Řešení úlohy č. 3

Tajemná zpráva

Algoritmus (šifrovací): Byl dán šifrovací algoritmus fungující na principu posouvání bitů. Nejprve byly znaky převedeny do binární podoby a následně se nad nimi provedla operace XOR, přičemž poslední hodnota zůstala nezměněná. Následně je volána další funkce přijímající výsledné pole bytů. Máme k dispozici tzv. abecedu, kterou budeme při šifrování používat. Šifrování probíhá na základě operací AND, LEFTSHIFT a RIGHTSHIFT, a je zřejmé, že výsledek bude mít nejméně 2 hodnoty z výsledné abecedy.

Algoritmus (dešifrovací): V zásadě budeme provádět opačný postup. Mezer, otazníků a vykřičníků si všímat nemusíme, jelikož se přidávají pouze na základě délky a nemají tudíž žádnou hodnotu. Nejprve je tedy potřeba získat hodnoty, jež jsou reprezentovány znaky z abecedy. Jak již bylo řečeno, pro dešifrování budeme potřebovat nejméně 2 hodnoty, ve kterých se výsledný byte skrývá. Z použité masky pro AND můžeme vidět, že se v prvních 2 hodnotách z abecedy skrývá nejméně jeden znak a případně část pro zjištění znaku následujícího. Tam, kde je to potřeba tedy aplikujeme inverzní masky pro AND a provedeme opačné bitshifty. Výsledné hodnoty náležící ke konkrétním původním znakům sečtu (ze dvou hodnot mohu spočítat hodnotu původní, bity se nepřekrývají a při sečtení dostanu hodnotu celou). Výsledné pole následně předám do další metody, která mi zajistí provedení XORU pro dosažení původní hodnoty znaků (lze toho dosáhnout díky poslední nezměněné hodnotě). Výsledek na závěr převedu zpátky do charů.

Časová složitost: Algoritmus obsahuje několik cyklů (4n), jejichž výsledná složitost je O(n), nic přesahující tuto složitost se v algoritmu nenachází, a tudíž můžeme říci, že se jedná o výslednou kategorii složitosti daného algoritmu.

Prostorová složitost: Bereme-li v úvahu, že prostorová složitost nemůže být vyšší, než časová a že obsazenost záleží na velikosti vstupu, vyjde nám složitost kategorie O(n).