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

Úlohy riešte samostatne a podrobne. 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 27. 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. Alica používa na podpisovanie jednoduchý „učebnicový“ RSA algoritmus (bez redundančnej a hashovacej funkcie) s modulom 33. Viem, že správu m = 4 podpísala číslom 31. Bez znalosti jej súkromného kľúča vypočítajte iné dve správy aj s ich podpismi. Alica odmietla podpísať správu m = 12. Akú inú správu (okrem správy m = 4) by som jej mal ešte dať podpísať, aby som vedel spočítať aj podpis pre m = 12 bez útoku na kľúč ? Popíšte postup.

2. Pri podpisovaní správ systémom Elgamal vyšla dvojica (r, s) tak, že s = 0. V tomto prípade si musí podpisujúci zvoliť iné náhodné číslo k, pretože z podpisu by sa dal zistiť súkromný kľúč podpisujúceho. Ako? Platí také isté varovanie aj v prípade DSA podpisu?

3. Pre ECDSA podpis použijeme krivku E: y2 = (x3 + 2x + 2) mod 17, generátor G = (5, 1) rádu q = 19 so súkromným kľúčom d = 10. Vypočítajte podpis správy s odtlačkom h(m) = 12, pre ktorý zvoľte vhodné náhodné k. Výsledný podpis overte. Pri riešení môžte používať simuátor generovania bodov EC. Svoj postup a priebežné výsledky popíšte.

\*. Popíšte postup a odhadnite počet testov prvočíselnosti, ktoré je potrebné urobiť na stanovenie prvočísel p a q pre najjednoduchšiu formu DSA s prvočíslom p veľkosti 1024 bitov a q veľkosti 160 bitov. (využite Gaussov odhad pre počet prvočísel do x funkciou x/ln(x) ).

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

1. Alice uses a simple "textbook" RSA algorithm for signing (without redundancy and hash function) with modulus 33. We know that she signed the message m = 4 with 31. Without knowing her private key, compute two other messages with their signatures. Alice refused to sign the message m = 12. What other message (other then the message m = 4) should we have her sign so that we can also compute the signature for m = 12 without attacking the key ? Describe the procedure.

2. When signing messages with Elgamal, the pair (r, s) came out such that s = 0. In this case, the signer must choose a different random number k, because the signer's private key could be determined from the signature. How? Does the same warning apply in the case of a DSA signature?

3. For an ECDSA signature, use the curve E: y2 = (x3 + 2x + 2) mod 17, generator G = (5, 1) of order q = 19 with private key d = 10. Compute the signature of the message with fingerprint h(m) = 12, for which choose a suitable random k. Verify the resulting signature. You can use the EC score generation simulator to solve. Describe your procedure and intermediate results.

\*. Describe procedure and estimate the number of primality tests that need to be performed to determine the primes p and q for the simplest form of DSA with a prime p of size 1024 bits and q of size 160 bits. (Use the Gaussian estimate for the number of primes up to x by the function x/ln(x) ).