

## Abstrak

Pengamanan data dalam sistem komputer memerlukan adanya usaha menjaga kerahasiaan dan keamanan data. Salah satu cara menjaga kerahasiaan data adalah dengan menggunakan kriptografi yang bertujuan untuk menghindari penggunaan data oleh pihak yang tidak berhak. FAT merupakan *file system* yang paling sering digunakan di sistem operasi Windows dan dapat diakses di berbagai *platform* lainnya. Di tingkat *driver* Windows, dapat ditambahkan lapisan untuk mengamankan data di media fisik secara *background* (transparan). Lapisan ini diimplementasikan sebagai *non-plug & play device driver* pada Windows.

Alasan pemilihan kriptosistem hibrid ditujukan untuk pengamanan data yang [cukup] kuat dan mempermudah *key-management* sehingga tidak merepotkan berbagai user dalam mengamankan data masing-masing. Kriptosistem hibrid ini terdiri dari *asymmetric cryptograph* menggunakan algoritma RSA, dan *symmetric cryptograph* menggunakan algoritma RC6. Panjang *key* dapat disesuaikan dengan kemampuan/spesifikasi *hardware* sistem komputer yang digunakan. Penyesuaian ini dilakukan agar pengamanan data yang terjadi secara transparan tidak menimbulkan penurunan kinerja sistem yang signifikan.

**Kata kunci:** *windows driver*, kriptosistem hibrid, RC6, RSA, *FAT file system*.