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

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 23. 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. Popíšte postup, ktorým by ste mohli rozhodnúť, či je anglický text zašifrovaný transpozičnou, monoalfabetickou alebo polyalfabetickou šifrou, keď viete, že nastala práve jedna z týchto možností.

2. Generátor pre prúdové šifrovanie je vytvorený z dvoch LFSR generátorov A, B, definovaných predpismi ai+3 = (ai+1 + ai) mod 2, bi+4 = (bi+3 + bi) mod 2. Generátor B bude určovať, či bit vygenerovaný generátorom A pôjde na výstup, alebo sa má zahodiť. Stanovte dĺžku periódy výslednej postupnosti a ukážte, či sa na výstupe budú objavovať jednotky a nuly v rovnakej početnosti. Aká by bola perióda a aký priemerný počet jednotiek na výstupe, keby sa vyberalo z reťazca, generovaného generátorom B podľa stavu generátora A ?

3. Na zašifrovanie textu abcdefghijklmnopqrstuvwx v ASCII kóde (8 bitovom) bola použitá 64 bitová bloková šifra. Pri prenose bol jeden bit šifrovanej správy invertovaný. Z výsledného dešifrovaného textu určte (a zdôvodnite) v každom z prípadov a) b) c), ktorý režim použitia blokovej kryptografie bol pri odosielaní použitý:

a)  abcdefgh@#!s0&%-qrspuvwx  
b)  ab#defgh}w-XsE)9qrstuvwx  
c)  abcdefgh(#j?\_A!7qrstuvwx

4. Ktoré režimy blokovej kryptografie umožňujú útočníkovi, ktorý má prístup k šifrovanému textu, invertovaním zvolených bitov v šifrovanom texte spôsobiť invertovanie týchto bitov aj v dešifrovanom texte ? Ako by sa dal tento prístup zneužiť ?

\*. Pre plaintext {000102030405060708090A0B0C0D0E0F} (128 bitov v hexadecimálnom tvare} a 128 bitový kľúč {01010101010101010101010101010101} zapíšte začiatočnú stavovú maticu 4x4 bajtov pre šifrovanie AES, jej stav po prvom AddRoundKey, stav po substitúcii SubBytes, stav po ShiftRows, MixColumns (aj s výpočtom) a druhom AddRoundKey (aj s postupom generovania rundového kľúča). V prípade nejasností pozrite aj kapitolu 4.4 učebnice Understanding Cryptography. Hodnotené budú len riešenia s komentárom a bez použitia simulátora.

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

1. Describe a procedure you could use to decide whether an English text is encrypted by a transposition cipher, a monoalphabetic cipher, or a polyalphabetic cipher when you know that one of these possibilities has occurred.

2. The generator for stream cipher is constructed of two LFSR generators A, B, defined by the rules ai+3 = (ai+1 + ai) mod 2, bi+4 = (bi+3 + bi) mod 2. Generator B will determine whether the bit generated by generator A goes to the output or is to be discarded. Determine the period length of the resulting sequence and show whether ones and zeros will appear in the output in equal frequency. What would be the period and what would be the average number of ones at the output if it were selected from the string generated by generator B according to the state of generator A ?

3. A 64 bit block cipher was used to encrypt the text abcdefghijklmnopqrstuvwx in ASCII code (8 bit). During transmission, one bit of the encrypted message was inverted. From the resulting decrypted text, determine (and justify) in each case a) b) c) which mode of block cryptography was used in the transmission:

a)  abcdefgh@#!s0&%-qrspuvwx  
b)  ab#defgh}w-XsE)9qrstuvwx  
c)  abcdefgh(#j?\_A!7qrstuvwx

4. Which block cipher modes of operation allow an attacker who has access to the ciphertext, by inverting selected bits in the ciphertext, to cause those bits to be inverted in the decrypted text as well? How could this approach be exploited?

\*. For the plaintext {000102030405060708090A0B0C0D0E0F} (128 bits in hexadecimal} and the 128 bit key {01010101010101010101010101010101}, write down the initial state matrix of 4x4 bytes for AES encryption, its state after the first AddRoundKey, the state after SubBytes substitution, the state after ShiftRows, MixColumns (with computation) and the second AddRoundKey (also with the round key generation procedure). In case of confusion, see also Chapter 4.4 of the Understanding Cryptography textbook. Only solutions with comments and without using the simulator will be evaluated.