Hak cipta dan penggunaan kembali:

Lisensi ini mengizinkan setiap orang untuk menggubah, memperbaiki, dan membuat ciptaan turunan bukan untuk kepentingan komersial, selama anda mencantumkan nama penulis dan melisensikan ciptaan turunan dengan syarat yang serupa dengan ciptaan asli.

Copyright and reuse:

This license lets you remix, tweak, and build upon work non-commercially, as long as you credit the origin creator and license it on your new creations under the identical terms.

Perpustakaan Univeristas Multimedia Nusantara

BAB V

SIMPULAN DAN SARAN

5.1 Simpulan

Dari penelitian ini, didapatkan bahwa sirkuit kuantum Shor telah berhasil diimplementasikan untuk peretasan kriptografi RSA. Berdasarkan hasil pada penelitian ini, terdapat beberapa simpulan lain yang didapatkan yaitu sebagai berikut.

1. Implementasi sirkuit kuantum Shor untuk peretasan RSA pada penelitian ini telah berhasil dimplementasikan dan dapat digunakan untuk melakukan peretasan terhadap kriptografi RSA yang telah di implementasikan. Implementasi yang dibuat dapat digunakan saat sudah ada backend yang mempunyai qubit dengan jumlah besar, untuk melakukan peretasan kepada system kriptografi RSA dengan jumlah bit yang lebih besar.
2. Performa implementasi sirkuit kuantum Shor untuk peretasan sistem kriptografi rsa berhasil diukur. durasi *user time* untuk melakukan peretasan RSA dengan menggunakan sirkuit kuantum Shor pada penelitian ini bergantung kepada jumlah *qubit* yang digunakan oleh sirkuit. Skenario pertama dengan 18 *qubit* memakan waktu 20 detik, skenario kedua dengan 22 *qubit* memakan waktu 194 detik, skenario ketiga dengan 26 *qubit* memakan waktu 2,395 detik, skenario keempat dengan 26 *qubit* memakan waktu 1,935 detik, skenario kelima dengan 26 *qubit* memakan waktu 6,417 detik, skenario keenam dengan 26 *qubit* memakan waktu 34,086 detik.

5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, ada beberapa saran untuk pengembangan penelitian lebih lanjut, yaitu sebagai berikut.

1. Mengembangkan aspek skalabilitas dari implementasi sirkuit kuantum Shor agar dapat mengurangkan penggunaan jumlah *qubit* untuk melakukan pemfaktoran *N* yang bernilai lebih besar.
2. Melakukan uji coba dan evaluasi berdasarkan hasil yang didapatkan dari menjalankan sirkuit kuantum Shor pada komputer kuantum sungguhan yang mempunyai *qubit* yang mencukupi untuk menjalankan sirkuit kuantum Shor untuk peretasan kriptografi RSA dengan ukuran *key* yang besar.