# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang

Kelemahan metode IDEA yang menggunakan *plaintext* 64 bit dan operasi perkalian modulo $2^{16} + 1$, diperbaiki oleh Joan Daemen dalam sebuah algoritma yang dinamakan MMB (*Modular Multiplication-based Block cipher*). Dengan menggunakan *plaintext* 64 bit (4 buah 16 bit *subblock text*), metode IDEA hanya dapat diimplementasikan pada prosesor 16 bit, sehingga dinilai tidak dapat mengikuti perkembangan teknologi pada saat ini yang kebanyakan telah menggunakan prosesor 32 bit. Kriptografi metode MMB menggunakan *plaintext* 128 bit dan algoritma iteratif yang terdiri dari langkah-langkah linier (seperti XOR dan aplikasi kunci) serta aplikasi paralel dari empat substitusi non linier besar yang dapat dibalik. Substitusi ini ditentukan oleh sebuah operasi perkalian modulo $2^{32} - 1$ dengan faktor konstan, yang memiliki tingkat sekuritas lebih tinggi bila dibandingkan dengan metode IDEA yang hanya menggunakan operasi perkalian modulo $2^{16} + 1$. MMB menggunakan 32 bit *subblock text* ($x_0$, $x_1$, $x_2$, $x_3$) dan 32 bit *subblock* kunci ($k_0$, $k_1$, $k_2$, $k_3$). Hal ini membuat algoritma tersebut sangat cocok diimplementasikan pada prosesor 32 bit. Sebuah fungsi non linier, f, diterapkan enam kali bersama dengan fungsi XOR.

Kerumitan algoritma ini, yang terletak pada proses operasi perkalian modulo $2^{32} - 1$, perhitungan fungsi non linier f pada proses enkripsi dan dekripsi, serta

operasi *invers* pada proses dekripsi, menyebabkan algoritma ini sulit diproses secara manual.

Berdasarkan uraian di atas, maka program *Microsoft Visual Basic 6.0* dipilih sebagai bahan utama.

## 1.2 Perumusan Masalah

Masalah pada pembuatan perangkat lunak bantu pemahaman kriptografi metode MMB ini dapat dirumuskan sebagai berikut :

1. Bagaimana pemrograman *Microsoft Visual Basic 6.0* yang hanya mendukung bilangan numerik maksimal 32 bit bisa melakukan operasi perkalian modulo$2^{32}$ tersebut.
2. Bagaimana menampilkan animasi prosedur kerja dari proses enkripsi, dekripsi dan fungsi f pada metode MMB.
3. Bagaimana mengetahui fungsi dan hasil proses algoritma yang digunakan.

## 1.3 Tujuan dan Manfaat Penulisan

Tujuan penyusunan skripsi ini adalah memperkenalkan metode kriptografi MMB dan mengetahui fungsi dan hasil proses algoritma yang digunakan, serta membuat suatu perangkat lunak untuk membantu pemahaman terhadap kriptografi metode MMB.

Manfaat dari penyusunan skripsi ini adalah sebagai berikut :

1. Bagi penulis
   - Memenuhi tugas akhir sebagai syarat kelulusan program strata-1 STMIK AMIKOM ( Sekolah Tinggi Manajemen Informatika dan Komputer ) yogyakarta.
   - Menerapkan pengetahuan yang telah diperoleh dari kegiatan perkuliahan di STMIK AMIKOM ( Sekolah Tinggi Manajemen Informatika dan Komputer ) yogyakarta.
2. Bagi Pengguna
   - Sarana belajar dan ilmu pengetahuan untuk memahami kriptografi
   - Untuk digunakan sebagai fasilitas pendukung dalam proses belajar mengajar.

## 1.4 Pembatasan Masalah

Pembatasan permasalahan dalam membuat perangkat lunak bantu pemahaman kriptografi metode MMB adalah sebagai berikut :

1. Perangkat lunak membatasi penggunaan algoritma dan fungsi-fungsi pendukung yang digunakan.
2. *Input* data berupa karakter (*string*) dengan panjang *plaintext*, *ciphertext* dan *key* adalah 16 karakter.

3. Perangkat lunak tidak menampilkan tahap – tahap konversi *string* ke dalam biner.
4. Perangkat lunak menyediakan teori – teori dasar dari kriptografi metode MMB.
5. Perangkat lunak akan menampilkan tahapan – tahapan pembentukan kunci, enkripsi, dekripsi dan fungsi f.

## 1.5 Metodologi Penyelesaian Masalah

Metode yang akan digunakan dalam pembuatan perangkat lunak ini terdiri dari langkah-langkah berikut :

1. Melakukan studi kepustakaan terhadap berbagai referensi yang berkaitan dengan kriptografi metode MMB dan mempelajari cara kerja dari kriptografi metode MMB.
2. Merancang sistem pembelajaran kriptografi metode MMB, kemudian mengimplementasikannya dengan membuat program aplikasinya menggunakan bahasa pemrograman *Visual Basic 6.0*.
3. Melakukan proses pengujian dan pengecekan kesalahan (*error*), cara kerja, dan hasil terhadap perangkat lunak yang telah dirancang.

## 1.6 Sistematika Penulisan

Sistematika penulisannya sebagai berikut :

1. Bab I. Pendahuluan

   Pada bab ini akan membahas Latar Belakang, Perumusan Masalah, Tujuan dan Manfaat, Pembatasan Masalah, Metodolagi Penyelesaian Masalah, Sistematika Penulisan.

2. Bab II. Landasan Teori

   Pada bab ini akan membahas tentang Pengenalan Kriptografi, Jenis Sistem Kriptografi, Cryptanalysis, Landasan Matematis Kriptografi, Metode MMB, Perangkat Lunak Pembelajaran.

3. Bab III. Pembahasan Dan Perancangan

   Pada bab ini akan membahas tentang Pembahasan,Perancangan.

4. Bab IV. Algoritma Dan Implementasi

   Pada bab ini akan menjelaskan tentang Algoritma,Implementasi Sistem.

5. Bab V. Testing Program Dan Analisa

   Pada bab ini akan menjelaskan tentang Pengetesan Program,Pengujian Terhadap Algoritma,perbandingan kecepatan

6. Bab VI . Kesimpulan Dan Saran

   Pada bab ini berisi tentang Kesimpulan Dan Saran