

IMPLEMENTASI ALGORITMA KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD* (AES) PADA KEAMANAN DATA DOKUMEN BERBASIS *WEBSITE*

Nama Mahasiswa : Andi Khadijah Anindita Putri
NIM : 10211015
Dosen Pembimbing Utama : Dwi Arief Prambudi, S.Kom., M.Kom
Dosen Pembimbing Pendamping : HENDY INDRAWAN SUNARDI, S.Kom, M.Eng

ABSTRAK

Di tengah pesatnya proses digitalisasi, keamanan informasi atau data telah menjadi aspek yang sangat penting. Sayangnya, keamanan data sering kali kurang mendapat perhatian atau bahkan dianggap remeh, hingga akhirnya banyak insiden merugikan terjadi karena kebocoran data yang tak terduga. Penelitian ini hadir untuk menjawab tantangan tersebut, dengan tujuan memberikan perlindungan terhadap konten pesan teks dan file dokumen khususnya dokumen yang bersifat rahasia melalui penerapan algoritma kriptografi *Advanced Encryption Standard* (AES) untuk proses pengamanannya dengan melakukan proses enkripsi yang terdiri dari beberapa tahapan yaitu add roundkey, sub bytes, shift rows, dan mix columns dan dekripsi yang terdiri dari beberapa tahapan yaitu add roundkey, inv sub bytes, inv shift rows. Algoritma ini akan diimplementasikan dalam sebuah platform berbasis *website*, sehingga dapat menjaga keamanan data ujian secara lebih efisien dan andal. Dengan demikian, kami berharap sistem ini mampu memberikan perlindungan yang optimal dan meningkatkan kepercayaan dalam pengelolaan data digital di lingkungan pendidikan. Pada penelitian ini menghasilkan sebuah sistem sederhana yang dapat melakukan proses enkripsi dan dekripsi dengan input pesan teks maupun file dokumen dengan format .pdf, .doc, .xlsx, .jpg dan .png yang dapat di *download*. Untuk mengevaluasi metode kriptografi yang diterapkan, penelitian ini melibatkan dosen dari program studi Sistem Informasi yang memiliki keahlian mendalam di bidang keamanan informasi, terutama dalam aspek kriptografi. Kehadiran penguji ahli ini membantu memastikan bahwa sistem yang dikembangkan tidak hanya efektif tetapi juga memenuhi standar keamanan yang dibutuhkan. Selain itu, pengujian validitas pada algoritma ini juga menggunakan skenario pengujian yang disediakan langsung oleh NIST.

Kata kunci : Keamanan Informasi, Kriptografi, *Advanced Encryption Standard*, Enkripsi, Dekripsi, *Website*, Pendidikan.