PENGANTAR

Alhamdulillah, puji dan syukur penulis panjatkan kepada Allah SWT, karena atas segala petunjuk dan nikmat-Nya lah skripsi ini dapat diselesaikan.

Skripsi berjudul "Pengembangan Algoritma Enkripsi Dekripsi Berbasis LFSR menggunakan Polinomial Primitif" ini disusun untuk memenuhi sebagian persyaratan memperoleh gelar Sarjana Teknik di Jurusan Teknik Elektro Universitas Brawijaya.

Penulis menyadari bahwa dalam penyusunan skripsi ini tidak terlepas dari bantuan berbagai pihak. Oleh karena itu, dengan ketulusan dan kerendahan hati penulis menyampaikan terima kasih kepada:

- Ayah dan Ibu atas segala nasehat, kasih sayang, perhatian dan kesabarannya didalam membesarkan dan mendidik penulis, serta telah banyak mendoakan kelancaran penulis hingga terselesaikannya skripsi ini,
- Kakak kakakku Mas dan Mbakku atas motivasi dan doanya,
- Paman saya Om Dewo dan Tante Yun yang senantiasa memberi dukungan dan percaya bahwa saya adalah anak laki laki yang sanggup berjalan dengan kaki saya sendiri.
- Bapak Dr. Ir. Sholeh Hadi Pramono., MS selaku Ketua Jurusan Teknik Elektro Universitas Brawijaya dan Bapak M. Aziz Muslim, ST., MT., Ph.D selaku Sekretaris Jurusan Teknik Elektro Universitas Brawijaya, serta Bapak Waru Djuriatno ST.,MT. selaku Ketua Kelompok Dosen Keahlian Rekayasa Komputer Jurusan Teknik Elektro Universitas Brawijaya,
- Bapak (Alm.) Dr. Agung Darmawansyah ST,MT. yang telah menasehati saya agar menjadi anak laki laki yang pantang menyerah dalam menggapai masa depan. Saya berjanji saya tidak akan pernah berhenti tersenyum di hadapan semua orang seberat apapun cobaan yang saya hadapi seperti yang telah Bapak nasehatkan kepada saya,
- Bapak Waru Djuriatno ST.,MT. selaku Dosen Pembimbing I atas bimbingannya selama saya menyusun skripsi, serta ajaran yang bapak

berikan kepada saya sebelum saya meninggalkan kampus elektro. Terima kasih karena telah mengajarkan saya cara untuk berusaha, berjuang, dan pantang menyerah. Saya tidak akan menyerah menggapai masa depan untuk membuktikan bahwa murid murid Bapak, anak anak zaman sekarang, bukanlah anak anak yang mengecewakan, melainkan adalah anak anak yang membanggakan.

- Bapak Adharul Muttaqin,ST.,MT. selaku Dosen Pembimbing II atas segala bimbingan, ide, nasehat, arahan, motivasi, saran, masukan yang telah diberikan selama penyusunan skripsi ini, dan atas kesabarannya selama saya belajar di kampus elektro ini,
- Mas Alan , Mas Steven, Mas Irfan, mereka adalah kakak kakak saya yang saya sayangi. Mereka senantiasamenemani saya dan tidak pernah marah meskipun tingkah laku saya sering merepotkan mereka.
- Teman teman saya angkatan 2007, yang mau menerima dan memahami apa yang saya rasakan. Terima kasih atas kebersamaannya selama ini.
- Pada akhirnya, seluruh keluarga besar Jurusan Teknik Elektro yang tidak sanggup saya sebutkan satu persatu. Terima kasih atas kehangatan yang kalian berikan kepada saya selama ini. Saya bahagia bisa menjadi bagian dari diri kalian.

Penulis menyadari bahwa skripsi ini masih belum sempurna. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun. Penulis berharap semoga skripsi ini dapat bermanfaat bagi pengembangan ilmu pengetahuan dan teknologi serta bagi masyarakat.

Malang, 04 Desember 2012

Penulis

repository.ub.ac.id

ABSTRAK

Anggun Triyogo, Jurusan Teknik Elektro Fakultas Teknik Universitas Brawijaya, Desember 2012, *Pengembangan Algoritma Enkripsi Dekripsi Berbasis LFSR Menggunakan Polinomial Primitif*, Dosen Pembimbing : Waru Djuriatno,ST.,MT. dan Adharul Muttaqin, ST.,MT.

Stream cipher adalah salah satu metode kriptografi modern yang populer karena di samping prosesnya yang memakan waktu lebih singkat, *stream cipher* juga menggunakan memori yang lebih sedikit. *Stream cipher*bekerja dengan melakukan operasi XOR antara data dengan bilangan acak. LFSR (*Linear Feedback Shift Register*) adalah salah satu jenis generator yang dapat menghasilkan bit semu acak. LFSR sering digunakan karena mampu menghasilkan bit semu acak dengan periode maksimal yang panjang dan mudah diaplikasikan dalam berbagai hal. Namun seiring dengan perkembangan zaman penggunaan sebuah LFSR sebagai generator bit semu acak rawan terhadap serangan kriptanalisis. Skripsi ini mencoba menerapkan metode *multi register* yang dapat mebuat bilangan semu acak lebih tahan terhadap serangan kriptanalisis.

Untuk menerapkan metode tersebut dibuat sebuah sistem multipleksing 3 buah LFSR, dimana keluaran dari generator LFSR pertama dan kedua berfungsi sebagai masukan multiplekser dan keluaran dari generator nomor tiga berfungsi sebagai fungsi select dari multiplekser.

Hasil pengujian menunjukkan bahwa multipleksing LFSR mampu melakukan proses enkripsi dekripsi denngan baik, bilangan semu acak yang dihasilkan oleh multipleksing generator lebih tahan terhadap kriptanalisis dibandingkan single LFSR, dan secara statistik nilai keacakan bilangan semu acak yang dihasilkan multipleksing generator tidak berbeda jauh dengan nilai statistik bilangan semu acak single LFSR. Dari beberapa kali proses pengujian statistik didapatkan nilai rata rata entropi 7.98155, arithmatic mean 127.441, dan serial coefficient correlation sebesar 0.07

Kata kunci :*Stream cipher, Linear Feedbak Shift Register*,multipleksing, uji statistik.

UNIVERSITAS BRAWIJAYA

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL