Ze vzpomínek Steplinga

Jednou, když jsem navštívil svého přítele Štěpána v lázních Bad Ischlu vyprávěl mi o velmi zajímavých transpozičních šifrách.

Štěpán napsal do levého sloupce otevřený text a do pravého sloupce šifrový text po transpozici.

MAR	R A M
MARI	R A I M
MARIE	R A I M E
MARIE T	R A I T M E
MARIE TE	R E A I T M E
MARIE TER	R E A I T R M E
MARIE TERE	R E A I T R M E E
MARIE TEREZ	R E A I T R Z M E E
MARIE TEREZI	R E I A I T R Z M E E

„Asi nevidíš pravidlo jak se text transformuje?“ , zeptal se mě.
„Ano, je těžké si jej uvědomit“ pokračoval Štěpán.
„V tomto konkrétním případě se text vepisuje do níže uvedené tabulky na místa označená hvězdičkami. Jakmile text vepíšeš, dostaneš šifrový text tak, že jednoduše opíšeš znaky nejprve z prvého řádku tabulky, pak z druhého a nakonec třetího.

		*		*						*			
	*		*		*		*		*		*		
*						*		*				*	

Tedy např. MARIE TEREZIE = R E I A I T R Z E M E E

		R				E				I			
	A		I		T		R		Z		E		
M				E				E				*	

Klíčem k této šifře je tedy domluvená tabulka (počet řádků) a způsob zápisu textu do této tabulky. Šifru vynalezli Angličané a protože jim psaní do sloupců v tabulce připomíná laťky v plotu, nazvali tuto šifru „podle plotu“ (Rail fence cipher). Angličané se domnívají, že je to poměrně bezpečná šifra, ale mýlí se ! Nedávno jsem jednu takovou dokázal rozluštit.“