DAFTAR ISI

ABSTRAK

ABSTRACT

KATA PENGANTAR i

DAFTAR ISI iv

DAFTAR GAMBAR vii

DAFTAR TABEL ix

DAFTAR SIMBOL x

DAFTAR LAMPIRAN…….. xi

BAB I PENDAHULUAN

1.1 Latar Belakang 1

1.2 Identifikasi Masalah 2

1.3 Maksud dan Tujuan 2

1.4 Batasan Masalah 3

1.5 Metodologi Penelitian 4

BAB II LANDASAN TEORI

2.1 Pengenalan Kriptografi 5

2.1.1 Sejarah Kriptografi..... 5

2.1.2 Definisi Kriptografi..... 8

2.1.3 Tujuan Kriptografi..... 10

2.2 Jenis Sistem Kriptografi..... 11

2.2.1 Kriptografi Kunci Rahasia..... 12

2.2.2 Kriptografi Kunci Public..... 29

2.3 Cryptanalysis. 30

2.3.1 Definisi Cryptanalysis..... 30

2.3.2 Bentuk Dasar dari Cryptanalytic Attack..... 31

2.3.3 Exhaustive Key Search……..……. 33

2.4 Landasan Matematis Kriptografi. 35

2.4.1 Aritmatika Modular…….. 35

2.4.2 Inverse Perkalian..... 35

2.4.3 Operasi XoR..... 36

2.4.4 Sifat-sifat Operasi XoR..... 38

2.4.5 Fungsi Linier..... 38

2.4.6 Fungsi Non Linier..... 39

2.5 Metode MMB 39

2.5.1 Pembentukan Kunci..... 40

2.5.2 Enkripsi..... 41

2.5.3 Dekripsi..... 44

2.5.4 Perbandingan Antara MMB dengan IDEA..... 48

BAB III ANALISIS DAN PERANCANGAN

3.1 Analisis 50

3.1.1 Algoritma..... 52

3.1.2 Algoritma Proses Pembentukan Kunci..... 52

3.1.3 Algoritma Proses Enkripsi..... 53

3.1.4 Algoritma Proses Dekripsi..... 55

3.1.5 Algoritma Fungsi Pendukung..... 57

3.2 Perancangan..... 64

3.2.1. Perancangan Animasi 64

3.2.2. Perancangan Tampilan 66

BAB IV IMPLEMENTASI DAN PENGUJIAN

4.1. Implementasi Sistem……. 84

4.2. Spesifikasi Perangkat Keras dan Lunak 84

4.3 Tampilan Output Perangkat Lunak..... 85

4.4 Analisa..... 90

BAB V KESIMPULAN DAN SARAN

5.1 Kesimpulan 92

5.2 Saran 92

DAFTAR PUSTAKA

LAMPIRAN