BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari hasil analisis dalam penelitian ini, maka dapat disimpulkan sebagai berikut :

1. Untuk membangkitkan bilangan acak prima sebagai kunci dalam penyandian pesan berdasarkan algoritma ElGamal dilakukan dengan proses pemilihan bilangan acak prima $p > 255$. Kemudian untuk mengetahui bilangan tersebut merupakan bilangan prima atau komposit dilakukan dengan menghitung$y \equiv a^{p-1}(mod\ p)$, jika $y = 1$ maka bilangan tersebut prima.
2. Pengamanan pesan dengan cara menyandikan pesan dan tanda tangan digital menggunakan algoritma ElGamal, dilakukan dengan proses berikut.
   a. Penyandian pesan
      - Pembentukan kunci. Prosesnya dengan memilih bilangan prima $p > 255$, elemen primitif $\alpha \in Z_p{}^*$, bilangan acak $a \in \{1, 2, \dots, p-2\}$. Kemudian menghitung $\beta = \alpha^a\ mod\ p$. Setelah proses perhitungan selesai publikasikan nilai (p, α, β), serta rahasiakan nilai a.
      - Proses Enkripsi. Prosesnya, pesan yang akan disandikan diubah menjadi blok-blok karakter dengan setiap blok adalah satu karakter pesan. Kemudian konversikan masing-masing karakter ke dalam kode ASCII. Selanjutnya memilih bilangan acak $k \in \{0, 1, \dots, p-2\}$. Kemudian menghitung $\gamma_i = 176^{k_i}\ mod\ 1907$ dan $\delta_i = 683^{k_i}.m_i\ mod\ 1907$. Setelah perhitungan selesai maka akan diperoleh cipherteks yaitu $(\gamma_i, \delta_i), i = 1,2, \dots, n$
      - Proses Dekripsi. Prosesnya dengan memasukkan kunci publik dan kunci rahasia juga cipherteks yang diperoleh pada proses pembentukan kunci dan proses enkripsi. Kemudian menghitung

$T_i = \gamma_i^{p-1-a} \ mod\ p$ dan $m_i = \delta_i . T_i \ mod\ p$. Setelah hasil perhitungan diperoleh, konversikan masing-masing m_i ke dalam karakter sesuai dengan kode ASCII-nya. Kemudian gabungkan semua karakter untuk mendapatkan pesan asli.

b. Proses tanda tangan digital

- Pembentukan kunci. Proses ini langkah-langkahnya sama dengan proses pembentukan kunci pada penyandian pesan.
- Proses penandatanganan. Prosesnya dengan menghitung nilai *hash* (*MD*) suatu pesan kemudian memilih k, yang relatif prima dengan $p-1$. Selanjutnya menghitung $R = \alpha^k \ mod\ p$ dan $T = (MD - aR)k^{-1} \ mod\ p-1$. Setelah proses perhitungan selesai diperoleh pasangan tanda tangan (R, T).. (R, T)inilah yang dinamakan tanda tangan digital yang akan dibubuhkan pada pesan tersebut
- Proses verifikasi. Proses ini dilakukan oleh pihak penerima pesan yaitu dengan menghitung nilai *MD*. Kemudian mengecek bahwa $1 \leq R \leq p-1$ terpenuhi dan menghitung $\beta^R R^T \equiv \alpha^{MD} \ mod\ p$

3. Jumlah karakter yang dapat diinput pada program pascal ini hanya 126 karakter dikarenakan keterbatasan pascal untuk menampilkan karakter.
4. Algoritma kriptografi asimetris, seperti algoritma ElGamal, sangat baik untuk mengatasi masalah distribusi kunci.
5. Agar dapat mempermudah dalam menentukan elemen primitif grup $Z_p^* *$, maka penentuan bilangan prima p sebagai kunci publik sebaiknya harus diketahui faktorisasi prima dari $p-1$, seperti bilangan prima aman, yaitu $p = 2.q + 1$, dengan q adalah bilangan prima.
6. Kelebihan dari algoritma ElGamal adalah proses enkripsi pada plainteks yang sama diperoleh chiperteks yang berbeda-beda, namun pada proses dekripsi diperoleh plainteks sama.

5.2 Saran

Setelah membahas proses pengamanan data pesan dan tanda tangan digital menggunakan algoritma ElGamal pada skripsi ini, penulis ingin menyampaikan beberapa saran sebagai berikut :

1. Sistem kriptografi ElGamal merupakan salah satu algoritma yang aman digunakan dalam pengamanan pesan. Meskipun termasuk dalam algoritma yang aman, kunci publik juga harus dijaga keamanannya dengan membuat kunci yang berbeda setiap melakukan komunikasi agar tidak dimanipulasi oleh pihak-pihak yang tidak bertanggungjawab.
2. Mengimplementasikan algoritma ElGamal menggunakan bahasapemrograman lain, seperti C/C++, Java, Visual Basic dan lain sebagainya.