Šestá sada domácích úloh

Příklad 1. *Určete (ručně)* $[391]^{-1}_{Z_{456}}$.

Příklad 2. *Martin chce Honzovi utajeně poslat známku studenta X.Y. z předmětu M. Pro komunikaci otevřeným kanálem zvolili RSA-algoritmus, přičemž Honza zvolil prvočísla* $p = 3259$ *a* $q = 3433$*, tedy základ* $N = pq$ *a dále si zvolil* $e = 323$ *a dopočítal inverzi* f *modulo* $\phi(N)$*. Martin dal studentovi známku* 2*. Jak bude tato zpráva zakódována ve zmíněném algoritmu? Při výpočtu smíte používat výpočetní techniky.*

Příklad 3. *Martin chce pro jistotu poslat Honzovi známku ještě pomocí šifry ElGamal. Domluvili se na cyklické grupě* Z^*_{29} *a Honza si zveřejnil veřejný kód* $(Z_{29}, 2, 9)$*. Martin si pouze pamatuje, že má zvolit náhodně nějaké číslo, zvolil číslo* 17*. Poraďte mu, jak má pokračovat*