BAB I
PENDAHULUAN

1.1 Latar Belakang

Tanda tangan adalah salah satu ciri khas semua manusia. Tanda tangan sering digunakan sebagai syarat pengesahan sebuah dokumen. Hal ini menjadi masalah ketika pengesahan tidak dapat dilakukan karena kedua belah pihak tidak dapat bertemu untuk melakukan tanda tangan. Seiring dengan kemajuan teknologi, penggunaan internet dalam berbagai aspek sudah menjadi kebutuhan. Penggunaan internet sangat luas dalam proses aktivitas sehari – hari.

Dalam membuat suatu surat-menyurat pada masa ini sudah sangat terbiasa digunakan oleh masyarakat baik secara individu maupun kelembagaan. Dari surat resmi yang dicetak maupun berupa digital dokumen surat selalu memberikan pengesahaan biasa berupa tanda tangan dan pembubuhan stempel, dan biasanya surat resmi terdapat suatu format atau template dalam pembuatannya. Pada era pandemi covid-19 banyak lembaga yang sudah terbiasa dalam menggunakan dokumen suratmenyurat dalam bentuk digital. (Hardiansyah, Ramdhani, & Arifai, 2022)

Pengguna dapat menandatangani banyak *file* atau dokumen melalui perangkat elektronik seperti *smartphone* atau komputer yang terhubung melalui jaringan internet. Terobosan seperti ini tentunya sangat membantu dalam pekerjaan yang membutuhkan banyak dokumen tanda tangan atau surat menyurat. Kondisi ini dimungkinkan di masa pandemi Covid-19 dengan melaksanakan pekerjaan dari rumah. Namun pengesahannya biasanya hanya meletakan gambar tanda-tangan maupun stempel. Hal tersebut menimbulkan kerawanan untuk dipalsukan, karena penggunaan gambar digital sangat rentan untuk dipalsukan.

Berdasarkan latar belakang tersebut maka dibuat suatu sistem untuk melakukan pengesahan dokumen. Adapun judul yang diambil untuk penyusunan laporan ini yaitu : "**Rancang Bangun Sistem Pengesahan Dokumen Menggunakan Algoritma AES Berbasis Website**".

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, dirumuskan masalah yaitu bagaimana mengimplementasikan algoritma AES untuk keamanan dokumen pada sistem pengesahan dokumen berbasis *website*.

1.3 Tujuan dan Manfaat

Tujuan dari penelitian ini adalah untuk mengimplementasikan algoritma AES untuk keamanan dokumen pada sistem pengesahan dokumen berbasis *website*. Adapun manfaatnya yaitu :

1. Mempermudah proses pengesahan dokumen.
2. Mengurangi kontak fisik secara langsung.
3. Efisiensi waktu.
4. Menjamin keaslian tanda tangan.

1.4 Batasan Masalah

Agar pengerjaan tugas akhir ini menjadi lebih terarah dan mendapatkan hasil yang lebih spesifik, maka sistem yang dirancang dibatasi pada ruang lingkup pembahasan sebagai berikut :

1. Data dari dokumen akan di enkripsi menggunakan algoritma AES.
2. Hasil enkripsi akan di konversi ke QR *code.*
3. *File* yang di upload berupa pdf.
4. QR *Code* digunakan untuk memvalidasi dokumen yang telah di berikan tanda tangan atau disetujui.
5. Berbasis *website.*

1.5 Metodologi Penelitian

Metodologi yang digunakan dalam tugas akhir ini adalah sebagai berikut :

1. Pengumpulan data

   Pengumpulan data dengan studi kepustakaan dilakukan dengan cara mempelajari jurnal, buku-buku, dan sumber terkait lainnya yang menjadi acuan dalam pembuatan program.
2. Analisis Sistem

Dilakukan analisis terhadap sistem dalam pembuatan atau pengembangansistem informasi yang bertujuan untuk menyelesaikan masalah secara efektif yang akan dibuat dengan menggunakan teknik pemodelan SDLC (*System Development Life Cycle*).

3. Perancangan

   Berupa perancangan data, perancangan struktur data menu serta perancangan *interface input* dan *output*.

4. Implementasi

   Perancangan sistem dibuat secara terstruktur, sesuai dengan tahapan-tahapan yang harus dilakukan. Sebuah sistem pengesahan dokumen.

1.6 *State of the art*

Dalam penyusunan tugas akhir ini, mengambil beberapa referensi materi dari peneliti sebelumnya, termasuk jurnal yang berkaitan dengan penelitian ini. Referensi dari beberapa jurnal beserta ringkasan nya sebagai berikut ini :

Tabel 1.1 *State of the art*

No	Jurnal	Ringkasan	Perbedaan
1	Judul : Implementasi Kriptografi Metode RSA (Revest Shamir Adleman) Pada Debitur Oleh : Muhammad Yusuf, Azanuddin, Jufri Halim Tahun : 2018	Jurnal tersebut membahas tentang keamanan data mitranya yang meliputi nama took, lokasi, no.hp dan aset.	Perbedaan jurnal tersebut dengan penelitian ini adalah algoritma yang digunakan pada penelitian ini adalah algoritma AES
2	Judul : The Use Of Digital Signatures In The Business World	Jurnal tersebut membahas tentang penggunaan tanda	Perbedaan jurnal tersebut dengan

	In The Industrial Revolution 4.0 Era Oleh : Wahyu Sardjono, Wowon Priatna, Pardiyo, Gustian Rama Putra, Hanny Juwitasary Tahun : 2021	tangan di era revolusi industry 4.0	penelitian ini adalah didalam jurnal tersebut tidak dijelaskan algoritma apa yang digunakan dalam penulisannya
3	Judul : Implementasi Tanda Tangan Digital Menggunakan RSA dan SHA-512 Pada Proses Legalisasi Ijazah Oleh : Fitri Nuraeni, Yoga Handoko Agustin, Irman Maulana Muharam Tahun : 2018	Jurnal tersebut membahas tentang implementasi tanda tangan digital pada legalisasi ijazah menggunakan algoritma RSA dan SHA – 512	Perbedaan jurnal tersebut dengan penelitian ini berbeda dalam hal inputan datanya, serta kombinasi algoritma yang digunakan juga sedikit berbeda
4	Judul : Implementasi Caesar Chiper and Advance Encryption Standard (AES) pada data Pajak bumi Bangunan Oleh : Fitri Nuraeni, Yoga Handoko Agustin, Angga Eka Purnama	Jurnal Tersebut membahas tentang pengelolaan data pajak bumi bangunan yang diamankan sistem kriptografi yang didalamnya menyediakan	Perbedaan jurnal tersebut dengan penelitian ini yaitu dalam hal mengelola data, penelitian ini berfokus pada pengesahan

	Tahun : 2020	fasilitas enkripsi dan deskripsi data.	dokumen dan validasi keaslian dokumen
5	Judul : Pemanfaatan Algotritma AES Dlam Pembuatan Sistem Enkripsi dan Dekripsi Dokumen Oleh : T. Ilhamsyah Tahun :2019	Jurnal tersebut membahas tentang cara kerja kriptografi AES pada proses enkripsi dan dekripsi	Perbedaan jurnal tersebut dengan penelitian ini yaitu pada penelitian ini tidak hanya membahas cara kerja algoritma aes, tapi mengelola data inputan menggunakan algoritma AES yang berguna untuk validasi.

1.7 Sistematika Penulisan

Secara garis besar, Sistematika penulisan tugas akhir ini tersusun sebagai berikut :

BAB I PENDAHULUAN

Pada bab ini memabahas tentang latar belakang, rumusan masalah, tujuan dan manfaat, batasan masalah, *State of the art*, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini membahas tentang tinjauan pustaka yang berkaitan dengan tugas akhir, seperti pengesahan dokumen, *website*, dan algoritma AES.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Pada bab ini membahas tentang analisis masalah kebutuhan sistem, pengumpulan data dan perancangan.

BAB IV IMPLEMENTASI

Pada bab ini membahas tentang pengujian dan hasil dari sistem untuk pengesahan dokumen.

BAB V PENUTUP

Pada bab ini berisi tentang kesimpulan dan saran dari hasil penelitian yang telah dilakukan.