Skúška z predmetu Základy kryptografie

13.12.2013

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. Zadanie si môžete nechať.

1. (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 Diffie-Hellmanov protokol výmeny kľúča pre dvoch účastníkov.

2. (a) (2 body) Uveďte definíciu Legendreovho symbolu a definíciu Jacobiho symbolu.

   (b) (8 bodov) Popíšte šifrovanie a dešifrovanie v Goldwasser-Micaliho kryptosystéme. Čo tvorí verejný kľúč? Čo tvorí tajný kľúč?

   (c) (2 body) Uveďte jednu výhodu a jednu nevýhodu Goldwasser-Micaliho kryptosystému v porovnaní s RSA.

3. (a) (6 bodov) Popíšte Rabin-Millerov test prvočíselnosti.

   (b) (3 body) Nech n je číslo, ktoré prešlo Rabin-Millerovym testom pri báze a. (t.j. výstup z Rabin-Millerovho testu je: „n je prvočíslo“.) Prejde n aj Fermatovym testom pri báze a? Svoju odpoveď dôkladne zdôvodnite.

4. (10 bodov) Zachytili ste správu, o ktorej viete, že bola zašifrovaná RSA algoritmom s verejným kľúčom $(n = 55, e = 3)$. Text správy je „12“. Vypočítajte súkromný kľúč a algoritmom rýchleho dešifrovania správu dešifrujte. Dôkladne popíšte svoj postup.

5. (Prémia za 4 body)
   Popíšte Diffie-Hellmanov protokol výmeny kľúča pre troch účastníkov.