JOINT

Journal of Informatics and Technology, Vol 1, No 3, Tahun 2012, p 84-89
http://ejournal-s1.undip.ac.id/index.php/joint

Implementasi Keamanan Pengiriman Pesan Suara dengan Enkripsi dan Dekripsi Menggunakan Algoritma Twofish

Fathonah Khusnul K

J2F 008 100

Program Studi Teknik Informatika, Jurusan Matematika, Universitas Diponegoro Semarang

e-mail : fathonah.khusnul.k@gmail.com

ABSTRAK

Komunikasi keamanan pesan suara dengan menggunakan jaringan internet telah banyak digunakan. Salah satu technology 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.

Kata Kunci : Enkripsi, Algoritma Twofish, Kabel Jaringan LAN.

1. PENDAHULUAN

Keamanan data suara banyak yang menggunakan *voice scrambling*. *Voice Scrambling works be taking a signal and turning it 'inside out', reversing the signal around a pre-set frequency* [8]. Langkah '*taking a signal and turning it'inside out''* ini dilakukan untuk membuat sinyal yang telah diubah menjadi tidak dapat diketahui oleh siapapun kecuali pihak yang mempunyai alat khusus yang telah dirancang untuk *voice scrambling*. Teknik *voice scrambling* ini mempunyai teknik keamanan yang rendah, sehingga banyak sekali pencurian data yang dilakukan. Solusi lain yang mempunyai tingkat keamanan lebih tinggi daripada *voice scrambling* adalah enkripsi.

Encryption is a much stronger method of protecting speech communications than any form of scrambling. Voice encryptors work by digitizing the conversation and applying a cryptographic technique to the resulting bit-stream. In order to decrypt the speach, the correct encryption method and key must be used [8].

Algoritma enkripsi yang digunakan untuk enkripsi suara bermacam-macam dan

masing-masing memiliki karakteristik sendiri. Belum ada satu algoritma tertentu yang menjadi standart enkripsi komunikasi suara, perlu ada usaha untuk menerapkan algoritma enkripsi lain untuk mengetahui algoritma tersebut dalam proses enkripsi suara. Algoritma enkripsi yang digunakan dan dibahas pada tugas akhir ini adalah Algoritma Twofish.

Algoritma Twofish telah banyak digunakan untuk berbagai penerapan, antara lain digunakan untuk pembuatan aplikasi enkripsi dekripsi pesan teks dan pesan gambar. Perancangan twofish memperhatikan kriteria-kriteria yang diajukan oleh *National Institute of Standards and technology* (NIST) untuk kompetisi *Advanced Encryption Standart* (AES) [2]. Berdasarkan kriteria-kriteria yang ada dalam Algoritma Twofish, algoritma ini mendukung untuk digunakan dalam sebuah proses enkripsi. Algoritma twofish ini sebuah *block chiper* 128 bit yang dapat menerima kunci dengan panjang variable 128 bit sampai dengan 256 bit. Algoritma ini bekerja lebih efisien, dan penggunaannya pun tidak mengeluarkan biaya karena memang tidak dipatenkan, selain itu algoritma ini mempunyai beberapa keuntungan antara lain yakni *rancangan simple* memudahkan untuk analisa maupun implementasi [2]. Algoritma Twofish merupakan algoritma *chiper* blok. Saat ini algoritma Twofish banyak diimplementasikan dengan menggunakan mode operasi *cipher block chaining* (CBC). Untuk itu akan digunakan *chiper block chaining* untuk pengoperasian chiper pada Algoritma Twofish. *The chiper block chaining (CBC) mode is a confidentiality mode whose encryption processfeatures the combining ("chaining") of the plaintext blocks with the previous chipertext blocks* [5].

Untuk pengiriman *file* dari komputer satu ke komputer tujuan akan digunakan kabel jaringan LAN. Kabel LAN mempunyai fungsi *transfer file* yang memudahkan dan cepat. Pada tugas akhir ini dibuat implementasi keamanan pengiriman pesan suara dengan enkripsi dan dekripsi menggunakan Algoritma Twofish dan *chiper block chaining* dengan menggunakan kabel LAN sebagai fasilitas *transfer file*.

2. Kriptografi

Kriptografi adalah ilmu sekaligus seni untuk menjaga keamanan pesan (*message*). Pengertian kriptografi menurut terminologinya adalah ilmu seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain [1]. Data yang dapat dibaca dan dipahami tanpa tindakan khusus disebut *plaintext*. Metode yang digunakan untuk menyamarkan *plaintext* sedemikian rupa untuk menyembunyikan substansinya disebut enkripsi (*encryption*) atau *enciphering*. Hasil enkripsi terhadap *plaintext* menghasilkan sebuah teks yag tidak dapat dibaca, disebut *ciphertext*. Enkripsi digunakan untuk memastikan informasi tersembunyi dari siapapun yang tidak memiliki wewenang. Proses untuk mengembalikan *ciphertext* ke *plaintext* disebut dekripsi (*decryption*) atau *deciphering*.

2.1. Algoritma Kunci Simetri

Algoritma kunci simetri disebut juga dengan algoritma kunci klasik, karena menggunakan kunci yang sama untuk enkripsi dan dekripsinya. Mengirimkan pesan dengan menggunakan algoritma ini, penerima pesan harus diberitau kunci dari pesan tersebut agar bisa mendekripsi pesan yang dikirim. Keamanan dari pesan yang menggunakan algoritma ini tergantung pada kunci, jika kunci diketahui oleh orang lain maka orang tersebut bisa melakukan enkripsi dan dekripsi terhadap pesan tersebut.

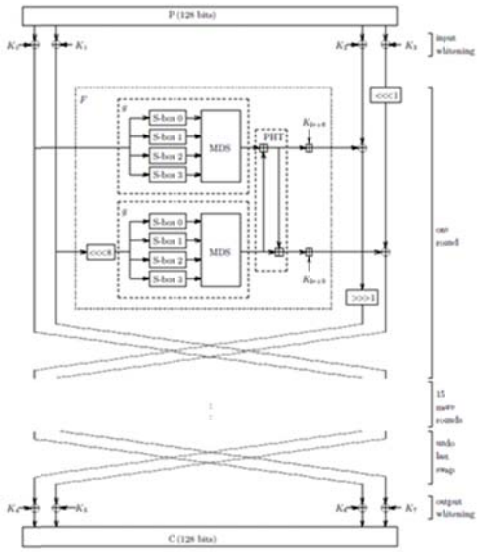
2.2. Chiper Block Chaining (CBC)

Dengan mode CBC, setiap blok *chiperteks* bergantung tidak hanya pada blok *plainteks*nya tetapi juga pada seluruh blok painteks sebelumnya. Keuntungan mode

CBC adalah karena blok-blok *plainteks* yang sama tidak menghasilkan blok-blok *chiperteks* yang sama sehingga kriptanalis menjadi lebih sulit [3]. Kelemahan pada CBC adalah karena blok *chiperteks* yang dihasilkan selama proses enkripsi bergantung pada blok-blok *chiperteks* sebelumnya, sehingga kesalahan satu bit pada sebuah blok *plainteks* akan merambat pada blok *chiperteks* yang berkoresponden dan semua blok *chiperteks* berikutnya. Keadaan ini berbeda halnya dengan dekripsi. Kesalahan satu bit pada blok *chiperteks* hanya mempengaruhi blok *plainteks* yang berkoresponden dan satu bit pada blok *plainteks* berikutnya (pada posisi bit yang berkoresponden pula).

2.3. Algoritma Twofish

Twofish merupakan algoritma yang beroperasi dalam mode blok. Perancangan Twofish dilakukan dengan memperhatikan kriteria-kriteria yang diajukan *National Institute of Standard and Technology* (NIST) untuk kompetisi *Advance Encryption Standart* (AES). Struktur Algoritma Twofish seperti gambar 1.



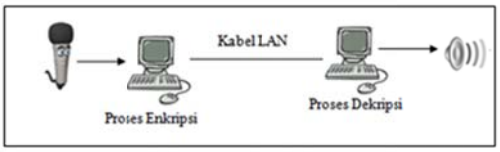
Gambar 1. Struktur Algoritma Twofish

Gambar 1 menunjukkan garis besar Algoritma Twofish. Twofish menggunakan 16 *round* struktur seperti Feitsel *Network*. *Plainteks* dibagi menjadi empat buah, masing-masing 32 bit words. Pada langkah *whitening* masukkan *plainteks* ini dilakukan XOR dengan 4 *words* kunci. Langkah ini dilanjutkan oleh enam belas *round* yang tiap *round*nya 2 *words* di kiri digunakan sebagai masukan untuk fungsi g. Langkah ini dilanjutkan dengan pencampuran linear berbasis matriks MDS. Hasil dari dua fungsi g dikombinasikan dengan menggunakan dengan menggunakan Transformasi Pseudo-Hadamard (PHT) dan 2 *keywords* ditambahkan. Dua hasilnya dilakukan XOR dengan *words* di sebelah kanan. Bagian kiri dan kanan lalu dipertukarkan untuk *round* berikutnya. Setelah semua *round* selesai dilakukan, pertukaran terakhir dikembalikan dan empat *words* tersebut dilakukan XOR dengan empat *keywords* untuk menghasilkan *chipertext*.

3. Analisis dan Perancangan

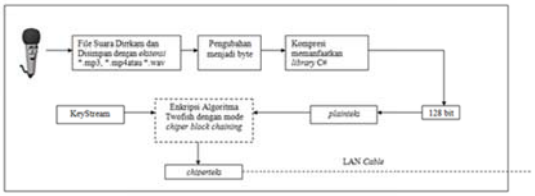
3.1. Deskripsi Umum Perangkat Lunak

File suara yang telah dienkripsi dikirimkan oleh *encryptor* dan diterima oleh *decryptor* dengan menggunakan kabel jaringan LAN. Gambar 2 menunjukkan arsitektur global sistem proses pengiriman dan penerimaan pesan suara.



Gambar 2. Arsitektur Global Sistem

Proses enkripsi pesan suara yang dilakukan dengan mengubah *file byte* dan pemasukan kunci pesan ditunjukkan dengan gambar 3.

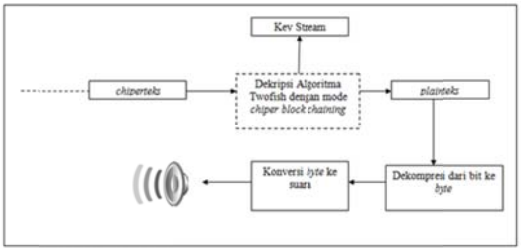


Gambar 3. Proses Enkripsi File Suara

Proses yang dilalui pada saat enkripsi yang ditunjukkan oleh gambar 3 adalah :

a) File direkam dan disimpan dengan ekstensi *.mp3, *.mp4 maupun *.wav
b) File suara dirubah menjadi *byte* dengan menggunakan fasilitas *library* C#
c) File suara yang telah dirubah menjadi *byte* dikompresi dengan menggunakan *library* C# menjadi 128 bit.
d) Plainteks 128 bit dienkripsi dengan menggunakan Algoritma Twofish dan KeyStream.
e) File berhasil dienkripsi dan dikirimkan ke komputer tujuan dengan menggunakan kabel jaringan LAN

Setelah berhasil dienkripsi, pesan suara dikirimkan oleh *encryptor* ke *decryptor* dengan menggunakan kabel jaringan LAN antara dua buah komputer. File yang telah diterima oleh *decryptor* akan didekripsi dengan menggunakan algoritma Twofish dengan kunci yang sama ketika dipakai untuk mengenkripsi. Untuk proses lebih jelas proses dekripsi dapat dilihat pada gambar 4.



Gambar 4. Proses Dekripsi File Suara

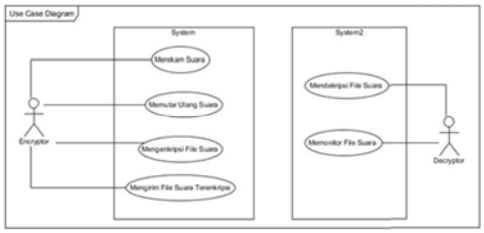
Proses pada saat dekripsi yang ditunjukkan oleh gambar 4 adalah :

a) *Chiperteks* didekripsi dengan menggunakan Algoritma Twofish juga dengan ekstraksi key stream
b) File suara berupa plainteks
c) Dekompresi dari bit ke *byte*, dari *byte* ke file suara kembali.
d) File suara berhasil didekripsi

3.2. Model *Use Case*

Model *use case* terdiri dari *actor* dan *use case*. Model *use case diagram* digunakan untuk menunjukkan hubungan antara *actor* dan *use case*. Diagram *use case* ini untuk sistem keamanan pengiriman pesan suara dengan enkripsi dan dekripsi menggunakan Algoritma Twofish yang mempunyai dua buah *actor* yakni *encryptor* dan *decryptor*.

Encryptor mempunyai empat buah *use case*, yakni merekam suara, memutar ulang suara, mengenkripsi file suara dan mengirim file suara terenkripsi, sedangkan pada *actor decryptor* mempunyai dua buah *use case* yakni mendekripsi file suara dan memonitor file.



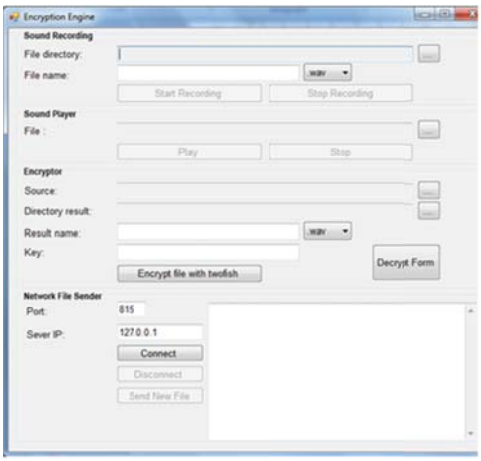
Gambar 5. Model *Use Case*

4. Implementasi dan Pengujian

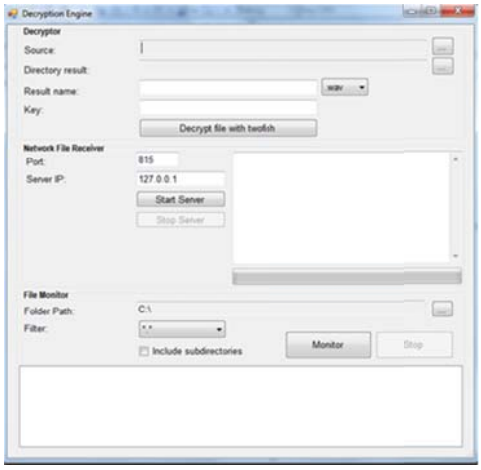
4.1. Implementasi Antarmuka

Aplikasi Keamanan Enkripsi dan Dekripsi Pengiriman Pesan Suara dengan Menggunakan Algoritma Twofish pada tugas akhir ini dibangun dengan bahasa pemrograman C# dengan menggunakan software Microsoft Visual Studi 2008. Implementasi perancangan antarmuka terbagi menjadi tiga bagian utama, yaitu implementasi rancangan layar home, implementasi rancangan layar encryption engine, implementasi rancangan layar decryption engine.

Gambar 6. Implementasi Home



Gambar 7. Implementasi Encryption Engine



Gambar 8. Implementasi Decryption Engine

4.2. Pengujian

Pengujian dilakukan dengen beberapa alat ukur diantaranya berdasarkan skenario normal, waktu, ekstensi file dan kunci. Pengujian berdasarkan beberapa parameter yang digunakan, dapat membuktikan bahwa enkripsi dan dekripsi pesan suara yang dilakukan berhasil juga perangkat lunak yang dihasilkan dapat dikatakan bagus karena tidak mengandung *delay* dan *error*.

5. Kesimpulan dan Saran

5.1. Kesimpulan

Kesimpulan yang dapat diambil dari penulisan tugas akhir ini adalah :

a. Aplikasi enkripsi dan dekripsi pengiriman pesan suara dengan menggunakan Algoritma Twofish dan proses tukar data dengan menggunakan Kabel Jaringan LAN telah berhasil dibangun.
b. Algoritma Twofish merupakan algoritma yang dapat diterapkan untuk melakukan enkripsi pesan suara dengan cukup baik. Kualitas suara setelah dienkripsi dan berhasil didekripsi tetap memiliki kualitas suara yang baik. Setelah dilakukan pengujian dari segi ukuran dan waktu tetap baik dan tidak mengalami perubahan, seperti ditunjukkan tabel 4.4 pada sub bab pengujian.
c. Pesan suara sebelum dienkripsi dan setelah didekripsi tidak mengalami perubahan waktu yang menunjukkan bahwa tidak terdapat delay dalam pesan suara

5.2. Saran

Saran yang diberikan penulis untuk pengembangan lebih lanjur adalah :

a. Kunci yang dapat digunakan dalam aplikasi enkripsi dan dekripsi pesan suara pada tugas akhir ini hanya 30 *character*, disebabkan karena terbatasnya perangkat keras yang digunakan.
b. Dalam pengembangan, diharapkan menambahkan *ekstensi file* agar terdapat beragam pilihan *file* suara.
c. Algoritma Twofish dapat digunakan untuk enkripsi dan dekripsi pesan suara secara *real time* dengan cara mengubah mode *chiper block* menjadi *chiper* aliran.

DAFTAR PUSTAKA

[1] Ariyus, Doni, 2006, *"Kriptografi Keamanan Data dan Komunikasi"*, Graha Ilmu, Yogyakarta.

[2] Ariyus, Doni, 2008, *"Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi"*, Andi, Yogyakarta.

[3] Munir, Rinaldi, 2007, *"Kriptografi"*, Informatika, Bandung.

[4] Vaudenay, Serge, 2006, *"A Classical Introduction to Cryptografy : Applications for Communications Security"*, Springer, New York.

[5] Dworkin, Morris, 2001, *"Recomendation for Block Chiper Modes of Operation"*

[6] Bruce Scheiner, et al, 1998, *"Twofish: a 128-Bit Block Chiper"*.

[7] Mukmin, Indra, diakses dari indormatia.stei.itb.ac.id/~rinaldi.../MakalahIF2153-0708-017.pdf, pada tanggal 30 Juni 2012, pukul 20.00 WIB.