BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi di era digital telah mendorong peningkatan penggunaan dokumen elektronik dalam berbagai aktivitas, baik di lingkungan pendidikan, pemerintahan, maupun perusahaan. Dokumen digital seperti surat resmi, sertifikat, laporan, dan dokumen administrasi lainnya digunakan karena memberikan kemudahan dalam penyimpanan, distribusi, dan pengelolaan data secara lebih efisien. Namun, meningkatnya penggunaan dokumen digital juga menimbulkan permasalahan baru, terutama terkait keamanan, keaslian, dan integritas dokumen. Dokumen digital sangat rentan terhadap tindakan manipulasi atau perubahan data oleh pihak yang tidak berwenang tanpa diketahui oleh penerima dokumen [1].

Permasalahan tersebut menyebabkan kebutuhan terhadap sistem keamanan dokumen digital semakin meningkat. Salah satu metode yang dapat digunakan untuk menjaga keaslian dan integritas dokumen adalah penerapan tanda tangan digital (*digital signature*). Tanda tangan digital merupakan mekanisme keamanan berbasis kriptografi yang digunakan untuk melakukan autentikasi terhadap suatu data atau dokumen sehingga penerima dapat memastikan bahwa dokumen benar-benar berasal dari pihak yang sah dan tidak mengalami perubahan setelah ditandatangani [2].

Salah satu algoritma yang banyak digunakan dalam implementasi tanda tangan digital adalah *Elliptic Curve Digital Signature Algorithm* (ECDSA). Algoritma ECDSA merupakan pengembangan dari konsep kriptografi kurva eliptik ECC (*Elliptic Curve Cryptography*) yang memiliki tingkat keamanan tinggi dengan ukuran kunci yang relatif lebih kecil dibandingkan algoritma kriptografi klasik seperti RSA. Penggunaan ukuran kunci yang lebih kecil membuat proses komputasi menjadi lebih efisien tanpa mengurangi tingkat keamanan sistem [3].

Pada implementasinya, algoritma ECDSA bekerja melalui beberapa tahapan utama, yaitu proses *hashing*, *signing*, dan *verification*. Dokumen digital terlebih dahulu diproses menggunakan fungsi *hash* kriptografi untuk menghasilkan nilai *hash* yang unik. Nilai *hash* tersebut kemudian ditandatangani menggunakan *private key* untuk menghasilkan tanda tangan digital. Selanjutnya, proses verifikasi dilakukan dengan menggunakan *public key* untuk memastikan bahwa *signature* sesuai dengan dokumen asli dan tidak mengalami perubahan [4].

Selain penggunaan algoritma kriptografi, teknologi *Quick Response Code* (QR Code) juga dapat dimanfaatkan sebagai media penyimpanan informasi tanda tangan digital. QR Code merupakan barcode dua dimensi yang mampu menyimpan data dalam jumlah cukup besar dan dapat diakses dengan cepat melalui proses pemindaian menggunakan perangkat *mobile* maupun *webcam*. Penggunaan QR Code memungkinkan proses distribusi dan verifikasi tanda tangan digital menjadi lebih praktis karena informasi *signature* dapat disimpan secara langsung pada dokumen [5].

Integrasi antara algoritma ECDSA dan QR Code dapat meningkatkan efisiensi proses autentikasi dokumen digital. Melalui sistem ini, pengguna hanya perlu melakukan pemindaian QR Code yang terdapat pada dokumen untuk melakukan proses verifikasi keaslian dokumen. Apabila isi dokumen mengalami perubahan, maka nilai *hash* dokumen juga berubah sehingga *signature* digital menjadi tidak valid. Dengan demikian, integritas dokumen dapat tetap terjaga.

Dalam penelitian ini, implementasi algoritma ECDSA dilakukan pada sistem berbasis *web* bernama "**AuthentiC**". Sistem ini dirancang untuk melakukan proses penandatanganan digital pada dokumen PDF dengan menghasilkan *signature* digital yang kemudian dikodekan ke dalam QR Code dan disisipkan pada dokumen. Selain itu, sistem juga menyediakan fitur verifikasi dokumen melalui proses pemindaian QR Code dan pencocokan *signature* menggunakan *public key*. Sistem berbasis *web* dipilih karena lebih fleksibel, mudah diakses, dan tidak memerlukan instalasi aplikasi tambahan pada perangkat pengguna.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk membangun sistem autentikasi dokumen digital berbasis *web* menggunakan algoritma ECDSA dan QR Code guna meningkatkan keamanan, keaslian, dan integritas dokumen PDF secara praktis, efisien, dan aman.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka rumusan masalah dalam penelitian ini adalah sebagai berikut :

1. Bagaimana mengimplementasikan algoritma ECDSA pada sistem "**AuthentiC**" untuk menghasilkan tanda tangan digital pada dokumen PDF?
2. Bagaimana tingkat efektivitas sistem "**AuthentiC**" dalam mendeteksi perubahan dokumen PDF melalui proses verifikasi QR Code?

1.3 Batasan Masalah

Untuk menjaga ruang lingkup penelitian ini lebih terfokus, ditetapkan beberapa batasan sebagai berikut :

1. Algoritma kriptografi yang digunakan adalah ECDSA.
2. Proses penandatanganan dilakukan terhadap nilai *hash* dokumen, bukan keseluruhan isi dokumen.
3. Sistem yang dikembangkan berbasis *web*.
4. Proses verifikasi dilakukan melalui situs *web* dan *scan* QR Code yang dihasilkan oleh sistem.
5. Dokumen yang diproses hanya berformat PDF.

1.4 Tujuan Penelitian

Tujuan yang akan dicapai oleh peneliti dalam penelitiannya adalah :

1. Mengimplementasikan algoritma ECDSA pada sistem tanda tangan digital.
2. Mengintegrasikan hasil tanda tangan digital ke dalam media penyimpanan QR Code.
3. Mengembangkan sistem verifikasi dokumen berbasis *web* yang mampu membaca QR Code dan memvalidasi keaslian dokumen.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut :

1. Memberikan kemudahan bagi pengguna dalam melakukan proses autentikasi dan verifikasi dokumen digital secara praktis dan efisien.
2. Menambah literatur mengenai penerapan nyata kriptografi tingkat lanjut dalam sistem keamanan informasi.

1.6 Sistematika Penulisan

Untuk mempermudah dalam memahami skripsi ini, maka penulisan materi skripsi ini disusun dengan sistematika sebagai berikut :

BAB I PENDAHULUAN, berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA, berisi tinjauan pustaka, dasar-dasar teori yang digunakan dan dijadikan dasar penelitian dalam skripsi ini.

BAB III METODE PENELITIAN, berisi metode penelitian dan tahapan pengembangan sistem.

BAB IV HASIL DAN PEMBAHASAN, bab ini merupakan tahapan yang penulis lakukan dalam menyajikan hasil implementasi sistem dan pengujian.

BAB V PENUTUP, berisi kesimpulan dan saran yang dapat peneliti rangkum selama proses penelitian yang penulis berikan untuk peneliti selanjutnya.