SEJONIJSKÉ ŠIFROVÁNÍ 1

Vězeňská a Petronilka jsou šifry, které ke svému vyluštění vyžadují klíč. U ***Petronilky*** *jde o* ***klíč proměnný****, bez jeho znalosti zprávu vyluštíš poměrně obtížně. U* ***Vězeňské*** *šifry je* ***klíč pevný****. Stačí poznat, že jde o vězeňskou šifru a můžeš luštit. Neustále stejný klíč si nosíš v hlavě.*

Vězeňská šifra

A	B	C	D	E	F	G	H	Ch
I	J	K	L	M	N	O	P	Q
R	S	T	U	V	W	X	Y	Z

Šifrovací mřiž vidíš na obrázku. Při šifrování nahrazuješ každé písmeno jedním obrázkem, podle pozice slova v mřížce. Oranžové čárky (na barvě samozřejmě nezáleží) označují trojici písmen v mříži. Tak třeba trojice ABC má oranžový lem jen dole a vlevo. Trojice LMN na všech stranách. A černá tečka označuje pozici písmenka v trojici. Například písmeno A je úplně vlevo, písmenko H uprostřed trojice. Takže slovo AHOJ zašifruješ jako :

Jak prosté ! Při dešifrování (převodu obrázků na text) postupuješ naopak. Jde tedy o šifru symetrickou (dešifrování je přesným opakem šifrování). Výhoda vězeňské šifry = jednoduchost, netřeba předávat klíč příjemci. Nevýhody vězeňské = kdo ji zná, tak šifrovaný text jednoduše přečte.

Petronilka

PETRONILKA
0123456789

Jednoduchá šifra. Vymyslíš klíčové desetipísmenné slovo, nebo shluk písmen (petronilka, mojiparybu, aeioumsbrt) ve kterém se neopakují písmena. Poté v šifrovaném textu nahradíš písmena, obsažená v klíčovém slově jeho pořadovým číslem. Pokud máš například klíčové slovo PETRONILKA, tak namísto písmenka P napíšeš 0, namísto K dosadíš číslo 8. Písmena v klíčovém slově neobsažená ponecháš beze změny. Tedy oblíbené **AHOJ** bys klíčovým slovem PETRONILKA zašifroval jako **9H4J**. Klíčové slovo musíš sdělit příjemci. Pokud je neuvedeš, dešifruje se podle Petronilky. Výhody = kdo nezná klíč, vyluští šifru jen s obtíženi (i když zná princip) Nevýhody = nutnost sdělit klíč příjemci, malý počet šifrovaných písmen.