# BAB I

# PENDAHULUAN

## 1.1 LATAR BELAKANG

Kecanggihan zaman yang berkemajuan, menjadikan proses kirim data dan informasi semakin tendensi untuk diperhatikan. Terlebih lagi dalam dunia pendidikan, keamanan informasi harus sangat dirahasiakan. Di dalam lembaga PESMA Al-Manar yang notabenenya dibawah naungan Universitas Muhammadiyah Ponorogo pasti juga memiliki banyak data dan informasi yang harus dijaga. PESMA Al-Manar merupakan lembaga pendidikan pesantren mahasiswa yang bergerak dalam mendidik mahasiswa baru agar memiliki wawasan agama. Setiap tahun PESMA Al-Manar selalu mengadakan wajib pondok yang apabila selesai melaksanakannya maka para mahasiswa akan mendapatkan surat tanda bukti berupa sertifikat. Surat tanda bukti PESMA Al-Manar adalah surat yang dibentuk khusus untuk mahasiswa yang sudah melaksanakan wajib pondok selama empat puluh hari dan data mahasiswa juga akan tersimpan didalam PESMA Al-Manar. Kegunaan sertifikat pondok PESMA Al-Manar yakni untuk memenuhi persyaratan administrasi lain seperti contohnya jika mendaftar kuliah kerja nyata yang harus mewajibkan para mahasiswa melampirkan *soft file* sertifikat PESMA Al-Manar.

Berdasarkan observasi yang telah dilakukan pada lapangan, maka ditemukan masalah yang sedang terjadi. Dikutip dari *database* PESMA Al-Manar angkatan 2018 terdapat tujuh Puluh tujuh mahasiswa melakukan kecurangan demi mendapatkan pengakuan yakni dengan cara mencetak ulang sertifikat melalui penggantian nama dan nim yang diubah. Padahal mahasiswa tersebut tidak lulus dalam pondok PESMA Al-Manar dan bahkan belum mengikuti sama sekali. Disaat bersamaan, tindakan sementara dari PESMA Al-Manar ketika melakukan pengecekan data dan informasi yakni secara manual dari *database*. Jika kecurangan tersebut diketahui pihak PESMA Al-Manar, maka PESMA Al-Manar akan memberikan teguran kepada mahasiswa tersebut, kemudian menindak lanjuti dengan mengharuskan ikut wajib pondok

pada tahun berikutnya. Oleh karena itu, Agar menjamin keaslian sertifikat, maka dilakukan penambahan keamanan berupa suatu mekanisme *digital signature* untuk menanggulangi penipuan yang sering terjadi. Secara alternatif *digital signature* berfungsi sebagai penguji dari keaslian suatu dokumen digital, disisi lain juga dapat mendeteksi perubahan dokumen dari hasil manipulasi ilegal [1]. *Rivest Shamir Adleman* (RSA) merupakan teknik dari sebagian teknik kriptografi yang istimewa, dikarenakan kunci untuk mengaplikasikan proses *encryption* bisa berbeda dengan kunci untuk menerapkan proses dekripsi. Kunci untuk melakukan proses *encryption* dinamakan sebagai kunci publik, sedangkan kunci untuk melakukan proses dekripsi yakni dinamakan kunci privat.

Pada PERPRES Nomor 95 ketetapan tahun 2018 tentang perihal Sistem Pemerintahan Berbasis Elektronik (SPBE), yakni sertifikat elektronik sudah ditetapkan norma pada pasal 40 ayat 6 terkait amanat implementasi dari SPBE. [2]

Setelah menganalisa latar belakang yang sedang terjadi, maka judul pada penelitian yakni "Implentasi *Digital Signature* Untuk Tanda Tangan Sertifikat PESMA AL-MANAR Menggunakan Algoritma RSA" Dengan aplikasi seperti ini maka diharapkan tidak ada lagi yang melakukan kecurangan atau pemalsuan sertifikat PESMA Al-Manar. Di satu sisi PESMA Al-Manar juga akan lebih ketat lagi kepada mahasiswa yang belum mengikuti wajib pondok sebagai administrasi syarat untuk mengikuti kegiatan selanjutnya dari kampus.

## 1.2 RUMUSAN MASALAH

Penulis mengangkat rumusan masalah yakni "Bagaimana cara implementasi tanda tangan *digital* pada *digital signature* untuk mendeteksi keaslian sertifikat dengan menggunakan Algoritma RSA?"

## 1.3 TUJUAN

Tujuan dari penelitian yakni membangun aplikasi keamanan sertifikat ber*software website* dengan menggunakan algoritma RSA (*Rivest Shamir Adleman*) untuk memastikan keaslian sertifikat PESMA Al-Manar.

## 1.4 BATASAN MASALAH

Supaya perancangan Aplikasi deteksi tanda tangan sertifikat berbasis *Website* menggunakan kriptografi ini dapat diterapkan. Oleh karena itu, batasan masalah yang diambil yakni :

1. Hanya meyelesaikan perancangan aplikasi *website* deteksi tanda tangan sertifikat menggunakan Algoritma RSA.
2. Aplikasi dapat dijalankan pada *Operating Systems Windows* menggunakan jenis bahasa program PHP dan Mysql.
3. Pengujian sistem pendeteksi tanda tangan sertifikat menggunakan Algoritma RSA dengan jumlah data uji 20 sertifikat mahasiswa angkatan 2018 berbentuk *file* PNG dan ZIP.

## 1.5 MANFAAT PENELITIAN

1. Diharapkan mengurangi kecurangan pemalsuan tanda tangan sertifikat PESMA Al-Manar
2. Mempermudah deteksi jika terjadi kecurangan tanda tangan sertifikat.