Šestá sada domácích úloh
Matematika IV, jarní semestr 2009

Pouze jeden příklad.

Příklad 1. *Martin chce Honzovi utajeně poslat známku studenta X.Y. z předmětu M. Pro komunikaci otevřeným kanálem zvolili RSA-algoritmus, přičemž Honza zvolil prvočísla* $p = 153607$ *a* $q = 168391$*, tedy základ* $N = pq$ *a dále si zvolil* $e = 1751143$ *a dopočítal inverzi* f *modulo* $\phi(N)$*. Martin dal studentovi známku* 4*. Jak bude tato zpráva zakódována ve zmíněném algoritmu (bez autentifikace)? Spočítejte prosím opravdu samostatně za pomocí Vašich oblíbených programovacích prostředků, které máte k disposici (bude nutno „inteligentně" naprogramovat umocňování modulo velká čísla). Prosím nepište řešení do diskusního fóra ani si jej nijak jinak nesdělujte.*