BAB I
PENDAHULUAN

1.1. Latar Belakang

Dengan berkembangnya zaman, algoritma kriptografi standar tidak lagi mampu merahasiakan suatu data dengan baik. Adanya penciptaan computer menjadi alasan utamanya. Algoritma-algoritma kriptografi klasik menjadi sangat mudah untuk dipecahkan. Jika pada zaman sebelum berkembangnya komputer untuk memecahkan suatu cipherteks yang dibentuk dari algoritma kriptografi klasik dilakukan secara manual dan tentunya membutuhkan waktu yang lama, kini dengan bantuan komputer dan perangkat lunak yang diciptakan untuk memecahkan cipherteks dengan algoritma tersebut, memecahkan cipherteks tersebut sangatlah mudah, bahkan tidak sampai hitungan jam.

Karenanya berkembanglah berbagai algoritma kriptografi modern seperti *Data Encription Standard* (DES) yang menandai mulainya era kriptografi modern. Namun dengan berkembangnya kemampuan dan kecepatan proses dari komputer, dimana sebuah komputer sudah mampu melakukan *brute force attack* dalam waktu yang cukup singkat terhadap DES yang hanya memiliki panjang 64 bit dengan 8 bit yang merupakan paritas, kini DES dirasa sudah tidak aman lagi. Karena hal tersebut, diperlukan algoritma baru yang dapat menggantikan DES.

National Institute of Standards and Technology (NIST) mengusulkan kepada Pemerintah Federal AS untuk sebuah standard kriptografi kriptografi yang baru. NIST mengadakan lomba membuat standard algoritma kriptografi yang baru untuk menggantikan DES. Standard tersebut diberi nama *Advanced Encryption Standard* (AES).

Diantara hasilnya, dirumuskan sebuah algoritma AES. Algoritma AES ditetapkan sebagai AES dan diharapkan dapat bertahan selama 10 tahun. Tidak seperti DES, Algoritma lebih aman. Algoritma *AES* merupakan algoritma kriptografi simetrik yang beroperasi dalam mode (*block cipher*) yang memproses blok data 128-bit dengan panjang kunci 128-bit, 192-bit, atau 256-bit sehingga dikenal dengan (*AES*-128), (*AES*192) dan (*AES*-256).

1.2. Perumusan Masalah

Berdasarkan latar belakang yang telah diuraikan sebelumnya, timbul beberapa masalah yang berhubungan dengan Skripsi ini. Adapun rumusan masalah dalam penelitian ini adalah :

1. Bagaimana cara melakukan mengenkripsi data dokumen dengan algoritma AES.
2. Bagaimana merancang aplikasi pengamanan file menggunakan Visual Basic.NET.

1.3. Batasan Masalah

Agar tujuan skripsi ini sesuai dengan yang diharapkan maka penulis membuat batasan masalah yaitu :

1. Aplikasi ini mengenkripsi data berbentuk teks.
2. Algoritma ini menggunakan AES 126 bit

1.4. Tujuan

Adapun tujuan penelitian ini adalah :

1. Untuk mengetahui proses enkripsi dan deskripsi dengan menggunakan algoritma AES.
2. Untuk merancang sebuah aplikasi sistem proteksi *File* dengan algoritma menggunakan *Visual Basic.NET*

1.5. Manfaat

Sedangkan manfaat dari penelitian ini adalah:

1. Sebagai bahan referensi mengenai cara penyandian kata kunci dengan algoritma AES.
2. Menghasilkan sebuah perangkat lunak yang dapat membantu mengunci dan mengamankan file yang menggunakan sistem operasi *windows 10*