BAB I

PENDAHULUAN

1.1. Latar Belakang

Kemajuan di bidang teknologi informasi telah memungkinkan berbagai pihak (khususnya industri musik) untuk melakukan interaksi dengan konsumen melalui jaringan komputer. Kegiatan - Kegiatan tersebut tentu saja akan menimbulkan resiko bila mana informasi yang sensitif dan berharga tersebut diakses oleh orang-orang yang tidak berkepentingan, sehingga keamanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi. Pada umumnya informasi pada industri musik berupa file audio. File audio yang umum digunakan adalah file MP3, yang mana dari segi ukuran file relatif kecil, meskipun tergantung pada file itu sendiri. Salah satu cara yang digunakan untuk pengamanan data adalah menggunakan teknik kriptografi yaitu dengan menyandikan isi informasi (plaintext) tersebut menjadi isi yang tidak dipahami melalui proses enkripsi, dan untuk memperoleh kembali informasi yang asli, dilakukan proses dekripsi, disertai dengan menggunakan kunci yang benar. Pada tahun 1998 diadakan suatu kompetisi untuk menetapkan metode algoritma enkripsi standard di Amerika. Pada kompetisi itu diperoleh lima finalis yaitu algoritma Rijndael, Serpent, Twofish, MARS, RC6. Pada kompetisi itu ditetapkan algoritma Rijndael sebagai algoritma standar untuk enkripsi di Amerika. Sedangkan Serpent dan Twofish sebagai juara dua dan juara tiga. Rijndael dipilih dikarenakan kecepatan proses enkripsinya dan kemudahan dalam pembentukannya. Sedangkan serpent tidak menjadi juara karena proses enkripsinya yang lama. Twofish gagal menjadi juara satu karena algoritmanya yang sulit dan waktu enkripsi yang relatif lama. Namun diantara semua metode tersebut algoritma twofish dianggap sebagai algoritma yang memiliki tingkat keamanan yang tinggi dan metode ini bebas digunakan (tidak dipatenkan ataupun diperdagangkan). Enkripsi dan dekripsi pada algoritma twofish menggunakan metode kriptografi block cipher.

Untuk proteksi data cukup penting dapat menggunakan program khusus proteksi atau enkripsi data. Sedangkan proses dekripsinya dapat juga dilakukan

terpisah ataupun jadi satu kesatuan dengan program enkripsi data. Proses dekripsi juga dapat dilakukan secara "*online*" ataupun secara "*offline*". Untuk proses dekripsi yang dilakukan secara "*online*" diasumsikan lebih aman dibandingkan dengan proses "*offline*", karena jika proses telah selesai dilakukan, maka file akan kembali terenkripsi. Dari segi konsumen / pengguna, tentu response time (waktu dari mulai file mp3 dipilih / dijalankan dengan suatu player tertentu hingga suara dari file tersebut keluar) yang cepat merupakan suatu parameter yang sangat penting dalam pengaksesan suatu file mp3.

1.2. Rumusan Masalah

1. Bagaimana menerapkan proses enkripsi secara *offline* untuk file mp3 menggunakan algoritma twofish dengan teknik partisi block cipher.
2. Bagaimana menerapkan proses dekripsi secara *online* untuk file mp3 menggunakan algoritma twofish dengan teknik partisi block cipher.
3. Bagaimana mendapatkan *response time* minimum dengan teknik partisi block cipher, yang diharapkan dengan teknik partisi ini tidak memberikan kenaikan yang signifikan terhadap penambahan ukuran file ciphertext.

1.3. Sistematika Penulisan

Tugas ini di susun berdasarkan sistematika sebagai berikut:

BAB I	**:**	**Pendahuluan**
		Pada bab ini dibahas tentang latar belakang, perumusan masalah , dan sistematika penulisan tugas.
BAB II	**:**	**Pembahasan**
		Pada bab ini di berisi penjelasan tentang sejarah twofish dan apa itu twofish.
BAB III	**:**	**Penutup**
		Pada bab ini diberikan kesimpulan dari hasil pembahasan dan saran pengembangan selanjutnya

BAB II

PEMBAHASAN

2.1. Sejarah Twofish

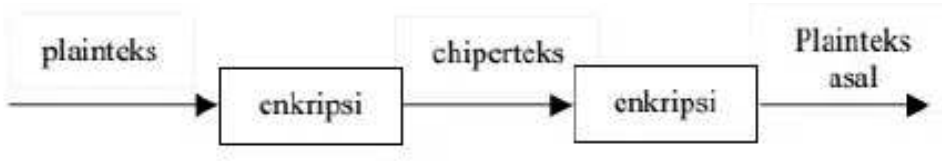
Pada tahun 1972 dan 1974 nama NIST (The Nationanl Institude of Standards and Technology) adalah National Bureau of Standards. NIST adalah publik pertama yang mengajukan suatu standar enkripsi NIST mengadakan sebuah sayembara untuk mencari kriteria algoritma kriptografi modern dan salah satu kandidat AES adalah algoritma twofish. Twofish didesain oleh Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, dan Niels Ferguson dari Laboratorium Counterpane System. Bruce Schneier juga mendesain algoritma Blowfish yang telah di implementasi oleh lebih dari 130 aplikasi komersial. Twofish yang resmi, yaitu dengan 16 putaran, sampai saat ini belum terpecahkan.

Namun untuk 5 putaran, telah berhasil dipecahkan dengan 222,5 plainteks terpilih dan 251 usaha (effort).

Twofish adalah block cipher 126 bit yang menerima kunci dengan panjang yang fleksibel sampai 256 bit. Cipher ini menggunakan cukup banyak metode dalam implementasinya, meliput jaringan Feistel (Feistel network), SBox, Matriks MDS, transformasi Pseudo-Hadamard, *whitening,* dan *key schedule*.

2.2. Pengertian Kriptografi

Kriptografi merupakan ilmu sekaligus seni untuk menjaga kerahasiaan pesan (data atau informasi) dengan cara menyamarkannya (*to cripyt*) menjadi bentuk tersandi yang tidak bermakna.[1] Pesan yang dirahasiakan dinamakan plainteks, sedangkan pesan hasil penyamaran dinamakan chiperteks. Proses penyamaran dari plainteks ke chiperteks disebut enkripsi (encryption) dan proses pembalikan dari chiperteks ke plainteks disebut dekripsi (decryption). Gambar dibawah memperlihatkan diagram kedua proses yang dimaksud.



Gambar 1: Proses Enkripsi dan Dekripsi

[1] *Rinaldi Munir, Matematika Diskrit, Prodi Teknik Informatika ITB, 2006*

Kriptografi tidak berarti hanya memberikan keamanan informasi saja, namun lebih ke arah teknik-tekniknya. Ada empat tujuan dari ilmu kriptografi, yaitu :

1. Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas,
2. Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain menyangkut penyisipan, penghapusan, dan pensubtitusian data lain ke dalam data yang sebenarnya
3. Autentikasi, adalah berhubungan dengan identifikasi, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain,
4. Non-repudiasi, yang berarti begitu pesan terkirim, maka tidak akan dapat dibatalkan.

2.3. Pengertian Twofish

Twofish merupakan algoritma kriptografi yang beroperasi dalam mode blok cipher berukuran 128 bit dengan ukuran kunci sebesar 256 bit, ukuran kunci yang besar ditujukan untuk meniadakan kemungkinan kunci lemah (*weak-key*). Algoritma Twofish sendiri merupakan pengembangan dari algoritma Blowfish. Perancangan Twofish dilakukan dengan memperhatikan kriteria-kriteria yang diajukan **National Institute of Standards and Technology (NIST)** untuk kompetisi Advanced Encryption Standard (AES), namun algoritma ini tidak terpilih sebagai basis standardisasi.

Tujuan dari perancangan Twofish yang selaras dengan kriteria NIST untuk AES adalah untuk membuat suatu algoritma kriptografi yang efisien dan portabel, rancangan yang fleksibel yang dapat menerima panjang kunci tambahan sehingga dapat diterapkan pada platform dan aplikasi yang sangat bervariatif serta cocok untuk cipher aliran, fungsi hash, dan MAC, serta rancangan yang sederhana agar memudahkan proses analisis dan implementasi algoritma.

Algoritma Twofish menggunakan struktur sejenis Feistel dalam 16 putaran dengan tambahan teknik *whitening* terhadap input dan output. Teknik whitening sendiri adalah teknik melakukan operasi XOR terhadap materi kunci sebelum putaran pertama dan sesudah putaran akhir. Elemen di luar jaringan feistel normal yang terdapat dalam algoritma twofish adalah rotasi 1 bit. Proses rotasi ini dapat dipindahkan ke dalam fungsi F untuk membentuk struktur jaringan Feistel yang murni, tetapi hal ini membutuhkan tambahan rotasi kata sebelum langkah output whitening.

2.4.Kriteria Algoritma Kriptografi Twofish

Algoritma Twofish merupakan salah satu algoritma yang direkomendasikan sebagai AES. Hal ini disebabkan pemenuhan kriteria desain oleh NIST sebagai standar AES yaitu :

1. Blok cliper simetris 128-bit
2. Memiliki panjang kunci antara lain : 128 bit, 192 bit, dan 256 bit.
3. Tidak terdapat kunci – kunci yang lemah.
4. Memiliki efisiensi pada software dan hardware dari platform yang berbeda.
5. Memiliki rancangan yang fleksibel, misalnya menerima panjang kunci tambahan, dapat diterapkan pada software dan hardware dari platform berbeda, cocok untuk stream chipper, fungsi hash dan MAC.
6. Desain yang simpel, memudahkan baik untuk analisa maupun implementasi.

2.5. Kelebihan Algoritma Kriptografi Twofish

Beberapa keunggulan algoritma kriptografi Twofish yaitu :

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

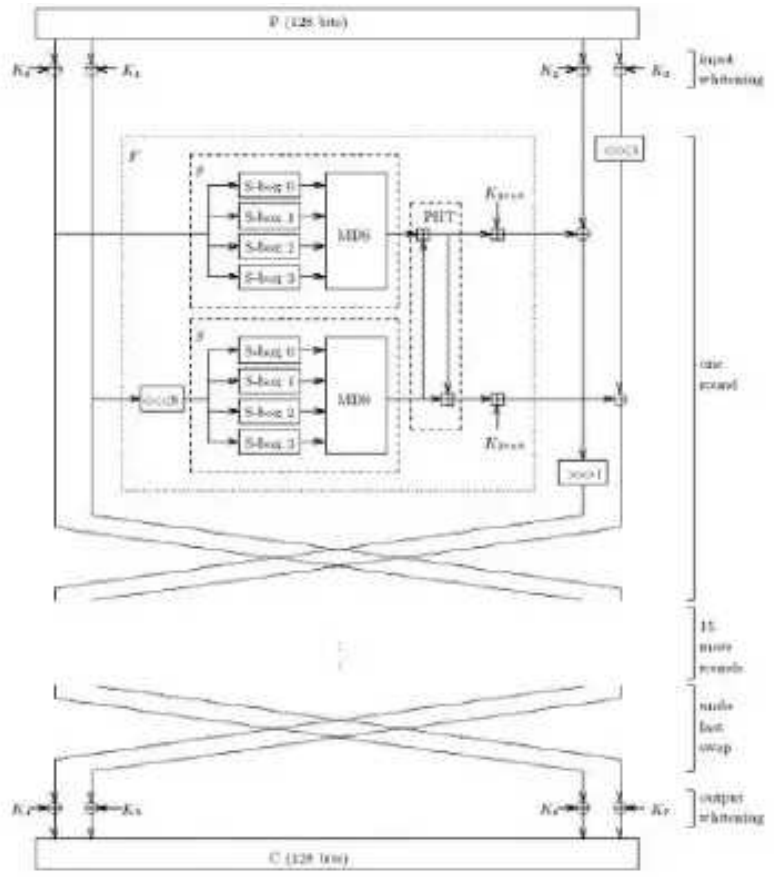
Pada implementasi algoritma Twofish, terdapat beberapa hal yang harus diperhatikan, antara lain :

Bit masukan sebanyak 128 bit akan dibagi menjadi empat bagian masing – masing 32 bit menggunakan konvensi little-Endian. Dua bagian bit akan menjadi bagian kanan, dan dua lainnya.

Bit input akan di-XOR terlebih dahulu dengan empat bagian kunci, atau dengan kata lain mengalami proses whitening. $R0,i = Pi \oplus\_Ki$ i = 0, …, 3 Dimana K adalah kunci, Ki berarti sub kunci yang ke-i.

Algoritma Twofish menggunakan struktur jaringan Feistel. Jaringan Feistel yang digunakan oleh Twofish terdiri atas 16 perulangan. Fungsi f pada algoritma Twofish terdiri atas beberapa tahap yaitu :

- Fungsi g, yang terdiri dari 4 s-box dan matriks MDS
- PHT (Pseudo-Hadamard Transformation) atau Transformasi Pseudo-Hadamard
- Penambahan hasil PHT dengan kunci



Gambar 1.Struktur Algoritma Twofish

2.6. Kelemahan Algoritma Kriptografi Twofish

1. 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.
2. 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”.
3. Apabila kunci sampai hilang atau dapat ditebak maka kriptosistem ini tidak aman lagi.

BAB III
PENUTUP

3.1. Kesimpulan

1. Twofish adalah cipher blok 128 bit yang menerima key dengan panjang variabel diatas 256 bits dan tidak memiliki kunci – kunci yang lemah.
2. Twofish memiliki empat macam key schedule dalam implementasinya yaitu : full keying, partial keying, minimal keying, dan zero keying dengan perbedaan dalam hal *key setu.*
3. Twofish dibentuk berdasarkan jaringan Fietsel yang terdiri atas masukan Whitening, S-boxes, keluaran Transformasi Pseudo Hadamard, dan keluaran Whitening.
4. Twofish memiliki kehandalan- kehandalan dalam implementasinya diatas berbagai platform microprocessor, smart card dan hardware yang dibuat sebagai perangkat enkripsi data.
5. Twofish memiliki resistensi yang tinggi terhadap related key attack, dan hanya dapat ditembus dengan menggunakan *brute force.*
6. Salah satu contoh implementasi Algoritma Twofish adalah penerapannya dalam proses enkripsi aliran pesan suara.
7. Untuk mendapatkan hasil yang maksimal, dilakukan modifikasi pada mode operasinya yaitu dengan mengganti mode operasinya menjadi Mode *Counter.*
8. Berdasarkan kelebihan yang dimilikinya, algoritma Twofish dapat dijadikan standar AES.

3.2. Saran

Untuk pengembangan lebih lanjut, diharapkan dapat menggunakan metode lain yang lebih baik sehingga hasil bisa lebih bagus lagi dan nilai kemiripan lebih tinggi.

DAFTAR PUSTAKA

- Rinaldi Munir, *Matematika Diskrit,* Prodi Teknik Informatika ITB, 2006
- https://ariemuzakir.wordpress.com/2010/08/31/algoritma-twofish-kriptografi/
- https://deviachrista.blogspot.co.id/2013/04/pengertian-algoritma-twofishblowfish.html
- http://susmisyahfrida.blogspot.co.id/2016/04/algoritma-twofish.html
- https://id.wikipedia.org/wiki/Twofish
- https://prezi.com/qyidtyu3ikvr/twofish/