BAB V
KESIMPULAN DAN SARAN

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

1.1. Kesimpulan

Berdasarkan penelitian, percobaan, dan pengujian terhadap sistem yang dibangun, didapatkan kesimpulan sebagai berikut:

1. Protokol keamanan diimplementasikan dalam validasi dokumen tugas kelas menggunakan *Digital Signature Algorithm* (DSA) untuk pembangkitan dan verifikasi *digital signature*, *text steganography* untuk menyisipkan *digital signature* ke dalam dokumen, dan algoritma kriptografi RC4 untuk enkripsi dan dekripsi dokumen tertanda tangan. DSA digunakan karena alasan keamanan dalam pembangkitan dan verifikasi *digital signature*, yakni DSA menawarkan kerumitan pencarian dua pasang bilangan prima yang besar. *Digital signature* menjamin tujuan kriptografi nir penyangkalan, karena perubahan sedikit saja pada dokumen dapat teridentifikasi ketidakasliannya. RC4 digunakan untuk tujuan kerahasiaan dokumen, karena DSA tidak dapat memenuhi enkripsi dan dekripsi terhadap dokumen. Kemudian untuk mengatasi pencontekan dan pengubahan dokumen yang dilakukan oleh pihak ketiga adalah dengan cara menyembunyikan *digital signature* ke dalam dokumen menggunakan *text steganography*.
2. Mengenai serangan tindak kecurangan akademik, yakni penjiplakan dan pengubahan isi dokumen yang dilakukan oleh pihak ketiga, protokol keamanan yang dibangun dapat mendeteksinya. Dilakukan 6 skenario *Man in the Middle Attack* untuk menguji ketahanan protokol keamanan terhadap serangan kecurangan akademik. Dari 6 skenario *Man in the Middle Attack*, 5 skenario terdeteksi kecurangan, dan hanya 1 skenario yang tidak terdeteksi kecurangan.
3. Dilakukan uji keacakan terhadap *chiperdoc* yang dihasilkan oleh algoritma kriptografi RC4 dengan dua tipe kunci yang berbeda, yaitu kunci biasa dan

kunci *message digest*. Hasil menunjukan *cipherdoc* yang dihasilkan dari kunci *message digest* lebih besar presentase lolos ujinya, yaitu 98,67%. Sedangkan dari kunci biasa dihasilkan presentase lolos uji 94,00%.

Dari ketiga *point* di atas, dapat disimpulkan bahwa tujuan pada penelitian ini yang dijelaskan pada BAB I tercapai. Kemudian kelebihan protokol keamanan pada penelitian ini mengacu pada kekurangan penelitian relevan adalah validasi dokumen tidak hanya dengan pembangkitan dan verifikasi *digital signature* saja, melainkan dilakukan pula enkripsi dan dekripsi dokumen tertandatangan, dan *digital signature* tidak dikirim terpisah dengan dokumen melainkan dibubuhkan atau disembunyikan ke dalam dokumen tersebut.

Di sisi lain, diperlukan penelitian lebih lanjut mengenai protokol keamanan pada penelitian ini. Seperti pada point 2 yang dijelaskan di atas, bahwa ada 1 skenario yang tidak terdeteksi kecurangan, padahal skenario tersebut termasuk skenario kecurangan akademik. Lebih jelasnya, saran untuk penelitian selanjutnya dijelaskan sebagai berikut.

1.2. Saran

Saran yang ingin penulis sampaikan untuk penelitian terkait selanjutnya yaitu:

1. Diperlukan penelitian lebih lanjut mengenai *text steganography* untuk menyisipkan *digital signature* ke dalam dokumen yang tahan terhadap manipulasi yang mengakibatkan *digital signature* rusak atau berubah nilainya.
2. Untuk kedepannya diharapkan sistem pengamanan dan validasi dokumen dapat digunakan untuk format lain selain .txt.