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

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 16. 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. Štvorbitový LFSR generátor vytvára kľúčový prúd (keystream) pre prúdové šifrovanie rekurentným predpisom si+4 = (si+3 + si+2 + si) mod 2. Zašifrovaný text (trojpísmenové slovo, kódované 8-bitovým ASCII kódom) vyzerá v binárnom tvare "10001010 11011001 01100001". Dešifrujte text bez znalosti počiatočného nastavenia generátora. Popíšte podrobne svoj postup.

2. Dešifrujte text „DFGDAXFFADXXFDFFFGDFXDDDFAGFGG“, šifrovaný systémom ADFGX s kľúčom „Polybius square“ pre šifrovaciu tabuľku a kľúčom „SEZAM“ pre transpozíciu. Ako by ste postupovali, keby ste nepoznali kľúč pre transpozíciu?

3. Na šifrovanie použijeme všeobecnú Feistelovu schému s tromi rundami a funkciu F tvorí operácia XOR po bitoch z rundového kľúča a pravej strany aktuálneho bloku (teda F(R,K) = R XOR K). Vieme, že C1 je zašifrovaním správy M1. Ako bude vyzerať zašifrovanie správy M1 XOR M2 ? Možno ju vyjadriť bez znalosti rundových kľúčov?

4. Šifrujeme modifikovaným 56-bitovým DES šifrovaním len s dvomi rundami (na prednáške sme ukazovali riešenie s jednou rundou). Ukážte, ako je možné so znalosťami dvoch dvojíc (M1,C1) a (M2,C2) otvoreného a zašifrovaného 64-bitového bloku zistiť obidva rundové kľúče na menej ako milión pokusov. Bude riešenie s veľkou pravdepodobnosťou jednoznačné?

\*. V snahe o prelomenie blokovej šifry sme napísali program, ktorý dokáže na slušnom viacjadrovom počítači otestovať desať miliárd kľúčov za sekundu. Máme k dispozícii dva bloky pred a po šifrovaní (KPA útok).   
a) Odhadnite, koľko času bude trvať nájdenie 56 bitového kľúča, 128 bitového a 256 bitového kľúča hrubou silou (vyskúšaním všetkých možností)?   
b) Naprogramovali sme aj vírus, ktorý lúštiaci program rozniesol na približne desať miliárd počítačov po Internete. Pokiaľ budú všetky spolupracovať, koľko bude trvať rozlúštenie 56, 128, resp. 256 bitového kľúča? Výsledky vo všetkých prípadoch vyjadrite v rozumných jednotkách (stačí s presnosťou na 2 platné cifry) a porovnaním s trvaním nejakých reálnych udalostí (nie len v sekundách).   
c) Podľa Moorovho pozorovania vzrastá od začiatku histórie elektronických počítačov ich výkon dvojnásobne za jeden a pol roka. Ak predpokladáme, že bude platiť Moorov zákon aj naďalej a po roku a pol stále vymeníme počítače za dvojnásobne výkonnejšie, koľko bude trvať rozlúštenie 128 a 256 bitového kľúča ?   
(v tejto úlohe môžete použiť kalkulátor)

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

1. The four-bit LFSR generator produces a keystream for stream encryption by the recurrent rule si+4 = (si+3 + si+2 + si) mod 2. The ciphertext (a three-letter word, encoded by the 8-bit ASCII code) looks in the binary form "10001010 11011001 01100001". Try to decrypt the text without knowing the initial settings of the generator. Describe your procedure in detail.

2. Decrypt the text "DFGDAXFFADXXFDFFFGDFXDDDFAGFGG", encrypted by the ADFGX system with the key "Polybius square" for the cipher table and the key "SEZAM" for the transposition. How would you proceed if you didn't know the transposition key?

3. For encryption, we use a general Feistel scheme with three rounds and the function F consists of an XOR operation over the bits from the round key and the right-hand side of the current block (i.e., F(R,K) = R XOR K). We know that C1 is an encryption of the message M1. What will the encryption of the message M1 XOR M2 look like ? Can it be expressed without knowing the round keys?

4. We encrypt with a modified 56-bit DES encryption with only two rounds (in the lecture we showed a solution with one round). Show how, with knowledge of the two pairs (M1,C1) and (M2,C2) of an opened and encrypted 64-bit block, it is possible to find out both round keys in less than a million tries. Will the solution be unique with high probability?

\*. In an attempt to break the block cipher, we wrote a program that can test ten billion keys per second on a multi-core computer. We have two blocks before and after encryption (KPA attack).   
a) Estimate how much time it will take to find a 56 bit key, a 128 bit key, and a 256 bit key by brute force (trying all possibilities)?   
b) We have also programmed a virus that the cracker has spread to around ten billion computers on the Internet. If they all cooperate, how long will it take to crack a 56, 128, or 256 bit key? In all cases, express the results in reasonable units (precision to 2 valid digits is sufficient) and compare them to the duration of some real events (not just in seconds).   
c) According to Moore's observation, since the beginning of the history of electronic computers, their performance has doubled in one and a half years. Assuming that Moore's law continues to hold and we are always replacing computers with computers that are twice as powerful after a year and half, how long will it take to decrypt a 128 and 256 bit key ?   
(you can use a calculator in this problem)