BAB V
PENUTUP

5.1. Kesimpulan

Berdasarkan penelitian yang telah dilakukan dan diuraikan pada bab-bab sebelumnya, maka pada bab ini diuraikan mengenai kesimpulan yang didapatkan, yaitu :

1. Penerapan algoritma Camellia dan DM-RSA pada skema *hybrid cryptography* dilakukan berdasarkan dengan rancangan *flowchart* yang telah dilakukan pada Bab 3. *Flowchart* dari algoritma-algoritma tersebut dapat dilihat pada Gambar 3.5 hingga Gambar 3.9 dan untuk penerapan dalam bentuk kode dapat dilihat pada Kode Program 1 hingga 17.
2. Pengembangan aplikasi dengan mengimplementasikan skema *hybrid cryptosystem* menggunakan algoritma DM-RSA dan Camellia serta metode E2EE memiliki tahapan yang dimulai dengan studi literatur, perancangan aplikasi, perancangan algoritma, dan pengujian. Pengembangan dimulai dengan perancangan atas tampilan dan alur dari proses tiap algoritma kriptografi. Setelah itu dilanjutkan dengan mengimplementasikan seluruh rancangan dan melakukan pengujian pada hasil implementasi tersebut. Penelitian ini berhasil menerapkan skema *hybrid cryptography* dengan menggunakan algoritma Camellia dan DM-RSA dan metode E2EE untuk sistem pengiriman *file*. Hasil akhir atau *output* yang dihasilkan selain hasil pengujian adalah aplikasi *desktop* yang menerapkan seluruh rancangan dan berhasil melalui seluruh pengujian.
3. Berdasarkan hasil dari pengujian *benchmark* atau kecepatan yang telah dilakukan, didapatkan bahwa skema *hybrid cryptosystem* pada skenario ukuran 600MB dan 1200MB memiliki performa yang serupa dengan perbedaan waktu tempuh sebanyak 25.2% dengan algoritma Camellia sebagai algoritma tercepat dalam hasil pengujian. Waktu tempuh untuk algoritma *hybrid* memiliki nilai yang tinggi untuk skenario ukuran data 20MB, yaitu 24.2% lebih lambat dari algoritma RSA, 338.5% lebih lambat dari algoritma AES, 1010.1% lebih lambat dari algoritma Camellia, dan 376.5% lebih cepat dibandingkan algoritma DM-RSA. Hal ini dikarenakan

proses pembangkitan kunci algoritma DM-RSA yang digunakan pada algoritma *hybrid*. Sedangkan, untuk skenario ukuran data 600MB dan 1200MB, waktu tempuh untuk pembangkitan kunci menjadi cukup bias, dikarenakan proses enkripsi dan dekripsi menjadi lebih dominan dengan digunakannya ukuran data yang besar. Sedangkan dibandingkan dengan algoritma DM-RSA, skema *hybrid cryptosystem* memiliki waktu tempuh 376.5% lebih pendek. Hal ini membuktikan bahwa skema *hybrid cryptosystem* memberikan dampak yang signifikan dalam kecepatan proses enkripsi dan dekripsi untuk algoritma Camellia dan DM-RSA.

5.2. Saran

Adapun beberapa saran yang dapat digunakan oleh penelitian selanjutnya berdasarkan dari hasil dan pengamatan yang dilakukan selama penelitian skripsi ini, antara lain:

1. Proses enkripsi pada aplikasi dilakukan secara *sequential* untuk tiap *block*. *Multithreading* dapat digunakan untuk melakukan proses enkripsi dan dekripsi dengan memecah *block* menjadi beberapa bagian dan menugaskan setiap bagian pada *thread* yang berbeda. Metode ini dapat meningkatkan performa atau kecepatan dari proses enkripsi dan dekripsi dari skema *hybrid cryptosystem* yang digunakan dalam penelitian ini.
2. Menggunakan metode yang lebih cepat untuk menentukan bilangan prima, karena bilangan prima sendiri merupakan komponen yang penting pada algoritma DM-RSA. Dengan menggunakan metode penentuan bilangan prima yang lebih cepat, maka dapat mengurangi waktu tempuh pada algoritma DM-RSA pada pembangkitan kunci. Contoh dari metode penentuan bilangan prima lainnya adalah *sieve of eratosthenes, sieve of sundaram, sieve of atkin* dan masih banyak lainnya.