MB104 – 7. demonstrovaná cvičení
Pravděpodobnost

Masarykova univerzita
Fakulta informatiky

3.4. 2012

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

Řešení. □

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.*

Řešení. 8703625. □

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*

Řešení. $(21, 8)$. □

Příklad *Mirek hodí $n+1$-krát mincí, Marek n-krát. Jaká je pravděpodobnost, že Mirkovi padne více hlav než Markovi?*

Příklad *Mirek hodí $n+1$-krát mincí, Marek n-krát. Jaká je pravděpodobnost, že Mirkovi padne více hlav než Markovi?*

Příklad *Dva korektoři četli nezávisle na sobě stejný text. První z nich objevil celkem a tiskových chyb, druhý celkem b tiskových chyb, z nichž c objevil také první korektor. Odhadněte, kolik neodhalených chyb v textu ještě zůstalo.*

Příklad *Máme dva klobouky. V prvním klobouku jsou 1 bílá kulička a 3 černé, ve druhém a dvě bílé a dvě černé. Náhodně zvolíme klobouk a z něho vybereme kuličku. Jaká je pravděpodobnost, že druhá vytažená koule z již vybraného klobouku bude černá?*