SKRIPSI

ENKRIPSI TEKS MENGGUNAKAN ALGORITMA TWOFISH

JOVI TANATO

NPM: 2012730011

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI DAN SAINS
UNIVERSITAS KATOLIK PARAHYANGAN
2017

UNDERGRADUATE THESIS

TEXT ENCRYPTION USING THE TWOFISH ALGORITHM

JOVI TANATO

NPM: 2012730011

DEPARTMENT OF INFORMATICS
FACULTY OF INFORMATION TECHNOLOGY AND SCIENCES
PARAHYANGAN CATHOLIC UNIVERSITY
2017

LEMBAR PENGESAHAN

ENKRIPSI TEKS MENGGUNAKAN ALGORITMA TWOFISH

JOVI TANATO

NPM: 2012730011

Bandung, 19 Mei 2017

Menyetujui,

Pembimbing

Mariskha Tri Adithia, P.D.Eng

Ketua Tim Penguji

Pascal Alfadian, M.Comp.

Anggota Tim Penguji

Claudio Franciscus, M.T.

Mengetahui,

Ketua Program Studi

Mariskha Tri Adithia, P.D.Eng

PERNYATAAN

Dengan ini saya yang bertandatangan di bawah ini menyatakan bahwa skripsi dengan judul:

ENKRIPSI TEKS MENGGUNAKAN ALGORITMA TWOFISH

adalah benar-benar karya saya sendiri, dan saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika keilmuan yang berlaku dalam masyarakat keilmuan.

Atas pernyataan ini, saya siap menanggung segala risiko dan sanksi yang dijatuhkan kepada saya, apabila di kemudian hari ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya, atau jika ada tuntutan formal atau non-formal dari pihak lain berkaitan dengan keaslian karya saya ini.

Dinyatakan di Bandung,
Tanggal 19 Mei 2017

Jovi Tanato
NPM: 2012730011

ABSTRAK

Kriptografi berasal dari bahasa Yunani yang berarti tulisan rahasia. Kriptografi adalah pembelajaran dan penerapan teknik untuk menjamin komunikasi yang aman di lingkungan yang tidak aman. Tujuan keamanan dari kriptografi untuk mencari aspek-aspek kerahasiaan, integritas, dan otentikasi. Kriptografi untuk menjaga kerahasiaan data berupa proses enkripsi dan dekripsi. Enkripsi dan dekripsi dapat dilakukan melalui penyandian kunci simetris dan penyandian kunci asimetris, dimana penyandian kunci simetris memiliki satu kunci untuk enkripsi dan dekripsi sedangkan penyandian kunci asimetris memiliki kunci yang berbeda untuk enkripsi dan dekripsi. Algoritma untuk penyandian kunci asimetris seperti Rivest-Shamir-Adleman (RSA) dan Elliptic Curve Cryptography (ECC) dan untuk algoritma penyandian kunci simetris seperti Data Encrytion Standard (DES) dan Advanced Encryption Standard (AES). Pada skripsi ini algoritma yang akan dibahas adalah algoritma Twofish.

Algoritma Twofish adalah algoritma penyandian kunci simetris. Algoritma Twofish menggunakan *block cipher* yang berukuran 128 *bits* dengan kunci yang dipakai dapat memiliki panjang sampai 256 *bits*. *Block cipher* adalah sebuah kriptografi simetris yang mengenkripsi satu blok *plaintext* dengan panjang tertentu dan menghasilkan satu blok *ciphertext* dengan panjang yang sama. *Plaintext* adalah pesan atau informasi yang akan dienkripsi dan *ciphertext* adalah hasil dari proses enkripsi. Pada skripsi ini hanya akan dibahas untuk panjang kunci 128 *bits*.

Kata-kata kunci: kriptografi, kerahasiaan, integritas, otentikasi, enkripsi, dekripsi, kunci simetris, kunci asimetris, Twofish, block cipher, plaintext, ciphertext

ABSTRACT

Cryptography comes from Greek word mean secret writing. Cryptography can also be interpreted as an art to change the message so that it becomes more secure and resistant from attack. The security purpose of cryptography is to get the aspects of confidentiality, integrity and authentication. Cryptography to keep data confidential is the process of encryption and decryption. Encryption and decryption can be done by using symmetric key cryptography which has one key for both encryption and decryption while asymmetric key cryptography has 2 different keys for encryption and decryption. Algorithm for asymmetric key cryptography is such as Rivest-Shamir-Adleman (RSA) dan Elliptic Curve Cryptography (ECC) and algorithm for symmetric key cryptography is Data Encryption Standard (DES) and Advanced Encryption Standard (AES). In this thesis the algorithm to be discussed is Twofish algorithm.

Twofish algorithm is a symmetric key cryptography algorithm. Twofish algorithm use 128 bits block cipher with key up to 256 bits. Block cipher is symmetric cryptography that encrypts one block of a certain length of plaintext and produces a block of ciphertext of the same length. Plaintext is message or information to be encrypted and ciphertext is the result of the encryption process. In this thesis will only be discussed 128 bits key length

Keywords: cryptography, confidentiality, integrity, authentication, encryption, decryption, symmetric key, asymmetric key, Twofish, block cipher, plaintext, ciphertext

Dipersembahkan kepada keluarga tercinta, teman-teman, semua orang yang berperan dalam pembuatan skripsi ini, dan diri sendiri

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Tuhan atas karunia yang sudah diberikan kepada penulis sehingga tugas akhir yang berjudul Enkripsi Teks Menggunakan Algoritma Twofish dapat selesai pada waktunya. Selama proses pembuatan tugas akhir ini, penulis mengalami masalah dan halangan yang menghambat perkembangan studi. Namun, berbagai pihak membantu dan memberikan dukungan kepada penulis sehingga tugas akhir ini dapat diselesaikan dengan baik. Oleh karena itu, penulis hendak mengucapkan terima kasih kepada seluruh pihak yang berperan dalam pembuatan skripsi ini baik yang berperan langsung maupun yang tidak langsung. Secara khusus penulis ingin mengucapkan terima kasih kepada :

- Keluarga yang selalu memberikan dukungan kepada penulis berupa doa dan bimbingan moral.
- Ibu Mariskha Tri Adithia selaku pembimbing tugas akhir yang telah memberikan dukungan, bimbingan, dan arahan mengenai tugas akhir ini dengan sabar.
- Bapak Pascal Alfadian dan Bapak Claudio Fransiscus selaku penguji yang telah memberikan kritik dan saran yang membangun sehingga tugas akhir ini menjadi lebih baik.
- Pihak-pihak lainnya yang sudah berpartisipasi dalam skripsi ini.

Bandung, Mei 2017

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Kriptografi berasal dari bahasa Yunani yang berarti tulisan rahasia. Kriptografi adalah pembelajaran dan penerapan teknik untuk menjamin komunikasi yang aman di lingkungan yang tidak aman. Tujuan keamanan dari kriptografi untuk mencapai aspek-aspek kerahasiaan, integritas, dan otentikasi. Kerahasiaan yaitu menjaga kerahasiaan isi data dari orang yang tidak berhak. Integritas yaitu mencegah isi data diubah oleh orang yang tidak berhak. Otentikasi yaitu memastikan bahwa orang tersebut benar-benar dirinya sendiri. Kriptografi untuk menjaga kerahasiaan data yaitu berupa enkripsi dan dekripsi. Enkripsi adalah proses mengamankan data sehingga tidak dapat dimengerti oleh orang lain tanpa bantuan khusus. Dekripsi adalah proses mengembalikan data yang telah dienkripsi menjadi data aslinya sehingga dapat dimengerti. Dalam pengembangannya, enkripsi dan dekripsi memerlukan kunci rahasia sehingga terdiri dari penyandian kunci simetris dan penyandian kunci asimetris. Penyandian kunci simetris adalah penyandian dengan kunci yang sama untuk enkripsi dan dekripsi. Penyandian kunci asimetris adalah penyandian dengan kunci yang berbeda untuk enkripsi dan dekripsi, dimana kunci enkripsi dapat diketahui oleh publik dan kunci untuk dekripsi hanya boleh diketahui oleh penerima saja. Contoh algoritma kunci simetris adalah Data Encrytion Standard (DES), Advanced Encryption Standard (AES) dan Twofish. Contoh algoritma kunci asimetris adalah Rivest-Shamir-Adleman (RSA) dan Elliptic Curve Cryptography (ECC).

Twofish adalah algoritma kriptografi simetris yang menggunakan *block cipher* dengan panjang 128 *bit* yang dibuat oleh Bruce Scheiner. Algoritma Twofish memiliki 16 ronde jaringan Feistel. Di dalam jaringan Feistel terdapat tabel substitusi, transformasi Pseudo Hadamard, rotasi terhadap nilai-nilai bit. Algoritma Twofish dapat menerima 3 panjang kunci yaitu 128, 192 atau 256 *bit*.

Teks yang akan dienkripsi pertama akan diubah dulu menjadi nilai *integer* yang diambil dari tabel *American Standard Code for Information Interchange*(ASCII) sebelum dienkripsi. Dan hasil dari enkripsi akan diubah menjadi nilai heksadesimal.

1.2 Rumusan Masalah

Rumusan masalah dari penelitian ini adalah:

- Bagaimana cara kerja algoritma Twofish?
- Bagaimana cara mengimplementasikan algoritma Twofish untuk mengenkripsi teks?

1.3 Tujuan

Tujuan dari penelitian ini adalah:

- Mempelajari cara kerja algoritma Twofish.
- Membangun perangkat lunak dengan algoritma Twofish untuk mengenkripsi teks.

1.4 Batasan Masalah

Berikut adalah batasan masalah yang diterapkan dalam penelitian ini:

- Panjang kunci dan teks yang akan dienkripsi maksimal 16 *byte* atau 128 bit.
- Hasil yang telah dienkripsi dikonversi ke nilai heksadesimal.

1.5 Metodologi Penelitian

Berikut adalah tahap-tahap yang dilakukan dalam penelitian ini:

- Melakukan studi pustaka tentang algoritma Twofish.
- Melakukan perhitungan secara manual untuk enrkipsi dengan menggunakan algoritma Twofish.
- Membuat perancangan antarmuka dan diagram kelas perangkat lunak.
- Membangun perangkat lunak berdasarkan perancangan yang telah dibuat.
- Melakukan eksperimen terhadapat hasil perangkat lunak dengan hasil tes enkripsi secara manual.
- Menarik kesimpulan dari hasil enkripsi.

1.6 Sistematika Pembahasan

Pembahasan dalam dokumen ini dilakukan secara sistematis sebagai berikut:

- Bab 1 Pendahuluan
  Berisi latar belakang, rumusan masalah, tujuan, batasan masalah, metodologi penelitian, dan sistematika pembahasan.
- Bab 2 Dasar Teori
  Berisi teori-teori tentang kriptografi dan algoritma Twofish.
- Bab 3 Analis
  Berisi analisis pengerjaan secara manual algoritma Twofish dan perancangan perangkat lunak.
- Bab 4 Perancangan
  Berisi perencangan antarmuka dan diagram kelas lengkap.
- Bab 5 Implementasi dan Eksperimen
  Berisi implementasi antarmuka perangkat lunak, dan hasil eksperimen algoritma Twofish.
- Bab 6 Kesimpulan dan Saran
  Berisi kesimpulan dari awal hingga akhir penelitian dan saran untuk penelitian selanjutnya.