ABSTRAK

Academic fraud (kecurangan akademik) sering ditemukan bahkan sudah mendarah daging dalam dunia akademis. Seperti yang dijelaskan oleh (Irianto, 2003) mengenai perilaku tidak etis pelajar, mahasiswa, dan alumnus perguruan tinggi. Hasil survei menunjukan bahwa 70-80% responden di lingkungan pendidikan menengah melakukan kecurangan akademik. Contoh tindakan kecurangan akademik yaitu menyalin sebagian maupun keseluruhan tugas yang dikerjakan orang lain dan diakui sebagai miliknya. Unsur yang banyak terdapat kecurangan di dalamnya adalah pada aktifitas tugas kelas. Berdasarkan masalah di atas, diperlukan sistem validasi dokumen tugas kelas. Salah satu teknik yang dapat digunakan untuk validasi dokumen elektronik adalah tanda tangan digital (*digital signature*) untuk memenuhi tujuan nir penyangkalan. Kemudian untuk kerahasiaan diperlukan penyandian atau enkripsi dokumen. Aturan-aturan yang mendukung validasi dokumen tugas kelas tersebut kemudian disebut protokol keamanan. Dilakukan pembangkitan dan verifikasi *digital signature* menggunakan *Digital Signature Algorithm* (DSA). Kemudian dilakukan penyisipan *digital signature* menggunakan teknik *text steganography*. Untuk enkripsi dan dekripsi dokumen digunakan algoritma kriptografi RC4. Pada *cipherdoc*, dilakukan perbandingan uji keacakan menggunakan *Randomness Test* terhadap *cipherdoc* tersebut yang dibangkitkan dari dua tipe kunci yang berbeda, yaitu kunci biasa dan kunci *message digest* yang dihasilkan dari *hashing* terhadap dokumen. Hasil menunjukan presentase lolos uji untuk kunci *message digest* adalah 98,67%, lebih besar dari kunci biasa yang memiliki presentase lolos uji sebesar 94,00%. Dilakukan pula pengujian dengan 6 skenario *Man in the Middle Attack* untuk menguji ketahanan protokol keamanan dari serangan pihak tidak bertanggung jawab. Hasil menunjukan 5 skenario berhasil terdeteksi kecurangan dan hanya 1 skenario yang tidak terdeteksi serangan.

Kata Kunci: Kecurangan akademik, protokol keamanan, *digital signature*, DSA, RC4, *text steganography*.

ABSTRACK

Academic fraud is often found even already ingrained hearts academic world. As explained by (Irianto, 2003) regarding not ethical students and college graduates of the university. Collecting results showed that 70-80% of respondents in the environment of secondary education academic cheating. Examples of actions academic cheating namely copy of any and all document and recognized as his own. There are elements of the many cheats in it is on classwork activities. Based on the problems, required system validation classwork document. One technique that can be used to review the validation of electronic documents is digital signature for review meet the goal of a non-denial. Then to review the confidentiality required encryption or document encryption. Rules supporting document validation telecoms the class then called security protocol. Do generation and verification of digital signatures using the Digital Signature Algorithm (DSA). Then do the insertion digital signatures using text steganography techniques. For a review of encryption and decryption of documents used cryptographic algorithm RC4. On cipherdoc, do comparison Randomness Test using the cipherdoc Randomness Test against the resurrected from prayer different type of key, i.e. a regular key and the key message digest the resulting of documents against hashing. The results show the percentage pass the test to review the key message digest is 98.67%, biger than regular lock whick has a percentage of 94.00% passed the test. Testing has also been conducted with 6 Man in the Middle Attack Scenarios for review durability testing security protocol from attacks not responsible parties. Results showed 5 scenarios successful detected fraud and only 1 scenario that is not detected attacks.

Keywords: *Akademic fraud, security protocol, digital signature, DSA, RC4, text steganography.*