Meno: ..... Trieda: ..... Dátum: .....

PRACOVNÝ LIST

ŠIFROVANIE – METÓDY TAJNÝCH AGENTOV

SKÚMANIE

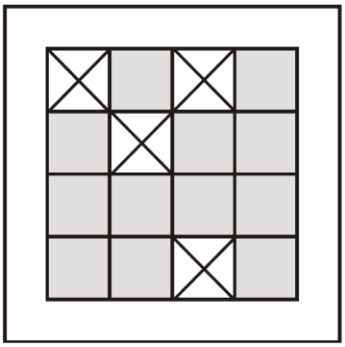
Úloha 1

Naštudujte jednu metódu šifrovania – každý člen skupiny svoju vybranú metódu

1. Fleissnerova otočná mriežka

Položte mriežku na tabuľku so zašifrovaným textom, ktorú ste dostali. Šifrovací kľúč je mriežka s otvorom. Počas prvej svetovej vojny bol tento šifrovací systém používaný aj v praxi nemeckou armádou, a použil to aj Jules Verne v knihe "Nový gróf Monte Christo".

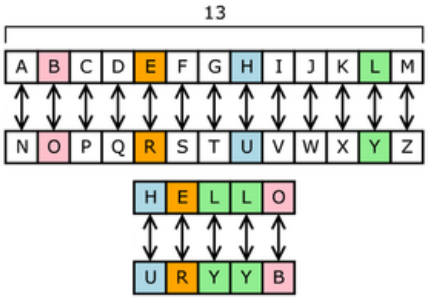
Podľa mriežky vyberte písmená na pozíciách otvorov v mriežke. Tie tvoria šifrovaný text, potom mriežku otočte v smere hodinových ručičiek a v otvoroch postupne prečítajte ďalšie písmená.



Napíšte riešenie zadanej šifry:

Vytvorte vlastnú zašifrovanú správu pomocou danej mriežky. Použite priloženú prázdnu mriežku.

2. Caesarova šifra



Je to druh šifry, pri ktorej je každé písmeno správy je posunuté o danú pozíciu ďalej v abecede.
Napríklad pri posunutí doprava o 13 miest písmeno A bude nahradený písmenom N. V prípade písmena vyskytujúceho sa na konci abecedy sa toto písmeno posunie opäť na začiatok abecedy.
Táto šifra patrí medzi najznámejšie a najstaršie šifrovacie systémy, používal ho rímsky cisár Caesar pred 2000 rokmi.

Najprv tu vytvorte vhodnú dešifrovaciu tabuľku na posunutie o 3 miesta.

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

Odšifrujte nasledovnú utajenú správu, kde šifra používa ***posunutie o 3 miesta****.*

O	D	V	N	D	K	R	U	B	S	U	H	Q	D	V	D

Meno: ..... Trieda: ..... Dátum: .....

Vymyslite vlastnú zašifrovanú správu:

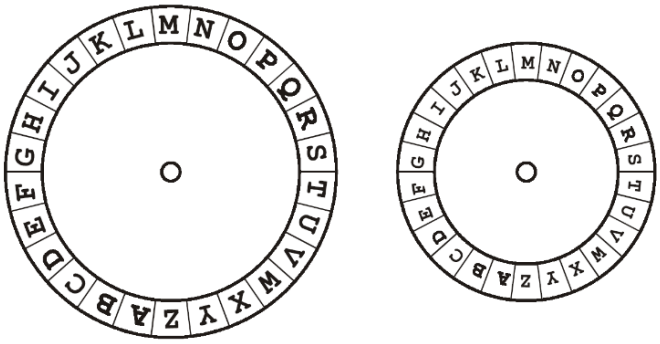
Vytvorte vlastnú dešifrovaciu tabuľku s vlastným posunutím.

Posunutie nech je:	

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

Správa:	
Zašifrovaná správa:	

3. Šifrovací disk



Je to šifrovacia pomôcka skladajúca sa z dvoch otočných kotúčov. Na každom z nich je napísaná abeceda. Vonkajšia predstavuje znaky abecedy a vnútorná šifrovú abecedu. Pootočením vnútorného kruhu o niekoľko políčok pod vonkajším písmenom sa nachádza vnútorné písmeno, čo predstavuje šifru daného písmena.

Šifrovací disk pôvodne slúžil na šifrovanie pomocou Caesarovej šifry.

Odšifrujte nasledovnú správu pomocou šifrovacieho disku, ***kde A → F***

Použite priložené šifrovacie disky.

Správa:										
Zašifrovaná správa:	**Q**	**F**	**X**	**Y**	**T**	**A**	**N**	**H**	**P**	**F**

Vymyslite vlastnú zašifrovanú správu:

Správa:	
Zašifrovaná správa:	

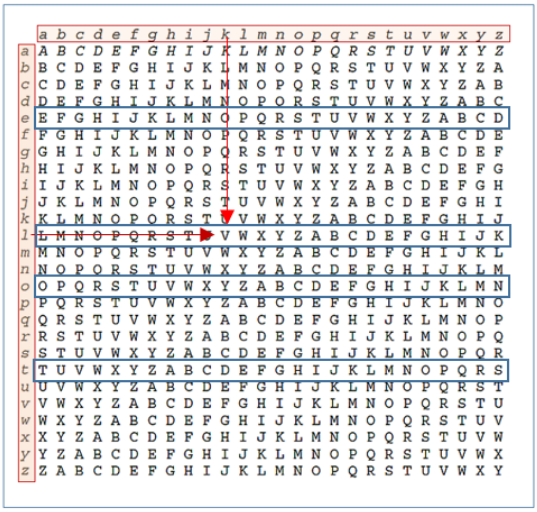
Meno: ..... Trieda: ..... Dátum: .....

4. Vigenerova šifra

Táto šifra používa 26 abecied posunutých o 1 miesto. Šifrovanie prebieha tak, že sa zvolí kľúčové slovo. Daný kľúč určuje, pomocou ktorej abecedy sa bude šifrovať.

*Pri šifrovaní sa používajú **riadky**, ktoré začínajú písmenami tvoriacimi kľúč. Nech je kľúč slovo LETO.*

*V **stĺpcoch** sa nachádzajú písmená správy.*



Ukážka šifrovania:

Správa:	K	O	S	I	C	E
Kód:	L	E	T	O	L	E
Zašifrovaná správa:	V					

Pomocou kľúča JAR odšifrujte správu:

Správa:						
Kód:	J	A	R			
Zašifrovaná správa:	V	E	U	E	E	U

Vymyslite vlastnú zašifrovanú správu:

Správa:															
Kód:															
Zašifrovaná správa:															

ROZŠÍRENIE

Úloha 2

Vymyslite novú, jednoduchú metódu šifrovania, a zašifrujte tajnú správu pre spolužiakov. Skúste vymyslieť správu, ktorá je dlhá maximálne 10 znakov.

Meno: ..... Trieda: ..... Dátum: .....

HODNOTENIE

ČO SME SA NAUČILI?

SEBAHODNOTIACI TEST

Úloha 3	***Označte správne tvrdenie*** ☒ ***:*** ☐ *Cieľom šifrovania je utajenie správy.* ☐ *Účelom šifrovania je utajenie pre bezpečnú ochranu údajov.* ☐ *Šifrovanú správu hocikto môže dešifrovať.*

SEBAHODNOTIACA TABUĽKA

Otázky na hodnotenie Vašej práce:	**áno**	**čiastočne**	**nie**
Viem kedy a kde sa používajú šifry?			
Viem šifrovať pomocou Fleissnerovej otočnej mriežky?			
Viem šifrovať pomocou Caesarovej šifry?			
Viem šifrovať pomocou šifrovacieho disku?			
Viem šifrovať pomocou Vigenerovej šifry?			