SOFTWAROVÝ PROJEKT

CAESAROVA ŠIFRA

SPSY (Specifikace požadavků na systém)

Jana Michnová

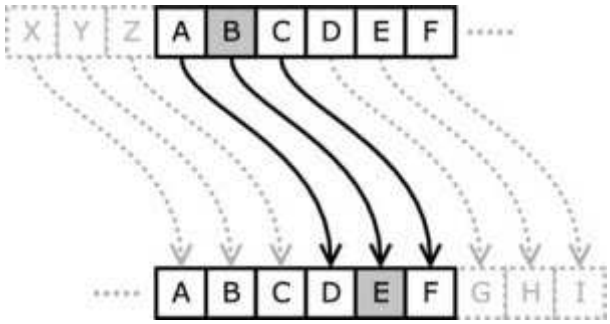
(michnjan@fel.cvut.cz)

Princip

Princip tohoto šifrování je založen na tom, že každé písmeno zprávy je během šifrování zaměněno za písmeno, které se abecedně nachází o pevně určený počet míst dále.

Počet možných variant klíče této šifry je o jedna menší než počet písmen (znaků) v použité abecedě. Zvolíme-li hodnotu posunu stejnou, jako je počet znaků použité abecedy bude zašifrovaná zpráva stejná s předlohou. Vyšším posunem, například posunem s klíčem o jedna větší než je počet písmen (znaků) abecedy dostaneme zašifrovanou zprávu odpovídající prostému posunu o klíč jedna, takže použití klíče hodnoty vyšší než počet znaků abecedy nemá význam.

Hlavní a neodstranitelnou slabinou této šifry je že každý konkrétní znak zdrojového textu odpovídá jednomu konkrétnímu znaku šifrovaného textu, tj. např. u klíče číslo 3 písmeno *'A'* zdroje odpovídá vždy písmenu *'D'* šifrované zprávy.



Obr. 1 Princip šifrace

Použití

Tuto šifru používal pro vojenskou komunikaci Julius Caesar a popsal ji v Zápiscích o válce galské. Caesar používal posun o tři místa, obecně je ale za Caesarovu šifru označováno jakékoli šifrování na principu prostého posunu písmen (znaků) o konstantní hodnotu. I když je tato šifra z dnešního hlediska snadno rozluštitelná a pro jednoduchost šifrování/dešifrování bývá často používána dětmi, Julius Caesar ji s úspěchem používal při svých vojenských taženích. Pro důležité úkoly se tato šifra dnes neužívá a slouží pouze k školním demonstracím slabin jednoduchých šifrovacích systémů.

Vlastnosti programu

Program Caesarova šifra je jednoduchým programem pro šifrování a dešifrovaní textu pomocí Caesarovy šifry zadaného uživatelem o velikost kroku (šifry) opět zadaného uživatelem. Jedná se tedy o zcela uživatelský program, kde si zákazník může všechna data zadávat sám.

Program tedy není plně automatický a to z důvodu multifunkčnosti.

Grafické rozhranní není v tomto programu nutné, jelikož své výsledky (šifrované i dešifrované texty) si může uživatel buď vypisovat přímo na obrazovku, nebo jej ukládat do souborů.

Stejně tak, jako si své výsledky může zákazník ukládat do souborů, tak si je může i ze souborů načítat. Tedy vezme nějaký textový dokument, který obsahuje samosebou nějaký text, který chce zašifrovat nebo dešifrovat a může si jej zašifrovat nebo dešifrovat do nového souboru, anebo opět vypsat na obrazovku.

Hlavní důraz se tedy v tomto programu klade na práci se soubory, jelikož samotný cyklus šifrace a dešifrace je velice triviální.