BAB V

KESIMPULAN DAN SARAN

5. 1 Simpulan

Dari dari analisis dan perancangan aplikasi keamanan data teks menggunakan algoritma SHA dan telah dilakukan juga pengujian terhadap aplikasi maka di dapatkan kesimpulan sebagai beriku:

1. *Secure Hash Algorithm* mempunyai cara kerja yang sangat unik yaitu *Secure Hash Algorithm* memiliki nilai awal yang sudah ditentukan untuk setiap iterasi hash. Nilai-nilai ini dihasilkan dari beberapa bilangan prima. Pesan yang akan di-hash dibagi menjadi blok-blok yang lebih kecil. Setiap blok biasanya memiliki panjang 512-bit. Pesan diisi atau dipad dengan bit tambahan agar memiliki panjang yang sesuai dengan aturan algoritma. *Padding* dilakukan agar panjang pesan dapat dibagi dengan 512. Setiap blok pesan diolah dengan menggunakan variabel-variabel sementara, dan ini dilakukan berulang kali untuk setiap blok. Setiap blok pesan diolah melalui serangkaian putaran. Jumlah putaran bergantung pada versi *SHA* yang digunakan (misalnya, *SHA-256* memiliki 64 putaran). Fungsi kunci menggabungkan nilai-nilai variabel sementara untuk menghasilkan nilai *hash* yang baru. Sesudah semua blok pesan diolah, nilai hash akhir dihasilkan. Nilai ini biasanya berupa serangkaian bit dengan panjang tertentu, seperti 256-bit untuk *SHA-256*.
2. langkah-langkah mengimplementasikan algoritma *SHA* dalam perancangan aplikasi keamanan data teks:

- Ambil data teks yang ingin diamankan.

- Konversi data teks menjadi format yang dapat diproses oleh algoritma *SHA*, seperti *ASCII* atau *Unicode.*
- Jalankan algoritma *SHA* pada data teks untuk menghasilkan nilai *hash.*
- Simpan nilai *hash* yang dihasilkan ke dalam *database* atau file terpisah.
- Saat ingin memverifikasi keaslian data teks, ambil kembali data teks yang ingin diverifikasi dan jalankan algoritma *SHA* pada data tersebut.
- Bandingkan nilai hash yang dihasilkan dengan nilai hash yang disimpan sebelumnya. Jika kedua nilai hash sama, maka data teks tersebut dapat dipastikan keasliannya.

Dengan mengimplementasikan algoritma *SHA* dalam perancangan aplikasi keamanan data teks, data teks dapat diamankan dengan lebih baik dan dapat dipastikan keasliannya.

5. 2 Saran

Untuk *SHA 256* ini agar lebih mendalami dan mengembangkan di bagian sisi blockhain, karena pembahasan *blockhain* sendiri lebih luas pembahasannya. Dan saran penelitian ini dikembangkan lagi dengan menambahkan metode *HMAC-SHA 256* untuk mendapatkan keamanan yang lebih akurat lagi dan testing pada aplikasi *SHA 256* ini boleh di coba improve lagi di bagian testingnya, mungkin ada test lainnya yang bisa di implementasikan.