BAB I
PENDAHULUAN

1.1. Latar Belakang

Academic fraud (kecurangan akademik) sering ditemukan bahkan sudah mendarah daging dalam dunia akademis. Seperti yang dijelaskan oleh (Irianto, 2003) bahwa survei yang dilakukan oleh Fortune, majalah bisnis terkemuka di Amerika mengenai perilaku tidak etis pelajar, mahasiswa, dan alumnus perguruan tinggi menunjukan bahwa 70-80% responden di lingkungan pendidikan menengah melakukan kecurangan akademik seperti menjiplak. Kemudian disebutkan pula bahwa kecurangan akademik di perguruan tinggi dilakukan oleh 40-50% responden.

Menurut (Kurniawan, 2011), perilaku kecurangan akademik dipandang sebagai suatu perilaku yang secara sengaja dilakukan oleh seseorang untuk mendapatkan nilai yang lebih baik. Contoh tindakan kecurangan akademik yaitu menyalin sebagian maupun keseluruhan tugas yang dikerjakan orang lain dan diakui sebagai miliknya.

Kemudian Kurniawan menjelaskan bahwa unsur yang banyak terdapat kecurangan di dalamnya adalah pada aktifitas tugas kelas. Beriringan dengan kemajuan teknologi informasi dan komunikasi yang menjadi alat bantu pemenuhan aktifitas sehari-hari, termasuk dalam aktifitas tugas kelas saat dilakukan transmisi dokumen jawaban tugas kelas yang dilakukan siswa/mahasiswa kepada guru/dosen, dokumen dapat disalahgunakan oleh pihak ketiga. Yakni diubah isinya yang mengakibatkan integritas data dokumen tersebut tidak terjamin, ataupun dijiplak sehingga keabsahan pengirimnya pun tidak terjamin.

Berdasarkan masalah di atas, diperlukan suatu sistem yang dapat menjaga integritas data (*data integrity*) dokumen tugas kelas dan keabsahan pengirim (*user authentication*) yang diharapkan dapat meminimalisir tindak kecurangan akademik. Salah satu cara menjaga *data integrity* dan *user authentication* adalah dengan melakukan validasi terhadap dokumen dan merahasiakan isi dokumen

tersebut sebelum ditransmisikan. Untuk melakukan hal tersebut, dibutuhkan aturan komunikasi antara pengirim dan penerima dokumen. Aturan yang melibatkan dua orang atau lebih untuk menyelesaikan suatu kegiatan (termasuk komunikasi) disebut protokol (Munir, 2006). Dalam hal ini, karena komunikasi yang diharapkan aman, maka protokol yang dimaksud adalah protokol keamanan. Untuk membangun protokol keamanan, diperlukan beberapa metode atau algoritma yang mendukung.

Kriptografi dan steganografi merupakan ilmu dan seni yang secara tujuan tidak jauh berbeda, yakni pengamanan data. Perbedaannya terletak pada cara mengamankannya. Seperti yang dijelaskan (Munir, 2006), bahwa kriptografi melakukan pengamanan pesan dengan melakukan penyandian pada pesan, sedangkan steganografi melakukan pengamanan pesan dengan menyembunyikannya ke dalam suatu media. Kriptografi dan steganografi dapat digunakan untuk membangun protokol keamanan.

Pada kriptografi, salah satu teknik yang dapat digunakan untuk validasi dokumen adalah tanda tangan digital (*digital signature*) yang dapat menjamin integritas data. Selain itu, *digital signature* juga menjamin masalah keamanan lainnya, yaitu nir-penyangkalan.

Pada implementasinya, *digital signature* dikirimkan bersama dokumen asli kepada penerima dokumen dengan cara dibubuhkan ke dalam dokumen seperti pada penelitian yang dilakukan oleh (Ramdhani, 2016) atau dikirimkan secara terpisah namun tetap bersamaan seperti pada penelitian yang dilakukan oleh (Haryatno, 2016). Hal tersebut menjadikan *digital signature* dapat dilihat oleh pihak ketiga dan disadari dokumen tersebut telah ditandatangani yang kemudian *digital signature* tersebut dapat dirusak. Sehingga diperlukan suatu teknik penyembunyian *digital signature* yang menjadikannya aman dari perusakan secara sengaja.

Steganografi dapat digunakan untuk penyembunyian *digital signature*. Steganografi membutuhkan media penampung sebagai tempat penyembunyian pesan rahasia (Munir, 2006). Pada penelitian ini, pesan yang disembunyikan adalah *digital signature* dan media penampungnya adalah dokumen jawaban tugas kelas. Dokumen jawaban tugas kelas pada penelitian ini berbentuk teks, sehingga

teknik steganografi yang digunakan adalah steganografi pada teks (*text steganography*).

Kemudian untuk mengatasi masalah keamanan *user authentication*, diperlukan penyandian (enkripsi) dokumen agar tidak dapat dipahami oleh pihak ketiga, sehingga penjiplakan yang berarti pula pengakuan karya orang lain (yang mengakibatkan tidak absahnya pengirim dokumen) dapat dihindari. Enkripsi tersebut sekaligus memenuhi tujuan kerahasiaan pesan (*confidentiality*).

Pada penelitian yang dilakukan (Paj & Ivaniš, 2011) dijelaskan mengenai *digital signature* menggunakan *Digital Signature Algorithm* (DSA) dan Rivest Shamir Adleman (RSA). DSA dipilih karena alasan keamanan. DSA menawarkan kerumitan pencarian dua pasang bilangan prima yang besar sehingga menyulitkan penyadap memecahkan algoritma ini.

Di lain sisi, DSA tidak dapat memenuhi enkripsi data, karena DSA dikhususkan untuk tanda tangan digital, bukan untuk enkripsi data (Munir, 2006). Penelitian yang dilakukan (Suryani, 2009) adalah mengenai enkripsi data menggunakan kriptografi kunci simetri, yaitu RC4. Suryani menyatakan bahwa RC4 adalah algoritma kriptografi terbaik dalam hal kecepatan pada kriptografi kunci simetri. Namun RC4 memiliki kelemahan, salah satunya adalah tingginya kemungkinan terisinya nilai array S yang sama dalam beberapa kali pembangkitan array S. Selain itu, RC4 merupakan algoritma kunci simetri yang rentan kerahasiaan kuncinya.

Kemudian mengenai penyembunyian teks pada media teks telah dilakukan penelitian oleh (Lip Yee Por, Chee, Ang, & Beh, 2011) dan penelitian oleh (L Y Por, Ang, & Delina, 2008) mengenai *text steganography* yang menyembunyikan pesan dengan memanfaatkan ruang kosong pada dokumen seperti spasi antarkata, antarbaris, maupun antarparagraf.

Berdasarkan kebutuhan protokol keamanan pada validasi dokumen tugas kelas dan penelitian terkait yang dijelaskan di atas, diperlukan beberapa metode atau algoritma yang kemudian diimplementasikan dan dilakukan modifikasi. Pada penelitian ini dilakukan pembangkitan dan verifikasi *digital signature* menggunakan DSA yang kemudian disembunyikan ke dalam dokumen tugas kelas menggunakan *text stenganography* dengan metode *inter-word spacing*.

Kemudian dalam enkripsi dokumen, algoritma yang digunakan adalah RC4. Untuk mengatasi kelemahan RC4, seperti yang diusulkan oleh (Suryani, 2009) yaitu menjadikan hasil *hash* 160 bit SHA (*message digest*) sebagai kunci. Selain itu untuk mengatasi kerahasiaan kunci RC4 yang termasuk kunci simetri, digunakan pula *text steganography* dengan metode *inter-word spacing* modifikasi.

Penelitian ini dilakukan untuk melihat ketahanan protokol keamanan pada validasi dokumen tugas kelas menggunakan algoritma DSA, RC4, dan *text steganography* dari serangan pihak ketiga yang diuji menggunakan *Man in the Middle Attack Scenario*. Kemudian dilakukan pula *randomness test* terhadap *cipherdoc* dari algoritma RC4 untuk dilihat perbandingannya antara enkripsi RC4 menggunakan kunci biasa dengan enkripsi RC4 menggunakan kunci *message digest*.

1.2. Rumusan Masalah

Berdasarkan latar belakang masalah di atas, dapat ditarik rumusannya sebagai berikut:

1. Bagaimana mengimplementasikan protokol keamanan (aturan komunikasi yang aman menggunakan prinsip kriptografi dan steganografi) untuk validasi dokumen tugas kelas?
2. Bagaimana pengaruh protokol keamanan menggunakan *digital signature* metode DSA, *text steganography*, dan algoritma kriptografi RC4 terhadap serangan tindak kecurangan akademik?
3. Bagaimana perbandingan presentase lolos uji *randomness test* antara *chiperdoc* hasil enkripsi RC4 yang dibangkitkan dari kunci biasa dengan yang dibangkitkan dari kunci *message digest*?

1.3. Batasan Masalah

Hal-hal yang membatasi masalah pada penelitian ini adalah sebagai berikut:

1. Dokumen tugas kelas adalah dokumen (*softfile*) jawaban dari tugas yang diberikan oleh dosen dalam kelas perkuliahan, berupa pekerjaan rumah atau

tugas yang dikerjakan di luar perkuliahan yang kemudian dikirimkan melalui internet.

2. Dokumen tugas kelas berformat .txt.
3. Dokumen tugas kelas hanya berisi tulisan.
4. Jenis serangan tindak kecurangan akademik hanya penjiplakan jawaban dan pengubahan isi jawaban oleh pihak ketiga.
5. Penjiplakan jawaban hanya dengan cara menyalin keseluruhan isi dokumen dan mengganti identitas menjadi identitas penjiplak jawaban.
6. *Randomness test* terhadap *cipherdoc* dari algoritma RC4 dilakukan dengan bantuan *software* Cryptool 1.4.3.
7. Sistem yang dibangun berdiri sendiri menggunakan *software* Matlab R2013 dan tidak diterapkan atau terhubung dengan sistem lain.

1.4. Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Mengimplementasikan protokol keamanan (aturan komunikasi yang aman menggunakan prinsip kriptografi dan steganografi) untuk validasi dokumen tugas kelas.
2. Mengetahui pengaruh protokol keamanan yang dibangun menggunakan *digital signature* metode DSA, *text steganography*, dan algoritma kriptografi RC4 terhadap serangan tindak kecurangan akademik.
3. Mengetahui perbandingan presentase lolos uji *randomness test* antara *chiperdoc* hasil enkripsi menggunakan RC4 yang dibangkitkan dari kunci biasa dengan yang dibangkitkan dari kunci *message digest.*

1.5. Struktur Organisasi Penulisan

Struktur organisasi penulisan pada penelitian ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini menjelaskan latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini dijelaskan landasan teori yang mendukung penelitian. Yaitu mengenai Kecurangan Akademik, Protokol Keamanan, Kriptografi, *Digital Signature*, Steganografi, *Randomness Test* dan *Man in the Middle Attack*, dan penelitian relevan.

BAB III METODOLOGI PENELITIAN

Pada bab ini dijelaskan mengenai metode pengumpulan data, metode pengambangan perangkat lunak, alat penelitian, dan bahan penelitian.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Pada bab ini dijelaskan mengenai hasil penelitian, skema dan proses protokol keamanan pada validasi dokumen tugas kelas, dan pengujian.

BAB V KESIMPULAN DAN SARAN

Pada bab ini dijelaskan mengenai kesimpulan dari penelitian yang dilakukan dan saran untuk penelitian selanjutnya.