BAB VI

PENUTUP

Berdasarkan hasil penelitian yang telah dibahas pada bab sebelumnya, maka pada bab ini akan disampaikan kesimpulan dan saran dari Penerapan Algoritma RSA dan AES 256 pada Pengamanan Data Transaksi Foodmochi Sukoharjo.

6.1 Kesimpulan

Berdasarkan pembahasan yang telah dilakukan pada bab sebelumnya, maka pada penelitian ini dapat ditarik kesimpulan yaitu:

1. Telah terciptanya sebuah sistem keamanan data transaksi pada Foodmochi Sukoharjo menggunakan algoritma RSA dan AES 256 bit dengan hasil data acak pada *database.*
2. Hasil pengujian validitas enkripsi dan dekripsi data sesuai harapan peneliti yaitu setiap data inputan atau *plaintext* yang di enkripsi menggunakan algoritma RSA dan AES 256 bit dan menghasilkan data *chipertext* akan di dekripsi menggunakan algoritma AES 256 bit dan RSA yang menghasilkan data yang sama dengan *plaintext.*
3. Hasil performa enkripsi dan dekripsi data, algoritma RSA memiliki waktu kecepatan yang lebih baik daripada algoritma AES 256 bit yaitu rata-rata kecepatan enkripsi algoritma RSA adalah 0.001605 detik, sedangkan algoritma AES adalah 0.120993 detik. Pada proses dekripsi, algoritma AES 256 bit lebih unggul dibandingkan algoritma RSA yaitu rata-rata

kecepatan dekripsi AES adalah 0.093832 detik, sedangkan algoritma RSA adalah 4.582242 detik.

6.2 Saran

Adapun saran yang dapat disampaikan peneliti agar penelitian selanjutnya terus berkembang yaitu :

1. Pada penelitian ini menggunakan 2 algoritma untuk enkripsi dan dekripsi data, untuk pengembangan penelitian selanjutnya dapat menggunakan 3 algoritma atau lebih.
2. Pada penelitian ini proses enkripsi menggunakan algoritma RSA jika menggunakan bilangan prima untuk memilih *p* dan *q* dengan angka *range* 1000-2000 mengalami kendala pada proses dekripsi yaitu lamanya waktu yang dibutuhkan untuk mendekripsi suatu data dan eksekusi php maksimal adalah 30 detik. Untuk penelitian selanjutnya, bisa dengan cara menggunakan *temperory* file untuk menyimpan data hasil proses dekripsi pertama dan selanjutnya akan dilakukan proses dekripsi kedua dengan mengambil data di *temperory* file proses dekripsinya. Sehingga proses dekripsi tidak memakan waktu yang terlalu lama.
3. Pada penelitian ini pengujian enkripsi data hanya menguji validitas dan performa enkripsi dekripsi pada algoritma RSA dan AES 256 bit, untuk pengembangan penelitian selanjutnya dapat menguji keamanan data.