DAFTAR ISI

LEMBAR JUDUL

LEMBAR PENGESAHAN

ABSTRAK ---------- i

ABSTRACK ---------- ii

KATA PENGANTAR ---------- iii

DAFTAR ISI ---------- v

DAFTAR TABEL ---------- xi

DAFTAR GAMBAR ---------- xii

DAFTAR SIMBOL ---------- xiv

DAFTAR LAMPIRAN ---------- xvii

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 ---------- 5

BAB II TINJAUAN PUSTAKA ---------- 7

2.1 Algoritma ---------- 7

2.2 Kriptografi ---------- 7

2.3 Algoritma kriptografi ---------- 8

2.4 Serangan terhadap kriptografi ---------- 11

2.4.1 Kriptanalisis ---- 11
2.4.2 Keamanan algoritma kriptografi ---- 12
2.4.3 Kompleksitas serangan ---- 13
2.4.3.1 Kompleksitas data ---- 13
2.4.3.2 Kompleksitas waktu ---- 13
2.4.3.3 Kompleksitas ruang memory ---- 13
2.4.4 Jenis – jenis serangan ---- 13
2.4.4.1 Berdasarkan keterlibatan penyerang dalam komunikasi ---- 13
2.4.4.2 Berdasarkan banyaknya inforamsi yang diketahui oleh kriptanalis ---- 15
2.4.4.3 Berdasarkan teknik yang digunakan dalam menemukan kunci ---- 18
2.5 Kriptografi kunci – publik ---- 19
2.6 Konsep kriptografi kunci – publik ---- 20
2.6.1 Kelebihan kriptografi kunci-publik (asimetri) ---- 23
2.6.2 Kekurangan kriptografi kunci-publik (asimetri) ---- 24
2.7 Kriptografi ElGamal ---- 24
2.8 Proses pembentukan kunci ---- 25
2.9 Enkripsi ---- 27
2.9.1 Algoritma enkripsi ---- 28
2.10 Dekripsi ---- 28
2.10.1 Algoritma dekripsi ---- 29
2.11 Flowchart pembentukan kunci, enkripsi dan dekripsi ---- 31

2.12 Metode *Fast Exponentiation* 32
2.12.1 Contoh perhitungan pangkat dengan *Fast Exponentiation* 32
2.12.2 Algoritma *Fast Exponentiation* 33
2.13 Bilangan acak semu *PRNG* (*pseudorandom number generator*) 34
2.13.1 Perancangan *CSPRNG* berbasis teori bilangan 35
2.13.2 Algoritma *CSPRNG* berbasis RSA 35
2.14 Pembagi persekutuan terbesar 36
2.14.1 Algoritma Euclide 37
2.15 Luhn 37
2.15.1 Analisis algoritma Luhn 38
2.15.2 Langkah pembuatan digit Luhn 38
2.15.3 Langkah pengecekan digit Luhn 39
BAB III ANALISIS DAN PERANCANGAN 40
3.1 Analisis sistem 40
3.1.1 Analisis kebutuhan non-fungsional 40
3.1.1.1 Analisis kebutuhan perangkat keras 41
3.1.1.2 Analisis kebutuhan perangkat lunak 42
3.1.2 Analisis kebutuhan fungsional 42
3.1.2.1 *Use Case Diagram* 42
3.2.2.1.1 Autentikasi admin 43
3.2.2.1.2 Koneksi kartu 44
3.2.2.1.3 Diskoneksi kartu 45
3.2.2.1.4 Masukan data baru 46

3.2.2.1.5 Baca data ---- 47
3.2.2.1.6 Gandakan kartu ---- 48
3.2.2.1.7 Cek sekurity kartu ---- 49
3.2.2.1.8 Securing card ---- 50
3.1.2.2 *Sequence Diagram* ---- 51
3.1.2.2.1 Autentikasi admin ---- 51
3.1.2.2.2 Koneksi kartu ---- 52
3.1.2.2.3 Diskoneksi kartu ---- 54
3.1.2.2.4 Masukan data baru ---- 54
3.1.2.2.5 Baca data ---- 56
3.1.2.2.6 Gandakan kartu ---- 57
3.1.2.2.7 Cek security kartu ---- 59
3.1.2.2.8 Securing card ---- 60
3.1.2.3 *Class Diagram* ---- 61
3.1.2.4 Spesifikasi kelas ---- 62
3.1.2.4.1 Kelas ReaderKartu ---- 62
3.1.2.4.2 Kelas OperasiFile ---- 63
3.1.2.4.3 Kelas Kartu ---- 65
3.1.2.4.4 Kelas FastExponentiaion ---- 67
3.1.2.4.5 Kelas ElGamal ---- 68
3.1.2.4.6 Kelas Enkripsi ---- 70
3.1.2.4.7 Kelas Dekripsi ---- 71
3.1.2.4.8 Kelas CSPRNG RSA ---- 72
3.1.2.4.9 Kelas Luhn ---- 72

3.1.2.4.10 Kelas FormUtama ---- 73
3.2 Perancangan antarmuka sistem ---- 75
3.2.1 Autentikasi ---- 78
3.2.2 Menu Utama ---- 79
3.2.3 Masukan Data Baru ---- 80
3.2.4 Cek Security Kartu ---- 82
3.2.5 Gandakan Kartu ---- 84
3.2.6 Tentang ---- 85
BAB VI IMPLEMENTASI DAN PENGUJIAN ---- 86
4.1 Implementasi sistem ---- 86
4.1.1 Lingkungan implementasi ---- 86
4.1.1.1 Perangkat keras yang digunakan ---- 86
4.1.1.2 Perangkat lunak yang digunakan ---- 87
4.1.2 Batasan implemantasi ---- 87
4.1.3 Implemenatsi program ---- 88
4.1.3.1 Implementasi kriptografi ElGamal ---- 88
4.1.3.2 Implementasi sistem ---- 89
4.1.3.2.1 Antarmuka autentikasi ---- 89
4.1.3.2.2 Antarmuka menu utama ---- 90
4.1.3.2.3 Masukan data baru ---- 92
4.1.3.2.4 Securing Card ---- 97
4.1.3.2.5 Gandakan kartu ---- 99
4.1.3.2.6 Cek security kartu ---- 101
4.1.3.2.7 Tentang ---- 104

4.2 Pengujian sistem ---- 104
4.2.1 Metode pengujian ---- 104
4.2.2 Rencana pengujian ---- 105
4.2.3 Pengujian ---- 106
4.2.3.1 Pengujian Autentikasi ---- 106
4.2.3.2 Pengujian Masukan Data Baru ---- 107
4.2.3.3 Pengujian Cek Security Kartu ---- 108
4.2.3.4 Pengujian Gandakan Kartu ---- 108
4.2.4 Pengujian menguunakan *Software Scripting Tool* ---- 109
4.2.5 Kesimpulan Hasil Pengujian ---- 113
BAB V KESIMPULAN DAN SARAN ---- 114
5.1 Kesimpulan ---- 114
5.2 Saran ---- 114
DAFTAR PUSTAKA ---- 116