Druhý test z predmetu Základy kryptografie

18.11.2015

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. (8 bodov) Zachytili ste správu, o ktorej viete, že bola zašifrovaná RSA algoritmom s verejným kľúčom $(n = 143, e = 7)$. Text správy je „15“.
   (a) Faktorizujte modul $n = 143$ pomocou Fermatovej metódy.
   (b) Vypočítajte dešifrovací exponent a dešifrujte správu pomocou algoritmu rýchleho dešifrovania.
2. (a) (4 body) Popíšte Diffie-Hellmanov protokol výmeny kľúča. Čo je v protokole verejné a čo je tajné?
   (b) (2 body) Predpokladajme, že útočník odpočúva komunikáciu medzi obidvoma stranami počas výmeny kľúča podľa Diffie-Hellmanovho protokolu. Dokáže útočník z obsahu komunikácie určiť tajný kľúč? Prečo?
3. (a) (4 body) Vytvorte inštanciu El Gamalovho kryptosystému nad $\mathbb{Z}_7^*$. 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.
4. (3 body) Nech $\gcd(a, P) = 1$. Predpokladajme, že P prešlo Fermatovym testom pri báze a. Prejde P Fermatovym testom aj pri báze a^2 ? Svoju odpoveď dôkladne zdôvodnite.
5. (Prémia za 3 body) Nech $\gcd(a, P) = 1$. Predpokladajme, že P prešlo Solovayovym testom pri báze a. Prejde P Solovayovym testom aj pri báze a^3 ? Svoju odpoveď dôkladne zdôvodnite.