Šifry

Prvé šifry vznikli za čias dávno minulých, kedy správy nosili poslovia. Už vtedy vyvstal problém, ako zabezpečiť, aby si správu neprečítal niekto iný než adresát. To sa dalo zaistiť rôzne, napríklad použitím vosku a kráľovskej pečate. Taká pečať na liste je fajn, ale šifrovanie správy ešte lepšie.

Cézarova šifra

Jednou z najstarších známych šifier je Cézarova šifra. Kto ju vymyslel, to už môžeme len hádať, ale hovorí sa, že ju používal sám Július Cézar pri komunikácii so svojimi generálmi. Preto nesie jeho meno. Princíp je veľmi jednoduchý – každé písmeno správy nahradíme písmenom, ktoré sa nachádza o niekoľko pozícií ďalej v abecede. Koľko pozícií? To si môžeme vopred dohodnúť. Toto číslo bude kľúčom k šifrovaniu.

My budeme používať klasickú 26 písmenovú anglickú abecedu: ABCDEFGHIJKLM NOPQRSTUVWXYZ, po Z pôjde opäť A a tak dokola. Výsledok tak bude síce bez mäkčeňov a dĺžňov, ale stále pochopiteľný.

Zašifrovať správu dokáže každý. Stačí mať pri sebe abecedu a

vedieť číslo posunu. Aby ste sa ale nemuseli trápiť s posúvaním každého písmenka, tu je aplikácia, ktorá to spraví za vás:

Sem napíš text, ktorý chceš zašifrovať, alebo odšifrovať:

Abeceda zjedla deda.

Číslo posunu:

1

Šifruj !

Výsledok:

Otázka je, ako odšifrovať šifrovanú správu. Ak poznáme číslo, o koľko sa písmená pri šifrovaní posúvali, je to hračka. Vychádzame z toho, že posun o 26 miest vráti to isté písmeno. Ak sme ho posunuli napr. o 6 pozícií, musíme ho posunúť ešte o 26 - 6 = 20 pozícií a dostaneme pôvodnú správu. Ak šifrujeme o 15 miest, dešifrujeme o 11 miest. Skúste si to.

Bezpečnosť šifry

Značnou nevýhodou Cézarovej šifry je skutočnosť, že nie je zas tak veľký problém rozšifrovať zašifrovanú správu, aj keď nepoznáme číslo posunu. Možností je iba 25. To sa dá vyskúšať. Schválne, skúste pomocou aplikácie hore rozšifrovať tento text:

Nová šifra

Cézarovi to problém nerobilo, keďže nepriatelia boli často negramotní a latinčina bola pre nich cudzí jazyk. Aj nám táto

šifra môže pomôcť, ak sa bavíme po slovensky medzi cudzincami. Môžeme im to sťažiť aj tak, že nebudeme používať medzery. Potom ťažko rozoznajú, že napr.: "STRMHLAVVPRED." je to správne rozšifrovanie.

Ale nebojte sa, ukážem vám, ako sa dá celkom spoľahlivo zašifrovať správu aj pred krajanmi.

Vigenèrova šifra

Vigenèrova šifra je podobná tej Cézarovej, ale nepoužíva rovnaký posun pre všetky písmená správy. Pri tomto šifrovaní potrebujeme kľúč, ktorý určí, o koľko a ktoré písmená sa budú posúvať. Najelegantnejšie riešenie je použiť nejaké slovo ako kľúč. Písmená tohto slova potom určujú posun. Napríklad, keby bol kľúč ALF, tak A je posun o 0 pozícií, L o 11 a F o 5 pozícií. Preto sa prvé písmeno správy neposunie, druhé sa posunie o 11, tretie o 5, štvrté sa neposunie, piate o 11 a tak ďalej.

Správa, ktorú chceme šifrovať:

Dedo skončil bez obeda.

Kľúč:

ALF

Šifruj !

Výsledok:

Takto zašifrovanú správu sa už nepodarí ľahko rozšifrovať bez kľúča. Pri krátkych správach a viacpísmenových kľúčoch sa to stáva až nemožným. Ako ale rozšifrovať správu, ak kľúč máme? Musíme si vytvoriť dešifrovací kľúč - kľúč opačný k danému. To bude kľúč, ktorý bude obsahovať písmená, ktorých číselná hodnota dá spolu s číselnou hodnotou pôvodného kľúča 26. Ak sme mali ALF, tak dešifrovací kľúč bude APV, pretože A=0,

L=11, 26 - 11 = 15=P,

F=5, 26 - 5 = 21=V.

Tu si môžete opačný kľúč zistiť jedným kliknutím:

Kľúč:
Vypočitaj

Opačný kľúč:

Mimochodom, aj toto je istý spôsob šifrovania.

Ďalšie spôsoby sú popísané na stránke Frekvenčná analýza a substitučné šifry .

Ako sa Vám páči táto stránka?
Podarilo sa Vám nájsť zaujímavý kľúč a k nemu opačný kľúč? Podeľte sa.

Meno:
Komentár:

Odošli

Komentáre

Majka	vynikajúce
Nikolaj	WoW
Jozef	Nice
J	Opačné kľúče: psina a lisna. :)