# BAB V
# KESIMPULAN DAN SARAN

## 5.1 Kesimpulan

Berikut kesimpulan dan saran dari penelitian Implementasi *digital signature* menggunakan algoritma AES dan algoritma RSA sebagai keamanan pada sistem disposisi surat adalah sebagai berikut:

1. Modifikasi skema *digital signature* dengan menambahkan proses enkripsi pesan dan proses enkripsi kunci saat melakukan pengiriman serta menambahkan proses dekripsi pesan dan dekripsi kunci saat menerima pesan. Enkripsi pesan dilakukan untuk memenuhi salah satu tujuan kriptografi yaitu kerahasiaan. Keakuratan pesan dapat terjamin karena *digital signature* sangat sensitif terhadap suatu perubahan data. Waktu yang diperlukan untuk eksekusi program akan bertambah karena sistem akan melakukan proses enkripsi algoritma AES dan RSA saat pengiriman pesan serta melakukan dekripsi dengan algoritma AES dan algoritma RSA saat menerima pesan.
2. Pengaruh *digital signature* menggunakan algoritma AES dan dan algoritma RSA pada sistem disposisi surat memenuhi 4 tujuan kriptografi yaitu kerahasiaan, integritas data, autentikasi dan nir-penyangkalan. *Digital signature* dapat memastikan keabsahan pengirim, keaslian pesan dan nir-penyangkalan. Algoritma AES dapat menjaga kerahasiaan dan intergritas data pesan pada proses pengiriman pesan. Dengan algoritma AES, pesan gambar seolah-olah menjadi pesan yang tidak bermakna. Autentikasi dan nir-penyangkalan dapat ditangani oleh algoritma RSA. Saat pertukaran kunci yang akan digunakan algoritma AES, kunci akan di enkripsi dan didekripsi oleh algoritma RSA dengan tujuan untuk otentikasi dan nir-penyangkalan.



**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

## 5.2. Saran

Berikut merupakan saran-saran pada penelitian ini untuk pengembangan lebih lanjut:

1. Diperlukan penelitian lebih lanjut terhadap *digital signature* baik memodifikasi skema maupun menambahkan metode seperti metode penyisipan pesan agar dapat memenuhi kebutuhan sistem disposisi surat maupun sistem informasi lainnya dan juga menambahkan skema validasi untuk memperkuat salah satu tujuan kriptografi yaitu integritas data atau keaslian pesan.
2. Menggunakan bahasa pemrograman selain PHP seperti Java atau bahasa pemrograman lainnya yang lebih cepat dalam hal proses eksekusi program, karena proses enkripsi dan dekripsi merupakan proses perhitungan transformasi matematis yang cukup rumit dan berulang-ulang.
3. Cara memperoleh *data image* yang lebih baik pada berkas jpg dengan tujuan plainteks dapat digunakan untuk proses enkripsi dan dekripsi oleh algoritma AES dan tidak terjadi *bug* atau kesalahan pada perangkat lunak.
4. Menggunakan berkas surat dengan format pdf karena pada praktiknya surat disposisi dikirim bersama lampiran dan lebih dari satu halaman. Penggunaan berkas surat dengan format pdf akan lebih efektif karena hanya dengan satu *file* saja bisa terdapat banyak halaman termasuk surat disposisi beserta lampiran surat lainnya.