

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada era globalisasi sekarang ini tingkat informasi dan teknologi semakin maju dan modern, pertukaran data melalui jaringan internet sangat mungkin dilakukan karena tentunya akan mempercepat dan memudahkan proses pertukaran data terutama dengan jarak yang jauh. Kemudahan ini tentunya berdampak pada munculnya resiko dan ancaman keamanan data, misalnya penduplikasian atau bahkan merusak informasi itu sendiri.

PT. Kelab 21 Retail juga pernah mendapatkan masalah dalam hal informasi. Dimana dokumen atau laporan keuangan yang tersimpan di dalam server diambil kemudian diubah informasi yang ada didalamnya oleh pihak yang tidak bertanggung jawab. Sehingga dengan kejadian seperti itu, PT. Kelab 21 Retail mengalami kerugian karena informasi yang ada tidak sesuai. Untuk itu diperlukan suatu metode keamanan yang dapat melindungi dokumen-dokumen tersebut.

Konsep perlindungan data dari suatu informasi dapat dilakukan dengan sistem enkripsi dan dekripsi menggunakan algoritma yang telah ditetapkan sebelumnya. Proses enkripsi di sini diartikan sebagai proses perubahan dari suatu pesan asli (*plain text*) menjadi suatu pesan yang terlindungi dalam hal ini pesan yang tersandi (*chiper text*), sedangkan untuk proses dekripsi adalah suatu proses pengembalian pesan tersandi yang terlindungi menjadi bentuk data asli pesan tersebut.

Pada kedua proses tersebut dibutuhkan suatu pengaman yang menjamin bahwa pesan tersebut terlindungi pada prosesnya, pengaman tersebut dinamakan *key*. Fungsi dari *key* ini adalah kunci untuk membuka atau mengawali tiap proses, pada penelitian ini *key* yang digunakan adalah algoritma kunci simetri (*Symmetric-key algorithm*) yaitu algoritma kunci yang sama pada saat melakukan proses enkripsi dan dekripsi.

Berdasarkan permasalahan yang telah diuraikan di atas, maka dirancang sebuah sistem pengenkripsian dokumen dengan judul **“Analisa dan Perancangan Sistem Enkripsi dan Dekripsi Dokumen Berbasis Android Dengan Metode Advanced Encryption Standard (AES) – 128 pada PT. Kelab 21 Retail”**



1.2. Rumusan Masalah

Berdasarkan uraian latar belakang di atas, dapat dirumuskan permasalahan yang dihadapi yaitu:

1. Bagaimana cara mengimplementasikan *Advanced Encryption Standard* (AES) – 128 untuk menjaga keamanan dokumen pada PT. Kelab 21 Retail?

1.3. Batasan Masalah

Batasan masalah pada penulisan Tugas Akhir ini adalah sebagai berikut:

1. Dokumen yang dapat diunggah memiliki format “.docx” , “.doc”, “.xlsx”, “.xlx”, “.pdf”, “.pptx”, dan “.txt”.
2. Dokumen berukuran ≤ 1 GB.
3. Algoritma yang digunakan dalam sistem keamanan enkripsi dan dekripsi ini adalah *Advanced Encryption Standard* (AES) – 128.

1.4. Tujuan dan Manfaat

1. Tujuan dari penelitian ini adalah:
 - a. Membangun sebuah sistem yang dapat melakukan enkripsi dan dekripsi dokumen menggunakan algoritma AES.
2. Sedangkan Manfaat dari penelitian ini adalah:
 - a. Meningkatkan dan menjaga keamanan informasi yang ada pada sebuah dokumen
 - b. Memperkecil terjadinya kebocoran dan penduplikasian dokumen

1.5. Sistematika Penulisan

Untuk mempermudah gambaran mengenai penulisan dalam tugas akhir ini pada setiap bab, maka penulisan dibagi menjadi 5 (lima) bab dengan susunan sistematika sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi tentang deskripsi umum dari skripsi ini yang meliputi latar belakang masalah, identifikasi masalah, batasan masalah, tujuan penelitian, dan sistematika penulisan tugas akhir.

BAB II LANDASAN TEORI

Bab ini membahas tentang pengertian sistem, Sistem Informasi, dan teori serta metode metode yang dipakai dalam penulisan.

BAB III METODE PENELITIAN

Bab ini berisi gambaran tentang Perusahaan dan menguraikan secara rinci mengenai pengumpulan data, analisis kebutuhan sistem, serta metodologi penelitian yang digunakan dalam analisis sistem dan perancangan sistem.

BAB IV IMPLEMENTASI DAN EVALUASI

Bab ini berisikan tentang hasil-hasil tahapan penelitian, mulai dari analisis, desain hasil testing dan cara mengimplementasinya.

BAB V PENUTUP

Bab ini berisikan tentang kesimpulan dan saran yang berkaitan dengan analisa dan optimalisasi Sistem berdasarkan yang telah diuraikan pada bab sebelumnya.

