SEMESTRÁLNE ZADANIE KSIF 2022

|16.txt|

autor: Róbert Šumšala

Prvé čo som spravil je, že som si poznačil, čo už viem zo zadania. A síce, text je v angličtine, použitá je vigenerova šifra s kľúčom dĺžky 8. Na základe toho som sa rozhodol ako prvé naprogramovať algoritmus na riešenie vigenerovej šifry brute forcom. To znamená, že algoritmus zistí všetky riešenia, všetkých kombinácií kľúčov.

Keďže ale viem, že budem používať brute force, rozhodol som sa, inšpirovaný zadaním rozdeliť kľúč na dve časti. To znamená, že algoritmus na riešenie vigenerovej šifry som upravil tak aby posúval o daný posun podľa kľúča len každé druhé 4-gramy.

Samozrejme, že nemá zmysel pozerať toľko výpisov manuálne. Preto bola treba vytvoriť nejakú fitnes funkciu. Na základe ktorej program za mňa vyberie správne riešenie.

Moja fitnes funkcia je založená na rozdiely frekvencii bigramov čiastočne dešifrovaného textu, dešifrovanej časťou testovaného kľúča a frekvencii bigramov anglického referenčného textu. Čiže na takzvanej Manhattenskej vzdialenosti. Čím bližšie sú hodnoty pre daný bigram, tým menšiu hodnotu vráti fitnes funkcia *evaluate*.

To znamenalo vytvoriť funkciu, ktorá zistí frekvencie bigramov zo vzorového anglického textu, a potom aj pre dešifrovaný text, zísakný použitím práve testovaného kľúča. To znamená, spočítať ako často sa v texte vyskytujú dva po sebe idúce znaky. Aj s prekrývaním. To znamená, že napríklad „abcd“ obsahuje 3 bigrami. Obsahuje „ab“, „bc“, „cd“. Ako vzorku som použil úryvok s anglického novinového článku. Tento článok som v textedite upravil tak, aby neobsahoval žiadne čísla, apostrofy, znamienka, nečitateľné znaky, medzery a podobne. Dalo sa to ošetriť aj kódom, ale ja som to spravil manuálne, keďže to zabralo menej času ako úprava kódu.

Po získaní vzorovej frekvencii bigramov, som použil brute force na nájdenie prvej polovice kľúča. To znamená že algoritmus dešifruje každé 4 znaky textu postupne všetkými kombináciami polovice kľúča. Pre dešifrované znaky, po použití každého kľúča, zistí Manhattenskú vzdialenosť medzi nimi a refrenčnými frekcenciami (princíp je uvedený vyššie). Výsledok, t.j. Manhattenskú vzdialenosť zlogaritmuje a vždy porovná s doteraz najnižším výsledkom. Ak je nový výsledok menší (lepší), zapamätá si ho a aj použitú polovicu kľúča. Po prejdení všetkých kombinácii skončí s najlepšou polovicou kľúča. Rovnakým spôsobom získa aj druhú polovicu. Akurát bude dešifrovať zvyšné štvorice znakov.

Na koniec tieto dve polovice spojí, a použije ich ako celkový kľúč na dešifrovanie celého textu a výsledok vypíše do konzoly.

Tento postup bol úspešný a program zbehol aj celkom rýchlo. Výsledok, ku ktorému som sa dopracoval je, že text bol zašifrovaný kľúčom **wbpplxpx** a výsledný, dešifrovaný text bol:

AGAINSTTHEFACTTHATTHEHUMANLANGUAGEPERMITSTHEUTTERANCEOFSTATEMENTSWHI
CHHAVENOEMPIRICALCONTENTATALLBUTNEVERTHELESSPRODUCEAPICTUREINOURIMAGIN
ATIONHENOTESONESHOULDBEESPECIALLYCAREFULINUSINGTHEWORDSREALITYACTUALLYE
TCSINCETHESEWORDSVERYOFTENLEADTOSTATEMENTSOFTHETYPEJUSTMENTIONEDSOHEIS
ENBERGALSOENDORSEDANINTERPRETATIONOFHISRELATIONSASREJECTINGAREALITYINWHI
CHPARTICLESHAVESIMULTANEOUSDEFINITEVALUESFORPOSITIONANDMOMENTUMHTTPW

WWAIPORGHISTORYHEISENBERGPCHTMBOHRDENIEDTHATCLASSICALCONCEPTSCOULDBEU
SEDTOATTRIBUTEPROPERTIESTOAPHYSICALWORLDINITSELFBEHINDTHEPHENOMENAIEPRO
PERTIESDIFFERENTFROMTHOSEBEINGOBSERVEDINCONTRASTCLASSICALPHYSICSRESTSONA
NIDEALIZATIONHESAIDINTHESENSETHATITASSUMESTHATTHEPHYSICALWORLDHASTHESEPR
OPERTIESINITSELFIEASINHERENTPROPERTIESINDEPENDENTOFTHEIRACTUALOBSERVATIONH
TTPPLATOSTANFORDEDUENTRIESQMCOPENHAGENBOHMSUGGESTSTHATTHEWHOLEUNIVE
RSECANBETHOUGHTOFASAKINDOFGIANTFLOWINGHOLOGRAMORHOLOMOVEMENTINWHI
CHATOTALORDERISCONTAINEDINSOMEIMPLICITSENSEINEACHREGIONOFSPACEANDTIMETH
EEXPLICATEORDERISAPROJECTIONFROMHIGHERDIMENSIONALLEVELSOFREALITYANDTHEAP
PARENTSTABILITYANDSOLIDITYOFTHEOBJECTSANDENTITIESCOMPOSINGITAREGENERATEDA
NDSUSTAINEDBYACEASELESSPROCESSOFENFOLDMENTANDUNFOLDMENTFORSUBATOMICP
ARTICLESARECONSTANTLYDISSOLVINGINTOTHEIMPLICATEORDERANDTHENRECRYSTALLIZIN
GTHEQUANTUMPOTENTIALPOSTULATEDINTHECAUSALINTERPRETATIONCORRESPONDSTOT
HEIMPLICATEORDERBUTBOHMSUGGESTSTHATTHEQUANTUMPOTENTIALISITSELFORGANIZE
DANDGUIDEDBYASUPERQUANTUMPOTENTIALREPRESENTINGASECONDIMPLICATEORDERO
RSUPERIMPLICATEORDERINDEEDH