IMPLEMENTASI ALGORITMA KRIPTOGRAFI CAST-128 TERHADAP TEKS

SKRIPSI

Oleh:
HILMAN FUADY
0510960031-96

PROGRAM STUDI ILMU KOMPUTER
JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS BRAWIJAYA
MALANG
2012


UNIVERSITAS BRAWIJAYA

IMPLEMENTASI ALGORITMA KRIPTOGRAFI CAST-128 TERHADAP TEKS

Skripsi

Sebagai salah satu syarat untuk memperoleh gelar
Sarjana dalam bidang Ilmu Komputer

Oleh:
HILMAN FUADY
0510960031-96

PROGRAM STUDI ILMU KOMPUTER
JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS BRAWIJAYA
MALANG

2012


UNIVERSITAS BRAWIJAYA

LEMBAR PENGESAHAN

IMPLEMENTASI ALGORITMA KRIPTOGRAFI CAST-128 TERHADAP TEKS

Oleh:
HILMAN FUADY
0510960031-96

Setelah dipertahankan di depan Majelis Penguji
pada tanggal 13 Agustus 2012
dan dinyatakan memenuhi syarat untuk memperoleh gelar
Sarjana dalam bidang ilmu komputer

Pembimbing I	Pembimbing II
Drs. Marji, M.T.	**Nurul Hidayat, S.Pd, M.Sc.**
NIP : 196708011992031001	**NIP : 196804302002121001**

Mengetahui,
Ketua jurusan matematika
Fakultas MIPA Universitas Brawijaya

Dr. Abdul Rouf Alghofari, M.Sc.
NIP : 196709071992031001


UNIVERSITAS BRAWIJAYA

LEMBAR PERNYATAAN

Saya yang bertandangan di bawah ini :

Nama	: Hilman Fuady
NIM	: 0510960031
Jurusan	: Matematika
Penulis Tugas Akhir Berjudul	: Implementasi Algoritma Kriptografi CAST-128 terhadap Teks

Dengan ini menyatakan bahwa :

1. Isi dai skripsi yang saya buat adalah benar-benar karya sendiri dan tidak menjiplak karya orang lain. Selain nama-nama yang termaktub di isi dan tertulis di daftar pustaka di skripsi ini.
2. Apabila di kemudian hari ternyata skripsi yang saya tulis terbukti hasil jiplakan, maka saya akan bersedia menanggung segala resiko yang akan saya terima.

   Demikian pernyataan ini dibuat dengan segala kesadaran

Malang, 13 Agustus 2012
Yang menyatakan,

Hilman Fuady
NIM : 0510960031

IMPLEMENTASI ALGORITMA KRIPTOGRAFI CAST-128 TERHADAP TEKS

ABSTRAK

Kriptografi adalah suatu ilmu untuk menyamarkan atau mengacak data dengan metode-metode tertentu, dalam kriptografi terdapat 2 proses yaitu enkripsi dan dekripsi. Enkripsi adalah suatu proses untuk menyamarkan atau mengacak suatu pesan yang masih asli (*plaintext*) menjadi pesan yang sudah teracak (*chipertext*). Salah satu algoritma yang terkenal adalah algoritma kriptografi *CAST-128* yang diciptakan oleh Carlisle Adams dan Stafford Adams pada tahun 1996. *CAST-128* memanfaatkan jaringan *feistel* 16 kali putaran, 64-bit blok teks-asli dibagi menjadi dua bagian yang sama yaitu bagian kiri dan bagian kanan dengan panjang yang sama dengan panjang 32bit, 8x32 entri *S-Box* dan masukan sebuah kunci dengan panjang sampai 128-bit. Terdapat tiga proses dalam *CAST-128* yaitu pembentukan *key* dimana nantinya akan dihasilkan 16 kunci masking dan 16 kunci rotasi yang baru kemudian proses enkripsi dan dekripsi yang memiliki jumlah putaran sebanyak 16. Operasi-operasi yang terdapat diantaranya yaitu XOR, penambahan dan subtitusi S-box.

Pada penelitian ini akan diimplementasikan perangkat lunak dengan menggunakan algoritma *CAST-128* untuk mengetahui kemampuan algoritma *CAST-128* mengenkripsi dan mendekripsi *file* teks. Selain itu juga akan dilakukan analisis terhadap waktu proses dan nilai *avalanche effect*. Nilai *avalanche effect* adalah suatu nilai untuk mengetahui ketahanan algoritma *CAST-128* terhadap serangan.

Dari analisis yang dilakukan di dapatkan waktu proses enkripsi untuk ukuran *file* 50KB rata-rata waktu enkripsi adalah sebesar 0,807s, untuk ukuran *file* 500KB rata-rata waktu enkripsi adalah sebesar 7,662s kemudian rata-rata waktu dekripsi untuk ukuran *file* 50KB adalah sebesar 0,794s, untuk ukuran *file* 500KB adalah sebesar 8,451s. Untuk nilai rata-rata *avalanche effect* yang ideal (45-60%) didapatkan pada pengujian terhadap perubahan *key* yaitu sebesar 50,12% pada perubahan *byte* dan 49,79% pada perubahan bit.

IMPLEMENTATION ALGORITHM CRYPTOGRAPHY CAST-128 TO TEXT

ABSTRACT

Cryptography is the practice and study of hiding data with certain methods. There are two methods for hiding the data, which are encryption and decryption. Encryption is the method of changing the data from plaintext to an unintelligible format (chipertext). CAST-128, which was invented by Carlisle Adams dan Stafford Adams at 1996, is one of the known algorithm for doing such purpose CAST-128 utilize 16 round Feistel network, 64-bit block of the original text is divided into two equal parts, namely the left and the right of equal length to the length 32bit, 8x32 S-Box entry and input key with a length up to 128 -bit. There are three processes in CAST-128, key schedulling which will be produced 16 rotation key and 16 masking key and then process the encryption and decryption with the round of 16. Operations that are among the XOR, addition and substitution of the S-box.

In this research, the algorithm was implemented on a software to know the CAST-128's ability to encrypt and decrypt text files. The results were also be measured based on the time taken to do the process and the value of avalanche effect. The value of avalanche effect is used to measure the defencive ability of CAST-128 to withstand attack.

Based on the anaysis, the time taken to encrypt 50kb files was in average 0,807s. For files with a size of 500kb, the average time was 7,662s. Meanwhile the decryption time taken for decrypting 50kb and 500 files were 0,794s and 8,451s respectively. The ideal avalanche effect's value (45-60%), was 50,12% for a change in the 1 byte key and 49,79% for 1 bit key.

KATA PENGANTAR

Dengan mengucapkan puji syukur kehadirat Tuhan Yang Maha Esa, atas segala rahmat dan karunia-Nya, penulis menyelesaikan skripsi dengan judul : ”IMPLEMENTASI ALGORITMA KRIPTOGRAFI CAST-128 TERHADAP TEKS”.

Penelitian ini ingin mengetahui kemampuan algoritma *CAST-128* dalam melakukan enkripsi dan dekripsi *file* teks dan juga untuk menguji waktu proses dan ketahanan algoritma tersebut.

Mulai perencanaan sampai penyelesaian skripsi ini, penulis telah banyak mendapat bantuan dari berbagai pihak, oleh karena itu dalam kesempatan ini penulis ingin mengucap banyak terimakasih kepada pihak-pihak sebagai berikut :

1. Drs. Marji, M.T, dan Nurul Hidayat S.Pd, M.Sc, selaku pembimbing skripsi yang telah sabar memberi bimbingan dan petunjuk, sehingga skripsi ini bisa terselesaikan.
2. Dr. Abdul Rouf Alghofari, M.Sc, selaku Ketua Jurusan Matematika Fakultas Matematika Dan Ilmu Pengetahuan Alam.
3. Drs. Marji, MT., selaku Ketua Program Studi Ilmu Komputer Jurusan Matematika.
4. Bondan Sapta Prakoso, ST, selaku pembimbing akademik yang telah sabar memberi bimbingan dan petunjuk selama masa studi.
5. Bapak ibu dosen Program Studi Ilmu Komputer Jurusan Matematika yang telah banyak memberikan ilmunya.
6. Para staf TU Jurusan Matematika yang telah banyak membantu segala macam urusan administrasi dan perlengkapan.
7. Dika, Rohmat, Adam, Werdha, Martheen, Nanang dan semua teman-teman di Prodi Ilmu Komputer yang telah memberikan banyak bantuan, masukan dan motivasi.
8. Humairah Fauziah yang terus menerus memberikan semangat untuk menyelesaikan skripsi ini.
9. Bapak dan Ibu orang tua yang telah memberikan dorongan dan doa restu, baik moral maupun material selama penulis menuntut ilmu.
10. Dan semua pihak yang telah membantu dalam pengerjaan skripsi ini yang tidak bisa penulis sebutkan satu persatu.

Semoga Tuhan Yang Maha Esa senantiasa memberikan Rahmat dan Karunia-Nya kepada semua pihak yang telah memberikan segala bantuan tersebut di atas. Skripsi ini tentu saja masih jauh dari sempurna, sehingga penulis dengan senang hati menerima kritik demi perbaikan. Kepada peneliti lain mungkin masih bisa mengembangkan hasil penelitian ini. Akhirnya semoga skripsi ini ada manfaatnya.

Malang, 30 Juli 2012

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR GRAFIK

DAFTAR SOURCECODE

UNIVERSITAS BRAWIJAYA


UNIVERSITAS BRAWIJAYA