

## BAB V

### KESIMPULAN DAN SARAN

#### 5.1 Kesimpulan

Kesimpulan dari penelitian modifikasi algoritma whirlpool, dan implementasi qr code pada sistem transaksi digital yang sudah dimodifikasi, algoritma whirlpool dan fungsi hash ke dalam aplikasi sistem transaksi digital berbasis android adalah sebagai berikut :

1. Hasil dari implementasi whirlpool dalam mengembangkan aplikasi keamanan sistem transaksi digital menunjukkan bahwa whirlpool dapat diimplementasikan dengan baik. sehingga hasil implementasi tersebut dapat digunakan dalam qr code dan fingerprint sebagai tambahan keamanan dalam bertransaksi. sehingga dari penelitian yang telah dilakukan dapat disimpulkan bahwa algoritma ini tahan terhadap kriptanalisis. Hasil dari pengujian aplikasi sistem transaksi digital dengan menggunakan man-in-the-middle-attack menunjukkan bahwa aplikasi sistem keamanan transaksi digital tahan terhadap kriptanalisis.
2. hasil implementasi dari qr code dan fingerprint pada aplikasi sistem keamanan transaksi digital menunjukkan bahwa penggunaan qr code dan fingerprint pada saat proses transaksi sangat baik. Karena pengguna qr payment dan fingerprint akan terus berkembang di indonesia dan akan menjadi salah satu pembayaran/transaksi utama dalam sebuah transaksi, dan memudahkan pengguna dalam melakukan proses transaksi. selain itu juga tingkat keamanan dari qr payment dan fingerprint sangat aman untuk digunakan dalam proses transaksi.
3. Pengujian aplikasi sistem transaksi digital dengan *Man-in-the-Middle-Attack* pada saat proses modifikasi berlangsung, menunjukkan bahwa sistem keamanan transaksi digital ini tahan terhadap kriptanalisis. Karena serangan kriptanalisis akan membutuhkan waktu yang lebih lama untuk memecahkan atau membongkar suatu ciphertext dari semua kemungkinan.

## 5.2 Saran

Berikut merupakan saran-saran pada penelitian ini untuk pengembang lebih lanjut:

1. Untuk penelitian selanjutnya modifikasi pada algoritma whirlpool di dalam aplikasi node js ini dapat melakukan proses hash lebih dari 1 blok. Dan juga bisa dikombinasikan dengan algoritma kriptografi lainnya seperti SHA,AES, dll.
2. Untuk penelitian selanjutnya, pada aplikasi sistem transaksi digital ini dapat memberikan integritas data. Dan juga bisa dikembangkan lebih lanjut untuk aplikasi lainnya seperti E-Tol, E-Money dll.