# BAB V
# KESIMPULAN DAN SARAN

Pada bab ini dijelaskan mengenai kesimpulan dari penelitian yang dilakukan serta saran untuk penelitian terkait kedepannya.

## 5.1 Kesimpulan

Berdasarkan penelitian, percobaan, dan pengujian terhadap protokol keamanan pada sistem resep elektronik menggunakan *digital signature algorithm* yang dibangun, didapatkan kesimpulan sebagai berikut:

1. Pembangunan aplikasi sistem resep elektronik dengan menerapkan *digital signature algorithm, d*engan mengintegrasikannya ke dalam sistem keakuratan pesan dapat terjamin karena tanda tangan digital sangat sensitif terhadap suatu perubahan data, sehingga dapat memastikan keamanan dan keabsahan pengirim.
2. Mengamankan resep elektronik dapat dilakukan dengan cara meletakan penyandian atau penandata tanganan pada posisi dokter saat proses penulisan resep, kemudian proses verifikasi dilakukan pada posisi apoteker saat penebusan resep obat di apotek. Penambahan fitur *QR Code* digunakan untuk mempermudah dalam proses penebusan resep dan data yang tersimpan juga dipastikan aman karena dapat terlihat ketika saat proses verifikasi pemindaian *QR Code* saat melakukan penebusan resep.
3. Pembuktian otentikasi dan integritas data pada protokol sistem resep elektronik sudah memenuhi dan menjamin tujuan kriptografi yaitu kerahasiaan, integritas data, autentikasi dan nir-penyangkalan. Resep yang dibuat dan diterima dipastikan aman karena terdapat tanda tangan dari pembuat pesan. Untuk membuktikan bahwa pesan asli dikirim dari pengirim yang bersangkutan yaitu dengan cara memvalidasi nilai *hash* pesan sebelum pesan dikirimkan dan pesan sesudah dikirimkan, jika nilai *hash* sama maka tidak ada perubahan pada saat pengiriman data serta pesan resep dapat ditampilkan saat proses pemindaian *QR Code*, jika nilai *hash* tidak sama maka pesan terjadi

perubahan pada saat transmisi data dan resep tidak dapat ditampilkan.

## 5.2 Saran

Berikut merupakan saran terhadap penelitian terkait untuk pengembangan lebih lanjut:

1. Diperlukan penelitian lebih lanjut terkait sistem yang dibuat dengan penambahan administrasi harga obat. Untuk penelitian berikutnya, perlu dikembangkan sistem kriptografi yang tahan akan serangan dan manipulasi sehingga pesan dalam resep tetap dapat dijaga dalam keadaan apapun.
2. Diperlukan adanya pengembangan lebih lanjut terkait cakupan lebih banyak format seperti PDF, foto *x-ray*, video dan lainnya. Dan juga bisa dikombinasikan dengan algoritma kriptografi lainnya ataupun dengan metode steganografi.

Menggunakan bahasa pemrograman selain PHP seperti android, java, matlab, visual studio ataupun bahasa pemrograman lainnya yang lebih kompatibel.