DAFTAR ISI

LEMBAR JUDUL

LEMBAR PENGESAHAN

LEMBAR PERNYATAAN

LEMBAR PERSEMBAHAN

ABSTRAK

ABSTRACT

KATA PENGANTAR……..…..……..i

DAFTAR ISI…….……iv

DAFTAR GAMBAR……...…...v

DAFTAR TABEL ……...…...…xvii

DAFTAR SIMBOL……...xviii

DAFTAR LAMPIRAN……xx

BAB I PENDAHULUAN

1.1 Latar Belakang Masalah……..…….1

1.2 Identifikasi Masalah……....…….....3

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

2.1 Algoritma…….....…….9

2.1.1 Algoritma Kriptografi……..….10

2.1.1.1 Mengenal Algoritma RC4……..…14

2.1.1.2 Sejarah Algoritma RC4…….....14

2.1.1.3 Uraian Algoritma RC4……...……15

2.1.1.4 Algoritma mengatur jadwal-kunci (KSA)……..17

2.1.1.5 Algoritma generasi pura-pura-acak (PRGA)……..18

2.1.1.6 Implementasi……..19

2.1.2 Algoritma SHA…….22

2.1.2.1 Sejarah Algoritma SHA……...……..24

2.1.2.2 Uraian Algoritma SHA-256……...……24

2.1.2.3 Deskripsi Algoritma SHA-256…….……..25

2.1.2.4 Pengujian Algoritma SHA-256……..27

2.1.2.5 Implementasi …….27

2.1.2.6 Perbandingan SHA-256 Dengan Algoritma Hash Lainnya…….……..30

2.2 *USB Flash Drives*……31

2.2.1 Teknologi *Usb Flash Drive*……..33

2.2.2 Sejarah *Usb Flash Drive*……..…….*35*

2.2.2.1 Generasi Pertama dan Pemasaran……..35

2.2.2.2 Generasi Kedua……..38

2.2.3 Desain dan Implementasi…….……39

2.2.3.1 Komponen-Komponen Penting…….……39

2.2.3.2 Ukuran dan Bentuk …….……..41

2.2.3.3 *File System*…….……42

2.2.4 Penggunaan Umum……..…….42

2.2.5 Keuntungan dan Kerugian *Flash Drive*…….....…….43

2.3 Bahasa Pemograman……45

2.3.1 Sejarah Delphi……..…….……45

2.3.2 Mengenal Delphi…….…….…46

2.3.2.1 Mengenal IDE Delphi…….....……...47

2.3.2.2 Struktur Program Delphi……48

2.4 Sistem……..52

2.4.1 Diagram Konteks…….54

2.4.2 Diagram Aliran Data……55

2.4.3 Kamus Data……..57

2.5 Microsoft Access XP……..58

BAB III ANALISIS DAN PERANCANGAN

3.1 Deskripsi Masalah.....59

3.2 Analisis Sistem.....60

3.2.1 Analisis Masalah dengan Menggunakan Algoritma RC4....60

3.2.1.1 Enkripsi dan Dekripsi RC4.....61

3.2.1.2 Permasalahan RC4 Stream Chiper.....63

3.2.1.3 Pemecahan Masalah.....64

3.2.1.4 Pengembangan RC4 Stream Cipher.....65

3.2.1.5 Implementasi.....65

3.2.2 Analisis Masalah dengan Menggunakan Algoritma SHA-256 67
3.2.2.1 Parameter.....68
3.2.2.2 Symbol.....69
3.2.2.3 Notasi dan Ketentuan.....69
3.2.2.3.1 Bit String dan Integer.....70
3.2.2.3.2 Operasi Pada Kata.....71
3.2.2.4 Fungsi SHA-256.....72
3.2.2.5 Harga Tetap Algoritma SHA-256.....72
3.2.2.6 Sebelum Proses algoritma SHA-256.....73
3.2.2.6.1 Penambahan Bit.....73
3.2.2.6.2 Uraian Penambahan Pesan.....74
3.2.2.6.3 Pengaturan Nilai Awal Hash.....74
3.2.2.7 Komputasi Hash SHA-256.....74
3.2.2.8 Implementasi.....76
3.2.2.9 Pengujian Algoritma SHA-256.....82
3.2.2.10 Digest Bukan Enkripsi.....83
3.3 Analisis Kebutuhan Sistem.....83
3.3.1 Analisis Kebutuhan User.....84
3.3.2 Analisis Kebutuhan Perangkat Keras.....84
3.3.3 Analisis Kebutuhan Perangkat Lunak.....85
3.4 Perancangan Fungsional.....85
3.4.1 Diagram Konteks.....86

3.4.2 Data Flow Diagram (DFD).....87

3.4.3 Spesifikasi Proses.....93

3.4.3.1 Kamus Data (Data Dictionary).....97

3.4.4 Entity Relationship Diagram.....101

3.5 Struktur Menu.....102

3.6 Perancangan Antarmuka.....104

BAB IV IMPLEMENTASI DAN PENGUJIAN

4.1 Implementasi.....119

4.1.1 Kebutuhan Perangkat Keras.....120

4.1.2 Kebutuhan Perangkat Lunak 120

4.1.3 Implementasi Database.....121

4.1.4 Implementasi Antarmuka.....125

4.1.4.1 Tampilan Antarmuka Authentication : Login.....126

4.1.4.2 Tampilan Antarmuka Ubah Password.....126

4.1.4.3 Tampilan Antarmuka Menu Utama.....127

4.1.4.4 Tampilan Antamuka Set USB Token.....130

4.1.4.5 Tampilan Antarmuka Lock.....132

4.1.4.6 Tampilan Antarmuka Unlock.....134

4.1.4.7 Tampilan Antarmuka Result.....135

4.1.4.8 Tampilan Antarmuka Aplication Help.....136

4.1.4.9 Tampilan Antarmuka About.....137

4.2 Pengujian.....138

4.2.1 Rencana pengujian.....138

4.2.2 Pengujian Alpha.....139

4.2.2.1 Pengujian set USB token.....140

4.2.2.2 Pengujian Lock.....147

4.2.2.3 Pengujian Unlock.....161

4.2.3 Analisa Hasil Pengujian.....169

BAB V KESIMPULAN DAN SARAN

5.1 Kesimpulan.....171

5.2 Saran.....172

DAFTAR PUSTAKA……173