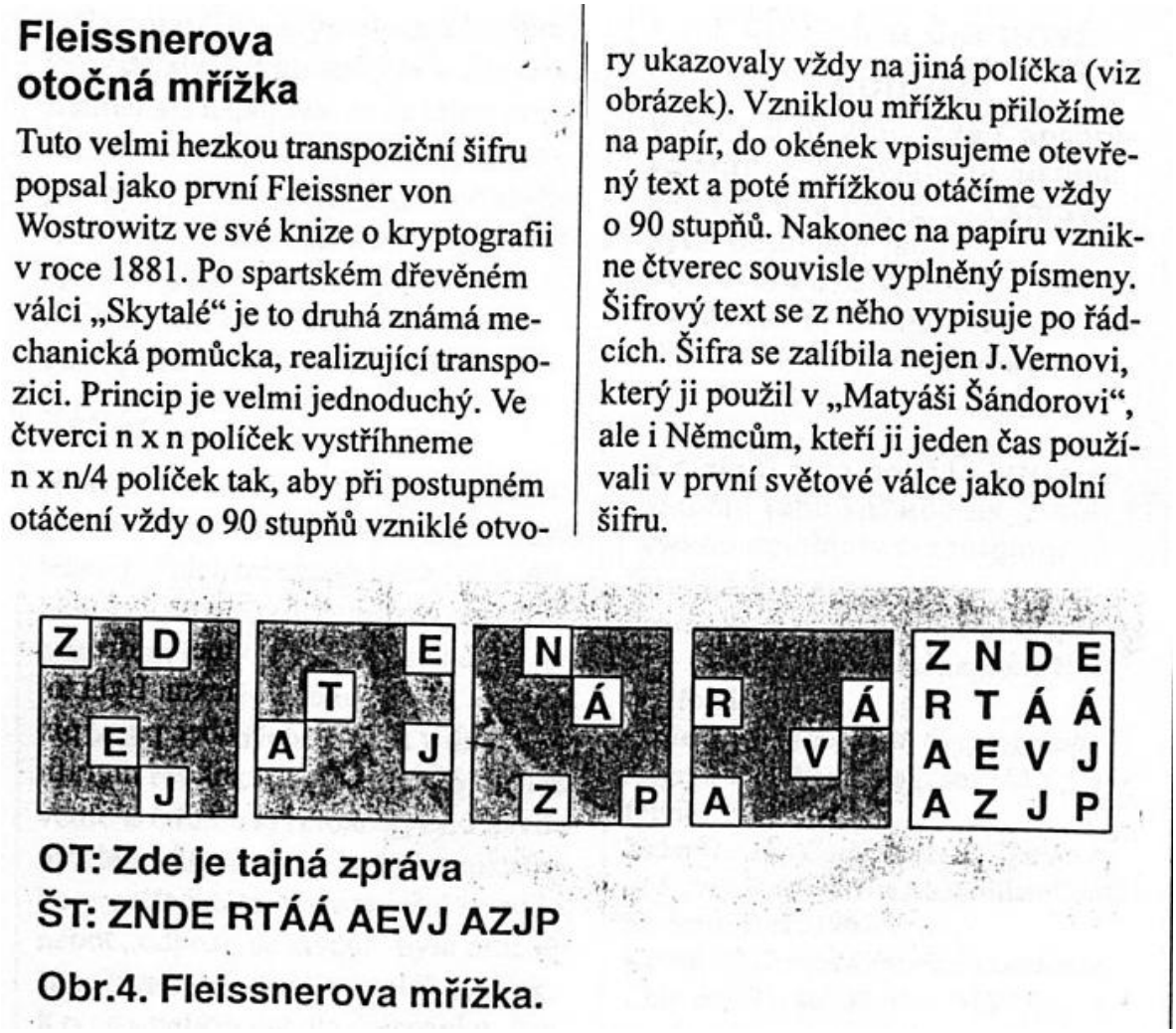
Jak postupovat při luštění Fleissnerovy mřížky

Nápověda pro řešitele Soutěže 2004 (http://soutez2004.crypto-world.info/)

Pavel Vondruška

Nejprve se seznamte s citací jednoho z mála článků v češtině, který se Fleissnerově systému věnuje a který lze na Internetu vyhledat. Tímto článkem je **V.Klíma: Utajené komunikace - 4.díl : Od novověku do 20. století, CHIP č.8, srpen 1994, str. 118 - 121.** ftp://ftp.decros.cz/pub/Archiv/Publications/1994/chip-1994-08-120-120.jpg



Fleissnerova otočná mřížka

Tuto velmi hezkou transpoziční šifru popsal jako první Fleissner von Wostrowitz ve své knize o kryptografii v roce 1881. Po spartském dřevěném válci „Skytalé" je to druhá známá mechanická pomůcka, realizující transpozici. Princip je velmi jednoduchý. Ve čtverci n x n políček vystříhneme n x n/4 políček tak, aby při postupném otáčení vždy o 90 stupňů vzniklé otvory ukazovaly vždy na jiná políčka (viz obrázek). Vzniklou mřížku přiložíme na papír, do okének vpisujeme otevřený text a poté mřížkou otáčíme vždy o 90 stupňů. Nakonec na papíru vznikne čtverec souvisle vyplněný písmeny. Šifrový text se z něho vypisuje po řádcích. Šifra se zalíbila nejen J.Vernovi, který ji použil v „Matyáši Šándorovi", ale i Němcům, kteří ji jeden čas používali v první světové válce jako polní šifru.

Obr.4. Fleissnerova mřížka.

Nyní se seznámíme se stručným návodem, jak lze luštit tento systém.
Pro jednoduchost budeme tyto rady konkretizovat pro mřížku uvedenou v citovaném článku :

1) Rozdělíme si šifrový text na sekvence délky 4 (obecně délky n)

ZNDE
RTÁÁ
AEVJ
AZJP

2) Odhadneme kolik znaků bude z každého úseku v hledaném otevřeném textu.

Víme, že při každém přiložení mřížky je potřeba přečíst 4 znaky otevřeného textu (jedná se o úplnou mřížku, tj. po čtyřech otočeních se vyčerpají všechny znaky tj. 16).
V jednom řádku lze tedy očekávat průměrně 1 znak otevřeného textu (přijměme hypotézu, že počet znaků otevřeného textu kolísá od 0 do 2 znaků).

3) Pokusíme se podle pravidel v bodě 2 sestavit čitelné slovo nebo alespoň úsek čitelného slova.

4) Zkontrolujeme správnost naší volby tím, že se podíváme jaké slovo by vznikalo otočením o 90, 180, 270 stupňů …

5) Nesmíme zapomenout, že otočením souvislého úseku délky menší než 4 (obecně pro tabulku n*n, úseku menší než n*n/4) nemusí vzniknout řetězec, který je „souvislý“, tj. v otočení mohou nějaké znaky chybět !
(porovnej: otočením písmen ÁZP(z třetí polohy uvedené mřížky), která v otevřeném textu za sebou následují , dostanu písmena RVA ve čtvrté poloze mřížky, která za sebou v otevřeném textu nenásledují!)

6) Řetězce, které získáme otočením čitelného úseku, se snažíme doplnit – rozšířit na slovo v čitelné podobě (samozřejmě, že vybíráme již pouze s písmen, která nebyla dosud použita ani v jednom z otočení námi vytipovaného řetězce).

7) Potvrzené slovo dále rozšiřujeme, resp. rozšiřujeme řetězce získané otočením a postupně takto rekonstruujeme celý text.

Vyzkoušejte si na příkladě, který je v článku uveden!