BAB V
SIMPULAN, IMPLIKASI, dan REKOMENDASI

5.1 Simpulan

Berdasarkan rumusan masalah dan tujuan penelitian serta hasil yang diperoleh dari penelitian ini, dapat disimpulkan bahwa penelitian Perancangan Algoritma Kriptografi *Block Cipher* Berbasis Permainan Pola Catur Sebagai Kunci Dinamis menghasilkan kesimpulan sebagai berikut:

1. Hasil pengujian algoritma ini menunjukkan nilai koefisien korelasi terlemah sebesar 0,00852, yang berarti bahwa plainteks dan cipherteks memiliki korelasi yang sangat lemah, sehingga proses kriptanalisis menjadi sangat sulit dilakukan. Selain itu, nilai rata-rata keseluruhan *Avalanche Effect* dari hasil pengujian adalah 49,1739%. Hasil ini dapat dikategorikan baik, karena berada dalam rentang 45 hingga 60%, dengan hasil yang sangat baik diperoleh jika nilai mendekati 50% (Echeverri, 2017).
2. Algoritma ini tidak menggunakan satu pola statis, namun pola dapat dibuat berbeda-beda oleh pengguna. Pola-pola ini dihasilkan oleh permainan pola catur yang dijadikan sebagai kunci kedua pada algoritma ini. Dengan memanfaatkan kunci pertama berupa 8 karakter atau setara dengan 64-bit dan sebuah matriks 8x8 (juga setara dengan 64-bit) yang dihasilkan dari permainan pola catur, algoritma ini menciptakan alternatif di mana kekuatan kuncinya setara dengan kunci 128-bit, namun tanpa perlu memasukkan kunci sepanjang 16 karakter.
3. Program aplikasi *website* dibuat menggunakan bahasa pemrograman *python*. Aplikasi *website* ini berhasil dirancang sesuai dengan perencanaan awal, termasuk pengujian fungsionalitas enkripsi dan dekripsi yang telah diuji secara manual.

5.2 Implikasi

Dengan mengacu pada hasil penelitian dan kesimpulan yang telah dikemukakan di atas, terdapat beberapa implikasi dalam bidang keamanan data digital. Algoritma ini dapat diterapkan dalam sistem kriptografi yang membutuhkan keamanan tinggi dan fleksibilitas kunci. Misalnya, dalam

aplikasi *website* atau perangkat lunak yang memerlukan perlindungan data dengan tingkat keamanan yang tinggi tetapi tidak ingin menggunakan kunci panjang. Penelitian ini juga dapat membuka jalan bagi pengembangan lebih lanjut dalam desain algoritma kriptografi yang memanfaatkan pola dinamis dan pendekatan kreatif seperti permainan pola catur untuk meningkatkan keamanan dan efisiensi.

5.3 Rekomendasi

Rekomendasi untuk melanjutkan pengembangan algoritma ini adalah sebagai berikut:

1. Kecepatan waktu komputasi algoritma masih tergolong lambat, sehingga diperlukan efisiensi dalam penulisan kode algoritma agar performa dapat ditingkatkan (seperti menggunakan bahasa pemrograman C).
2. Pengujian algoritma saat ini hanya menggunakan Korelasi dan *Avalanche Effect*. Oleh karena itu, disarankan untuk melakukan pengujian tambahan dengan aplikasi khusus untuk uji coba algoritma kriptografi.
3. Mengembangkan algoritma ini agar tidak hanya menggunakan satu bidak catur sebagai kunci, melainkan mempertimbangkan penggunaan beberapa bidak catur untuk meningkatkan kompleksitas dan keamanan.
4. Fungsionalitas pola catur yang dimasukkan pada kunci 2 di aplikasi *website* harus sesuai dengan pola yang dapat dilakukan bidak catur (hanya langkah valid dari bidak tersebut).
5. Sediakan permainan catur yang dilakukan dalam aplikasi *website* yang dibuat. Sehingga, proses pembuatan kunci 2 dapat dilakukan di aplikasi *website* dan tidak dikirim melalui *private channel*.