BAB I
PENDAHULUAN

Pada bagian ini akan diuraikan mengenai latar belakang penelitian, rumusan masalah, tujuan penelitian, batasan masalah pada penelitian, dan sistematika penulisan.

1.1 Latar Belakang

Semakin berkembangnya teknologi saat ini memberikan pengaruh yang cukup besar terhadap segala aspek kehidupan, tidak terkecuali pada aspek informasi dan komunikasi, seperti pada pendistribusian informasi melalui pengiriman pesan. Dengan perkembangan teknologi yang ada, keamanan dari pengiriman suatu pesan menjadi salah satu hal yang perlu diperhatikan. Karena dengan adanya teknologi saat ini, tidak menutup kemungkinan saat proses pengiriman pesan tersebut ada campur tangan pihak ketiga yang tidak bertanggung jawab untuk merubah isi pesan tersebut sehingga merusak integritas data *(data integrity).*

Salah satu cara untuk menjaga keamanan dan kerahasiaan pesan *(confidentiality* atau *privacy)* pada saat proses pengiriman pesan tersebut yaitu dengan melakukan penyandian terhadap pesan yang dikirim dengan menjadikan pesan tersebut kode-kode atau bentuk pesan lain yang tidak dapat dipahami sehingga tidak dapat diketahui isi pesan yang sebenarnya. Akan tetapi jika hanya melakukan penyandian terhadap pesan yang dikirim, tidak menutup kemungkinan isi pesan tersebut masih bisa dirubah oleh pihak ketiga. Oleh karena itu seiring dengan perkembangan teknologi saat ini, untuk memperkuat keamanan, kerahasiaan, serta otentikasi *(auhentication)* pesan yang dikirim, telah berkembang pengamanan pesan dengan *digital signature.* Namun saat ini dalam penerapannya, *digital signature* masih memerlukan pengembangan lebih lanjut. Selanjutnya untuk mengatasi permasalah diatas dapat diselesaikan dengan kriptografi. Selain untuk mengatasi masalah diatas, kriptografi dalam *digital signature* dapat mengatasi masalah penyangkalan *(repudiaton).* Kriptografi tidak

hanya menyediakan alat untuk keamanan pesan, tetapi juga sekumpulan teknik yang berguna (Munir, 2006).

Kriptografi (*cryptography*) berasal dari Bahasa Yunani yaitu *"cryptós"* yang artinya *"secret"* atau rahasia, sedangkan *"gráphein"* artinya *"writing"* atau tulisan. Jadi, kriptografi berarti *"secret writing"* atau tulisan rahasia (Munir, 2006). Definisi Kriptografi sendiri yaitu bahwa kriptografi adalah ilmu yang mempelajari teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, otentikasi entitas, dan otentikasi data asal. Kriptografi bukan satu-satunya sarana untuk memberikan keamanan informasi, melainkan satu set teknik (A. Menezes & Oorschot, 1996). Pada kriptografi terdapat dua proses utama, yaitu enkripsi dan dekripsi. Proses menyandikan *plainteks* menjadi *cipherteks* disebut enkripsi *(encryption)* atau *enciphering* (standard nama menurut ISO 7498-2). Sedangkan proses mengembalikan *cipherteks* menjadi *plainteks* semula dinamakan dekripsi *(decryption)* atau *deciphering* (standard nama menurut ISO 7498-2) (Munir, 2006).

Terdapat beberapa penelitian sebelumnya yang menjadi landasan untuk dilakukan penelitian ini. Penelitian-penelitian berikut berkaitan dengan *digital signature. Digital Signature* di sini bukanlah tanda tangan yang di- dijitasi dengan alat *scanner*, tetapi suatu nilai kriptografis yang bergantung pada pesan dan pengirim pesan. Hal ini kontras dengan tanda tangan pada dokumen kertas yang bergantung hanya pada pengirim dan selalu sama untuk semua dokumen (Alfry Aristo Jansen Sinlae, 2013). Pada penelitian yang berjudul "Studi dan Implementasi Tanda Tangan Digital Menggunakan Algoritma ElGamal" tahun 2009 memberikan kesimpulan perlunya penjagaan kerahasiaan data-data sensitif dalam kriptosistem dan untuk memperkecil ukuran tanda tangan digital hasil ElGamal, dapat dilakukan perhitungan *hash* sehingga didapat *message digest* yang lebih kecil (Fernando, 2009). Pada penelitian yang berjudul "Pembuatan Tanda Tangan Digital Menggunakan *DSA (Digital Signature Algorithm)*" tahun 2013 memberikan saran untuk dilakukannya penelitian yang membahas tentang cara menyelesaikan logaritma diskrit secara mendalam (Nurhasanah et al., 2013), dan penelitian (Fernando, 2009) menyatakan bahwa algoritma ElGamal dibangun

dengan mendasarkan kekuatannya pada sulitnya memecahkan logaritma diskrit. Pada penelitian yang berjudul "Penerapan Grup Multikatif Atas Zp* dalam Pembuatan Tanda Tangan Digital ElGamal" tahun 2011 memberikan kesimpulan bahwa masih terdapat kelemahan pada perhitungan fungsi *hash* yaitu *collision* pada nilai *hash,* sehingga diperlukan penelitian lebih lanjut mengenai penanganan masalah *collision* pada fungsi *hash* (Arizka & Abadi, 2011). Pada penelitian yang berjudul "Analisis Kriptosistem Menggunakan *Digital Signature* Berbasis Algoritma SHA-512 dan RSA" tahun 2012 menyimpulkan bahwa fungsi SHA-512 *(Secure Hash Algorithm - 512)* dapat digunakan bersamaan dengan Algroritma RSA untuk enkripsi dan dekripsi pada *digital signature* (Alfry Aristo Jansen Sinlae, 2013). Dan terakhir Pada penelitian yang berjudul "*Implementation & Analysis of RSA and ElGamal Algorithm*" pada tahun 2014 disimpulkan bahwa algoritma ElGamal lebih aman dibandingkan dengan algoritma RSA karena menghasilkan teks *cipher* yang lebih kompleks (Sharma, Attri, Devi, & Sharma, 2014).

Berdasarkan hal di atas, yang disoroti pada penelitin ini yaitu mengenai penanganan masalah *collision* pada fungsi *hash* yang terjadi pada pembuatan *digital signature*. Maksud dari *collision* yang terjadi yaitu adanya dua buah nilai *hash* yang sama namun berasal dari pesan yang berbeda. Dengan begitu, jika terdapat pihak yang ingin mengubah isi pesan, maka ia akan megacak isi pesan tersebut asalkan nilai *hash* yang dihasilkan sama (Arizka & Abadi, 2011). Mengingat pentingnya hal tersebut, perlu adanya solusi untuk menangani *data collision* yang terjadi. Oleh karena itu pada penelitian ini akan dilakukan analisis dan implementasi algoritma ElGamal dan penerapan fungsi SHA-512 pada *digital signature* yang dilandasi oleh penelitian-penelitian yang telah dipaparkan diatas. Dengan penelitian yang akan dilakukan, diharapkan penerapan fungsi SHA-512 dapat digunakan bersamaan dengan algoritma ElGamal untuk menangani masalah *collision* pada nilai *hash* yang sebelumnya terjadi pada pembuatan *digital signature*.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas, maka dirumuskan permasalahan utama yang akan dikaji pada penelitian ini, yaitu:

1. Bagaimana implementasi dan metode analisis terhadap penggunaan Algoritma ElGamal & SHA-512 untuk penanganan *data collision* pada *digital signature*?
2. Bagaimana hasil analisis dan implementasi Algoritma ElGamal & SHA-512 untuk penanganan *data collision* pada *digital signature*?

1.3 Tujuan Penelitian

Tujuan dari dilakukannya penelitian ini adalah sebagai berikut, yaitu:

1. Untuk melakukan implementasi dan analisis terhadap penggunaan Algoritma ElGamal dan SHA-512 untuk penanganan *data collision* pada *digital signature.*
2. Untuk mengetahui hasil analisis dan implementasi algoritma ElGamal & SHA-512 untuk penanganan *data collision* pada *digital signature.*

1.4 Batasan Masalah

Batasan masalah dan ruang lingkup penelitian ini yang dilakukan adalah sebagai berikut:

1. Implementasi program pada penelitian ini yang meliputi perhitungan, penyandian, dan pembuatan *digital signature* menggunakan perangkat lunak Matlab R2013a.
2. Hasil implementasi dari penelitian ini hanya berupa aplikasi keluaran dari perangkat lunak Matlab R2013a dan tidak diterapkan pada *hardware* atau sistem lain.
3. Data yang digunakan pada proses pengujian sistem adalah dokumen berupa *text* dalam format *.txt.
4. Jenis serangan atau manipulasi dokumen/pesan pada saat pengujian hanya dalam bentuk manipulasi yang menyebabkan *data collision.*
5. *Randomness test* dilakukan dengan bantuan *software* Cryptool 1.4.3

6. Penelitian ini tidak membahas mengenai kesulitan dan cara-cara untuk memecahkan mekanisme persandian.

1.5 Sistematika Penulisan

Adapun sistematika penulisan karya ilmiah dalam bentuk skripsi untuk penelitian ini adalah sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini dijelaskan latar belakang masalah yang melandasi dilakukannya penelitian mengenai analisis dan implementasi algoritma ElGamal dan SHA-512 untuk penanganan *data collision* pada *digital signature*. Kemudian memaparkan solusi yang penulis tawarkan serta harapan penulis terhadap penelitian ini. Selain itu, pada bab ini akan diuraikan mengenai rumusan masalah, tujuan penelitian, batasan masalah, dan sistematika penulisan.

BAB II KAJIAN PUSTAKA

Pada bab ini akan dipaparkan landasan teoritis yang mendukung dan berhubungan dengan penelitian yang dilakukan. Bagian ini memiliki peran yang sangat penting karena memberikan rujukan terhadap permasalahan yang sedang diteliti.

BAB III METODOLOGI PENELITIAN

Bab ini merupakan bagian yang bersifat prosedural, yaitu bagian yang akan memaparkan serta mengarahkan pembaca agar mengetahui bagaimana peneliti merancang alur penelitiannya, mulai dari metode penelitian yang diterapkan, instrumen yang digunakan, hingga langkah-langkah analisis yang dijalankan. Secara umum akan disampaikan pola paparan yang digunakan dalam menjelaskan bagian metode penelitian dari sebuah karya ilmiah dalam hal ini adalah sebuah skripsi.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Pada bab ini akan dilakukan pembahasan secara mendalam mengenai permasalahan yang telah dirumuskan pada bagian rumusan masalah. Adapun inti dari bab ini yaitu membahas hasil penelitian untuk menjawab pertanyaan penelitian yang telah dirumuskan sebelumnya, yaitu mengenai hasil analisis dan implementasi algoritma ElGamal dan SHA-512 untuk penanganan *data collision* pada *digital signature*.

BAB V KESIMPULAN DAN SARAN

Bagian ini akan menyajikan kesimpulan yang merupakan temuan dan jawaban peneliti atas pertanyaan yang telah dirumuskan pada rumusan masalah. Selain itu bagian ini juga akan memaparkan beberapa hal penting yang dapat dimanfaatkan dari penelitian ini sebagai saran untuk pengembangan dan penelitian selanjutnya.