BAB V
PENUTUP

5.1. Kesimpulan

Berdasarkan penelitian yang telah dilakukan, dapat disimpulkan bahwa kombinasi algoritma MD5 dan Elgamal dapat digunakan untuk menjaga integritas dokumen, khususnya ijazah. Berdasarkan hasil pengujian, proses *hashing* yang dilakukan oleh MD5 dapat menghasilkan nilai yang berbeda terhadap isi data maupun dokumen, meskipun hanya sedikit perubahan pada dokumen tersebut. Hal ini menunjukkan MD5 sensitif terhadap modifikasi isi file.

Setelahnya, algoritma Elgamal yang digunakan untuk menandatangani nilai hash tersebut, akan menghasilkan *ciphertext* yang akan diubah ke dalam QR Code dan disisipkan ke dalam file ijazah. QR Code digunakan untuk menyederhakan *ciphertext*, sehingga mempersingkat proses verifikasi. Proses verifikasi tetap dapat dijalankan dengan baik meskipun terjadi perubahan kombinasi kunci setelah proses *signing*. Hal ini disebabkan kunci publik yang digunakan untuk proses verifikasi telah tercantum pada QR Code saat proses *signing*. Proses verifikasi dapat dilakukan oleh siapapun juga yang ingin melakukan verifikasi data yang tersimpan di database. Hal ini bertujuan untuk mempermudah pengguna dalam memverifikasi keaslian dokumen secara mandiri tanpa harus login terlebih dahulu.

5.2. Saran

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, disarankan agar ke depannya dilakukan pengembangan dengan menambahkan tautan pada QR-Code. Dengan demikian, saat QR-Code dipindai, sistem akan secara otomatis membuka situs web dan langsung menjalankan proses verifikasi.