BAB 6

KESIMPULAN DAN SARAN

Pada bab ini akan dibahas mengenai kesimpulan dan saran dari hasil penyusunan skripsi.

6.1 Kesimpulan

Subbab ini akan membahas mengenai kesimpulan dari hasil penyusunan skripsi yang telah dikerjakan. Kesimpulan dari skripsi ini diperoleh setelah melakukan beberapa langkah-langkah pengerjaan skripsi. Berikut adalah langkah-langkah pengerjaan skripsi yang telah dilakukan:

1. Mempelajari cara kerja metode *secret sharing* Shamir
2. Mempelajari cara kerja metode *secret sharing* Blakley
3. Membangun perangkat lunak yang dapat mengimplementasikan pembagian *password* menggunakan metode *secret sharing* Shamir dan metode *secret sharing* Blakley.

Setelah melakukan langkah-langkah tersebut, penulis dapat memperoleh kesimpulan bahwa metode *secret sharing* Shamir dan metode *secret sharing* Blakley dapat diimplementasikan untuk membagikan *password* dengan menggunakan perangkat lunak yang telah dibangun. Penulis juga memperoleh kesimpulan berdasarkan hasil pengujian fungsional dan pengujian eksperimental pada perangkat lunak yang dibangun. Pada Bab 5 Implementasi dan Pengujian dapat dilihat rincian dari hasil pengujian fungsional dan pengujian eksperimental yang telah dilakukan.

Berdasarkan pengujian fungsional yang telah dilakukan, dapat disimpulkan bahwa perangkat lunak yang dibangun telah berhasil mengimplementasikan penggunaan metode *secret sharing* Shamir dan metode *secret sharing* Blakley. Pada Subbab 5.2, dapat dilihat bahwa perangkat lunak berhasil menampung masukan dari pengguna dan melakukan proses pembagian *password* dan penggabungan *share* dengan menggunakan metode *secret sharing* Shamir dan metode *secret sharing* Blakley.

Berdasarkan pengujian yang dilakukan pada Subbab 5.3, dapat disimpulkan bahwa perangkat lunak dapat mengimplementasikan penggunaan metode *secret sharing* Shamir untuk membagikan *password* tanpa membatasi panjang karakter dari masukan *password*. Berdasarkan pengujian tersebut juga dapat disimpulkan bahwa panjang karakter *password* yang ingin dibagikan dengan menggunakan metode *secret sharing* Blakley maksimal 15 karakter. Seperti yang sudah dibahas sebelumnya pada Subbab 3.2.2, proses rekonstruksi pada metode *secret sharing* Blakley memanfaatkan penggunaan operasi baris elementer, sehingga panjang karakter *password* yang menjadi masukan sangat mempengaruhi hasil dari operasi baris elementer yang dilakukan. Semakin panjang karakter *password* yang dimasukkan, maka akan semakin besar juga nilai desimal dari *password* yang disimpan. Hasil dari operasi baris elementer yang dilakukan akan menghasilkan keluaran yang tidak sesuai dengan yang diharapkan apabila nilai desimal yang dihitung terlalu besar, karena akan semakin kecil kemungkinan ditemukan nilai desimal unik yang merepresentasikan *password*. Sehingga dapat disimpulkan bahwa pada skripsi ini maksimal panjang karakter *password* yang dapat dimasukkan pada metode *secret sharing* Blakley adalah 15 karakter.

6.2 Saran

Berikut adalah beberapa saran untuk pengembangan skripsi ini lebih lanjut :

- Pada skripsi ini, *share* yang dihasilkan perangkat lunak berupa deretan angka. Pada pengembangan selanjutnya *share* yang dihasilkan dapat dikembangkan menjadi kombinasi dari angka dan huruf alfabet.
- Metode *secret sharing* Blakley yang diimplementasikan pada skripsi ini menggunakan skema *secret sharing* $(3, 3)$. Metode ini dapat dikembangkan sehingga dapat mengimplementasikan pembagian *password* dengan menggunakan skema (k, n) dengan nilai k dan n yang dapat ditentukan dengan bebas.
- Perangkat lunak yang dibangun pada skripsi ini hanya dapat mengimplementasikan metode *secret sharing* Blakley dengan masukan *password* yang memiliki panjang maksimal 15 karakter. Untuk pengembangan selanjutnya, dapat dibangun perangkat lunak yang dapat mengimplementasikan metode *secret sharing* Blakley tanpa membatasi panjang karakter dari masukan *password*.

DAFTAR REFERENSI

[1] Stamp, M. (2006) *Information Security: Principles and Practice*, 1st edition. John Wiley and Sons, Hoboken.

[2] Forouzan, B. A. (2008) *Cryptography and Network Security*. McGraw-Hill, London.

[3] van Tilborg, H. C. A. (1999) *Fundamentals of Cryptology: A Professional Reference and Interactive Tutorial*. Kluwer Academic Publisher, Eindhoven.

[4] Mao, K. H. (2004) Secret sharing schemes: A cryptographic application of finite projective geometry. Skripsi. National University of Singapore, Singapore.

[5] Munir, R. (2006) *Kriptografi*, 1st edition. Informatika Bandung, Bandung.

[6] Bozkurt, I. N., Kaya, K., Selcuk, A. A., dan Guloglu, A. M. (2008) Threshold cryptography based on blakley secret sharing. *3rd Information Security and Cryptology Conference With International Participation*, Ankara, Turkey, 25-27 December, pp. 183–186. Bildiriler KitabyÌĄ, Turkey.

[7] Ragucci, J. (2008) Shared secret cryptography. http://www.demoivre.org/courses/CIS628/chapter15.pdf. 25 October 2017.

[8] Mackenzie, C. E. (1980) *Coded Character Sets: History and Development*, 1st edition. Addison-Wesley Publishing Company, Boston.

[9] Hicklin, J., Moler, C., Webb, P., Boisvert, R., Miller, B., Pozo, R., dan Remington, K. (1998) Jama: A java matrix package. math.nist.gov/javanumerics/jama/. 30 November 2017.