BAB V

KESIMPULAN DAN SARAN

Berdasarkan rumusan masalah dan hasil penelitian serta pembahasan terhadap hasil penelitian sebagaimana yang diuraikan pada bab sebelumnya maka diperoleh kesimpulan dan saran dari hasil penelitian tersebut.

5.1 Kesimpulan

Berdasarkan penelitian ini, dapat ditarik kesimpulan sebagai berikut:

1. Pengembangan kriptografi yang diperoleh dari penggabungan kriptosistem *hill cipher* dengan kunci matriks persegi panjang dan *elliptic curve cryptography* adalah suatu kriptosistem yang memiliki tiga tahapan dengan $\mathcal{P}$ dan $\mathcal{C}$ merupakan himpunan karakter alfanumerik. Tahapan pertama merupakan pembangkitan kunci yang dibutuhkan untuk melakukan enkripsi dan dekripsi, yaitu

$$\mathcal{K} = \{(K, G, \alpha, \beta, A_1, B_1) | A_1 = \alpha G, B_1 = \beta G\}$$

dengan $A_1, B_1 \in E$ merupakan kunci publik, dan $\alpha, \beta \in \mathbb{Z}_{\boldsymbol{p}}, G \in E, K \in \mathbb{Z}_p^{m \times n}$ merupakan kunci privat. Tahapan kedua merupakan enkripsi ketika pengirim pesan mengubah *plaintext* menjadi sebuah *ciphertext*, yaitu

$$e_k^{(1)}(p) = K(p - 32)$$

$$e_k^{(2)}\left(c^{(1)}\right) = (\alpha G, c^{(1)} + \alpha B_1)$$

Tahapan ketiga merupakan dekripsi ketika penerima pesan mengembalikan *plaintext* dari *ciphertext* yang diperoleh, yaitu

$$d_k^{(1)}\left(c_1^{(2)}, c_2^{(2)}\right) = c_2^{(2)} - \beta c_1^{(2)}$$

$$d_k^{(2)}\left(c^{(1)}\right) = (K^{-1} c^{(1)}) + 32$$

Kriptosistem gabungan *hill cipher* dengan kunci matriks persegi panjang dan *elliptic curve cryptography* dapat mempersulit kriptanalisis karena selain kriptanalis harus meretas kedua algoritma tersebut dengan tingkat keamanan yang tinggi, kemungkinan kunci yang dapat digunakan lebih luas akibat modifikasi *hill cipher*.

2. Implementasi kriptosistem gabungan modifikasi *hill cipher* dan *elliptic curve cryptography* dilakukan dengan mengonstruksi suatu program aplikasi komputer menggunakan *MATLAB R2016a*. Langkah-langkah atau proses pemograman menggunakan fitur GUIDE kemudian mengkompilasi program dengan bantuan perintah *deploytool* sehingga terbentuk sebuah program yang dapat digunakan untuk mempermudah proses pembangkitkan kunci, enkripsi, dan dekripsi. Program tersebut dapat digunakan oleh pengirim maupun penerima pesan.

5.2 Saran

Berdasarkan kesimpulan dalam makalah penggabungan *hill cipher* dengan kunci matriks persegi panjang dan *elliptic curve cryptography*, adapun saran dari penulis untuk penelitian selanjutnya, yaitu:

1. Menganalisa keamanan kriptosistem gabungan modifikasi *hill cipher* dengan kunci matriks persegi panjang dan *elliptic curve cryptography.*
2. Membandingkan kinerja antara kriptosistem gabungan *hill cipher* dan *elliptic curve cryptography* yang menggunakan kunci matriks persegi dengan kriptosistem gabungan *hill cipher* dan *elliptic curve cryptography* yang menggunakan kunci matriks persegi panjang.
3. Mengimplementasikan kriptosistem gabungan modifikasi *hill cipher* dan *elliptic curve cryptography* menggunakan bahasa pemograman lain.