Zadání úlohy – Afinní šifra (lineární posun)

Popis této šifry byl uveden na přednáškách nebo na cvičeních.

Každopádně jedná se o jednoduchou mono-alfabetickou substituci, kdy zdrojovou abecedu A - Z označíme indexy 0 - 25 a šifrovaný text získáme pomocí vzorce:

ŠT = (a*OT + b) mod 26

kde: a, b jsou klíče - udávají konstanty lineárního posunu.

Např. ŠT = (3*OT + 5) mod 26 (poté písmenko A bude zašifrováno jako F)

Poznámka k šifře - číslo a musí být nesoudělné s číslem 26. -> GCD hodnot a a hodnoty 26 musí být roven 1.

Vytvořte dvě NEZÁVISLÉ funkce. První funkce vrátí zašifrovaný řetězec. Druhá funkce naopak zadaný zašifrovaný text dešifruje.

Velikost lineárního posunu (obou klíčů) si bude možné nastavit. (Vstup od uživatele)

Tento úkol je hodnocený a jeho správné, včasné a samostatné vypracování je podmínkou pro získání zápočtu.

Celkově je možno získat 10 bodů.

- 2b za filtraci vstupních dat (diakritika a jiný balast co do šifer nepatří + ošetření klíče (čísla a)) - Úprava diakritiky (č -> C), odstranění speciálních znaků (!>.-, apod.), Zachování mezer z původního textu (znak " " mezera bude pro zachování nahrazena znaky "XMEZERAX" -> po dešifrování je potřeba zase vrátit znaky mezera - " " zpět)
  - Dále bude umožněno šifrovat čísla 0..9 -> provedení, aby to fungovalo, nechám na Vás.

Příklad -> OT bude klídně moct "Ahoj Pepo, sejdeme se v 5 u mostu." -> lze šifrovat a po dešifrování zpět uživatel získá "AHOJ PEPO SEJDEME SE V 5 U MOSTU" -> mezery a čísla je potřeba zachovat !!!

- 2b za funkci pro šifrování -> výstup (šifrový text) bude ošetřen tak, že bude zobrazen po pěticích znaků -> "ASFFS JSDFH" (odděleno mezerami)
- 2b za funkci pro dešifrování (včetně ošetření přípustných hodnot a)
- 3b za zobrazení výsledků v GUI (tj zašifrovaného příp. dešifrovaného textu, zašifrovaný text by měl být nějak slušně upraven, jak bývá běžné - tj velkými písmeny a dělen po pěticích). Dešifrovaný text by měl obsahovat mezery na stejných místech jako před šifrováním. Ve výpisu bude i abeceda, šif. abeceda a vyfiltrovaný text před vstupem do šifrování (mezery, případně reprezentace čísel a vybraných speciálních znaků).
  - GUI by mělo obsahovat
    - Pole zadání textu k šifrování
    - Pole pro zadání klíče - hodnot a, b
    - Pole pro zadání zašifrovaného textu

    - Pole pro zobrazení zašifrované/dešifrované zprávy
- 1b za umělecký dojem

Uvedené rozdělení bodů je pouze orientační !

Tento úkol odevzdejte 14 dní od zadání na cvičení. (viz podmínky k zápočtu)

Máte na vypracování čas cca 14 dní, tj do přespříštího cvičení. Je to tak schválně, abyste během příštího cvičení mohli konzultovat s vyučujícím případné problémy, co se týče naprogramování úkolu.

Jak by výsledek mohl vypadat, ilustruje odkaz níže ;)

http://www.dcode.fr/affine-cipher

V případě dotazů se ptejte.