ŠIFROVACÍ KROUŽEK - 5. hodina

Substituční šifry: V šifrovaném textu jsou nahrazeny jednotlivé znaky jinými znaky, nebo symboly. Nejjednodušší (co se týče dešifrování) substituční šifry jsou **monoalfabetické**, tzn. že se jeden znak nahrazuje znakem jiným. Složitější jsou pak **homofonní** šifry, které umožňují jeden znak nahradit několika jinými znaky. Ještě složitější jsou potom **polyalfabetické** šifry, které pracují s více abecedami. Speciální kategorií jsou šifry polygrafické, které nepracují s jednotlivými znaky, ale např. s takovými bigramy (dvojicí znaků). Nejsložitější, resp. Nerozluštitelná šifra je šifra **Vernamova**, o té si povíme nakonec.

Monoalfabetické substituční šifry:

Opět šifrujeme text: **SIFROVACI KROUZEK**

Atbaš (Atbash cipher):

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

Písmena abecedy nahradíme tak, že obratíme abecedu odzadu.

Výsledek: **HRUI LEZX RPIL FAVP**

Albam (Albam cipher):

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

Atbaš a Albam jsou hebrejské šifry staré asi 2500 let. Jsou v nich dokonce zašifrované některé pasáže Starého zákona (bible). Obě šifry se jednoduše dešifrují - stejně jako při šifrování.

Kroužek vede: Richard Kába – RIK
Email: richard.kaba@centrum.cz
Tel.: +420 731 137 569
Kdykoli mě kontaktujte!

I.Quest
Pořádá RADIOKLUB OK1KPI Písek

Výsledek: **FVSE BINP VXEB HMRX**

Caesarova šifra: Tuto šifru vymyslel a úspěšně používal Gaius Julius Caesar pro soukromou korespondenci. Její princip spočívá v tom, že se abeceda posunula o 3 písmena.

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

Výsledek: **VLIU RYDF LNUR XCHN**

Všem šifrám, které posouvají abecedu o určitý počet písmen se říká Caesarovy šifry.

Augustova šifra: Octavianus Augustus byl Caesarův synovec a vymyslet tuto variantu Caesarovy šifry:

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
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	A

Výsledek: **TJGS PWBD JLSP VAFL**

ROT13: Velmi obvyklý typ Ceasarovy šifry, posun o 13 znaků. Je to vlastně šifra Albam, viz. Výše

Substituce s klíčem: U této šifry si definujeme nějaký klíč (ve kterém se nesmí opakovat písmenko), např. slovo „HESLO". To napíšeme do substituční tabulky a poté doplníme zbylá písmena abecedy:

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

Nevýhodou samozřejmě je, že poslední písměna abecedy jsou stejná.

Výsledek: **RDAQ MVHS DGQM UZOG**

Substituci s klíčem můžeme zároveň kombinovat s posunutím, jako u Caesarovy šifry.

Kroužek vede: Richard Kába – RIK
Email: richard.kaba@centrum.cz
Tel.: +420 731 137 569
Kdykoli mě kontaktujte!

Homofonní šifra:

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
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
27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78
79	80	81	82	83				84		85	86	87	88	89	90		91	92	93	94	95	96	97	98	99

Výsledek pak může být různý, např:

19 35 58 44 89 22 27 81 9 63 70 15 94 26 31 11

Polyalfabetické šifry:

Albertiho šifra: Tuto šifru vymyslel Leon Battista Alberti, který se narodil roku 1404 ve Florencii. Používá dvě šifrované abecedy a v textu střídá pravidelně jednu a druhou. Dosáhne tím toho, že jedno písmeno je šifrované dvěma způsoby, podobně jako u homofonní. Šifry:

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

Kroužek vede: Richard Kába – RIK
Email: richard.kaba@centrum.cz
Tel.: +420 731 137 569
Kdykoli mě kontaktujte!

I.QUEST
Pořádá RADIOKLUB OK1KPI Písek