Zadání úlohy – Playfair

Šifra Playfair - docela záludná potvůrka, na první pohled jednoduchá, ale nepodcenit!!!

Popis šifry Playfair najdete například na Wikipedii (anglické). Vytvořte dvě funkce. První funkce bude mít jako závislou proměnnou řetězec znaků a klíč, vrátí zašifrovaný řetězec. Druhá funkce naopak zadaný zašifrovaný text dešifruje.

Stručný popis šifry: Nejdříve je nutné vytvořit tabulku 5x5, kde se zapisují znaky abecedy po řádcích, a to takto: Nejdříve je zapsán klíč (každý znak v klíči musí být unikátní) a poté se pokračuje zápisem zbývajících znaků anglické abecedy, přeskakují se znaky použité v klíči.

Délka klíčového slova by měla být rozumná, ale ve své podstatě může být neomezená. (S tím, že od určitého znaku délka nehraje roli, pokud jsou vyčerpané znaky a šifrovací tabulka je plná)

Uvažujeme-li fakt, že anglická abeceda má 26 znaků a do tabulky 5x5 se dle tabulek malé násobilky pro 2. třídu základní školy vleze 25 znaků, dochází k časoprostorovému paradoxu, a aniž by byl potřeba doktorát z matfyzu je jasné, že bude nutno zasáhnout do tabulky. V případě česko-slovenského jazyka se ustanoví rovnost Q = O, tj. každé dvojité w, jež je v těchto jazycích použito velmi sporadicky je nahrazeno obyčejným v a voilá máme vyhráno :-) V angličtině se používá rovnost J = I.

Pokračujeme tedy dále. Playfair je bigramová či digramová šifra (což není sprosté slovo), nýbrž pracuje s dvojicí znaků. Je nutné ale toto upravit, pokud se ve dvojici vyskytnou dva stejné znaky, je nutné mezi ně **vložit** zvolený znak (např. X) a další dvojice "předvojicovat". Pokud je konečný počet znaků lichý, doplní se jako posledním opět zvoleným znakem. POZOR! můžeme se dostat do paradoxní situace, kdy věta s lichým počtem znaků končí např. znakem "x" a chceme doplnit X, takže bychom získali stejnou dvojici, kterou bychom rozdělili také znakem X, tím pádem bychom získali lichý počet znaků, ale pořád stejnou dvojici.... a jsme v pytli :-) Proto je nutno mít dvojici možných doplňujících znaků. (Obvykle X, Q, W -> zde pozor na zvolenou abecedu)

Poté se pracuje s tabulkou a dvojicím znaků otevřeného textu jsou přiřazeny dvojice znaků podle tabulky. Výpis opět po pěticích.

Pro práci s tabulkou existují 3 logická pravidla. Ta byla přednesena na přednášce, a jsou uvedena i na wikipedii (ovšem je nutné probudit tu mozkovou buňku co umí anglicky). Odkaz

Důležitá je opět reprezentace MEZER tak, aby byly mezery na stejném místě jako před zašifrováním a to stejné platí i pro čísla.

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

Celkově je možno získat 10 bodů.

* 1b za správnou filtraci vstupních dat – ošetření na speciální znaky, mezery a čísla jako u afinní šifry. (Ošetření platí i pro klíč !!)

* 2b za funkci pro šifrování

* 2b za funkci pro dešifrování

* 4b za zobrazení výsledků pomocí grafického uživatelské rozhraní - GUI (To znamená tlačítka pro šifrování/dešifrování, volba CZ/EN, zobrazení šifrovací tabulky, možnost zadat klíč uživatelem, zadání vstupního textu - otevřený text/šifrový text a zobrazení výstupu - zašifrovaný text/dešifrovaný text)

* 1b za umělecký dojem