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

Úlohy riešte samostatne a podrobne. Pri riešení **nepoužívajte počítač** (na rozdiel od úloh, ktoré sú z cvičení)! Hľadajte vhodné jednoduché postupy, ktoré nevyžadujú podporu počítača (nebude ani pri záverečných testoch). Celý postup zaznamenajte a komentujte. Odpovedajte na položené otázky. Odpovede zdôvodňujte celými vetami. Na prvom liste uveďte svoje meno, priezvisko, študijné zameranie 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 25. 9. 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. Pokúste sa rozšifrovať bez znalosti kľúča (a bez pomoci počítača) nasledujúci text (pôvodne v angličtine), zašifrovaný monoalfabetickou substitučnou šifrou (medzery ostali nezašifrované):
 „QTSMUJCGFT GY N IQNTY FH NCCNGTGTE YQSZMQ SFIJZCNCGFT FLQM GTYQSZMQ SXNTTQDY BU ZYGTE QTSMUJCGFT VQ OGYEZGYQ CXQ IQYYNEQ YF CXNC QLQT GH CXQ CMNTYIGYYGFT GY OGLQMCQO CXQ IQYYNEQ VGDD TFC BQ MQLQNDQO“.
Jednotlivé kroky popíšte a vypíšte aj šifrovací kľúč (aspoň jeho časť). Frekvenčná tabuľka pre angličtinu je v slajdoch z prednášky.

2. Po zašifrovaní textu afinnou šifrou použijeme na výsledok ďalšiu (inú) afinnú šifru (obidve mod 26). Zvýši sa bezpečnosť (odolnosť proti útokom hrubou silou)? Aká bude veľkosť množiny kľúčov? Ako sa zmení odolnosť, ak na výsledok afinnej šifry použijeme inú monoalfabetickú substitučnú šifru ?

3. Dešifrujte text, zašifrovaný systémom Playfair s kľúčom „Dobre utajena sprava“:
„CUCETVKIZCINBY“. Popíšte aj celý svoj postup.

4. Pre kryptoanalýzu CPA pomocou vybraného textu (choosen plaintext attack) môžeme vybrať text, ktorý dostaneme aj v zašifrovanej forme. Aký (čo najkratší) text by ste vybrali pre analýzu
a) monoalfabetickej substitučnej, b) afinnej, c) Hillovej, d) Playfair šifry ?
Zdôvodnite a popíšte v každom prípade aj postup zistenia kľúča.