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

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 2. 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. Text „FDOKRRVV“ vznikol použitím Vigenérovej Autokey šifry s jednopísmenovým kľúčom. Pokúste sa dešifrovať text (bez znalosti kľúča a bez použitia počítača) keď viete, že posledným znakom otvoreného textu je písmeno E. Postup zaznamenajte. Aký je kľúč?

2. Máme dva zašifrované texty, ktoré vznikli zašifrovaním toho istého otvoreného textu Vigenérovou šifrou, len boli použité rôzne kľúče rovnakej dĺžky. Ako je možné túto vlastnosť využiť pri kryptoanalýze?

3. Slabá substitučná šifra je taká, že dvojnásobným zašifrovaním dostanem pôvodný text (pre všetky znaky x platí E(E(x)) = x). Uvažujme šifrovanie jednoduchou monoalfabetickou substitúciou.
a) Ako sa dajú charakterizovať slabé monoalfabetické substitučné šifry a koľko ich je (pre 26 písmenovú abecedu) ?
b) Koľko z nich je takých, že zmenia všetky písmená (pre všetky x je E(x)≠x) ?
c) Po zašifrovaní slabou šifrou použijeme na výsledok inú slabú šifru. Vznikne v tomto prípade zložením dvoch slabých šifier opäť slabá šifra? (dokážte, alebo uveďte protipríklad)

4. Nainštalujte zo strany https://www.ciphermachinesandcryptology.com/en/enigmasim.htm simulátor Enigmy (verzia 7.0.6) a postupujte podľa manuálu (zobraziť stlačením F1 v simulátore, resp. pdf súbor v adresári, kde je simulátor nainštalovaný). Nastavte verziu Enigmy pre Wehrmacht s reflektorom B a s rotormi v poradí II, III, IV s nastavením KEY (pri vkladaní rotorov). Prepojovacie pole nastavte takto: (AS) (BC) (DH) (EQ) (FG) (JK) (LN) (PX) (RZ) (UO). Táto Enigma už nepoužívala opakované trojice kľúčov, ale na predídenie omylom používala prvú päticu zašifrovaného textu ako kontrolu (prečítajte v manuáli str.6 – pri dešifrovaní stačí preskočiť).
Podľa postupu v manuáli rozlúštite správu

= 23 = BAC NXF =
EXTGY CAQTM KPPKQ WUXND BEAHF FAB=
Postup a svoje zistenia popíšte !

1. The text „FDOKRRVV“ was created using Vigenere's Autokey cipher with a one-letter key. Try to decrypt the text (without knowing the key and without using a computer) when you know that the last character of the plaintext is the letter E. Describe your procedure. What is the key?

2. We have two ciphertexts that were created by encrypting the same plaintext with the Vigenere cipher, only different keys of the same length were used. How can this particular property be used in cryptanalysis?

3. The weak substitution cipher is one such that encrypting twice yields the original text (for all characters x, E(E(x)) = x ). Consider encryption by simple monoalphabetic substitution.
a) How can we characterize weak monoalphabetic substitution ciphers and how many are there (for a 26-letter alphabet) ?
b) How many of them are such that they change all letters (for all x is E(x)x) ?
c) After encrypting with a weak cipher, we apply another weak cipher to the result. In this case, does the composition of the two weak ciphers again produce a weak cipher? (prove or give a counterexample)

4. Install the Enigma simulator (version 7.0.6) from https://www.ciphermachinesandcryptology.com/en/enigmasim.htm and follow the manual (view by pressing F1 in the simulator, or the pdf file in the directory where the simulator is installed). Set the Enigma version for Wehrmacht with reflector B and with rotors in order II, III, IV with KEY setting (when inserting rotors). Set the connection field as follows: (AS) (BC) (DH) (EQ) (FG) (JK) (LN) (PX) (RZ) (UO). This Enigma no longer used repeated triplets of keys, but to prevent mistakes it used the first quintuplet of the ciphertext as a check (see manual page 6 - just skip when decrypting).
Follow the procedure in the manual to decrypt the message

= 23 = BAC NXF =
EXTGY CAQTM KPPKQ WUXND BEAHF FAB=

Describe the steps and your findings !