# Druhý test z predmetu Základy kryptografie

10.11.2016

Inštrukcie:

- Na vypracovanie písomky máte 90 minút.
- Príklady vypracujte aj s postupom, aby bolo jasné, ako ste dané výsledky dostali.
- Na každom papieri na odovzdanie uveďte svoje meno, číslo z AIS a meno fakulty, ktorú navštevujete (FEI alebo FIIT).
- Na prvú stranu tiež uveďte, koľko papierov odovzdávate.
- Multiplikatívne inverzné prvky môžete hľadať hrubou silou.
- Zadanie si môžete nechať.

Úlohy:

1. Zachytili ste správu „21“, o ktorej viete, že bola zašifrovaná RSA algoritmom s verejným kľúčom ($n = 247, e = 7$).
   (a) (2 body) Faktorizujte modul $n = 247$ pomocou Fermatovej metódy.
   (b) (2 body) Vypočítajte dešifrovací exponent.
   (c) (4 body) Dešifrujte správu pomocou algoritmu rýchleho dešifrovania.

   Dôkladne popíšte svoj postup.
2. (a) (3 body) Vytvorte inštanciu El Gamalovho kryptosystému nad $\mathbb{Z}_{11}^*$. Čo je verejný kľúč? Čo je tajný kľúč?
   (b) (2 body) Pomocou Vášho kryptosystému zašifrujte správu $x = 6$. Predpokladajte, že náhodný generátor vygeneroval $r = 2$.
   (c) (2 body) Zašifrovanú správu následne dešifrujte.
3. (3 body) Predpokladajme, že útočník zachytil správu zašifrovanú El Gamalovým algoritmom. Útočník pozná verejný kľúč, ale nepozná súkromný kľúč. Predpokladajme tiež, že útočník pozná náhodné číslo $r$, ktoré bolo použité pri šifrovaní správy. Dokáže útočník zistiť pôvodnú správu? Svoju odpoveď dôkladne zdôvodnite.
4. (5 bodov) Majme eliptickú krivku nad $\mathbb{Z}_{11}$ danú rovnicou $y^2 = x^3 + 2x + 2$. Nájdite (okrem bodu v nekonečne) 2 rôzne body tejto krivky (označme ich $P$ a $Q$) a vykonajte s nimi operácie sčítania na krivke: $P + P$ a $P + Q$. Dôkladne popíšte svoj postup.
5. (2 body) Vysvetlite, akú výhodu má Menezes-Vanstoneov algoritmus v porovnaní s El Gamalovým algoritmom s eliptickými krivkami.
6. (Prémia za 3 body) Nech $n$ a $a$ sú čísla také, že $\gcd(a, n) = 1$. Predpokladajme, že číslo $n$ prešlo Solovayovým testom pri báze $a$. (t.j. výstup zo Solovayovho testu je: „$n$ je prvočíslo“.) Prejde $n$ aj Fermatovým testom pri báze $a$? Svoju odpoveď dôkladne zdôvodnite.