KEAMANAN INFORMASI

“Algoritma Twofish ”

Dosen pembimbing : Nazruddin Safaat,MT

Kelompok 2 :

1. Muhammad Irfan ( 11551100481 )
2. Qishatul Ifki ( 11551105040 )
3. Rani Sesrika ( 11551200525 )
4. Zulfakhri ( 11551102843 )

Kelas : TIF 5D

JURUSAN TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU

2017

1. **SEJARAH ALGORITMA TWOFISH**

Pada tahun 1972 dan 1974, US the National Bureau of Standards (sekarang bernama the National Institute of Standards and Technology, atau NIST - sebuah lembaga yang mengatur tentang standar-standar) mengeluarkan publikasi pertama untuk sebuah standar enkripsi, yang menghasilkan algoritma data Encryption Standard (DES) [NBS77], yang tidak dapat disangkal sebagai algoritma kriptografi yang sangat terkenal dan sangat berhasil.Disamping kepopulerannya, DES sering diserang dengan berbagai kontroversi. Beberapa orang kriptografer mempertanyakan desain algoritma DES yang mengimplementasikan kunci dan ukuran blok yang terlalu kecil. Dengan berkembangnya pengetahuan tentang kunci terdistribusi akhir-akhir ini, tidak ada keraguan bahwa DES memang memiliki ukuran blok dan kunci yang tidak sesuai dengan kebutuhan masyarakat saat ini.  
Triple-DES ditawarkan untuk menjawab pertanyaan diatas, dan memang merupakan solusi sementara dari permasalahan diatas. TDES telah diadopsi oleh banyak sekali aplikasi yang membutuhkan tingkat keamanan tinggi seperti perbankan namun algoritma TDES dirasakan sangat lamban, apalagi dengan hardware pada saat itu.Merespon kebutuhan masyarakat untuk pengganti DES, NIST mengeluarkan semacam sayembara bernamakan program Advanced Encryption Standard (AES) pada tahun 1997 [NIS97a]. Sebuah sayembara untuk para kriptografer dunia untuk merancang algoritma kriptografi baru sebagai calon pengganti DES.

Twofish dirancang oleh Bruce Schneier. Twofish adalah suksesor dari blowfish. Twofish merupakan algoritma yang beroperasi dalam mode block. Algoritma twofish sendiri merupakan pengembangan dari algoritma Blowfish. Perancangan Twofish dilakukan dengan memperhatikan kriteria-kriteria yang diajukan National Institute Standard (AES), namun algoritma ini tidak terpilih sebagai basis standarisasi.

1. **PROSES ALGORITMA TWOFISH**

**Tahapan Proses Enkripsi dan Dekripsi**

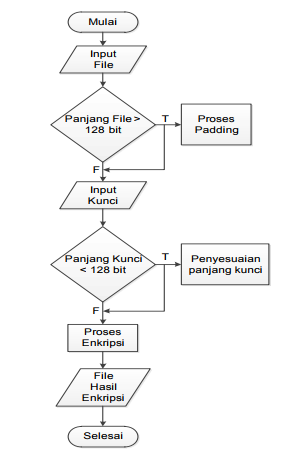
Tujuan algoritma twofish adalah untuk mengamankan file sehingga file menjadi tidak dapat terbaca. Proses utama pada pembuatan aplikasi perangkat lunak ini adalah melakukan enkripsi dan dekripsi.

**Proses Enkripsi**

Langkah-langkah dalam melakukan proses Enkripsi File :

1. Memulai proses enkripsi.
2. *Input* fileyangakan dienkripsi.
3. Jika *Plaintext* berukuran 128 bit maka tidak akan terjadi proses *Padding*. Jika *Plaintext* berukuran lebih dari 128 bit,maka proses *Padding* akan dilakukan.
4. *Input* kunci untuk mengenkripsi.
5. Jika panjang kunci yang di *input* kurang dari 128 bit maka akan dilakukan penyesuaian panjang kunci untuk mencapai 128 bit.
6. Proses enkripsi.
7. Menampilkan hasil enkripsi.
8. Selesai.

Digram alur proses enkripsi file terlihat pada gambar dibawah ini :

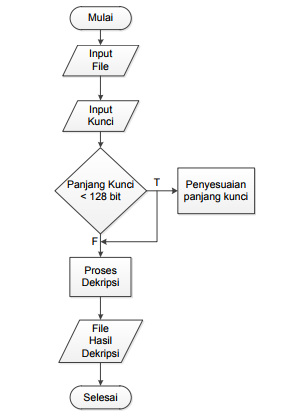
****

**Proses Dekripsi**

Langkah-langkah dalam melakukan proses Dekripsi File :

1. Memulai proses dekripsi.
2. *Input* file yang akan di dekripsi.
3. Input kunci untuk mendekripsi file.
4. Jika panjang kunci yang akan di *input* kurang dari 128 bit maka akan dilakukan penyesuaian panjang kunci untuk mencapai panjang 128 bit.
5. Proses dekripsi.
6. Menghapus padding.
7. Menampilkan hasil dekripsi.
8. Selesai.

Diagram alur proses dekripsi file terlihat pada gambar dibawah ini :

****

**Perancangan Proses**

Proses yang dirancang pada perangkat lunak ini berdasarkan pada algoritma Twofish. Algoritma Twofish sendiri merupakan algoritma yang menggunakan kunci simetris. Secara lebih jelas tahapan-tahapan algoritma twofish akan dijabarkan sebagai berikut. Penjadwalan Kunci :

a. Sebelum melalui tahapan enkripsi, maka harus melalui penjadwalan kunci. Panjang kunci yang didefiniksikan twofish sepanjang 128 bit, 192 bit dan 256 bit. Apabila input kunci yang dimasukkan kurang dari ketentuan tersebut, maka akan ditambahkan *zero* *byte* sampai panjang kunci memenuhiketentuan.

b. Setelah itu kunci dibagi menjadi vector Me, Mo dan S. Vector Me dan Mo digunakan pada fungsi h sebagai *list*, sedangkan vector S digunakan untuk tahap enkripsi pada fungsi g.

1. Masukkan masing-masing *word* kunci Kj yang diekspansi yaitu 2i dan 2i+1 kedalam fungsi h yaitu melalui pemutasi q0 dan q1 dilanjutkan dengan matrik MDS.
2. Hasil dari *word* 2i melalui proses PHT, sedangkan *word* 2i+1 sebelum melalui proses PHT dilakukan rotasi ke kiri sejauh 8 bit. Maka hasil dari proses tersebut menjadi kunci yang sudah terjadwal.

**Tahap Enkripsi :**

1. Input *Plaintext* sebesar 128 bit akan dibagi menjadi empat *word* yaitu P0, P1, P2, P3 yang masing-masing sebesar 32 bit. P0 dan P1 akan menjadi bagain kiri, sedangkan P2 dan P3 akan menjadi bagian kanan.
2. *Plaintext* akan melalui proses *input whitening* yaitu *input* akan di-XORdengan empat *word* kunci yang telah terjadwal yaitu K0, K1, K2 dan K3.
3. Proses berikutnya input akan melalui proses pada fungsi F yang meliputi di dalamnya adalah fungsi g dan dilanjutkan dengan PHT, dan dilakukan penambahan hasil PHT dengan kunci. Proses fungsi F tersebut dilakukan secara bertahap . R0 dan R1 yang merupakan hasil whitening akan menjadi input untuk fungsi F.
4. R0 dan R1 akan dimasukkan ke dalam fungsi g yang merupakan bagian awal dari fungsi F. Untuk R1 sebelum dimasukkan ke dalam fungsi g akan dirotasi ke kiri sejauh 8 bit. R0dan R1 melalui S-Box dan selanjutnya akan dikalikan dengan menulis matriks MDS. Hasil dari fungsi g ini masing-masing menjadi T0 dan T1.
5. T0 dan T1 akan melalui proses PHT yang merupakan penggabungan T0 dan T1 dimana T0+T1 dan T0+2T1. Setelah itu hasil dari PHT tersebut masing-masing akan ditambahkan dengan kunci yang sudah terjadwal yaitu K2r+8 dan K2r+9. Hasil dari fungsi F adalah F0 dan F1, maka dengan demikian fungsi F telah terpenuhi.
6. Setelah itu F0 dan F1 masing-masing di-XOR dengan R2 dan R3. Hasil dari R2 XOR F0 dirotasi ke kanan sejauh 1 bit. Sedangkan R3 XOR F1, sebelumnya R3 dirotasi ke kiri sejauh 1 bit.
7. Setelah itu, maka akan dilakukan iterasi sebanyak 16 kali. Setiap iterasi sama dengan proses sebelumnya.
8. Hasil dari swap blok terakhir adalah penukaran bagian kanan dan kiri yang di-*undo.*
9. Hasil dari 16 *round* enkripsikan melalui *output whitening* yaitu proses peng-XORan 16 *round* enkripsi dengan K4, K5, K6 dan K7.

**Tahap Dekripsi**

Pada proses dekripsi, cara yang dilalui sama dengan proses enkripsi tetapi hanya arahnya saja yang berlawanan. Proses yang dilalui secara berurutan yaitu : *Output Whitening,* Swap Blok Terakhir, 16Iterasi Dekripsi, dan *Input Whitening*. Inputnya adalah *chipertext* dan kunci untuk memperoleh *plaintext*. Kunci untuk dekripsi sama saja dengan kunci enkripsi, begitupun juga panjang maksimal kunci yaitu 256 atau 32 karakter.

1. **SOURCE CODE DAN PROJECT**

Berikut merupakan source code dalam bentuk visual basic (VB) yaitu :

1. Tentukan kalimat yang akan dienkrip



1. Tentukan kata kunci enkripsi yang digunakan



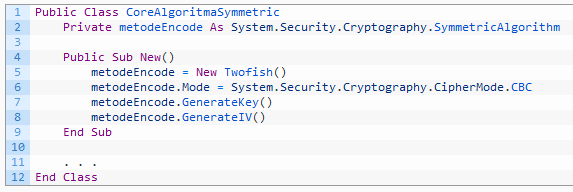
1. Lakukan inisialisasi variabel yang digunakan oleh metode ini  
   Penjelasan lebih detail tentang fungsi ini dapat dilihat pada penjelasan skrip dibawah ini



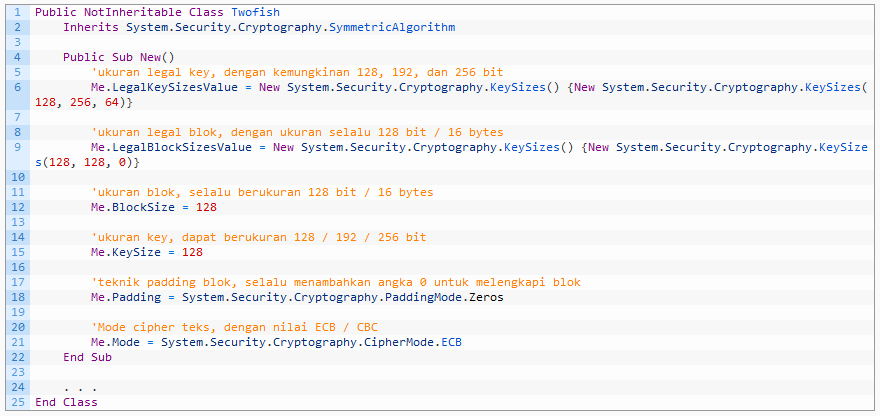
Skrip tersebut akan melakukan inisialisasi pada Class CryptCore. Class ini adalah inti class untuk pemanggilan fungsi enkripsi dan dekripsi yang mengacu pada algoritma Twofish. Deklarasi Class CryptCore adalah sebagai berikut:



Pada saat melakukan proses InitCore, maka proses tersebut akan melakukan inisialisasi pada Class CoreAlgoritmaSymmetric. Pemanggilan fungsi enkripsi / dekripsi pada Class sebelumnya akan mengarah pada Class ini untuk selanjutnya dilakukan perhitungan enkripsi / dekripsi yang sebenarnya. Deklarasi Class CoreAlgoritmaSymmetric adalah sebagai berikut:



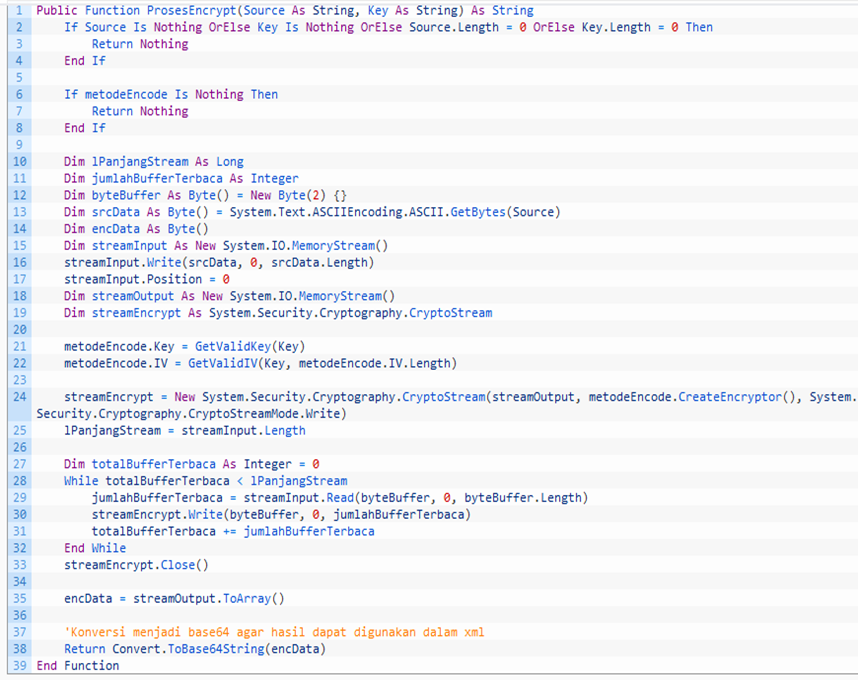
Pada saat menginisialisasi variabel metodeEncode, maka proses tersebut akan melakukan inisialisasi pada Class Twofish. Class ini berisi tentang beberapa properti dan fungsi yang menggantikan properti dan fungsi yang diturunkan dari Class SymmetricAlgorithm. Deklarasi Class Twofish adalah sebagai berikut:



1. Lakukan enkripsi kalimat awal menggunakan algoritma ini. Penjelasan lebih detail tentang fungsi ini dapat dilihat pada penjelasan skrip dibawah ini

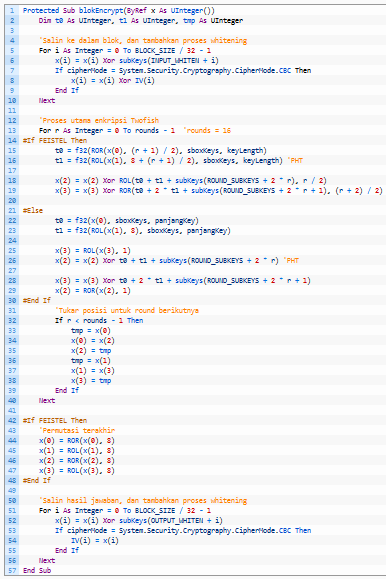


Skrip tersebut akan menjalankan proses enkripsi yang terdapat dalam Class CoreAlgoritmaSymmetric.





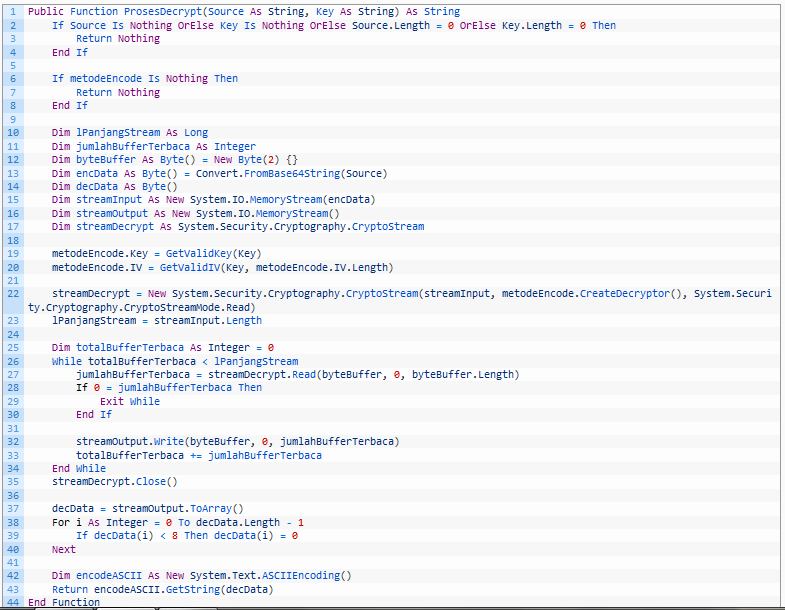
Sedangkan proses enkripsi utama algoritma Twofish adalah sebagai berikut



1. Lakukan dekripsi dari kalimat yang telah terenkripsi. Penjelasan lebih detail tentang fungsi ini dapat dilihat pada penjelasan skrip dibawah ini



Skrip tersebut akan menjalankan proses dekripsi yang terdapat dalam Class CoreAlgoritmaSymmetric.

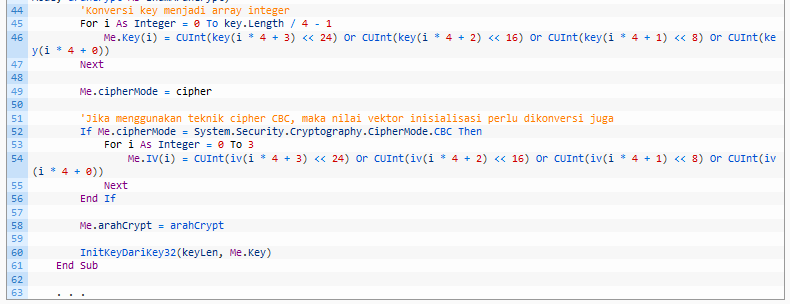


Sedangkan proses dekripsi utama algoritma Twofish adalah sebagai berikut

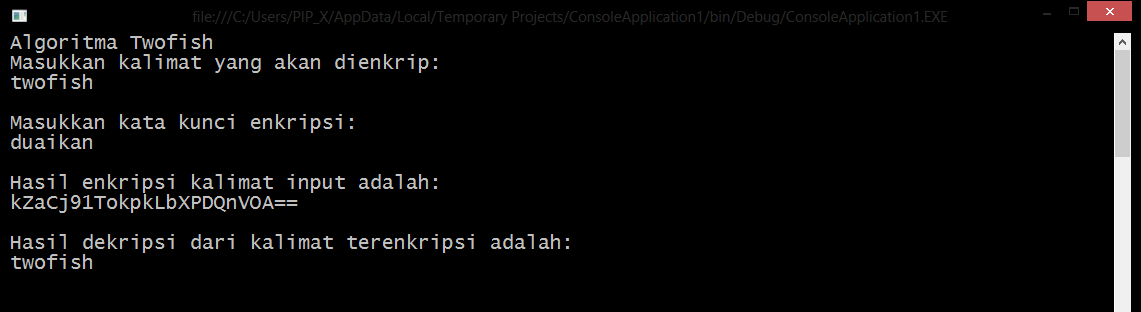


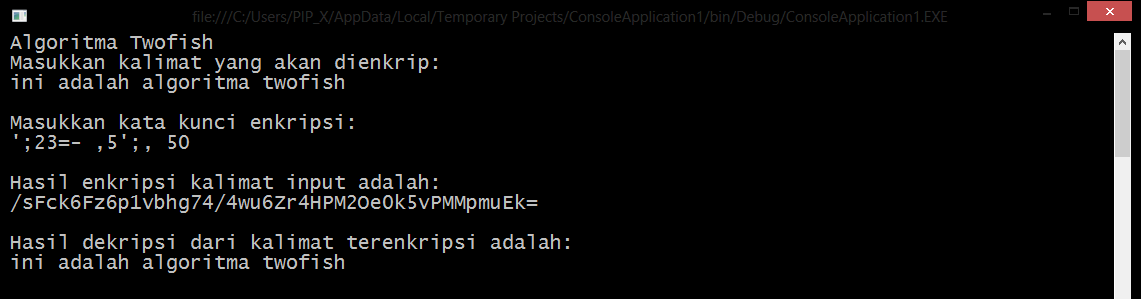
Secara keseluruhan, skrip ini membutuhkan 2 Class tambahan yaitu Class TwofishBase dan Class TwofishAlgoritma. Class TwofishBase berisi tentang key yang digunakan SBOX, subkey, IV, round, dan fungsi utama enkripsi dan dekripsi dengan metode Twofish. Class TwofishAlgoritma adalah hasil implementasi Class Twofish yang berisi tentang beberapa properti dan fungsi yang menggantikan properti dan fungsi yang diturunkan dari Class TwofishBase dan SymmetricAlgorithm. Deklarasi kedua Class tersebut adalah sebagai berikut:





Hasil akhir dari source code diatas adalah :

****

****

1. **KELEBIHAN DAN KEKURANGAN**
2. Kelebihan Algoritma Twofish
3. Waktu proses untuk enkripsi dan dekripsi relatif cepat, hal ini disebabkan karena efisiensi yang terjadi pada pembangkit kunci, Karena cepatnya proses enkripsi dan dekripsi, maka algoritma ini dapat digunakan pada sistem secara real-time seperti saluran telepon digital.
4. Memiliki varian dengan sebuah nomor variable dari setiap round.
5. Memiliki key schedule yang dapat diprakomputasikan untuk kecepatan maksimum dan penggunaan memori minimum.
6. Cocok sebagai stream chipper, fungsi hash satu arah, MAC dan pseudo random number generator, dengan  menggunakan metode konstruksi yang dapat dimengerti.
7. Memiliki varian famili-key untuk memungkinkan versi chipper yang berbeda dan non interrupterable.
8. Kekurangan Algoritma Twofish

Untuk tiap pasang pengguna dibutuhkan sebuah kunci yang berbeda, sedangkan sangat sulit untuk menyimpan dan mengingat kunci yang banyak secara aman, sehingga akan menimbulkan kesulitan dalam hal manajemen kunci. Perlu adanya kesepakatan untuk jalur yang khusus untuk kunci, hal ini akan menimbulkan masalah yang baru karena tidak mudah u menentukan jalur yang aman untuk kunci, masalah ini sering disebut dengan “Key Distribution Problem”. Apabila kunci sampai hilang atau dapat ditebak maka kriptosistem ini tidak aman lagi.

1. **APLIKASI ATAU SISTEM YANG MASIH MENGGUNAKAN ALGORITMA TWOFISH**

Komunikasi keamanan pesan suara dengan menggunakan jaringan internet telah banyak digunakan. Salah satu teknologi komunikasi suara yang menggunakan jaringan internet dan sering digunakan adalah voice scrambling, namun voice scrambling mempunyai tingkat keamanan rendah. Solusi untuk menangani tingkat keamanan yang rendah adalah dengan enkripsi pesan suara. Enkripsi merupakan salah satu langkah pengkodean pesan, sehingga tidak semua orang dapat memahaminya. Algoritma enkripsi pesan suara yang digunakan adalah Algoritma Twofish. Algoritma Twofish baik digunakan untuk enkripsi dan dekripsi pesan suara karena kualitas suara yang dihasilkan dari proses dekripsi sama dengan suara sebelum proses enkripsi.