BAB V
PENUTUP

V.1 Kesimpulan

Berdasarkan pembahasan mengenai aplikasi kriptografi untuk pengamanan e-dokumen dengan metode Penggabungan Tandatangan Manual dan DSA (*Digital Signature Algorithm)* dapat diambil kesimpulan:

a. Tandatangan manual/ *offline* pengguna dapat digunakan untuk membuat kunci privat. Kunci privat yang dihasilkan, digunakan untuk membuat kunci publik pasangannya. Panjang kunci antara 512 sampai 1024 bit sesuai standar keamanan yang dikeluarkan oleh FIPS (Federal Information Processing Standard). Dari masukan satu tandatangan offline dapat menghasilkan lebih dari satu pasang kunci. Hal ini menunjukkan pembangkitan kunci secara dinamis sebagai konsep baru pada penggunaan kunci untuk satu kali pakai.
b. Keamanan implementasi tandatangan dan DSA pada penelitian ini didasarkan atas satu e-dokumen jika ditandatangani oleh n signer maka harus diverifikasi sebanyak n kali. Jika semua n verifikasi bernilai valid berarti telah menembus n lapis keamanan dalam hal verifikasi. Sebaliknya jika salah satu atau lebih hasil verifikasi tidak valid maka verifier dapat mengetahui jika e-dokumen yang diterima sudah tidak otentik dan atau salah satu atau lebih dari signer adalah bukan orang yang sebenarnya menandatangani e-dokumen tersebut. Selain itu keamanan pada kunci yang dihasilkan adalah pada sulitnya mencari pemfaktoran bilangan prima besar khususnya pada 1024 bit (Feng, H;& Chong Wa,C. 2002).
c. Pada implementasi tandatangan digital dengan metode Penggabungan Tandatangan dan DSA terpenuhi kebutuhan keamanan e-dokumen dalam hal :

1) Kerahasiaan (confidentiality) signature hanya dapat didekrip oleh verifier dengan kunci publik pasangan kunci privat pada pihak signer.
2) Keutuhan atau keotentikan (integrity) e-dokumen yang ditransmisi, dijamin dengan hash SHA-1 dari e-dokumen tersebut.
3) Jaminan atas identitas dan keabsahan (authenticity) n signer dengan n signature yang dihasilkan serta hasil verifikasinya, dimana n = 1,2,3,....

V.2 Saran

Saran yang dapat diberikan terkait dengan implementasi tandatangan digital dengan metode Penggabungan tandatangan manual dan DSA yang telah diteliti yaitu :

a. Untuk lebih mengoptimalkan sisi keamanan transmisi e-dokumen lewat internet adalah dengan menggunakan tandatangan offline dan menambahkan algoritma pencocokan tandatangan. Algoritma pencocokan tandatangan offline misalnya dengan metode P-tree pada AHVS (Automatic Handwritten Verification System) (Najmul, 2006).
b. Program ini dapat dipakai sebagai masukan pada infrastruktur kunci publik di Indonesia dengan penambahan sertifikat digital, sehingga tujuan kriptografi dalam hal nir-penyangkalan (non-repudiation) dapat tercapai.
c. Pada kunci privat yang dihasilkan dapat tidak ditampilkan (disembunyikan) atau disimpan dengan menyandikannya, misalnya dengan algoritma 3DES atau algoritma enkripsi yang lain. Hal ini dilakukan untuk meningkatkan keamanan dalam hal penyimpanan kunci privat yang bersifat rahasia.