BAB I
PENDAHULUAN

1.1. Latar Belakang Masalah

Kegiatan surat-menyurat sangat populer di era modern ini. Bentuk surat dapat berupa surat elektronik atau non-elektronik. Pada umumnya surat non-elektronik dikirim melalui mekanisme pengirim menyampaikan surat kepada penerima dengan menggunakan perantara jasa kurir dan sebagainya, sedangkan untuk surat elektronik dikirim melalui email atau situs-situs lainnya di internet.

Jika dikaitkan dengan kegiatan instansi atau perusahaan, maka surat yang bersifat resmi harus dikelola, itu sebabnya instansi atau perusahaan mendirikan divisi khusus untuk menangani permasalahan yang berikaitan dengan pengelolaan surat. Bentuk pengelolaan surat tersebut jika surat non-elektronik maka surat cukup diarsipkan, sedangkan surat elektronik bisa memanfaatkan *email client* untuk mendokumentasikannya. Surat masuk akan dikelola oleh bagian tata persuratan. Surat yang asli akan diarsipkan kemudian diserahkan pada pimpinan instansi untuk ditanda tangani sebagai aspek legalitas. Setelah itu arsip digitalnya didisposisikan pada divisi-divisi yang dituju sehingga dapat diterima pada waktu itu juga.

Karena pendistribusian ini menggunakan media elektronik, maka surat tersebut harus dijaga kerahasiaannya agar tidak terjadi hal-hal yang tidak diinginkan. Jika pada surat biasa pengamanannya berupa keutuhan kemasan, sedangkan untuk media digital menggunakan teknik tertentu. Teknik yang bisa dipakai salah satunya menggunakan pemberian tanda khusus yaitu *digital signature*. *Digital signature* merupakan nilai kriptografis yang bergantung pada pesan dan pengirim pesan. dimana perubahan suatu data sangat berpengaruh terhadap suatu pesan (Munir, 2006).

Keamanan data merupakan bagian terpenting dalam sebuah sistem pada jaringan komputer. Saat distribusi surat, bisa saja pihak lain secara ilegal

Try Haryatno, 2016
IMPLEMENTASI DIGITAL SIGNATURE MENGGUNAKAN ALGORITMA KRIPTOGRAFI AES DAN ALGORITMA KRIPTOGRAFI RSA SEBAGAI KEAMANAN PADA SISTEM DISPOSISI SURAT
Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

mengubah isi surat tanpa diketahui pengirim dan penerima. Suratpun menjadi tidak jelas dan patut dipertanyakan legalitasnya. Untuk memenuhi aspek-aspek

keamanan data pada sistem maka diperlukan metode keamanan data dan informasi yang disebut kriptografi.

Pada penelitian Wisnu Wendanto (2013), sistem disposisi surat menggunakan *digital signature* dan algoritma RSA. Keamanan data file surat yang dikirim akan lebih aman jika ada proses *hash* dan enkripsi nama file, sehingga file surat yang diterima bisa dipertanggung jawabkan keasliannya. Namun pada penelitian Wisnu tidak melakukan pengamanan pada isi pesan surat yang akan dikirimkan.

Penelitian Ibnu Berliyanto G. A., Amir Hamzah, Suwanto Raharjo (2014) *digital signature* dengan algoritma CRC32 digunakan pada transkrip nilai sebagai otentikasi data. Menurut penelitian Ibnu dkk. *digital signature* merupakan salah satu solusi metode keamanan data yang baik karena mempunyai tingkat keakuratan nilai yang cukup tinggi terhadap suatu perubahan data.

Penelitian Aji Setiyo Sukarno (2013) mengembangkan aplikasi pengamanan dokumen digital menggunakan *digital signature* RSA, algoritma AES dan *invisible watermarking*. Sehingga *output* dari penelitian Aji menghasilkan gambar yang telah terenkripsi dan sebuah berkas yang berisi tanda verifikasi dari *digital signature*. Namun penelitian Aji hanya berlaku untuk file berekstensi .pdf saja. Pengembangan aplikasi belum dilakukan proses *management key* sehingga pengelolaan kunci asimetrik yaitu RSA, dan kunci simetrik AES seutuhnya dikelola oleh entitas yang melakukan pertukaran data.

Penelitian ini menggunakan kombinasi algoritma kriptografi asimetris dan simetris, yaitu algoritma RSA dan algoritma AES. Algoritma RSA merupakan algoritma kriptografi asimetris yang paling sering digunakan saat ini dikarenakan dengan keunggulannya. Salah satunya yaitu panjang kunci dalam bit dapat diatur dengan semakin panjang bit maka semakin sulit untuk dipecahkan karena sulitnya memfaktorkan dua bilangan yang sangat besar, namun membutuhkan waktu yang cukup lama untuk proses dekripsinya. Algoritma AES merupakan algoritma

Try Haryatno, 2016

IMPLEMENTASI DIGITAL SIGNATURE MENGGUNAKAN ALGORITMA KRIPTOGRAFI AES DAN ALGORITMA KRIPTOGRAFI RSA SEBAGAI KEAMANAN PADA SISTEM DISPOSISI SURAT

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

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 digunakan saat proses tanda tangan digital. Sedangkan algoritma AES digunakan saat proses penyandian pesan yang akan dikirimkan pada penerima.

Jadi sistem disposisi surat dibuat dengan *digital signature* dan algoritma RSA untuk tanda atau simbol bahwa benar pesan yang dikirimkan terjaga legalitasnya dan menggunakan algoritma AES untuk keamanan saat penyandian pesan. Penelitian dilakukan untuk melihat pengaruh *digital signature* dengan kombinasi algoritma RSA dan AES terhadap sistem disposisi surat berdasarkan tujuan kriptografi.

1.2. Rumusan Masalah

Rumusan masalah dalam penelitian ini adalah:

1. Bagaimana memodifikasi skema *digital signature* dengan algoritma kriptografi RSA dan AES?
2. Bagaimana pengaruh algoritma RSA, AES dan *digital signature* pada sistem disposisi surat berdasarkan tujuan kriptografi, yaitu *confidentially* (kerahasiaan), data *integrity* (integritas data), *authentication* (autentikasi), dan *non-repudiation* (nir-penyangkalan)?

1.3. Batasan Masalah

Batasan masalah yang diteliti antara lain adalah:

1. Format file surat yang digunakan merupakan file gambar .jpg.
2. Berkas .jpg yang diunggah merupakan berkas surat disposisi 1 halaman.
3. Pesan yang dikirim berupa gambar yang telah terenkripsi dan hasil dari *digital signature*.

Try Haryatno, 2016
IMPLEMENTASI DIGITAL SIGNATURE MENGGUNAKAN ALGORITMA KRIPTOGRAFI AES DAN ALGORITMA KRIPTOGRAFI RSA SEBAGAI KEAMANAN PADA SISTEM DISPOSISI SURAT
Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

4. Hasil *digital signature* terpisah dari gambar dan dikirimkan secara bersamaan.
5. Menggunakan AES-128 dengan panjang kunci sebesar 128bit.
6. Menggunakan 2 bilangan prima dengan rentang 1000 sampai 2000 pada saat pembangkitan kunci RSA.

1.4. Tujuan Penelitian

Sesuai dengan permasalahan yang telah dirumuskan, maka tujuan yang ingin dicapai pada penelitian ini adalah:

1. Menghasilkan skema *digital signature* yang baru dengan algoritma kriptografi RSA dan AES.
2. Mengetahui pengharuh *digital signature* terhadap sistem secara keseluruhan berdasarkan tujuan kriptografi yaitu *confidentially* (kerahasiaan), data *integrity* (integritas data), *authentication* (autentikasi), dan *non-repudiation*(nir-penyangkalan).

1.5. Sistematika Penulisan

Sistematika penulisan skripsi ini adalah sebagai berikut

BAB I PENDAHULUAN

Bab ini berisi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian yang akan dilakukan, serta sistematika penulisan.

BAB II TINJUAN PUSTAKA

Bab ini berisi penjelasan tentang teori-teori kriptografi, *digital signature*, operasi XOR, algoritma RSA, algoritma AES yang digunakan dalam penelitian.

BAB III METODE PENELITIAN

Bab ini berisi penjelasan langkah-langkah yang akan dilakukan dalam penelitian.

Try Haryatno, 2016

IMPLEMENTASI DIGITAL SIGNATURE MENGGUNAKAN ALGORITMA KRIPTOGRAFI AES DAN ALGORITMA KRIPTOGRAFI RSA SEBAGAI KEAMANAN PADA SISTEM DISPOSISI SURAT

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Pada bab ini membahas mengenai hal-hal yang dilakukan selama penelitian berlangsung, mulai dari proses memodifikasi sistem disposisi surat, pembangunan perangkat lunak, hingga pengujian sistem disposisi surat menggunakan *digital signature* dengan algoritma RSA dan algoritma AES yang akan digunakan untuk menjawab apa yang sudah dirumuskan dalam rumusan masalah.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi tentang kesimpulan dari BAB IV dan saran yang akan diajukan agar dapat menjadi bahan pertimbangan untuk rekomendasi penelitian selanjunya.

Try Haryatno, 2016

IMPLEMENTASI DIGITAL SIGNATURE MENGGUNAKAN ALGORITMA KRIPTOGRAFI AES DAN ALGORITMA KRIPTOGRAFI RSA SEBAGAI KEAMANAN PADA SISTEM DISPOSISI SURAT

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

Try Haryatno, 2016

IMPLEMENTASI DIGITAL SIGNATURE MENGGUNAKAN ALGORITMA KRIPTOGRAFI AES DAN ALGORITMA KRIPTOGRAFI RSA SEBAGAI KEAMANAN PADA SISTEM DISPOSISI SURAT

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu