BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil dan pembahasan penelitian pada bab sebelumnya, diperoleh kesimpulan sebagai berikut:

1. Skema kriptografi hibrida *Blum Blum Shub*-Vernam *Cipher* dan Merkle Hellman *Knapsack* dimulai dengan proses pembangkitan kunci untuk mendapatkan kunci publik dari algoritma Merkle-Hellman *Knaspsack*. Selanjutnya dilakukan proses enkripsi terhadap plainteks dengan membangkitkan kunci Vernam terlebih dahulu menggunakan algoritma *Blum Blum Shub* kemudian plainteks dienkripsi menggunakan algoritma Vernam *Cipher*. Setelah itu, dilakukan proses enkripsi terhadap kunci Vernam menggunakan algoritma Merkle-Hellman *Knapsack* (kunci publik). Hasil dari proses enkripsi adalah berupa cipherteks dan *cipherkeys*. Selanjutnya dilakukan proses dekripsi terhadap *cipherkeys* menggunakan algoritma Merkle-Hellman *Knapsack* (kunci privat). Setelah diperoleh kunci Vernam, dilakukan proses dekripsi terhadap cipherteks menggunakan algoritma Vernam *Cipher* sehingga diperoleh plainteks.
2. Program aplikasi dikonstruksi menggunakan bahasa *Graphical User Interface* (GUI) Python. Terdapat 4 menu utama, yaitu pembangkitan kunci, enkripsi, dekripsi dan uji *avalanche effect*. Menu pembangkitan kunci dan dekripsi digunakan oleh Bob atau penerima pesan untuk mengembalikan pesan bersandi. Menu enkripsi digunakan oleh Alice atau pengirim pesan untuk penyandian pesan. Sementara itu, menu uji *avalanche effect* digunakan untuk mengukur tingkat keamanan kriptografi.
3. Pengujian *Avalanche Effect* menunjukkan bahwa kombinasi *Blum Blum Shub* dan Vernam *Cipher* menghasilkan rata-rata 55.625% perubahan bit pada cipherteks, mendekati nilai ideal 50%. Hal ini mengindikasikan sifat

Avalanche Effect yang kuat, sehingga meningkatkan keamanan sistem secara keseluruhan. Akan tetapi, meskipun kriptografi Merkle-Hellman *Knapsack* memiliki nilai yang tergolong rendah, kriptografi ini memiliki dasarr matematis yang kuat karena didasarkan pada *knapsack problem*.

5.2 Saran

Setelah melakukan penelitian mengenai implementasi kriptografi hibrida *Blum Blum Shub*-Vernam *Cipher* dan Merkle-Hellman *Knapsack* dalam penyandian pesan teks terdapat beberapa saran dari penulis untuk penelitian selanjutnya, yaitu sebagai berikut.

1. Menggunakan algoritma asimetris yang berbeda untuk meningkatkan keamanan pesan, seperti RSA dan lainnya.
2. Selain pengujian *Avalanche Effect*, disarankan untuk melakukan pengujian lainnya seperti pengujian *known plaintext attack* untuk menguji resistensi terhadap serangan kriptanalisis dan pengujian lainnya.
3. Mengembangkan penggunaan algoritma ini pada objek lain, seperti gambar, audio ataupun video.