BAB V

KESIMPULAN DAN SARAN

Dalam bab ini akan dijelaskan tentang kesimpulan dari penulisan tugas akhir dan percobaan yang telah dilakukan serta terdapat saran pengembangan untuk bahasan tugas akhir ini.

5.1 Kesimpulan

1 Program MD5 berjalan sesuai dengan algoritmanya setelah dibandingkan dengan hasil dari memo Ron Rivest

2 Fungsi *hash* adalah fungsi matematis yang mengambil input panjang variabel dan mengubahnya ke dalam urutan biner dengan panjang yang tetap. Sifat dari fungsi *hash* yaitu perubahan satu bit saja akan menghasilkan keluaran/nilai *hash* yang berbeda. Tujuan fungsi *hash* untuk menjamin integritas data.

3 Perubahan satu karakter dalam MD5 merubah keluaran dari MD5

4 MD5 dengan digital signature mampu menjaga integritas data dari pada hanya MD5

5.2 Saran

Adapun beberapa saran pengembangan terhadap tugas akhir ini adalah:

1 Dalam Algoritma MD 5 masih dapat dikembangkan lagi salah satunya dengan mengubah aturan dari padding bit dengan mengubah bit pertama 0 serta selanjutnya 1.
2 Mengubah dari fungsi-fungsi F, G, H, dan I.