BAB I
PENDAHULUAN

1.1. Latar Belakang

Surat merupakan salah satu media komunikasi yang sangat penting disuatu instansi, perusahaan maupun organisasi, baik untuk berkomunikasi dengan pihak diluar organisasi (eksternal) maupun didalam organisasi (internal). Tandatangan tradisional dalam surat masih menjadi penentu keaslian dari sebuah surat tersebut, sehingga sering kali menjadi faktor penghambat implementasi dari sebuah sistem persuratan. Diperlukan waktu panjang untuk proses tandatangan yang manual ini, seperti mendistribusikan surat kepada yang menandatangani, pemeriksaan kertas surat dan proses penandatanganan.

Dalam sebuah sistem persuratan, autentikasi atau keaslian sebuah dokumen sangat penting dan kritikal sehingga diperlukan sebuah sistem yang dapat menjadi pelengkap sekaligus dapat mempercepat secara signifikan pemrosesan dokumen digital yaitu *E-Signature* atau biasa disebut juga *Digital Signature*. *Digital Signature* pada dasarnya adalah sebuah proses untuk memastikan dokumen elektronik (email, spread sheet, dokumen) otentik. Otentik yang artinya dapat mengetahui siapa yang berhak mengesahkan dan tidak diubah setelah dokumen tersebut disahkan oleh yang berhak. *Digital signature* bukanlah sebuah tandatangan fisik yang di scan lalu ditambahkan kedalam dokumen. Lebih dari itu sebuah tandatangan digital menggunakan teknik kriptografi yang dapat memastikan keaslian dan transparansi dari sebuah dokumen sehingga dokumen tersebut dapat dipertanggungjawabkan (*Pratama Persadh, 2015*). Tanda tangan digital yang telah dirubah menggunakan teknik kriptografi tersebut disimpan dalam bentuk *QRCode*. Dengan *QRCode* informasi keaslian surat menjadi lebih sederhana atau simple dengan mengetikkan informasi kode validasi pada surat tersebut untuk keperluan komersil.

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentifikasi (*Menezes, 1997*). Sedangkan sistem kriptografi merupakan kumpulan yang terdiri dari plaintext berupa pesan asli yang akan dikirimkan,

ciphertext berupa pesan yang telah disandikan, kunci, enkripsi serta dekripsi. Sistem kriptografi dibagi menjadi dua, yaitu sistem kriptografi kunci simetri dan kriptografi asimetri atau yang lebih dikenal sebagai kriptografi kunci publik. Perbedaan pada kedua sistem kriptografi tersebut ada pada kuncinya, jika pada sistem kriptografi kunci simetri hanya diperlukan kunci privat, sedangkan pada kriptografi kunci publik diperlukan kunci privat dan juga kunci publik. Kunci privat merupakan kunci yang tidak boleh diketahui oleh pihak lain kecuali dua pihak yang berkomunikasi, sedangkan kunci publik dapat diketahui oleh siapapun.

Penelitian ini menggunakan kombinasi algoritma kriptografi asimetris dan simetris, yaitu algoritma AES (Advanced Encryption Standard) dan RSA (Rivest Shamir Adleman). Algoritma AES merupakan algoritma simetris yang cukup aman untuk mengamankan data atau informasi yang bersifat rahasia. Pada tahun 2001, AES digunakan sebagai standar algoritma kriptografi terbaru yang dipublikasikan oleh Nasional Institute of Standard and Technology (NIST). AES menggunakan blok cipher simetris yang dimaksudkan untuk mengganti algoritma DES (*Stalling, 2011*). Algoritma RSA merupakan algoritma kriptografi asimetri, dimana kunci yang digunakan untuk mengenkripsi berbeda dengan yang digunakan untuk mendekripsi. Kunci yang digunakan untuk mengenkripsi disebut dengan kunci public, dan yang digunakan untuk mendekripsi disebut dengan kunci privat. Berdasarkan uraian latar belakang yang telah dikemukakan, maka dilakukanlah penelitian dengan judul "Implementasi Algoritma AES (Advanced Encryption Standard) Dan RSA (Rivest Shamir Adleman) Untuk Pengamanan Surat Di HUMANIKA".

1.2. Perumusan Masalah

Permasalahan yang dijadikan objek penelitian pada tugas akhir ini berdasarkan latar belakang yang telah dipaparkan adalah : Apakah *QRCode* dan algoritma *Advanced Encryption Standard* dan *Rivest Shamir Adleman* dapat menjamin keamanan tanda tangan surat pada sistem informasi manajemen persuratan di Humanika ?

1.3. Batasan Masalah

Untuk lebih memfokuskan pengerjaan penelitian ditetapkan pembahasan hanya dibatasi pada :

1. Data yang digunakan dalam penelitian ini adalah file yang berupa surat.
2. Penelitian hanya menggunakan metode *Advanced Encryption Standard* dan *Rivest Shamir Adleman*.
3. Studi kasus penelitian di Himpunan Mahasiswa Teknik Informatika Muhammadiyah Jember
4. Jenis surat yang digunakan adalah surat undangan dan surat keterangan aktif organisasi.
5. Bahasa pemrograman yang digunakan dalam penelitian ini adalah *php* (*Hypertext Prepocessor*).
6. Hasil enkripsi adalah *chippertext* yang berupa *QRCode* dan hasil dari dekripsi adalah *plaintext*.

1.4. Tujuan

Tujuan penelitian pada tugas akhir ini adalah menerapkan QRCode dan algoritma *Advanced Encryption Standard* serta *Rivest Shamir Adleman* untuk menjamin keamanan tanda tangan surat pada sistem informasi manajemen persuratan.

1.5. Manfaat

Adapun manfaat dari penelitian ini antara lain :

1. Bagi Peneliti, bisa menerapkan dan mengembangkan ilmu kriptografi yang diperoleh selama peneliti kuliah.
2. Bagi Kalangan akademik, diharapkan skripsi ini dapat dijadikan bahan pertimbangan untuk penelitian dan pengembangan lebih lanjut.