Šifrování – přehled

Od té doby, kdy si lidé začali posílat důležité zprávy, snažili se jiní lidé tyto zprávy zachytit. Jednou z možností, jak ochránit své vzkazy před zvědavci bylo zajistit jim silný (pokud možno ozbrojený doprovod), druhou možností pak napsat zprávu tak, aby na první pohled nedávala smysl – zašifrovat ji.
Jenže lidé byli (jsou a budou) zvědaví, proto se snažili tajné zprávy rozluštit – dešifrovat. Dodnes však existují šifry, které ještě nikdo nerozluštil. Například některé spisy slavného vědce, anglického mnicha Rogera Bacona, který žil ve 13. století, dosud čekají na svého čtenáře.

Vyzkoušejte si několik jednoduchých šifer. Zašifrujte třeba **své jméno** nebo nám šifrovaně **napište krátký vzkaz**.

Tady jsou příklady, jak na to:

Šifrování pozpátku:

Příklad: město Rakovník

...

kínvokaR otsěm

Jak šifrovat:
Šifrování je velmi jednoduché - jednoduše píšeme zprávu pozpátku.

Jak rozluštit:
Pokud chceme dešifrovat, prostě text přečteme pozpátku.

Šifrování – přehled

Šifrování odpředu a odzadu:

Příklad: Rakovník

...

Rkvíknoa

Jak šifrovat:

Při šifrování si rozpočítáme místo pro celou šifru a šifrujeme tak, že na začátek zapíšeme první písmeno. Na konec pak druhé písmeno. Třetí písmeno šifrované zprávy napíšeme na druhou pozici. Jako předposlední písmeno zapíšeme další písmeno zprávy. Je to vlastně střídavě zapisovaný text od začátku a od konce.

Jak rozluštit:

Při dešifrovaní čteme text postupně po písmenech od začátku ke konci.

Falešná písmena:

Příklad: Rakovník (heslo: x)

...

AKYxRtxatqexkyxozgixvtxnjbhxíoboxk

Jak šifrovat:

Pokud šifrujeme napíšeme nejprve několik náhodných písmen, pak následuje písmeno, podle kterého poznáme, že následující znak je písmeno šifry (písmeno x). Po tomto písmenu následuje jedno písmeno šifry. Pokračujeme zase od začátku - napíšeme několik náhodných písmen...

V písmenech, která jsme zvolili jako matoucí se samozřejmě nesmí objevit ono písmeno, protože potom by mohla být šifra zašifrována špatně.

Jak rozluštit:

Zjistíme, zda se v šifře neopakuje podezřele často některé písmeno. Pokud ano, pak máme podezření, že se jedná právě o tento typ šifry. V textu vždy nalezneme ono často se opakující se písmeno a text zprávy je vždy postupně psán po tomto písmenu.

Šifrování – přehled

Vložení hesla za každé písmeno:

Příklad: Rakovník (heslo dub)

...

Rdubadubkdubodubvdubndubídubkdub

Jak šifrovat:

Při šifrování zapisujeme mezi každá dvě písmena zprávy krátký shluk hlásek (heslo: dub).

Jak rozluštit:

Pokud vidíme, že se v šifře vyskytuje až podezřele často jedna skupina hlásek, pak se může zřejmě jednat o tuto šifru. Přezkoumáme, zda se v celém textu opakuje jedna stejná skupina hlásek, kde vždy mezi dvěma skupinami jedno písmeno. Pokud je tomu tak, pak vždy blíže neurčená písmena mezi dvěma skupinami tvoří text zprávy.

Místo písmen čísla:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
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

Příklad: Rakovník

...

18;1;11;15;22;14;9;11;

Jak šifrovat:

Písmena v abecedě očíslujeme čísly od 1 do 26. Písmena zprávy pak nahrazujeme těmito čísly.

Jak rozluštit:

Pokud se text skládá maximálně dvojciferných čísel (nebo je napsán jako množství číslic jsoucích za sebou), jejich hodnota nepřesahuje 26, pak máme podezření, že se jedná právě o tuto šifru. Při dešifrování bychom měli mít očíslovanou abecedu. Potom podle této abecedy začneme převádět písmena.

Šifrování – přehled

Mobilová šifra:

Příklad: **Rakovník**

…

777 2 55 666 888 66 444 55

Jak šifrovat:

Každý, kdo někdy posílal nějakou krátkou textovou zprávu na tlačítkovém mobilním telefonu, jistě poznal tento jednoduchý způsob. Každé jednotlivé písmeno se šifruje tak, že se vždy napíše číslo tlačítka tolikrát, kolikáté je dané písmeno na daném tlačítku zobrazené. Jako mezera se používá číslo 1. Zdá se, že nutnou pomůckou pro šifrování i dešifrování je nutný samotný mobilní telefon, nebo alespoň nějaký nákres, protože písmena na mobilním telefonu nejsou uspořádána nijak pravidelně

Jak rozluštit:

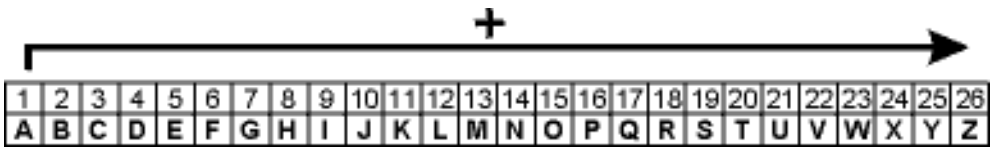
Pokud máte k dispozici tlačítkový mobilní telefon stačí podle šifry mačkat jednotlivá tlačítka a zpráva se sama objeví (platí u starších mobilních telefonů). Nebo jednoduše můžeme postupovat podle klávesnice nebo náčrtku.

Posun písmen

Příklad: **Rakovník**

…

Sblpwojl



Jak šifrovat:

Základem je napsaná abeceda bez háčků a čárek bez Ch. Při zašifrovávání pak vyhledáme každé písmeno v abecedě a do šifry zapisujeme toto písmeno vždy posunuté v abecedě o několik znaků (zde o jeden). A=B

Jak rozluštit:

Při dešifrování posunujeme každé písmeno v abecedě o několik znaků nazpátek (zde o jeden). Tento postup však použijeme přímo tehdy pokud již daný posun známe.

Šifrování – přehled

Posun písmen (postupně):

Příklad: **Rakovník**

...

Rbmrzsor

Z	E	L	E	N	I	N	A
+0	+1	+2	+3	+4	+5	+6	+7
Z	F	N	H	R	N	T	H

Jak šifrovat:

Při šifrování máme očíslovanou abecedu. Každé písmeno postupně posunujeme v abecedě tak, že první písmeno necháváme nezměněno, druhé posuneme o jednu pozici v abecedě dále, další písmeno o dvě pozice, další o tři atd. Pokud se při posunu dostaneme za písmeno Z pokračujeme v počítání zase od začátku abecedy.

Jak rozluštit:

Při dešifrování posunujeme každé písmeno postupně zase opačným směrem, než při šifrování. Pokud při posunu dojdeme k písmenu A odečítáme od konce abecedy od písmene Z.

Velký polský kříž

Příklad: **Rakovník**

...

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

Jak šifrovat:

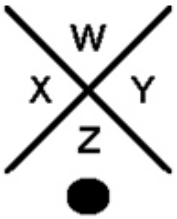
Šifrujeme podle následující tabulky. Místo písmene, které šifrujeme nakreslíme čáry, které jsou okolo trojice písmen. Aby se jedno písmeno odlišilo od ostatních z trojice napíšeme tečku doprostřed, buď více nalevo, napravo nebo do středu.

Jak rozluštit:

Použijeme tabulku a snažíme se najít umístění písmene podle nákresu.

Šifrování – přehled

Malý polský kříž:



Příklad: Rakovník

...

Jak šifrovat:

Šifrujeme podle následující tabulky (malý kříž). Místo písmene, které šifrujeme nakreslíme čáry, které jsou okolo písmen. Aby se jedno písmeno odlišilo od ostatních z dvojice napíšeme tečku doprostřed.

Jak rozluštit:

Použijeme tabulku (malý kříž) a snažíme se najít umístění písmene podle nákresu.

Morseova abeceda

Příklad: Rakovník

...

.-./.-/-.-/---/...-/-./../-.-///

A	·—	akát
B	—···	blýskavice
C	—·—·	cílovníci
D	—··	dálava
E	·	erb
F	··—·	Filipíny
G	——·	Grónská zem
H	····	hrachovina
Ch	————	Chléb nám dává
I	··	ibis
J	·———	jasmín bílý
K	—·—	krákorá
L	·—··	lupíneček
M	——	mává

N	—·	nástup
O	———	ó náš pán
P	·——·	papírníci
Q	——·—	kvílí orkán
R	·—·	rarášek
S	···	sobota
T	—	tón
U	··—	učený
V	···—	vyvolený
W	·——	Waltrův vůz
X	—··—	Xénie má
Y	—·——	ý se ztrácí
Z	——··	známá žena

Jak šifrovat:

Poněvadž je použijí Morseovy abecedy opravdu rozsáhlé, není v mých silách zde popsat všechny možnosti šifrování a použití.
Nejjednodušší způsob šifrování je převod do podoby na papíře jako znaky tečka, čárka, lomítko.
Použití je opravdu velké množství, například pro přenos můžeme použít pískání, světlo baterky, různé zakrývání svíček, signalizaci praporky...
Můžeme na papír nakreslit malé a velké stromečky, prostě co nás napadne.

Jak rozluštit:

Dešifrujeme podle přijímaných znaků. Každé písmeno, číslici nebo jiný znak tvoří skupina teček a čárek (dlouhých a krátkých signálů). Odděleny jsou lomítkem (nebo delší časovou mezerou).

Šifrování – přehled

Morseova abeceda

A	.-	akát	M	--	mává
B	-...	blýskavice	N	-.	nástup
C	-.-.	cílovníci	O	---	ó náš pán
D	-..	dálava	P	.--.	papírníci
E	.	erb	Q	--.-	kvílí orkán
F	..-.	filipíny	R	.-.	rarášek
G	--.	Grónská zem	S	...	sekera
H	....	Hrachovina	T	-	trám
CH	----	chléb nám dává	U	..-	učený
I	..	ibis	V	...-	vyučený
J	.---	jasmín bílý	W	.--	vagón klád
K	-.-	krákorá	X	-..-	xénokratés
L	.-..	lupíneček	Y	-.--	ý se ztrácí
			Z	--..	známá žena

1	.----		6	-....	
2	..---		7	--...	
3	...--		8	---..	
4	....-		9	----.	
5	.....		0	-----	

otazník	?	• • — — • •
čárka, vykřičník	, !	— — • • — —
tečka	.	• — • — • —
středník	;	— • — • — •
zlomková čára	/	— • • — •
rovnítko	=	— • • • —

pomlčka	-	— • • • • —
odsuvník		• — — — — •
závorka	( )	— • — — • —
uvozovka	„ “	• — • • —
dvojtečka	:	— — — • • •
podtrhnutí	_	• • — — • —

Šifry budete potřebovat k luštění zítřejšího úkolu.