### Úlohy na precvičenie – KRS 2023 – séria G

Úlohy riešte samostatne a podrobne. Pri riešení nepoužívajte počítač. Celý postup zaznamenajte a komentujte. Odpovedajte na položené otázky. Odpovede zdôvodňujte celými vetami. Na prvom liste uveďte svoje meno a zdroje, ktoré ste pri riešení použili. Za každé správne a vyčerpávajúce riešenie (samozrejme aj s postupom) v tejto sérii možno získať bod. Zlomky bodov možno získať aj za čiastočné riešenia. Riešenia tejto série je nutné doručiť do 6. 11. 2023, 15:20 (do začiatku prednášky). Pred týmto termínom je možné odovzdať riešenia na sekretariáte Ústavu informatiky (do môjho priečinka). Neskôr dodané riešenia a plagiáty nebudú opravované ani hodnotené. Problémy môžete konzultovať po prednáške alebo e-mailom na adrese jozef,jirasek at upjs sk.

1. Dešifrujte správu C = 3 z úlohy 2 série F (p = 13, q = 17, e = 133) s využitím Čínskej vety o zvyškoch (slajd 22) bez použitia kalkulačky a počítača.

2. Popíšte konkrétne kroky Miller-Rabinovho testu, ktorým chceme overiť prvočíselnosť 113 pre voľbu a = 2 a a = 3. Výpočet (bez použitia kalkulačky) rozpíšte pre tieto konkrétne prípady po jednotlivých krokoch a okomentujte výsledok.

3. Alica i Bob si na (učebnicové) RSA šifrovanie (bez redundancie a bez randomizácie) zvolili rovnaké číslo n = 55, verejný kľúč Alice je (55, 3) a verejný kľúč Boba (55, 7). Pre obidvoch poslal Cyril tú istú správu M zašifrovanú ako 27 pre Alicu a 42 pre Boba. Vypočítajte pôvodnú správu M bez útoku na kľúč (bez toho, aby ste museli rozložiť 55 na prvočísla resp. inak získať súkromné kľúče Alice a Boba).

4. Pri hľadaní prvočísel pre RSA šifrovanie s dĺžkou kľúča 4096 bitov chceme použiť Miller-Rabinov test. Približne koľko čísel budeme musieť vyskúšať, aby sa nám to podarilo? (využite Gaussov odhad pre počet prvočísel do x funkciou x/ln(x) - na tento výpočet môžete použiť kalkulačku).

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. Decipher the message C = 3 from problem 2 of Series F (p = 13, q = 17, e = 133) using the Chinese reminder theorem (slide 22) without using a calculator or computer.

2. Describe the steps of the Miller-Rabin test to verify the prime number 113 for the choices a = 2 and a = 3. Describe the calculation (without using a calculator) for these particular cases step by step and comment on the results.

3. Alice and Bob both choose the same number n = 55 for (textbook) RSA encryption (without redundancy and without randomization), Alice's public key is (55, 3) and Bob's public key is (55, 7). For both, Cyril sent the same message M encrypted as 27 for Alice and 42 for Bob. Compute the original message M without attacking the key (without having to decompose 55 into primes or otherwise obtain the private keys of Alice and Bob).

4. We want to use the Miller-Rabin test to find prime numbers for RSA encryption with key length 4096 bits. Approximately how many numbers will we need to try to succeed? (Use the Gaussian estimate for the number of primes up to x by the function x/ln(x) - you can use a calculator to do this calculation).