarta.

Valmik, NehaKhatri dkk (2014). Blowfish Algorithm. India.