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

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 30. 10. 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.

Plný počet bodov v tejto sérii je len za **ručný výpočet (bez kalkulačky)** s postupom.

1. Alica a Bob používajú pre prenos správ trojprechodový protokol (slajd 12) s modulom 17. Alica si zvolila šifrovací kľúč 11 a Bob šifrovací kľúč 5. Vypočítajte dešifrovacie kľúče Alice aj Boba. Alica chce poslať Bobovi správu 2. Ako budú postupne vyzerať tri správy, ktoré prebehnú sieťou ? Urobte pre kontrolu aj posledný Bobov výpočet, ktorým definitívne dešifruje správu od Alice. V tejto úlohe môžete použiť ľubovoľné (komentované) ručné postupy (aj skúšanie možností).

2. Pre RSA šifrovanie sme zvolili prvočísla 13 a 17. Šifrovací (verejný) kľúč bude 133 (a súčin 13.17). Rozšíreným Euklidovym algoritmom (zjednodušeným) spočítajte dešifrovací (súkromný) kľúč.

3. Pomocou dešifrovacieho kľúča z úlohy 2 dešifrujte šifrovanú správu C = 3 pomocou rýchleho modulárneho umocňovania.

4. Ktoré z nasledujúcich dvojíc je možné použiť ako verejné kľúče (n,e) pre šifrovanie RSA? Zdôvodnite! Ak sa dvojica dá použiť, spočítajte aj súkromný kľúč. a) (87,7) b) (89,3) c) (91,7)

\*. Poznáme verejný (n,e) aj súkromný kľúč (n,d) pre šifrovanie RSA. Zabudli sme ale p, q aj 𝜙(n). Je možné len pomocou e a d faktorizovať n ? Ako ? Skúste bez pomoci prehľadávania Internetu.

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

Full points in this series is only for manual calculation (no calculator) with description of the process.

1. Alice and Bob use a three-pass protocol (slide 12 of the lecture) with modulus 17 for message passing. Alice chooses encryption key 11 and Bob chooses encryption key 5. Calculate the decryption keys of both Alice and Bob. Alice wants to send Bob a message 2. What will the three messages that pass through the network look like ? Do also Bob's last computation, by which he finally decrypts the message from Alice. You can use any (commented) manual methods to solve this problem (even trialling the possibilities).

2. For RSA encryption, we chose the prime numbers 13 and 17. The encryption (public) key will be 133 (and the product 13.17). Use the extended Euclidean algorithm (slide 10) to compute the decryption (private) key.

3. With the private key from Problem 2, decrypt the encrypted message C = 3 using fast modular exponentiation (slide 5).

4. Which of the following pairs can be used as public keys (n,e) for RSA encryption? Explain! If the pair can be used, compute the private key as well. a) (87,7) b) (89,3) c) (91,7)

\*. We know both the public key (n,e) and the private key (n,d) for RSA encryption. But we have forgotten p, q and 𝜙(n). Is it possible to factorize n using e and d ? How ? Try to solve without the help of the Internet.