BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari pemaparan pada bab-bab sebelumnya maka dapat ditarik kesimpulan sebagai berikut:

1) Dari segi perancangan, *digital signature* menggunakan SHA-256 dengan skema penandatanganan Diffie-Hellman-RSA memiliki tiga proses utama yaitu pembangkitan kunci, *signing* atau penandatanganan sertifikat digital, dan *verifying* atau proses verifikasi keaslian sertifikat digital. Dari proses pembangkitan kunci akan menghasilkan sepasang kunci publik yang boleh diketahui umum dan kunci privat yang bersifat rahasia. Kunci publik digunakan untuk proses *signing*, sedangkan kunci privat digunakan untuk proses *verifying*. Selain itu *digital signature* menggunakan SHA-256 dengan skema penandatanganan Diffie-Hellman-RSA dapat diterapkan pada penandatanganan dokumen sertifikat digital dengan ekstensi .pdf.
2) *Digital signature* menggunakan SHA-256 dengan skema penandatanganan Diffie-Hellman-RSA dapat dikonstruksi menjadi sebuah program aplikasi komputer untuk memudahkan penerapan *digital signature*. Program aplikasi dibuat menggunakan bahasa pemrograman Python dengan beberapa library yang digunakan yaitu, *hashlib* untuk melakukan hash, *tkinter* untuk membuat tampilan dari program, dan webbrowser untuk memudahkan pindah dari satu menu ke menu lain. Program dibuat dengan 3 menu utama yaitu menu pembangkitan kunci, menu *signing* atau penandatanganan, dan menu *verifying* atau verifikasi keaslian dari sertifikat digital.

5.2 Saran

Adapun saran penulis untuk penelitian ini adalah:

1) Dapat dilakukan penelitian lebih lanjut mengenai keamanan dari *digital signature* ini baik dari segi fungsi hash maupun segi skema penandatanganan Diffie-Hellman-RSA, dan dapat pula mengkaji mengenai waktu yang dibutuhkan untuk melakukan kriptanalisis skema Diffie-Hellman-RSA

2) Dapat dikaji mengenai penandatanganan digital dengan dokumen lain semisal video.
3) Dapat dilakukan penelitian untuk meningkatkan keamanan *digital signature* dengan mengimplementasikan fungsi hash yang lebih kompleks dan lebih aman.
4) Dapat pula dikaji mengenai efisiensi skema penandatanganan Diffie-Hellman-RSA dengan skema penandatanganan lainnya.
5) Hasil penelitian ini dapat diimplementasikan pada suatu lembaga atau instansi yang melakukan verifikasi keaslian suatu dokumen digital.