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

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 9. 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.

1. LFSR generátor vygeneroval postupnosť 001101110101000. Vieme, že register má najviac 7 bitov. Aké budú ďalšie štyri bity postupnosti? (riešte bez použitia počítača! – tak ako aj všetky ďalšie úlohy).

2. Šesťbitový LFSR generátor, definovaný predpisom si+6 = (si+5 + si+4 + si+3 + si+1 + si) mod 2 inicializujeme vektorom (kľúčom) [1,1,0,0,1,0] (t.j. postupnosťou [s0,s1,s2,s3,s4,s5]). Nájdite **čo najmenší** LFSR generátor a jeho inicializačný vektor tak, aby generoval postupnosť, ktorá je **negáciou** postupnosti si generovanej pôvodným generátorom. Nezabudnite na skúšku správnosti riešenia – do koľkého člena postupnosti je nutné generátor skontrolovať?

3. Predpokladajme, že po aplikácii kľúča pre šifru RC4 ostalo pole S v počiatočnom stave (platí S[i]=i pre všetky i). Dešifrujte v tomto prípade sekvenciu „ALWEHE“, zapísanú štandardným 8-bitovým ASCII kódom. Úlohu riešte bez počítača, výsledok si môžete overiť na simulátore RC4.

4. Uvažujme prúdový generátor ChaCha20 s kľúčom K=0, inicializačným vektorom 0 a počítadlom cnt=0. Ako bude vyzerať 512b blok po prvej runde (po aplikovaní transformačnej funkcie na 4 stĺpce počiatočného nastavenia)? Komentujte postup (aspoň v prvom stĺpci) a vypíšte výsledok formou postupnosti šestnástich 32-bitových čísel v hexadecimálnom tvare. Skúste riešiť bez pomoci počítača.

\* (bonusová úloha). Nájdite aspoň jeden kľúč pre prúdovú šifru RC4, ktorý nechá pole S nezmenené (bude aj po inicializácii platiť S[i]=i).

1. The LFSR generator generated the sequence 001101110101000. We know that the register has at most 7 bits. What will be the next four bits of the sequence? (solve without using a computer! - just like all the other problems).

2. Initialize the six-bit LFSR generator, defined by the rule si+6 = (si+5 + si+4 + si+3 + si+1 + si) mod 2, with the vector (key) [1,1,0,0,1,0] (i.e., the sequence [s0,s1,s2,s3,s4,s5]). Find **the smallest possible** LFSR generator and its initialization vector such that it generates a sequence that is a **negation** of the sequence si generated by the original generator. Don't forget to test the correctness of the solution - up to how many members of the sequence does the generator need to be checked?

3. Suppose that after applying the key for the RC4 cipher, the field S remains in the initial state (it holds S[i]=i for all i). In this case, decrypt the sequence "ALWEHE", written in standard 8-bit ASCII code. Solve the problem without a computer; you can verify the result on the RC4 simulator.

4. Consider the stream generator ChaCha20 with key K=0, initialization vector 0 and counter cnt=0. What will the 512b block look like after the first round (after applying the transformation function to the 4 columns of the initial setup)? Comment on the procedure (at least in the first column) and write out the result as a sequence of sixteen 32-bit numbers in hexadecimal. Try to solve without the use of a computer.

\* (bonus problem). Find at least one key for the RC4 stream cipher that leaves the field S unchanged (S[i]=i will remain valid even after initialization).