BAB I

PENDAHULUAN

Bab ini berisi bagian mendasar yang menjadi landasan utama bagi bab-bab selanjutnya. Pada bab ini akan dijelaskan mengenai latar belakang masalah, rumusan masalah, tujuan penulisan, batasan masalah, manfaat penulisan, metodologi pembahasan, dan sistematika penulisan. Berikut ini penjelasan tentang ketujuh hal di atas yang disusun ke dalam subbab-subbab secara terpisah.

1.1 Latar Belakang Masalah

Kemajuan di bidang teknologi informasi telah memungkinkan semua orang dapat melakukan interaksi dengan orang lain melalui jaringan komputer. Kegiatan-kegiatan tersebut tentu saja akan menimbulkan resiko bilamana informasi yang sensitif dan berharga yang kita miliki dapat diakses oleh orang-orang yang tidak berhak. Oleh karena itu dalam pengiriman informasi dengan beberapa teknik kriptografi, dibutuhkan suatu cara agar informasi yang ingin disampaikan dapat diterima dengan aman oleh orang yang memang berwenang untuk mendapatkannya.

Beberapa tahun ke belakang, telah banyak ditawarkan berbagai macam teknik untuk meningkatkan keamanan dari suatu rahasia. Akan tetapi masih ada kelemahan yang umum, yaitu semua data rahasia berada pada satu pembawa informasi dan data rahasia tidak dapat dikembalikan lagi jika pembawa informasi hilang atau rusak. Jika digunakan teknik duplikasi untuk mengatasi

kelemahannya, resiko keamanannya tetaplah tinggi. Untuk mengatasi permasalahan tersebut, skema pembagian rahasia menjadi solusi yang mungkin (Thien dan Lin, 2002: 765).

Secara garis besar, skema pembagian rahasia merupakan metode untuk melakukan pembagian suatu *secret*, biasanya berupa kunci, menjadi beberapa bagian yang disebut *share*, kepada sejumlah pihak yang disebut *participant P*, dengan kondisi-kondisi tertentu. Kondisi yang dimaksud menyangkut sekelompok *participant* mana saja yang memungkinkan untuk menyatukan kembali *secret* yang telah dibagi-bagi tersebut. Dewasa ini, skema pembagian rahasia telah digunakan pada bidang-bidang aplikasi yang beragam, misalnya kontrol akses, peluncuran senjata, membuka kotak deposito, dan lain-lain.

Skema pembagian rahasia *(secret sharing schemes)* diperkenalkan pertama kali oleh George Blakley dan Adi Shamir, konsep tersebut dikenal dengan nama *threshold scheme* (t, w). Banyak skema yang lahir setelahnya seperti *Asmuth and Bloom scheme, Brickell scheme, Karnin-Greene-Hellman* (KGH *method*).

Suatu skema pembagian rahasia dikatakan sempurna jika suatu *unauthorised set* $B \subseteq P$, tidak diperbolehkan mengetahui rahasia, mengumpulkan *share* mereka, maka mereka tidak akan mendapatkan hasil apa-apa untuk mengetahui rahasia *K. Karnin-Greene-Hellman* (KGH) adalah salah satu skema pembagian rahasia yang menerapkan hal tersebut (Baskoro, E.T., *et al*, 2007: 2). Oleh karena itu penulis menggunakan metode KGH dalam tugas akhir ini.

Skema pembagian rahasia dapat diterapkan pada graf. Data yang akan diamankan berupa pola pewarnaan sisi suatu graf, sehingga rahasia yang akan

dibagi menjadi beberapa *share* merupakan barisan bilangan yang menunjukkan pola pewarnaan sisi dari graf tersebut. Pola pewarnaan sisi dari graf tersebut sebelum dibagi menjadi beberapa *share* terlebih dahulu dienkripsi dengan menggunakan salah satu metode kriptografi kunci publik *Polly Cracker*. Metode kriptografi *Polly Cracker* merupakan sistem yang menitikberatkan pada proses aljabar komutatif.

Berdasarkan uraian di atas, maka tugas akhir ini selanjutnya diberi judul "**Aplikasi Skema Pembagian Rahasia pada Graf Sisi Terwarnai**".

1.2 Rumusan Masalah

Berdasarkan pada uraian latar belakang, maka rumusan masalah penulisan tugas akhir adalah :

1. Bagaimana cara mengenkripsi pola pewarnaan sisi pada graf dengan menggunakan metode kriptografi kunci publik *Polly Cracker*?
2. Bagaimana penerapan metode skema pembagian rahasia KGH untuk mengamankan pola pewarnaan sisi graf yang telah dienkripsi?

1.3 Tujuan Penulisan

Tujuan penulisan makalah ini adalah :

1. Mengetahui cara mengenkripsi pola pewarnaan sisi pada graf dengan menggunakan metode kriptografi kunci publik *Polly Cracker*;
2. Mengetahui penerapan metode skema pembagian rahasia KGH untuk mengamankan pola pewarnaan sisi graf yang telah dienkripsi.

1.4 Batasan Masalah

Adapun batasan masalah penulisan tugas akhir adalah :

1. Aplikasi skema pembagian rahasia hanya pada graf sederhana dengan pola pewarnaan sisi graf tersebut dalam bentuk matriks telah diketahui;
2. Pesan rahasia yang disisipkan atau disembunyikan berupa pesan dalam bentuk angka;
3. Pemakaian *software* dalam pembuatan program aplikasi yaitu dengan menggunakan *Borland Delphi 7*.

1.5 Manfaat Penulisan

Manfaat yang diharapkan dari penulisan makalah ini adalah :

1. Bagi penulis, diharapkan dapat menerapkan ilmu yang selama ini diperoleh dan menambah pengetahuan terhadap ilmu-ilmu yang baru dipelajari;
2. Memberikan sumbangan pemikiran pengembangan ilmu, sehingga dapat memperluas wawasan mengenai skema pembagian rahasia.

1.6 Metodologi Pembahasan

Metodologi pembahasan yang digunakan adalah :

1. Karena pembahasan lebih bersifat teoritis, metode penelitian yang dilakukan adalah studi literatur dengan cara mengumpulkan dan menelaah berbagai konsep dari sumber informasi yang berkaitan seperti buku-buku, artikel, jurnal dan lain-lain;
2. Pembuatan, pengujian, dan analisa hasil dari program aplikasi.

1.7 Sistematika Penulisan

Penulisan makalah ini ditulis dengan susunan sebagai berikut:

BAB I : PENDAHULUAN

Bab ini berisi uraian latar belakang permasalahan yang akan dibahas, rumusan masalah, tujuan penulisan, batasan masalah, manfaat penulisan, metodologi pembahasan, dan sistematika penulisan;

BAB II : LANDASAN TEORITIS

Bab ini menyajikan tentang dasar-dasar teori yang berguna dalam memahami pembahasan selanjutnya, khususnya graf, grup, kriptografi kunci publik, skema pembagian rahasia;

BAB III : PEMBAHASAN

Bab ini menjelaskan inti dari permasalahan dan pembahasan dalam penulisan, yaitu aplikasi skema pembagia rahasia pada graf sisi terwarnai;

BAB IV : HASIL KAJIAN

Bab ini berisi tentang bagaimana skema pembagia rahasia pada graf sisi terwarnai ini ke dalam sebuah program aplikasi. Melakukan pengujian terhadap program aplikasi yang telah dibuat dan menganalisa hasilnya;

BAB V : KESIMPULAN DAN SARAN

Bab ini menjelaskan kesimpulan dan saran dari keseluruhan penulisan.