# BAB V

# PENUTUP

## V.1 Kesimpulan

Berdasarkan hasil dari penelitian yang telah dilakukan, penulis dapat menarik kesimpulan sebagai berikut:

a. Model pengamanan berkas menggunakan kriptografi asimetri RSA dan algoritma kompresi PPM mampu mengamankan berkas karena memiliki hasil *ciphertext* yang dihasilkan bersifat acak. Proses *encode* yang diawali dengan mengompresi berkas mampu mengurangi redudansi data dan proses enkripsi berkas mampu mengubah isi berkas, sehingga berkas tidak dapat dimaknai isinya oleh orang yang tidak memiliki kunci privat untuk memaknai isi berkas tersebut. Proses *decode* yang diawali dengan mendekripsi berkas mampu membalikan isi berkas ke sedia kala, sehingga berkas kembali dapat dimaknai oleh orang yang memiliki kunci privat untuk memecahnya dan proses dekompres akan mengembalikan ukuran berkas ke sedia kala.

b. Dengan membandingkan penelitian sebelumnya yang menggunakan kompresi LZW dan kriptografi *Twofish* dari pengujian yang menggunakan 30 berkas, hasil yang didapat berupa model pengamanan berkas ini memiliki rasio kompresi rata-rata sebesar 15,3031% dan waktu pemrosesan sebesar 0,8485 detik dengan rata-rata ukuran berkas sebesar 885.368 *bytes*. Sedangkan pada penelitian ini yang menggunakan kompresi PPM dan kriptografi RSA yang menggunakan 50 berkas, hasil yang didapat berupa model pengamanan berkas ini memiliki rasio kompresi rata-rata sebesar 32,0667% dan waktu pemrosesan sebesar 1,1430 detik dengan rata-rata ukuran berkas sebesar 28.280 *bytes*. Model pengamanan menggunakan kompresi PPM dan kriptografi RSA memiliki waktu pemrosesan lebih besar dengan selisih sebesar 0,2945 detik, meskipun rata-rata ukuran berkas yang digunakan lebih kecil dengan selisih -857.088 *bytes* dibandingkan dengan model LZW *Twofish* dikarenakan kriptografi RSA memiliki kombinasi kunci yang besar, sehingga pemrosesan enkripsinya memakan waktu yang lebih lama. Sedangkan rata-rata rasio kompresi dari model pengamanan menggunakan kompresi PPM dan kriptografi RSA lebih besar dengan selisih sebesar 16,7636%. Hasil dari perhitungan waktu komputasi dan rasio kompresi dapat dilihat dalam tabel 4.4.

c. Waktu komputasi proses *encode* dan *decode* berbanding lurus dengan ukuran berkas yang digunakan. Semakin besar ukuran berkas yang digunakan, maka semakin banyak waktu komputasi yang digunakan. Proses *encode* juga memakan waktu yang lebih banyak dibanding proses *decode* dengan rata-rata waktu komputasi proses *encode* sebesar 1,1430 detik, sedangkan *decode* sebesar 0,0177 detik, sehingga selisih dari waktu komputasi keduanya adalah 1,1253 detik, dengan proses *encode* sebagai proses yang memakan waktu komputasi lebih besar. Hasil dari perhitungan waktu komputasi proses *encode* dapat dilihat dalam tabel 4.4, sedangkan *decode* dalam tabel 4.5.

d. Hasil komputasi dengan menggunakan perangkat dengan spesifikasi yang berbeda juga memengaruhi waktu komputasi. Spesifikasi perangkat yang memiliki RAM, dan SSD atau HDD yang berbeda memiliki peran terhadap perbedaan hasil komputasi. Semakin besar spesifikasinya maka semakin cepat waktu komputasinya. Perangkat 1 dengan RAM 8 GB HDD 500 GB menghasilkan waktu komputasi sebesar 0,33 detik yang ditunjukan dalam tabel 4.6. Perangkat 2 dengan RAM 16 GB HDD 1000 GB SSD 240 GB menghasilkan waktu komputasi sebesar 0,1246 detik yang ditunjukan dalam tabel 4.7. Perangkat 3 dengan RAM 2 GB HDD 320 GB menghasilkan waktu komputasi sebesar 0,98 detik yang ditunjukan dalam tabel 4.8.

e. Kompresi PPM mampu mengurangi waktu pemrosesan berkas. Dari hasil pengujian model pengamanan berkas yang menggunakan kompresi PPM dan kriptografi RSA dan model pengamanan berkas yang hanya menggunakan RSA saja memiliki waktu pemrosesan yang berbeda dengan selisih sebesar 2,6023 detik, dimana yang menggunakan kompresi PPM memiliki waktu pemrosesan 0,3323 detik yang bisa dilihat pada tabel 4.10, sedangkan yang tidak menggunakan kompresi PPM memiliki waktu pemrosesan 2,9346 detik yang bisa dilihat pada tabel 4.11.

f. *Server* yang digunakan berpengaruh dalam waktu pemrosesan berkas. Dari hasil pengujian model pengamanan berkas yang menggunakan *server* dimana satu *server* terdapat lebih dari satu *website* dengan spesifikasi yang kurang lebih sama dengan *server* lain yang hanya terdapat satu *website*, waktu pemrosesan yang dihasilkan berbeda, dimana pada *server* yang hanya terdapat satu *website* memiliki waktu pemrosesan yang lebih cepat. Hal ini didasari karena dengan spesifikasi yang sama, *server* yang terdapat lebih dari satu *website* didalamnya harus membagi *disk space*-nya ke sejumlah *website* yang ada, sehingga tidak menggunakan keseluruhan *disk space* yang

disediakan. Jadi, semakin besar *disk space* dan *bandwidth* yang digunakan, maka semakin cepat waktu pemrosesannya.

g. Koneksi internet yang digunakan berpengaruh dalam waktu pemrosesan berkas. Dari hasil pengujian model pengamanan berkas dengan menggunakan tiga koneksi internet yang berbeda waktu pemrosesan yang dihasilkan juga berbeda. Semakin besar kecepatan koneksi internet yang digunakan, maka semakin cepat waktu pemrosesannya. Percobaan pertama, yang dapat dilihat dari tabel 4.14, dengan koneksi mengunggah sebesar 15,98 Mbps dan mengunduh 31,20 Mbps menghasilkan waktu komputasi sebesar 0,2469 detik, percobaan kedua, yang dapat dilihat dari tabel 4.15, dengan koneksi mengunggah sebesar 2,98 Mbps dan mengunduh 8,72 Mbps menghasilkan waktu komputasi sebesar 0,2676 detik, dan percobaan ketiga, yang dapat dilihat dari tabel 4.16, dengan koneksi mengunggah sebesar 3,69 Mbps dan mengunduh 10,10 Mbps menghasilkan waktu komputasi sebesar 0,26 detik.

## V.2 Saran

Berdasarkan hasil dari penelitian yang telah dilakukan, penulis memiliki beberapa saran yang dapat diberikan untuk penelitian selanjutnya, diantaranya:

1. Penggunaan algoritma kompresi selain PPM untuk memberikan hasil kompresi yang berbeda yang memiliki performa lebih baik, misalnya bzip2, *Associative Coder of Buyanovsky* (ACB), *Dynamic Markov Compression*, dan lain sebagainya.

2. Model pengamanan berkas ini hanya bisa digunakan dengan mengakses *website*, diharapkan kedepannya dapat dikembangkan menjadi *mobile application*.

3. Model pengamanan berkas ini hanya menerima berkas dengan format *string*, diharapkan kedepannya dapat dikembangkan untuk menerima format gambar, *video*, atau *audio*.