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

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 13. 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. Nájdite (bez podpory počítača) aspoň dva generátory multiplikatívnej grupy Zp\* pre p = 73. Postup popíšte (využite zjednodušené testovanie podľa deliteľov čísla p-1, a rýchle modulárne umocňovanie).

2. Správu (7,9) zašifrovanú kryptosystémom ElGamal s generátorom 3 multiplikatívnej grupy Z19 dostal adresát s verejným kľúčom 5. Zistite jeho súkromný kľúč (hrubou silou) a podľa **štandardného postupu s**právu dešifrujte. Výpočty urobte efektívne bez podpory počítača.

3. Chybná implementácia kryptosystému ElGamal spôsobila, že generuje čísla k za sebou podľa pravidla kn+1 = kn + 1. Poznáme verejné kľúče a otvorený aj zašifrovaný text správy M1 , C1 = (r1, s1). Možno pomocou týchto informácií dešifrovať (bez použitia hrubej sily) nasledujúcu správu M2 ak poznáme C2 = E(M2) = (r2, s2) ? Je možné pomocou týchto informácií vypočítať (bez použitia hrubej sily) súkromný kľúč ? V oboch prípadoch ukážte postup, resp. dokážte, že to nie je možné. Pri úprave modulárnych rovníc dávajte veľký pozor pri násobení (delení).

4. Uvažujme riešenie G = [2, 6] rovnice y2 = x3 + x + 4 mod 11. Určte ďalšie prvky (G+G=2G, G+G+G=3G ...) cyklickej grupy bodov eliptickej krivky E11(1,4), ktorá vznikne z generátora G (bude tam patriť aj bod G – G = O ?). Alicin súkromný kľúč je 4. Spočítajte ručne bez podpory počítača Alicin verejný kľúč. Pomocou tohto verejného kľúča zašifrujte správu, odpovedajúcu bodu [9,7] krivky s voľbou k = 2. Výsledok (dvojicu bodov (R,S) ) späť dešifrujte (pomocou Alicinho súkromného kľúča). Pri riešení môžete použiť simulátor výpočtov EC (okrem výpočtu Alicinho verejného kľúča), prezentovaný na prednáške (https://andrea.corbellini.name/ecc/interactive/modk-add.html).

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

1. Find (without computer support) at least two generators of the multiplicative group Zp\* for p = 73. Describe the procedure (use simplified testing by factors of p-1, and fast modular exponentiation).

2. A message (7,9) encrypted by the ElGamal cryptosystem with generator 3 of multiplicative group Z19 was received by an recipient with public key 5. Find out his private key (by brute force) and decrypt the message according to the standard procedure. Do the computations efficiently without computer support.

3. A flaw in the implementation of the ElGamal cryptosystem caused it to generate k consecutive numbers according to the rule kn+1 = kn + 1. We know the public keys and both the plaintext and ciphertext of the message M1 , C1 = (r1, s1). Can we use this information to decrypt (without brute force) the following message M2 if we know C2 = E(M2) = (r2, s2) ? Is it possible to compute (without using brute force) the private key using this information ? In either case, show the method or prove that it is not possible. When solving modular equations, take great care in multiplication (division).

4. Consider the solution G = [2, 6] of the equation y2 = x3 + x + 4 mod 11. Determine the other elements (G+G=2G, G+G+G=3G ...) of the cyclic group of points of the elliptic curve E11(1,4) which will arise from the generator G (will the point G - G = O belong there ?). Alice's private key is 4. Compute Alice's public key by hand without computer support. Using this public key, encrypt the message corresponding to the point [9,7] of the curve with the choice k = 2. Decrypt the result (the pair of points (R,S) ) back (using Alice's private key). You can use the EC computation simulator (except for the computation of Alice's public key), at https://andrea.corbellini.name/ecc/interactive/modk-add.html, to solve the problem.