DAFTAR ISI

LEMBAR JUDUL

LEMBAR PENGESAHAN

ABSTRAKSI

ABSTRACT

KATA PENGANTAR i

DAFTAR ISI iv

DAFTAR TABEL viii

DAFTAR GAMBAR x

DAFTAR SIMBOL xiii

DAFTAR LAMPIRAN xv

BAB I PENDAHULUAN 1

1.1 Latar Belakang 1

1.2 Identifikasi Masalah 2

1.3 Maksud dan Tujuan 3

1.4 Batasan Masalah 3

1.5 Metodologi Penelitian 4

1.6 Sistematika Penulisan 7

BAB II LANDASAN TEORI 8

2.1 Pengertian Simulasi 8

2.2 Pengacakan (Randomize) 9

2.3. Bilangan Acak 11

2.3.1. Pembangkit Bilangan Acak (Random Number Generator) 11

2.3.2 Pembangkit Bilangan Acak Semu (Pseudo Random Number Generator) 12

2.3.3 Algoritma Pembangkit Bilangan Acak Semu 12

2.3.3.1 Linear Congruential Generator (LCG) 13

2.3.3.2 Non Linear Feedback Shift Register (NLFSR). 14
2.3.3.3 ISAAC 15
2.3.3.4 Lagged Fibonacci Generator (LFG) 15
2.3.3.5 Mersenne Twister 16
2.3.3.6 Fortuna 18
2.3.3.7 Blum-Blum Shub (BBS) 18
2.4. Linear Feedback Shift Register (LFSR) 18
2.4.1 Geffe Generator 22
2.4.2 Jennings Generator 23
2.4.3 Threshold Generator 24
2.4.4 Multispeed Inner-Product Generator 25
2.4.5 Gollmann Cascade Generator 26
2.4.6 Beth-Piper Stop-and-Go Generator 27
2.4.7 Alternating Stop-and-Go Generator 28
2.4.8 Bilateral Stop-and-Go Generator 29
2.4.9 Self-Decimated Generators 30
2.5 Operator Logika 31
2.5.1 Operasi NOT 31
2.5.2 Operasi AND 32
2.5.3 Operasi OR 33
2.5.4 Operasi XOR 35
2.6 Landasan Matematis Kriptografi 36
2.6.1 Pergeseran Bit (Shift) 36
2.6.2 Rotasi Bit (Rotate) 37
2.7 Stream Cipher 38
2.8 Perangkat Lunak Pembelajaran 39
2.9 Pemograman Visual Basic 40
2.9.1 IDE Visual Basic 40
2.9.2 Jendela IDE pada Visul Basic 41

BAB III ANALISIS DAN PERANCANGAN..... 42

3.1 Deskripsi Masalah 42
3.2 Analisis Masalah 43
3.2.1 Metode Beth – Piper-Step Go 43
3.2.2 Proses Simulasi Pembangkit Bilangan Acak Beth Piper Step Go 46
3.2.3 Pembahasan Proses Perhitungan dan Pembangkitan Bilangan Acak 47
3.3 Analisis Kebutuhan Non Fungsional 54
3.3.1 Kebutuhan Hardware 54
3.3.2 Kebutuhan Software 54
3.3.3 Kebutuhan User 55
3.4 Perancangan Sistem 55
3.4.1 Perancangan Fungsional 56
3.4.1.1 Diagram Context 56
3.4.1.2 Data Flow Diagram (DFD) 57
3.4.1.3 Spesifikasi Proses 61
3.4.2 Perancangan Prosedural 64
3.4.2.1 Perancangan Proses Simulasi Beth Piper Step Go Generator 64
3.4.2.2 Perancangan Proses Penentuan Nilai Awal LFSR 66
3.4.2.3 Perancangan Proses Penentuan posisi bit Feedback 67
3.4.2.4 Perancangan Proses Perhitungan Bilangan Acak 69
3.5 Perancangan Antar Muka 71
3.5.1 Struktur Menu Program 71
3.5.2 Perancangan Tampilan Form 72
3.5.2.1 Form Menu Utama 72
3.5.2.2 Form Input 73
3.5.2.3 Perancangan Form Prosedur Kerja 75

3.5.2.4 Perancangan Form Hasil Output 76
3.5.2.5 Perancangan Form Detail Proses 77

BAB IV IMPLEMENTASI DAN PENGUJIAN 79
4.1 Implementasi 79
4.1.1 Kebutuhan Perangkat Keras 79
4.1.2 Kebutuhan Perangkat Lunak 80
4.1.3 Implementasi Antarmuka 80
4.2 Pengujian 86
4.2.1 Rencana Pengujian 86
4.2.2 Kasus dan Hasil Pengujian 87
4.2.3 Kesimpulan Hasil Pengujian Alpha 90
4.3 Pengujian Untuk Pembangkitan Bilangan Acak 91
4.3.1 Kesimpulan Pengujian Pembangkitan Bilangan Acak 115

BAB V KESIMPULAN DAN SARAN 117
5.1 Kesimpulan 117
5.2 Saran 118

DAFTAR PUSTAKA 119