Skúška z predmetu Základy kryptografie

6.12.2017

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.
- Zadanie si môžete nechať.

Úlohy:

1. Popíšte algoritmus AES. Uveďte:
   - (2 body) veľkosť bloku
   - (2 body) veľkosť kľúča
   - (1 bod) počet kôl
   - (4 body) ako vyzerá jedno kolo
   - (1 bod) ako vyzerá posledné kolo
   - (2 body) ako sú reprezentované medzivýsledky v priebehu šifrovania
2. Zachytili ste správu "24", o ktorej viete, že bola zašifrovaná RSA algoritmom s verejným kľúčom ($n = 253, e = 3$).
   (a) (4 body) Faktorizujte modul $n = 253$ pomocou Fermatovej metódy.
   (b) (4 body) Vypočítajte dešifrovací exponent.
   (c) (8 bodov) Dešifrujte správu pomocou algoritmu rýchleho dešifrovania.

   Dôkladne popíšte svoj postup.
3. (a) (5 bodov) Nech p je prvočíslo. Uveďte definíciu primitívneho prvku (t.j. generátora) v grupe $\mathbb{Z}_p^*$. Definujte problém diskrétneho logaritmu.
   (b) (7 bodov) Popíšte šifrovanie a dešifrovanie v ElGamalovom kryptosystéme. Čo tvorí verejný kľúč? Čo tvorí tajný kľúč?
4. (10 bodov) Majme eliptickú krivku nad $\mathbb{Z}_{11}$ danú rovnicou $y^2 = x^3 + x + 6$. 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.