Druhý test z predmetu Základy kryptografie

14.11.2014

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 a číslo z AIS.
- Na prvú stranu tiež uveďte, koľko papierov odovzdávate.
- Multiplikatívne inverzné prvky môžete hľadať hrubou silou.
- Zadanie si môžete nechať.

Úlohy:

1. (7 bodov) Zachytili ste správu, o ktorej viete, že bola zašifrovaná RSA algoritmom s verejným kľúčom $(n = 187, e = 3)$. Text správy je „19“.

   (a) Faktorizujte modul $n = 187$ pomocou Fermatovej metódy.

   (b) Vypočítajte dešifrovací exponent a dešifrujte správu pomocou algoritmu rýchleho dešifrovania.

   Dôkladne popíšte svoj postup.

2. (a) (3 body) Nech p je prvočíslo. Uveďte definíciu primitívneho prvku (t.j. generátora) v grupe $\mathbb{Z}_p^*$. Definujte problém diskrétneho logaritmu.

   (b) (6 bodov) Popíšte šifrovanie a dešifrovanie v ElGamalovom kryptosystéme. Čo tvorí verejný kľúč? Čo tvorí tajný kľúč? Aký je prenosový pomer?

3. (3 body) Uveďte definíciu hašovacej funkcie. Aké kritériá musí hašovacia funkcia spĺňať? Čo znamená, že hašovacia funkcia je odolná voči kolíziam?

4. (6 bodov) Nastavte parametre Merkle-Hellmanovho kryptosystému tak, aby ním bolo možné šifrovať 4-bitové správy, ale 5-bitové už nie. Vaším kryptosystémom zašifrujte správu $x = 11$. Zašifrovanú správu následne dešifrujte. Dôkladne popíšte svoj postup.

5. (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.